JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY

3/2016

(Contents Continued on Back Cover)

Editorial Board

Editor-in Chief: ..... ***Paweł Szczepański***

Associate Editors: ..... ***Krzysztof Borzycki***
Marek Jaworski

Managing Editor: ..... ***Robert Magdziak***

Technical Editor: ..... ***Ewa Kapuściarek***

Editorial Advisory Board

Chairman: ..... ***Andrzej Jajszczyk***
Marek Amanowicz
Hovik Baghdasaryan
Wojciech Burakowski
Andrzej Dąbrowski
Andrzej Hildebrandt
Witold Hołubowicz
Andrzej Jakubowski
Marian Kowalewski
Andrzej Kowalski
Józef Lubacz
Tadeusz Łuba
Krzysztof Malinowski
Marian Marciniak
Józef Modelski
Ewa Orłowska
Andrzej Pach
Zdzisław Papir
Michał Pióro
Janusz Stokłosa
Andrzej P. Wierzbicki
Tadeusz Więckowski
Adam Wolisz
Józef Woźniak
Tadeusz A. Wysocki
Jan Zabrodzki
Andrzej Zieliński

ISSN 1509-4553 on-line: ISSN 1899-8852

© Copyright by National Institute of Telecommunications
Warsaw 2016

Circulation: 300 copies

Sowa – Druk na życzenie, www.sowadruk.pl, tel. 22 431-81-40

JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY

Preface

This issue of the *Journal of Telecommunications and Information Technology* is devoted to three areas: routing and other subjects related to communication networks, security issues and solutions, and radio technology.

The largest part of the publication is networking, especially mobile networks – reflecting their steady technical development and worldwide expansion, and to routing solutions – in a technology-neutral manner, as the problems and their solutions presented are independent of transmission medium being used.

As the ultimate purpose of a communication network is cost-efficient provision of services meeting contractual quality requirements, there is a need for traffic engineering ensuring effective utilization of available network resources and generation of highest income for network operator, while still providing the Quality of Service (QoS) expected by its customers. Importantly, pursuing those two goals simultaneously is often in conflict. Another big issue is monitoring the QoS received by customers, e.g. for use by market regulator or service provider. The latter is particularly important in case of mass-market Internet access offered for consumers and small business users, who usually lack the knowledge and tools necessary to monitor service quality themselves.

The next set of papers in this issue covers security matters and technologies useful for communication networks, in this case user identification, secure network control, management, and algorithms useful for data encryption. The importance network of security solutions, in effort to make it more resistant to hacking, tampering, illegal access or eavesdropping, is rapidly growing. Alas, network operators and service providers are currently on the defensive, as the growing number of reported security breaches and data leaks confirms. For security researchers and designers of communication systems and equipment, this situation means increasing amount of work (with more funding available) due to demand for technical solutions providing adequate level of security at acceptable cost, and without unacceptable burden on network users.

The set of papers on networks begins with *Link Quality and Energy Aware Geographical Routing in MANETs using Fuzzy Logics* by P. Mishra, Ch. Gandhi, and B. Singh. Authors have analyzed routing in mobile ad hoc networks (MANETs), finding that the algorithms used must deal with problems specific to mobile networks with battery-powered devices (nodes),

in particular variable link quality (due to user movement, propagation issues and variable number of users per base station) and limited, varying energy reserve at each node. The solution proposed is a mix of both greedy and compass routing.

In the next article, G. Zalewski and W. Ogryczak in a paper *Comparison of Selected Fair-optimization Methods for Flow Maximization between given Pairs of Nodes in Telecommunications Network* look at optimizing traffic control in a core network, finding that simple maximization of operator's revenues results in "starvation" or outright blocking of less profitable paths, services and customers. This is not acceptable, and "fair" traffic optimization methods are necessary; two methods analyzed being: ordered weighted average (OWA) and the reference point method (RPM).

P. Białoń in his paper *A Practical Approach to Traffic Engineering using an Unsplittable Multicommodity Flow Problem with QoS Constraints* deals with content-aware networks, where both capacity and QoS demands must be met simultaneously for each path. The author proposes a relatively simple mixed algorithm offering short and predictable calculation time, as well as provision (in case a solution meeting input demands is found impossible) of approximately-feasible solution, showing how to modify demands to retain feasibility. Its disadvantage with respect to other solutions is less efficient utilization of network resources.

The next subject, studied by M. Krzysztoń and E. Niewiadomska-Szynkiewicz in a paper *Heavy Gas Cloud Boundary Estimation and Tracking using Mobile Sensors* is use of field deployed, mobile wireless sensors, forming a MANET, for centralized tracking of a moving cloud of low-lying gas, with estimation of its boundaries. The solution presented is of obvious use in emergency situations (chemical leak, poison gas attack, etc.) and can be adopted for detection and location of other dangerous agents, e.g. radioactive contamination.

The only paper about optical fiber communications is *Variable-Weight Optical Code Division Multiple Access System using Different Detection Schemes*, by S. Seyedzadeh, M. Moghaddasi, and S. B. A. Anas. It includes comparative analysis of Variable Weight OCDMA (VW-OCDMA) system using KS code with three optical detection schemes: Direct Decoding (DD), Complementary Subtraction (CS) and AND subtraction. Of those, the DD variant was found to offer the best performance, with highest number of users simultaneously served.

In the last paper devoted to networks, *Concept for a Measurement Management System for Internet Access Service*, J. H. Klink, M. J. Podolska, and T. Uhl look at very important (also for the consumer) subject of ensuring and monitoring the quality of service (QoS) in Internet access networks, dealing first with applicable European standards and regulations, than with methodology of QoS measurements. The authors propose introduction of a Measurement Management System (MMS) to aid the design, execution and evaluation of efficient, automatic QoS measurements in networks.

Network security is dealt with at multiple levels, complementing each other. On the high level, we have security-oriented network management. A. Wilczyński, A. Jakóbik, and J. Kołodziej, in a paper *Stackelberg Security Games: Models, Applications and Computational Aspects* present use of so-called Stackelberg games (where one player, e.g. network administrator, has privileged position and makes decision before others) for decision support when security issues are the crucial.

Down to the individual user, for secure access, the individual must be reliably identified, preferably without resorting to additional, dedicated hardware or onerous procedures. Two possible biometric solutions are presented and analyzed in papers: *Application of Recurrent Neural Networks for User Verification based on Keystroke Dynamics* by P. Kobojek and K. Saeed and *Cross-spectral Iris Recognition for Mobile Applications using High-quality Color Images* by M. Trokielewicz and E. Bartuzi. The first paper includes results of experiments proving that keystroke sequence can reliably identify a person, in particular avoiding dangerous false positives. One can see this work as extension of familiar method of identifying a wired or wireless telegraph operator by "rhythm" of his keystrokes, successfully used during WWI and WWII. However… a simple keyboard sniffer planted on a victim's PC can provide hackers with enough data for easy replication of his/her biometric signature, possibly by another module of the same malware… The second paper looks on the problem of matching iris scans obtained with different cameras, e.g. low resolution infrared black and white (typical for iris scanners installed at bank, high security facilities, etc. Such images are stored as reference in most security systems) and high resolution, color (RGB, no infrared channel) image generated by camera in a smartphone or other consumer device. The

authors found that grayscale conversion of color images with selective RGB channel choice depending on the iris coloration could improve recognition accuracy for some combinations of eye colors, with error rates reduced to 2%, the best result published so far.

The last line of defense in case of successful hack or eavesdropping is data encryption. In his paper "*Faster Point Scalar Multiplication on Short Weierstrass Elliptic Curves over F_p using Twisted Hessian Curves over F_{p^2}*", M. Wroński proposes new, more computationally efficient variant of elliptic curve cryptography, with estimated gain of 24–30%. Such reduction of processor load is particularly desirable in battery-powered mobile devices.

Radio engineering in this issue of JTIT is represented by two, substantially different papers.

The first one, *Curved-Pentagonal Planar Monopole Antenna for UHF Television Reception* by R. Yuwono, E. B. Purnomowati, and M. Y. Amri is devoted to computer simulations and optimization of mass-produced, household item – TV antenna. While relatively low-tech, this device is still essential for provision of TV broadcast services for consumers living beyond reach of cable or broadband Internet networks.

The last paper: *On Radio-Frequency Spectrum Management* by R. Strużak, T. Tjelta, and J. Borrego, deals with matter of extreme importance: allocation of scarce, limited resource – radio spectrum, to multiple competing networks and applications, especially taking into account rapid evolution of technology and services, and exponential growth of traffic volume, and overall shortage of spectrum. With LTE/5G networks becoming dominant mode of broadband access in many territories, spectrum management has currently huge economic importance, and must be done transparently and carefully. There is also the persistent issue of treating radio licenses primarily as revenue generator for the government. The paper presents evolution of spectrum exploitation, a vision of future, and major dilemmas and challenges.

Krzysztof Borzycki
Associate Editor

Paper

Link Quality and Energy Aware Geographical Routing in MANETs using Fuzzy Logics

Priya Mishra[1], Charu Gandhi[1], and Buddha Singh[2]

[1] *Department of Computer Science and Information Technology, JIIT Noida, India*
[2] *School of Computer and System Sciences in Jawaharlal Nehru University, New Delhi, India*

Abstract—In literature, varieties of topology and geographical routing protocols have been proposed for routing in the MANETs. It is widely accepted that the geographical routings are a superior decision than topological routings. Majority of geographical routing protocols assume an ideal network model and choose the route that contains minimum number of hops. However, in reality, nodes have limited battery power and wireless links are additionally unreliable, so they may highly affect the routing procedure. Thus, for reliable data transmission, condition of the network such as link quality and residual energy must be considered. This paper aims to propose a novel multi-metric geographical routing protocol that considers both links-quality and energy metric along with progress metric to choose the next optimal node. The progress is determined by utilizing greedy as well as compass routing rather than pure greedy routing schemes. To combine these metrics, fuzzy logics are used to get the optimal result. Further, the protocol deals with "hole" problem and proposes a technique to overcome it. Simulations show that the proposed scheme performs better in terms of the packet delivery ratio, throughput and residual energy than other existing protocols.

Keywords—GPSR, LAR, MANET, RSSI, SINR, SNR.

1. Introduction

A mobile ad hoc network (MANET) is a self-organizing infrastructure-less network that communicates over wireless links through mobile nodes. These nodes are free to move randomly and form a temporary network without the help of centralized administration. Hence, these nodes play a major role in the routing process, being as host as well as router at the same time. These nodes can communicate directly to other node if they reside within the transmission range of each other. However, if nodes reside beyond the transmission range, then they have to be dependent on each another to forward messages from source to the destination. Therefore, in such multi-hop scenarios, routing protocols are needed to route data.

A variety of routing protocols have been proposed to route data in MANETs. These routing protocols are often classified as topology based and position based routing protocols. The topology based routing protocols do flooding of messages, maintain a routing table to record routes between nodes, and find a path from source to destination. The topology based routing protocols are reactive or proactive in nature. The proactive routing protocols maintain complete routing information about the network. On the other hand, reactive routing protocols start path discovery only to the destination and maintain the information about only active routes instead of maintaining the overall network information. These routing protocols broadcast route request blindly that produces the high routing overhead and chance of collisions. Another issue would be caused by breakage of the links. If the nodes are moving with high speed, it will produce frequent link changes and these changes will reduce successful delivery of packets, increasing traffic overhead, increase packet drop rates, excess energy consumption and increase end-to-end delay.

To overcome these problems geographical routing protocols are accepted potentially, scalable and efficient solution for routing in MANETs. The geographical routing utilizes location information of nodes to enhance the route discovery process by limiting the forwarding zone to decrease the number of nodes participating in routing process. Since in geographical routings, the nodes locally select next hop node based on the neighborhood information and destination location. They do require neither route establishment information nor predestination state like topological routing protocols.

The main component of geographic routing is usually a greedy forwarding mechanism, whereby each node forwards a packet to the neighbor that is closest to the destination. Each intermediate node applies this greedy principle until the destination is reached. However, original greedy forwarding mechanism does not consider any other factors that can influence routing procedure, e.g. link quality and energy level. Several recent researches have verified that traditional wireless routing protocols treat the wireless link as a wired link, and focus on finding a fixed path between a source and destination. However, links are broken often due to the mobility and depleted energy level of the nodes. In such scenarios, wireless links are highly unreliable in MANET [1], [2], this may increase retransmission as well as energy wastage. Therefore, reliable data transmission and energy efficiency are biggest challenges in MANET. The another major problem of greedy forwarding is, "hole" problem which may arise due to smaller request zone or energy exhaustion of the hole boundary nodes. The nodes

located on the boundaries of holes may suffer from excessive energy consumption of the whole boundary nodes. To overcome hole problem, various perimeter routing protocol such as GPSR [3], GOAFR [4] and GAF [5], have been proposed. According to these schemes, boundaries nodes are used for data delivery instead of general node and it results excessive energy consumption and congestion at hole boundary nodes.
Therefore, in this paper a novel geographical routing protocol that discovers an optimal route by considering the link quality and residual energy of nodes is presented. The key features of proposed protocol include:

- Selecting an optimal next forwarding node by considering the both link quality, energy metric and progress metric. To combine these metrics we use the fuzzy logic interface.
- Design an efficient hole identification and detection mechanism for effective routing in presence of the hole.
- Comparison of proposed protocol and its outcomes with other geographic routing protocols.

The remainder of this article is organized as follows. In Section 2, the existing works that deal with energy and link stability related issues in geographical routing protocols are discussed. The Section 3 describes the metrics used in this work. In Section 4 the key features of proposed work are outlined. The results of simulation that evaluates the performance of proposed protocol against other existing protocols are described in Section 5. Conclusion and future directions are presented in Section 6.

2. Related Work

2.1. Link Quality Aware Routing Protocols

In literature, a majority of researches assume that the wireless links are reliable and stable. However, links are highly unreliable and unstable. Dube *et al*. [6] proposed a novel route discovery scheme by considering both signal strength and link stability of the nodes to choose a longer-lived route. The protocol selected the node based on its average signal strength to exchange a packet. Zuniga and Krishnamachari [7] worked in the direction of variation in link quality (poor or good) against distance metric. They found that quality of links highly affects the greedy forwarding scheme. As a result, packet drops rate and energy consumptions would be increased by doing retransmissions.
In paper [8], the authors used the signal strength as a parameter to estimate the link stability of the route. In this work, the authors considered power control techniques along with the location information of the nodes to reduce a significant amount of energy consumption and communication overhead.
Chen *et al*. in [9] proposed Link Quality Estimation Based Routing (LQER) protocol that takes decisions about data forwarding on the basis of a dynamic window that stores the history of successful transmission over the link. In paper [10], the authors have presented a new link quality estimation method that effectively calculates the link quality of the nodes. To measure the link quality of the nodes, the authors categorized links as short and long-term quality links. In addition, they have also worked with variation in link quality. Tsai *et al*. [11] enhanced the route discovery process of AODV routing protocol by considering SINR and hop count metric. The protocol monitors and maintains the link quality by measuring the SINR values of all the received packets from its neighbors and selects the route, which has, SINR value above a certain predetermined threshold values to make a stable route from source to destination. Few recent works in the direction of link quality are also discussed in [1], [2], [12], [13].

2.2. Energy Aware Ad Hoc Routing Protocols

Energy-aware routing is an important issue in MANETs and in literature extensive research works had been proposed in this area. Yu *et al*. [14] proposed Geographical and Energy Aware Routing (GEAR), which uses energy metric and location information to design a selection heuristics to route a packet towards the destination. The key feature of GEAR is to restrict the number of interests in direct diffusion within a certain region rather than sending the interests to the whole network. As a result, the protocol can conserve more energy than direct diffusion method. In paper [15], the authors have introduced an energy aware routing protocol, naming, Energy Efficient Location Aided Routing (EELAR) protocol that tries to achieve significant reduction in terms of the energy consumption and routing overhead by limiting the route discovery into a small forwarding zone.
In [16] the authors proposed a loop free energy efficient routing protocol with less communication overhead, naming as Energy-efficient Beaconless Geographic Routing (EBGR). EBGR selects the next node based on the energy-optimal forwarding distance. Then, they defined the upper and lower limits for hop count as well as energy usage for a route between source and destination node. The results demonstrate that the expected total energy consumption for a route is closer to the lower bound.
GAF protocol [5] had been introduced as a solution to reduce energy consumption during routing process. The protocol tries to save energy not only at the time of transmission and reception of packets but also considers the energy consumption in idle (or listening) mode. The authors divided the whole network's region into fixed square grids by using the location information of nodes. The protocol ranked the nodes according to their residual energy level and nodes can switch between sleeping and listing mode within its own grid. Each grid has only one active sensor node based on defined ranking rules and a higher ranker node handles routing within its grid. This scheme extends the lifetime of network.
Another span energy aware routing protocol [17], had been

proposed which broadcasts a route request messages locally to discover a route instead of using location information of nodes. The protocol elects coordinators among all nodes in the network, on rotation basis. These elected coordinators performed multi-hop packet routing within the ad hoc network, while other nodes stay in power saving mode and wait for their chance to become a coordinator. To forward packets, greedy forwarding scheme is used. A similar work had been proposed to extend the lifetime of network naming as, energy-aware data-centric routing (EAD) [18] based on the concept of virtual backbones. MECN [19] is a location-based protocol, which uses mobile sensors to maintain a minimum energy network. For this purpose, it computes an optimal spanning tree with sink as a root and selects only a minimum power path from source to destination. The other energy efficient routing protocols naming, location based energy efficient reliable routing in wireless sensor network (LEAR), discussed in [20] also contributes to reduce the energy consumption and makes greedy routing energy efficient. The most recent research works in this direction is also presented in [21]–[24].

2.3. Link Quality and Energy Aware Routing Protocol

In literature, a very few protocols are proposed to deal with the link quality and energy metric together during route discovery and maintenance phases. In papers [25], [26] authors aimed to evaluate the performance of network in the presence of wireless link errors and tried to relate how link error rates affect the retransmission-metric. The protocol computes a cost function to capture the energy expended in reliable data transfer, for both reliable and unreliable link layers.

In paper [27], another work had been done in the direction of finding an energy efficient reliable path in presence of unreliable links. The protocol integrates the power control techniques with the energy metric to find a stable energy efficient path between source and the destination.

Range *et al*. [28] proposed a routing protocol, which considers link stability and residual energy of mobile nodes while selecting a next forwarding node. Multi-objective linear programming methods are used to formulate the mathematical model to balance the opposite effects of energy aware and link stable routing protocols. By doing this, the protocol tries to find a more stable and shorter path between source and destination.

In paper [29], the authors proposed a routing protocol by combining link stability and energy drain rate metric into the route discovery procedure naming as, link stability and energy aware routing protocol (LAER). The protocol tries to reduce the traffic load on the nodes as well as significant reduction in control overhead. However, LAER does not able to discriminate between links of the same age.

In paper [30], authors designed an energy efficient and link stable routing scheme for the route discovery and the route maintenance phases. The protocol computed the link stability by measuring the received signal strength (RSS) of consecutive packets. Further, these link stability scores are added to compute the route stability of the constructed route.

Vazifehdan *et al*. [31], focused on the major issues, i.e. energy, reliability and prolonging the lifetime of the network and proposed two energy efficient routing methods for wireless ad hoc networks. The first one is called as Reliable Minimum Energy Cost Routing (RMECR) that considers the energy metric as well as link quality to find energy-efficient and reliable paths to increase the network lifetime. On the other hand, the second one considers only energy metric to minimize the total energy required for end-to-end packet traversal and named as Reliable Minimum Energy Routing (RMER).

2.4. Hole Detection based Routing Protocol

Generally, geographical routing protocols use Greedy forwarding [32] scheme to route data. This scheme tries to find the most suitable neighbor node to minimize the distance to the destination in each step to bring the message closer to the destination. However, this scheme fails in the presence of hole. The face routing, or perimeter routings have been proposed as a solution to overcome the hole situations. Karp *et al*. [3] designed a perimeter routing as the solution of this problem to improve the greedy forwarding protocol. This scheme is known as GPSR (Greedy Perimeter Stateless Routing). GOAFR [4] is another method, admired to deal with the hole problem in greedy routing. This scheme combined the greed forwarding with Adaptive Face Routing (AFR) to identify and recover the holes.

In [33], the authors defined hole as simple region enclosed by a polygonal circle, containing all the nodes where local minima can appear. The authors categorized the stuck node as weak and strong stuck node. The protocol bypasses these stuck nodes and tried to find the route outside the local minima for successful transmission. Several other researchers also discussed the hole with their solutions in [34]–[36].

3. Metrics Overview

In this section, we provide the definition of each metric for the better understanding of our proposed work. The notations used to define metrics are listed in Table 1 with their descriptions.

3.1. Energy Metric

Due to limited battery power of nodes, energy is the most important issue in the MANETs. The energy level of the nodes can deplete quickly if they involve in multi-hop communication. For reliable and successful communication, the protocol should consider energy states of the nodes during route finding. Therefore, proposed protocol keeps track of the energy state of the nodes based on the concept

Table 1
Used notations

Notation	Description
$E_{fw(m,d)}$	Energy used in transmitting and receiving m packets
$E_{Tx(m,d)}$	Transmitter energy consumption
$E_{Rx(m)}$	Receiver energy consumption
M	Number of packets
$E_{elec.}$	Electronics energy consumption per bit in the transmitter and receiver mobile nodes
ε_{fs}	Amplifier energy consumption in transmitter nodes in free space
ε_{mp}	Amplifier energy consumption in transmitter nodes in multipath
E_{resi}	Residual energy of node
E_{inital}	Initial energy of mobile nodes
D	Euclidian distance between transmitter and receiver
Pt	Transmission power of transmitter
Pr	Power received at the receiver
Gt	Gain of transmitter antenna
Gr	Gain of receiver antenna
Λ	Wave length of RF signal
$Pref$	Reference power
N	Signal propagation constant
C	Received signal strength at a distance of one meter

of residual energy of the node. For better utilization of energy, authors need energy models to prevent more energy consumption in MANETs.

In this work, the first order radio model to compute the energy consumption during transmitting and receiving of packets is used. The first order model is the basic model in the area of routing protocol evaluation in MANETs. According to this model, the energy consumed for transmitting and receiving m bit data over distance d is calculated by formula given in Eq. (1). In Eq. (2) the energy required to transmit a packet m over distance d is to be dependent on the distance between the nodes and calculated by Eq. (2). In Eq. (3) energy to receive, this message is calculated and the residual energy of the node is given in Eq. (4). The notation employed in energy models are given with their meanings in Table 1.

$$E_{fw(m,d)} = E_{Tx(m,d)} + E_{Rx(m)}\,, \tag{1}$$

$$E_{Tx(m,d)} = \begin{cases} mE_{elec.} + m\varepsilon_{fs}d^2 & \text{if } d < d0 \\ mE_{elec.} + m\varepsilon_{mp}d^4 & \text{if } d \geq d0 \end{cases}, \tag{2}$$

$$E_{Rx(m)} = mE_{elec.}\,, \tag{3}$$

$$E_{resi} = E + E_{inital} - E_{fw}\,. \tag{4}$$

3.2. Link Quality Metric

The geographical routing protocols choose routes based on shortest path criterion. The greedy forwarding is the best example of this criterion and selects farthest neighbor node as a next forwarding node without thinking about the link quality of the nodes. A small movement in selected node may lead link breakage and cause unstable routes. These unstable routes can increase packet loss and control overhead. Thus, the shortest path is not always the best one, other metrics should also be considered while selecting next neighbor node in a range.

In literature, majority of works evaluate the link quality Received Signal Strength Indicator either (RSSI) or Packet Reception Rate (PRR) parameters. These schemes perform well on a sparse network, where the chance of interference among nodes is low. However, as the network density increases, interference among the nodes will also increase. Under such situations, RSSI or PRR does not give a good indication of link quality. For example, if the interference does not exist among nodes, higher RSSI reading generally translates into a higher PRR. As interference increases, a higher RSSI may not result in a higher PRR.

The researches reveal that a node may not always be able to accurately differentiate between packet loss due to a weak signal quality and due to interference among the nodes. Thus, the paper aims to evaluate the link quality more accurately by considering all the factors like signal strength, noise and interference. In theory, the relation between RSSI and interference is calculated and known as a Signal to Interference Plus Noise Ratio (SINR). To understand the SINR, there is need to understand the concept of RSSI first. RSSI provides a measure of the signal strength at the receiver end and it can be correlated to the distance between two nodes. According to Frii's free space transmission equation, the received signal strength decreases as distance increases. The relation between RSSI and distance is given in Eq. (5):

$$\text{RSSI} = -10 \cdot n \log d + C\,. \tag{5}$$

The idea behind RSSI is that the configured transmission power at the transmitting device Pt directly affects the receiving power at the receiving device Pr According to Friis' free space transmission equation, the detected signal strength decreases quadratically with the distance to the sender is shown in Eq. (6).

$$Pr = Pt \cdot Gt \cdot Gr \cdot \frac{\lambda^2}{4\pi d^2}\,. \tag{6}$$

The Received Signal Strength (RSS) is usually converted into RSSI that is defined as a ratio of the received power to the reference power $Pref$. Typically, the reference power represents an absolute value of $Pref = 1$ mW, RSSI, and SINR values are calculated in Eqs. (7) and (8) respectively.

$$\text{RSSI} = 10 \log \frac{Pr(Signal)}{Pref}\,. \tag{7}$$

$$\text{SNIR} = \frac{\text{RSSI}}{Noise + Interference}\,. \tag{8}$$

3.3. Progress

The pure geographical routing protocols choose the next-forwarding node either as distance-based strategy (MFR) [32] to reduce the hop count, or as direction-based strategy (Compass) [37] to minimize the spatial distance. The distance based routing schemes help to reduce the end-to-end delay, however badly affect the energy usage of the nodes. On contrast, the direction based routings increase the stability and consumes less energy but increases overall end to end delay. To overcome these issues of distance and direction based routing protocols, our study considers both the strategies and propose a hybrid progress scheme to find an optimal forwarding node in a range. Distance and direction are represented as Dis_Progress and Dir_Progress respectively. The calculations of these metrics are shown in Eqs. (9) and (10) respectively:

$$\text{Dis\_Progress} = \frac{R-d}{R}, \tag{9}$$

$$\text{Dir\_Progress} = \frac{\theta-\alpha}{\theta}, \tag{10}$$

where R is transmission range, d is the distance between two nodes, θ is angle formed by the request zone with line of sight and α is the angle formed by node inside the request zone.

4. Proposed Protocol

Most of the geographical routing protocols elect the routes based on greedy scheme without considering the condition of the network such as link quality and residual energy of the nodes, which incur the unstable and unreliable route. In addition, once a link failure occurs, a re-route discovery mechanism is initiated that produce high routing overheads. Thus, in this study, authors try to propose a protocol to improve the routing process by combining multiple metrics, e.g. energy level, SINR and progress rather than single metric.

4.1. Network Model and Assumptions

The mobile ad hoc network (MANET) which includes mobile nodes that are randomly deployed in a two dimensional area and each node has its own distinctive position. Every node knows its own location info through Global Position System (GPS), and might acquire different nodes location via a location service protocol. The source is aware of its own location as well as location information of destination. Here, it is assumed that the nodes are same and having a same transmission range R. The communication links between the nodes are bidirectional. The nodes are assumed to be connected only when the distance between them is less than transmission range. The nodes have equal initial energy level and they have the capability of forwarding an incoming packet to one among its neighboring nodes as well as receive information from a transmitting node.

4.2. Protocol Overview

When source S wants to send data to destination D, S utilizes the known location information about destination D to define the expected zone around the destination. Then it defines request zone that includes both the source and complete expected zone. The concept of expected and request zone is originally proposed by the authors of LAR [38]. They proposed a small rectangle shaped request zone. The request zone includes the source and circular region around destination. In this work, the triangular shape request zone is used instead of the rectangular size request zone to forward the route request. The triangular shape request zone contains less number of nodes than rectangular shaped request zone due to its smaller area. It helps to minimize the probability of collisions and reduces the significant amount in routing overheads.

Once a sources defines request zone, it sends route request to other nodes. When a node receives the request, it uses the location information for determining if it resides in a request zone or not. There are many methods in mathematics to find a node in triangular zone. For example, in Fig. 1, the node determines its angle and distance by using the Eqs. (1) and (2). If its angle is smaller than angle θ and distance is less than $d+r$, than nodes Y, V, X and U will reside within the triangular request zone and they can take part in routing process. However, the nodes W, N and Z discard the request, as they are not inside the request zone.

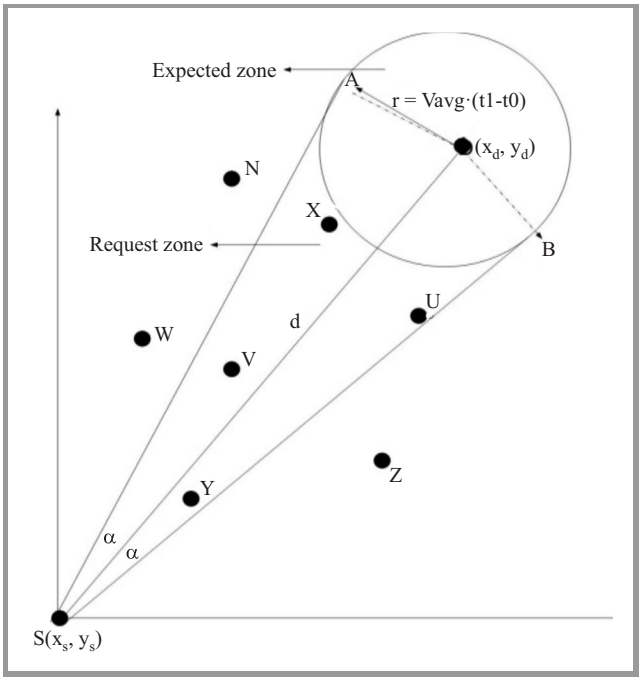


Fig. 1. Request zone formation.

4.3. Forwarding Strategy

The geographical routing protocol uses greedy forwarding scheme, which assumes an ideal network model and completes data transmission without considering other major factors like energy consumption and link quality. These

factors may highly influence the routing procedure. Hence, these factors should also be considered while routing data from source and destination. Therefore, in this section a fuzzy based multi-metric scheme is proposed to select an optimal next forwarding node, which increases the quality of route in terms of both stability and reliability over conventional geographical routing schemes. The protocol combines link quality and energy metric to select the optimal next neighbor node. Generally, the multi-metric routing protocols use the weight factors to combine multiple metrics to get the final score over an available path. Although a weight factor is easy and popular way to combine multiple metrics, for best score, there are no predefined rules to determine the weight factors between metrics. The fixed weights cannot satisfy all the network scenarios. Therefore, to overcome these limitations of the weight selection problem, the fuzzy logics is taken as a solution. To select the next forwarding node, all the metrics are taken as an input for the fuzzy logic engine. Then, fuzzy rules are applied on these inputs and results show the probability of next forwarding node.

Fuzzy logics are a computational framework based on the concepts of the theory of fuzzy sets, fuzzy rules, and fuzzy inference. In traditional logic, an object takes on a value of either zero or one. In fuzzy logic, a statement can assume any real value between 0 and 1 representing the degree to which an element belongs to a given set. Fuzzy system has three main components: a fuzzification block, fuzzy rule base for inferencing (decision-making unit), and a defuzzification interface. The fuzzification (input) maps the (crisp) input values into fuzzy values, by computing their membership in all linguistic terms defined in the corresponding input domain. The inference engine maps inputs by combining a set of membership functions with the fuzzy rules to get fuzzy outputs. The defuzzification interface computes the (crisp) output values by combining the output of the rules and performing a specific transformation. Centroid of the area (COA), mean of maximum (MOM) and fuzzy mean (FM) are a wide variety of methods for defuzzifying the fuzzy output.

Table 2 shows, each input is being presented by three linguistic values: weak, medium, and high, for link quality. The values good, average and low are taken for residual energy parameter. The use of very far, far and close for distance and the values for deviation are set as less, mid and more directed. The values of very high, high, good, average, low and very low are used for output parameters. The triangular membership function is used for fuzzification of given input since it produces low computation overheads. Mamdani fuzzy interface system is used as fuzzy inference system to evaluate the rules. These fuzzy rules consist if and then parts which are used to formulate the conditional statements that comprise fuzzy logic.

Table 2
Linguistic values for inputs

Input parameter	Values		
Residual energy	High	Average	Low
Link quality	Good	Medium	Weak
Dis_Progress	Close	Far	Very far
Dir_Progress	More deviated	Mid deviated	Less deviated

In general, one rule alone is not effective to produce the solution. Two or more rules that can play off one another are needed to merge for output. The proposed protocol takes 4 input variables which are converted into linguistic values by using the membership functions to determine the membership degree of nodes.

The outcomes of fuzzification process are passed to the inference engine for further processing. Inferencing process applies fuzzy rules on these fuzzified values and in this work, there are 3^4 i.e. 81 different fuzzy rules. The Table 3 shows a few samples of rules used in presented research work. The output of each rule is a fuzzy set and the output (optimum cost) value lies between 0 and 1. Finally, the resulting output set is defuzzified by using a COA method in a single output.

Table 3
Few fuzzy rules used for inferencing

Link quality	Residual energy	Dir_Progress	Dis_Progress	Optimal function
Good	High	More_Directed	Close	Very high
Good	Hihg	More_Directed	Far	High
Good	High	Mid_Directed	Far	Average
Medium	High	More_Directed	Close	Good
Medium	Average	Mid_Directed	Close	Average
Good	Low	More_Directed	Far	Low
Weak	Average	More_Directed	Close	Low
Weak	Low	Less_Directed	Far	Very low

In Fig. 2, source node S has 13 neighbors within its transmission range. As was discussed earlier, nodes, which lie

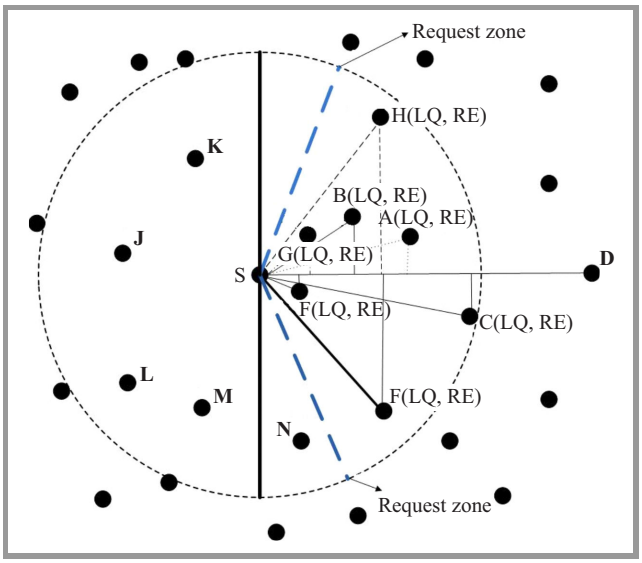


Fig. 2. Selection of optimal node.

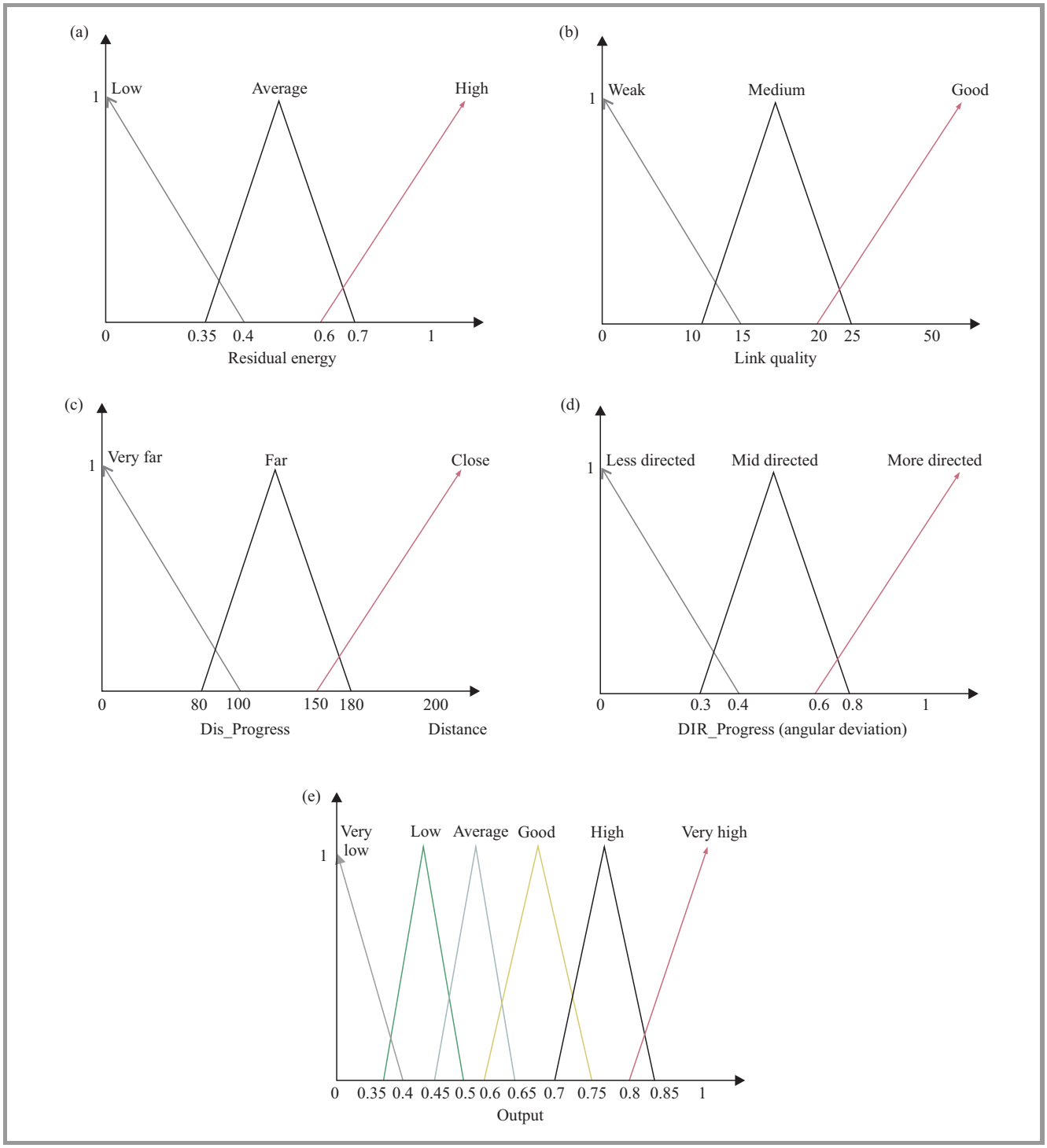


Fig. 3. (a) membership function for residual energy, (b) membership function for link quality, (c) membership function for input distance, (d) membership function for input direction, (e) output of given inputs.

inside the request zone may only be the next forwarding node. Thus, only those neighbors are evaluated, which are in the request zone towards the destination D. The protocol compares the residual energy, link-quality, distances and deviations (direction) of the nodes A–H.

Suppose the residual energy, link quality (SINR), distances and angular deviations of nodes are $(E_A, LQ_A, d_A, \alpha_A)$, $(E_B, LQ_B, d_B, \alpha_B)$, $(E_C, LQ_C, d_C, \alpha_C)$, $(E_E, LQ_E, d_E, \alpha_E)$, $(E_F, LQ_F, d_F, \alpha_F)$, $(E_G, LQ_G, d_G, \alpha_G)$ and $(E_H, LQ_H, d_H, \alpha_H)$ respectively. The residual energy(RE), link quality(LQ), Dis_Progress (d) and Dir_Progress (α) of nodes are given as $(E_A > E_B > E_G > E_H > E_F > E_C)$, $(LQ_G > LQ_A > LQ_E > LQ_B > LQ_F > LQ_H > LQ_C)$, $(d_C > d_A > d_H > d_F > d_B > d_G > d_E)$ and $(\alpha_A < \alpha_C < \alpha_B < \alpha_B < \alpha_G < \alpha_F < \alpha_H)$.

Based on the information node A is selected as the next forwarding node since, it has high link quality, good residual

energy level, less deviated from LOS and closer to destination.

For an example, if there is a fuzzy rule like, "if SINR (link quality) is high, residual energy is good, Dis_progress (distance) is close and Dir_Progress (deviation) is very high then the fuzzy cost is very high". Suppose a node having a link quality 30 dBm, residual energy is 0.8 J, distance is 180.56 m and value of the deviation is 0.864 then the output value is 0.886. This output value indicates the fuzzy cost for specified node and it is high for the above-mentioned rule. The fuzzy system gives output, compromised all the routing metrics and selects the node, which is optimal in all the terms.

Figures 3a-d respectively, show the membership functions of the residual energy, link quality, distance, and direction (angular deviation) amount.

Figure 3e depicts the membership function of the output unit before the defuzzification of results. The input parameters are taken by a membership function with degree one and it becomes a fuzzy value.

In the example discussed in Fig. 2, nodes A–H may be the next forwarding node, thus for these nodes, all metrics are considered as input parameters and the result table shows outcomes for optimally selected node in Table 4. The result shows that the value of fuzzy cost increases on increasing the values of all metrics. In Fig. 2 node A scores the greatest fuzzy cost among all the nodes so node A will be selected as next forwarding nodes in a range.

Table 4
Result table

Node	Input (link quality, residual energy, distance, direction)	Output (node selected)
A	[30, 0.8, 180.56, 0.864]	0.886
B	[20, 0.76, 155.65, 0.634]	0.586
C	[11, 0.4, 195,0.732, 0.703]	0.347
E	[22, 0.723, 120.43, 0.845]	0.625
F	[18, 0.632, 160.43, 0.543]	0.619
G	[32, 0.743, 130.32, 0.432]	0.645
H	[17, 0.702, 170.43, 0.345]	0.483

4.4. Hole Detection Scheme

The smaller request zone is the better choice to reduce routing overhead. However, the too small size request zone can be a reason for no or unstable routing in the request zone, still there exist a stable path outside the request zone. This situation is known as hole in the request zone. Besides the smaller request zone, there may be various other reasons for hole problem like border node selection, energy depletion etc. Therefore, in this section, a scheme to overcome the hole problem is proposed by announcing the hole's information and suggest a local healing solution for successful routing.

In example shown in Fig. 4, to forward the messages, source S first checks its neighbor table to find an optimal next forwarding neighbor within the request zone towards the destination. To find the optimal node source applies the forwarding mechanism discussed in Subsection 4.4. If source S, does not get any node in its transmission range, routing protocol gets in a hole and node S is called a stuck node. In this situation, most of the geographical routing protocols depend on perimeter routing [3] to find a detour path, that makes routing inefficient.

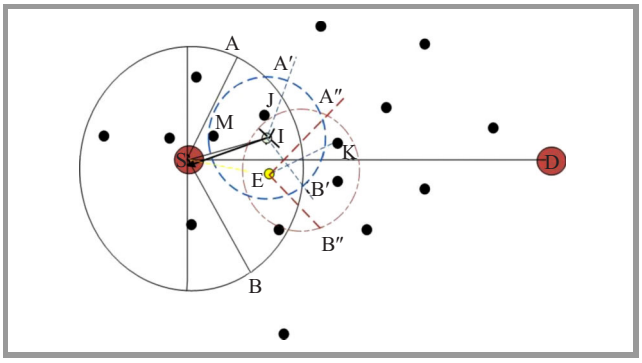


Fig. 4. Hole detection scheme. (See color pictures online at www.nit.eu/publications/journal-jtit)

Hence, to overcome the hole problem, this protocol, first, suggest a mechanism for immediate detection of holes. After that, the information about the hole is announced among the nearby nodes (about the request zone angle θ and hole size).

In Fig. 4, source S chooses node I as a next forwarding node. Node I defines its own triangular shaped request zone ($IA'B'$) and starts finding a node in its transmission range within defined request zone. Unfortunately, the node I does not find any node to forward a packet to a given destination.

Thus, node I will consider itself as a stuck (blocked) in this direction and I will advertise this hole information to its neighbors. As neighbors get the information, they mark node I as stuck node and they will not choose node I for further communications.

Based on this information, S marks I as stuck node and tries to find another optimal neighbor in its range to forward the messages. After marking I as stuck node E is selected as a next forwarding node. The request zone formed by source S is ASB given by black lines. The transmission range of node I is given by blue dotted circle and request zone $A'IB'$ by blue dotted lines. The request zone $A'IB'$ does not contain any node to forward the message. Red color dotted lines show the transmission range and request zone of node E is EA "B". Then node E selects the K as a next forwarding node to route data to destination D.

5. Performance Evaluation

In this section, to evaluate the performance of the proposed protocol, implementation is carried out in Matlab 7.0 and simulation results are compared with greedy perimeter stateless routing (GPSR) and Location-Aided Routing scheme (LAR).

The nodes vary from 50 to 250 and uniformly deployed in 1000 m^2 area. The nodes have speeds between 0 to 25 m/s with 30 s as pause time. Each node has equal transmission range and equal initial energy levels. The transmission range is set 200 m and node's initial energy is taken as 1 J. For simulation work, the channel capacity of mobile nodes is 2 Mb/s and Random Waypoint Mobility Model is implemented as the mobility model. The antenna heights and gains of all nodes are taken at 1 m and 1 m respectively. Two Ray path loss model is used as the radio propagation model. The simulation runs for 300 s. The IEEE 802.11b is used to simulate the MAC layer, which contains all the mechanisms, which use the CSMA/CA technique based on the Distributed Coordination Function (DCF) access method (Table 5). Authors correlate the link quality with SINR and in this work, the SINR is calculated in terms of SNR. To calculate the SNR values, the nodes in Additive White Gaussian Noise (AWGN) environment is deployed along with external RF interference noise sources.

Table 5
Simulation parameters

Name	Value
Topology size	1000×1000 m
Number of nodes	50–250
Speed	5–25 m/s
Mobility model	Random way point
Simulation time	300 s
Channel rate	2 Mb/s
Channel type	Wireless channels
Mobility model	Random way point
MAC Layer protocol	IEEE 802.11b
Radio propagation model	Two ray ground
Transmission range	200 m
Traffic type	CBR
CBR Packet size	100 bytes

5.1. Performance Metrics

Packet delivery ratio. This metric is defined as the number of delivered data packets to destination and calculated as the ratio of number of received data packets to the number of sent data packets. This metric represent the reliability of the protocol in terms of data delivery.

Average energy consumption. This metric indicates energy consumed in the nodes of the network. This metric is important for prolonging the network lifetime.

Average end-to-end delay. This metric indicates latency in the communication network. It is calculated as the ratio of the total time taken by all the packets to reach the destination of the total number of packets. The protocol should have minimum average delay for prompt data transfer.

Throughput. It is defined as rate of successful message delivery over a communication channel and generally, it is measured in bits per second.

5.2. Simulation Impact of Node Density

In this section, the influence of node density on the above discussed metrics and analyzed the behavior of protocols in dense and sparse network are discussed. In simulation, the nodes are varying from 50, 100, 150, 200 and 250. The speed is kept on 10 m/s. Four traffic connections are used from source to destination including CBR traffic pattern. The proposed protocol combines link quality (SINR), progress (distance, direction) and residual energy when selecting a next forwarding node. This can avoid the occurrence of the worst situations, such as choosing the most distant neighbor that may has a poor link quality.

First, the packet delivery ratio of proposed and existing protocols (GPSR, LAR) is compared with the varying number of nodes. The results are shown in Fig. 5a. The packet delivery ratio of the proposed protocol is comparatively high in comparison with LAR and GPSR since, proposed scheme selects the next hop by combining the link quality and residual energy with distance metric. By using these important metrics, the proposed protocol improves the packet delivery ratio in comparison with existing single metric protocols.

In presence of hole, the LAR does retransmission and GPSR switches to perimeter mode to route data. As a consequences delay increases during the packet transmission, which causes lower packet delivery ratio. In this situation, our protocol performs better than others do. Our scheme reduces the retransmissions counts by healing the hole by applying the scheme proposed in Subsection 4.4. The results also show that packet delivery ratio of the all protocols drop as number of nodes increases. Figure 5b presents energy consumption vs. varying nodes for GPSR, LAR and our proposed protocol. The result shows that the proposed solution performs better in terms of energy consumption than GPSR and LAR routing protocols and the network lifetime is improved significantly. Figure 5c shows that the average delay of the proposed work is higher than the LAR and GPSR protocol. The proposed protocol focuses on residual energy, link quality and distance to select next forwarding node instead of shortest path. It produces computation overheads and enhances the end-to-end delay. Figure 5d, illustrates that the proposed protocol improves the network throughput in comparison with GPSR and LAR protocols. On average, it achieves better throughput than GPSR and LAR because it considers link quality metric when choosing the next node. By using this metric, the protocol saves bandwidth and this saved bandwidth can be utilized to transmit other packets. As a result, it improves network throughput. The reason behind the better throughput of presented protocol is that it reduces the retransmission counts. On the other hand, in GPSR retransmission is taken place when node dies and, in LAR when greedy forwarding fails. In these bad situations, retransmission

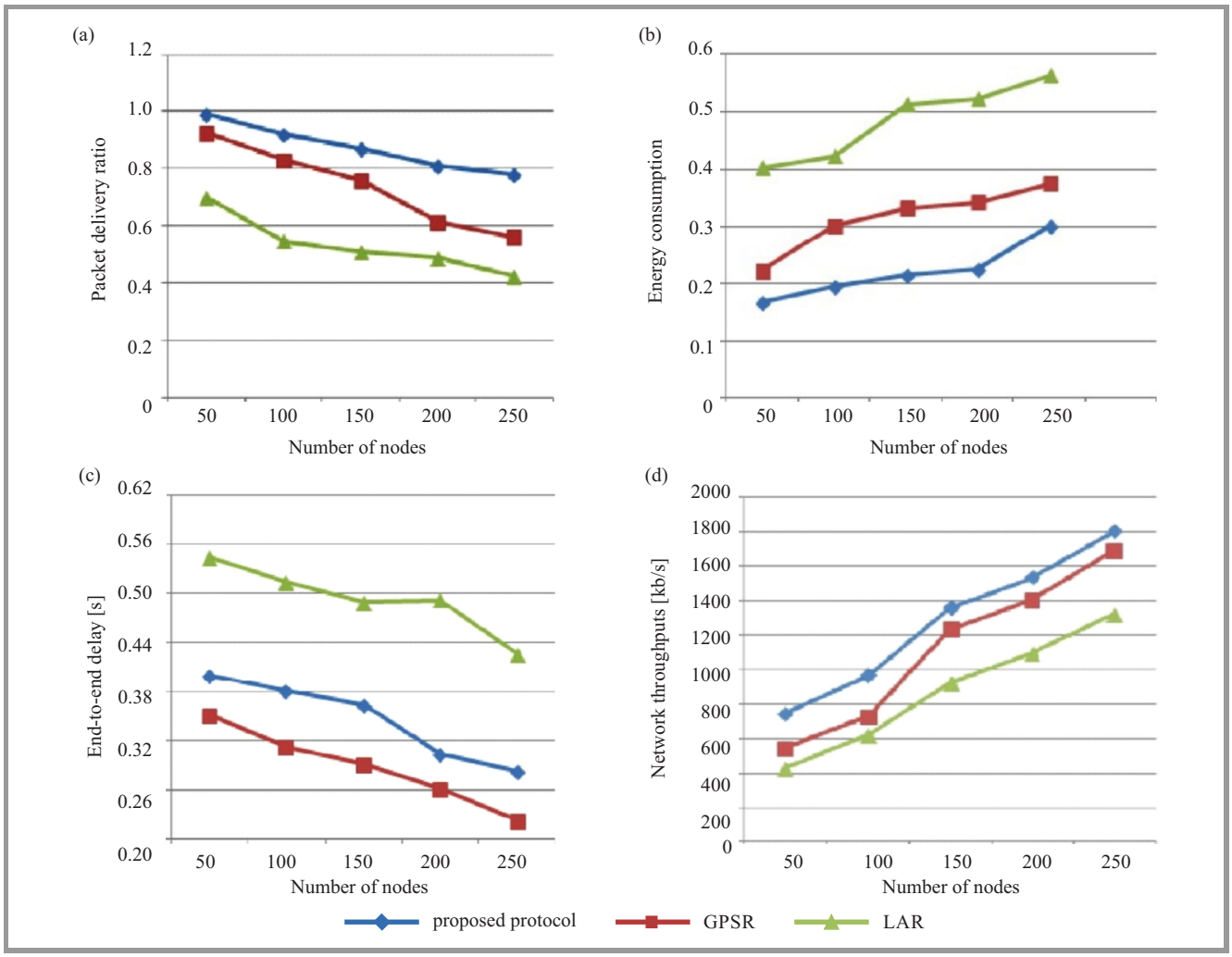


Fig. 5. (a) packet delivery ratio, (b) energy consumption, (c) end-to-end delay, and (d) network throughput at 10 m/s.

will take place heavily and consume excessive amount of spectrum. As a result, in GPSR and LAR the network throughput is low. The results also show that on increasing the nodes the value of throughput goes down for all the nodes.

To study the impact of speed, the node speed is varied from 5 to 25 m/s while the number of nodes are fixed at 50. The other parameters and settings are kept same. The higher speed will cause the large number of link failures as well as a large number of collisions due to frequent movements of nodes. Therefore, an increase in speed definitely affects the performance of routing protocols.

The results show that the packet delivery ratio of the proposed protocol is better than other routing protocols since, it considers the good link quality nodes to route data (Fig. 6a). On the other hand, LAR and GPSR select the node, closer to the destination that may have a bad link quality. The packet delivery ratio of all the protocols rises in starting and then goes down with the increase in node's speed. The reason behind is that if the node's speed increases, the connectivity between nodes causes a lower packet delivery ratio.

The result reveals that energy consumption throughput of all the routing protocols that decreases with an increase in velocity of a node (Fig. 6b) in Fig. 6c, the plot for the end-to-end delay vs. varying speeds is given that shows the end-to-end delay of all the protocols go down with the increasing velocity of nodes. The reason behind this huge fall is that the time to carry and forward a packet decreases with the increase in speed. As speed increases, the throughput goes down for all the protocols (Fig. 6d).

6. Conclusions

Due to the dynamic nature and limited battery power of mobile nodes, link quality and energy metrics play an important role for successful and reliable communication in MANETs. Hence, these parameters should be considered while designing an efficient and optimal routing protocol. In this paper, a novel multi-metric optimal routing protocol for reliable and stable communication in MANET was presented. It combines link quality information and residual energy with progress metric to select the next forwarding node. Fuzzy logics are used to combine these

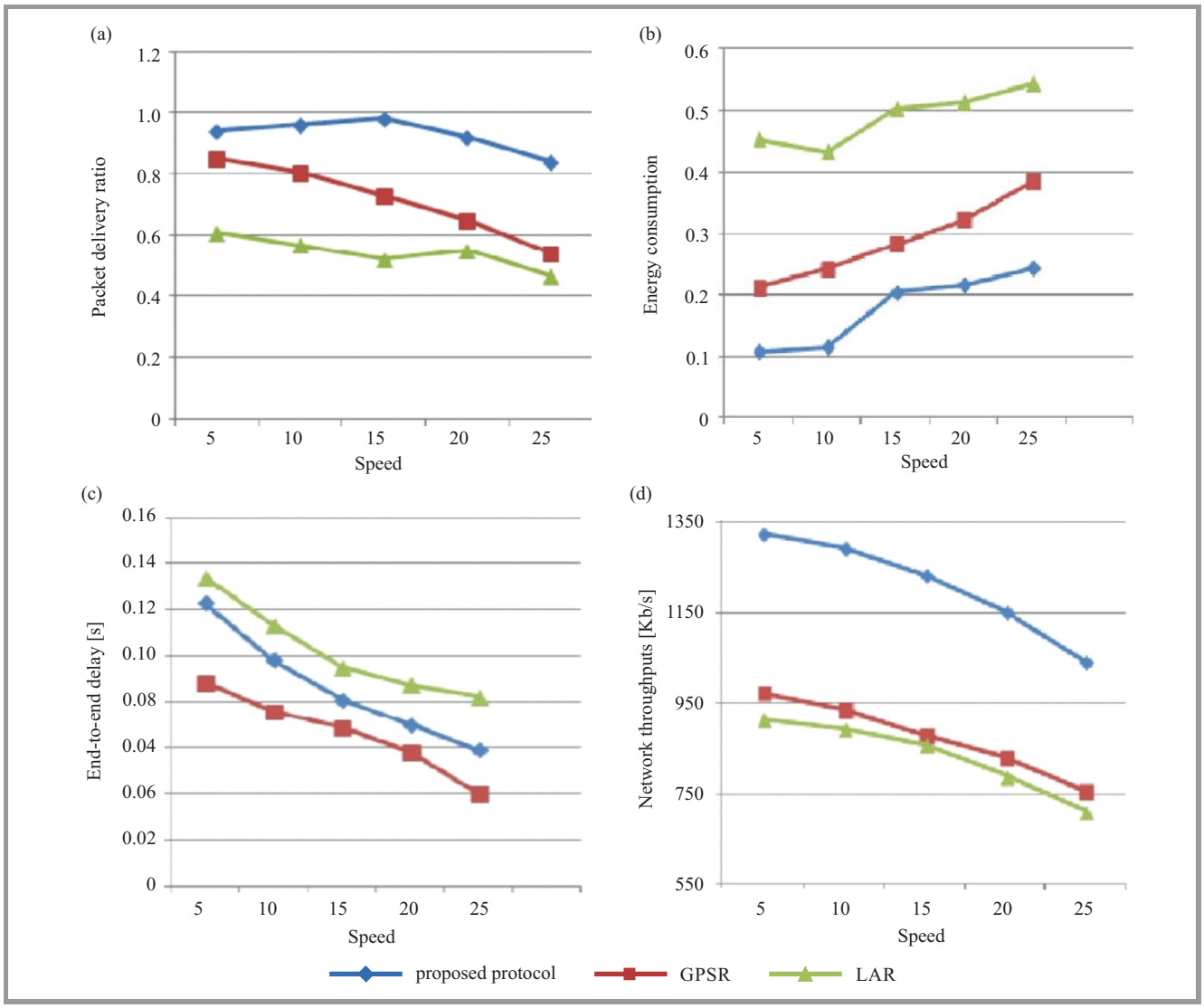


Fig. 6. (a) packet delivery ratio, (b) energy consumption, (c) end-to-end delay, (d) throughput.

metrics, which help to o find the optimal output in terms of optimal forwarding nodes. Further, the protocol aims to deal with the hole problem and proposes a method to overcome it. Matlab software is used to simulate the proposed work. The results are compared with GPSR and LAR for all the metrics at varying node density and varying speeds. The results reveal that the proposed protocol is more energy efficient and reliable than GPSR and LAR routing protocols. It improves the packet delivery rate, throughput and reliability of the transmission of data with a small delay.

References

[1] F. Entezami, M. Tunicliffe, and C. Politis, "Find the weakest link: Statistical analysis on wireless sensor network link-quality metrics", *Veh. Technol. Mag.*, vol. 9, no. 3, pp. 28–38, 2014.

[2] C. H. E. N. Guowei, "Enhancement of beaconless location-based routing with signal strength assistance for Ad-hoc networks", *IEICE Trans. on Commun.*, vol. 91, no. 7, pp. 2265–2271, 2008.

[3] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks", in *Proc. 6th Annual Int. Conf. Mob. Comput. and Netw. MobiCom 2000*, Boston, MA, USA, 2000, pp. 243–254.

[4] H. Frey and I. Stojmenovic, "On delivery guarantees of face and combined greedy-face routing in ad hoc and sensor networks", in *Proc. 12th Ann. Int. Conf. Mob. Comput. & Netw. MobiCom 2006*, Los Angeles, CA, USA, pp. 390–401.

[5] M. A. Mikki, "Energy efficient location aided routing protocol for wireless MANETs", *Int. J. of Comp. Science and Inform. Secur. (IJCSIS)*, vol. 4, no. 1 and 2, 2009.

[6] R. Dube, C. D. Rais, K. Y. Wang, and S. K. Tripathi, "Signal stability-based adaptive routing (SSA) for ad hoc mobile networks", *Personal Commun.*, vol. 4, no. 1, pp. 36–45, 1997.

[7] M. Zuniga and B. Krishnamachari, "Analyzing the transitional region in low power wireless links", in *Proc. 1st Ann. IEEE Commun. Soc. Conf. Sensor & Ad Hoc Commun. and Netw. IEEE SECON 2004*, Santa Clara, CA, USA, 2004, pp. 517–526.

[8] A. Triviño-Cabrera, I. Nieves-Pérez, E. Casilari, and F. J. González-Cañete, "Ad hoc routing based on the stability of routes", in *Proc. 4th ACM Int. Works. Mob. Manag. Wirel. Access MobiWac 2006*, Torremolinos, Spain, 2006, pp. 100–103.

[9] J. Chen, R. Lin, Y. Li, and Y. Sun, "LQER: A link quality estimation based routing for wireless sensor networks", *Sensors*, vol. 8, no. 2, pp. 1025–1038, 2008.

[10] C. Renner, S. Ernst, C. Weyer, and V. Turau, "Prediction accuracy of link-quality estimators", in *Wireless Sensor Networks*, C. Renner, S. Ernst, C. Weyer, and V. Turau, Eds. *LNCS*, vol. 6567, pp. 1–16. Springer, 2011.

[11] H. M. Tsai, N. Wisitpongphan, and O. K. Tonguz, "Link-quality aware ad hoc on-demand distance vector routing protocol" in *1st Int. Symp. Wirel. Pervasive Comput. ISWPC 2006*, Phuket, Thailand, 2006, pp. 6–12.

[12] K. Srinivasan, P. Dutta, A. Tavakoli, and P. Levis, "An empirical study of low-power wireless", *ACM Trans. on Sensor Netw. (TOSN)*, vol. 6, no. 2, article no. 16, 2010.

[13] T. Braun, M. Heissenbüttel, and T. Roth, "Performance of the beacon-less routing protocol in realistic scenarios", *Ad Hoc Netw.*, vol. 8, no. 1, pp. 96–107, 2010.

[14] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks", Tech. Rep. UCLA/CSD-TR-01-0023, UCLA Computer Science Dept. May, 2001.

[15] H. Zhang and H. Shen, "Energy-efficient beaconless geographic routing in wireless sensor networks", *IEEE Trans. on Paral. and Distrib. Syst.*, vol. 21, no. 6, pp. 881–896, 2010.

[16] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad hoc routing", in *Proc. 7th Ann. Int. Conf. Mob. Comput. & Netw. MobiCom 2001*, Rome, Italy, 2001, pp. 70–84.

[17] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks", in *Proc. 7th Ann. Int. Conf. Mob. Comput. & Netw. MobiCom 2001*, Rome, Italy, 2001, pp. 85–96.

[18] A. Boukerche, X. Cheng, and J. Linus, "Energy-aware data-centric routing in microsensor networks", in *Proc. 6th ACM Int. Worksh. Model. Anal. & Simul. of Wirel. and Mob. Syst. MSWIM 2003*, San Diego, CA, USA, 2003, pp. 42–49.

[19] V. Rodoplu and T. H. Meng, "Minimum energy mobile wireless networks", *IEEE J. on Selec. Areas in Commun.*, vol. 17, no. 8, pp. 1333–1344, 1999.

[20] Y. Lan, W. Wenjing, and G. Fuxiang, "A real-time and energy aware QoS routing protocol for multimedia wireless sensor networks", in *7th World Congr. Intell. Control and Autom. WCICA 2008*, Chongqing , China, 2008, pp. 3321–3326.

[21] E. Amiri, H. Keshavarz, M. Alizadeh, M. Zamani, and T. Khodadadi, "Energy efficient routing in wireless sensor networks based on fuzzy ant colony optimization", *Int. J. Distrib. Sensor Netw*., article no. 768936, 2014 (doi: 10.1155/2014/768936).

[22] J. Wang, J. U. Kim, L. Shu, Y. Niu, and S. Lee, "A distance-based energy aware routing algorithm for wireless sensor networks", *Sensors*, vol. 10, no. 10, pp. 9493–9511, 2010.

[23] H. Y. Zhou, D. Y. Luo, Y. Gao, and D. C. Zuo, "Modeling of node energy consumption for wireless sensor networks", *Wirel. Sensor Netw.*, vol. 3, no. 1, pp. 18–23, 2011 (doi: 10.4236/wsn.2011.31003).

[24] S. Banerjee and A. Misra, "Minimum energy paths for reliable communication in multi-hop wireless networks", in *Proc. 3rd ACM Int. Symp. Mob. Ad Hoc Netw. & Comput. MobiHoc 2002*, Lausanne, Switzerland, 2002, pp. 146–156.

[25] Q. Dong, S. Banerjee, M. Adler, and A. Misra, "Minimum energy reliable paths using unreliable wireless links", in *Proc. 6th ACM Int. Symp. Mob. Ad Hoc Netw. & Comput. MobiHoc 2005*, Urbana-Champaign, IL, USA, 2005, pp. 449–459.

[26] B. Xu and Y. Li, "A novel link stability and energy aware routing with tradeoff strategy in mobile ad hoc networks", *J. Commun.*, vol. 9, no. 9, pp. 706–713, 2014.

[27] X. Y. Li, Y. Wang, H. Chen, X. Chu, Y. Wu, and Y. Qi, "Reliable and energy-efficient routing for static wireless ad hoc networks with unreliable links", *IEEE Trans. Parall. & Distrib. Syst.*, vol. 20, no. 10, pp. 1408–1421, 2009.

[28] F. De Rango, F. Guerriero, S. Marano, and E. Bruno, "A multiobjective approach for energy consumption and link stability issues in ad hoc networks", *IEEE Commun. Lett.*, vol. 10, no. 1, pp. 28–30, 2006.

[29] F. De Rango, F. Guerriero, and P. Fazio, "Link-stability and energy aware routing protocol in distributed wireless networks", *IEEE Trans. Parall. & Distrib. Syst.*, vol. 23, no. 4, pp. 713–726, 2012.

[30] P. Srinivasan and P. Kamalakkannan, "REAQ-AODV: Route stability and energy aware QoS routing in mobile Ad Hoc networks", in *Proc. 4th Int. Conf. Adv. Comput. ICoAC 2012*, Chennai, India, 2012, pp. 94–98.

[31] J. Vazifehdan, R. V. Prasad, and I. Niemegeers, "Energy-efficient reliable routing considering residual energy in wireless ad hoc networks", *IEEE Trans. Mob. Comput.*, vol. 13, no. 2, pp. 434–447, 2014.

[32] H. Takagi and L. Kleinrock, "Optimal transmission ranges for randomly distributed packet radio terminals", *IEEE Trans. Commun.*, vol. 32, no. 3, pp. 246–257, 1984.

[33] Q. Fang, J. Gao, and L. J. Guibas, " Locating and bypassing holes in sensor networks", *Mob. Netw. and Appl.*, vol. 11, no. 2, pp. 187–200, 2006.

[34] M. R. Senouci, A. Mellouk, and K. Assnoune, "Localized movement-assisted sensor deployment algorithm for hole detection and healing", *IEEE Trans. Parall. & Distrib. Syst.*, vol. 25, no. 5, pp. 1267–1277, 2014.

[35] X. Fan and F. Du, "An efficient bypassing void routing algorithm for wireless sensor network", *J. Sensors*, vol. 2015, article ID 686809 (doi: 10.1155/2015/686809).

[36] W. Wei, X. L. Yang, P. Y. Shen, and B. Zhou, "Holes detection in anisotropic sensor nets: topological methods", *Int. J. Distrib. Sensor Netw.*, vol. 8, no. 10, 2012 (doi: 10.1155/2012/135054).

[37] E. Kranakis, H. Singh, and J. Urrutia, "Compass routing on geometric networks", in *Proc. 11th Canadian Conf. Computat. Geometry CCCG'99*, Vancouver, Canada, 1999.

[38] Y. B. Ko and N. H. Vaidya, "Location-Aided Routing (LAR) in mobile ad hoc networks", *Wireless Netw.*, vol. 6, no. 4, pp. 307–321, 2000.

Priya Mishra received her Master of Computer Application (MCA) degree from Rani Durgawati Vishwavidyalaya, Jabalpur, India. She received her M.Tech. degree in Computer Science and Engineering from Uttar Pradesh Technical University, India. She has total 13 years teaching experience and working as a Guest Faculty in Gautam Buddha University, Gr. Noida in ICT department. She is Ph.D. candidate in the field of mobile ad hoc network in JIIT University Noida, India. Her research interests are mobile ad hoc network, mobile computing, and soft computing.

E-mail: amipriya@gmail.com
Department of Computer Science
and Information Technology
JAYPEE Institute of Information Technology, University
A-10 Sector 62
Noida, India

Charu Gandhi received her B.Sc. degree in Computer Science and Engineering, from Kurukshetra University, Kurukshetra, India. She received M.Tech. from Banasthali Vidyapith, Rajasthan and Ph.D. degree in Computer Science from Kurukshetra University, Kurukshetra. She has total 12 years experience in teaching and research. She is working as an Associate Professor in computer science department in JIIT University Noida, India. Her expert areas are mobile ad hoc networks and wireless sensor networks.
E-mail: charu.kumar.jiit@jiit.ac.in
Department of Computer Science
and Information Technology
JAYPEE Institute of Information Technology, University
sector 128
Noida, India

Buddha Singh received his B.Sc. degree in Information Technology from Madhav Institute of Technology and Science, Gwalior, India. He received his M.Tech. and Ph.D. degree in Computer Science and Technology from Jawaharlal Nehru University, New Delhi, India. He is working as an Assistant Professor in school of Computer and System Sciences in Jawaharlal Nehru University, New Delhi, India. His research areas of interest are mobile ad hoc networks, wireless sensor networks, cognitive radio big data analytics, complex networks, mobile computing.
E-mail: b.singh.jnu@gmail.com
Department of Computer Science
and Information Technology
School of Computer and System Sciences
in Jawaharlal Nehru University
New Delhi, India

Paper

Comparison of Selected Fair-optimization Methods for Flow Maximization between Given Pairs of Nodes in Telecommunications Network

Grzegorz Zalewski[1] and Włodzimierz Ogryczak[2]

[1] *National Institute of Telecommunications, Warsaw, Poland*
[2] *Institute of Control and Computation Engineering, Warsaw University of Technology, Warsaw, Poland*

Abstract—Dimensioning of telecommunications networks requires the allocation of the flows (bandwidth) to given traffic demands for the source-destination pairs of nodes. Unit flow allocated to the given demand is associated with revenue that may vary for different demands. Problem the decision-making basic algorithms to maximize the total revenue may lead to the solutions that are unacceptable, due to "starvation" or "locking" of some demand paths less attractive with respect to the total revenue. Therefore, the fair optimization approaches must be applied. In this paper, two fair optimization methods are analyzed: the method of ordered weighted average (OWA) and the reference point method (RPM). The study assumes that flows can be bifurcated thus realized in multiple path schemes. To implement optimization model the AMPL was used with general-purpose linear programming solvers. As an example of the data, the Polish backbone network was used.

Keywords—allocation problem, decision problems, fair-optimization, linear programming, multi-criteria, networks, ordered weighted averaging, OWA, reference point method, RPM.

1. Introduction

Many times in real life people meet with decision problems affecting on different ranks to various types of business, organizations, systems, networks or other more or less complex structures. Even in the household, everyone meets with decision problems affects to people comfort of living, safety, etc. In each of these problems, the decision-maker is taking some specific preferences and selecting according to them. If the problem can be written in the form of linear constraints and objective function, then existing software can be used to generate solutions of specific kind of problems [1], [2]. This could be the production problems, the knapsack problems, the selection of the optimal structure of the investment portfolio, whole range of problems related to networks [2] or the problem related to planning the allocation of resources [3].

Telecommunications networks are facing increasing demand for many services. Therefore, the problem to determine how much traffic of every demand (traffic stream) should be admitted into the network and how the admitted traffic should be routed through the network so as to satisfy the requirements of high network utilization and guarantee fairness to the users, is one of the most challenging problems of current telecommunications networks design [4], [5]. The problem, usually referred to as the network-dimensioning problem, is related to planning deployment of the network resources (bandwidth, link capacity, etc.) [3]–[5]. There are two main objectives against which the decision is optimized. The first one is to maximize the profit from each unit of the transmitted load on each demand, and the second one is to guarantee some fairness to prevent blocking the paths where profit is less attractive.

Figure 1 shows the case of overlapping demands. Assuming that the capacity of arc e_3 is less than the capacity of both e_1 and e_2 consider the problem of the allocation of load demands d_1 and d_2. Each unit load attributed to demand is profitable. When the value of the unconsolidated profit will be different, the optimal solution may result in larger load values assigned to more profitable paths discriminating those less attractive.

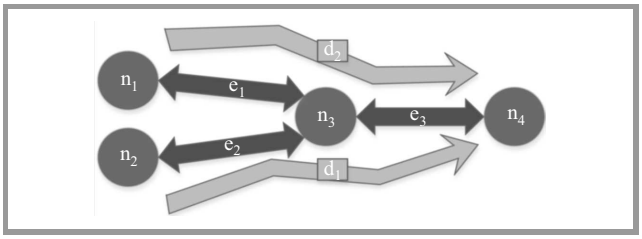


Fig. 1. An example illustrates bandwidth allocation problem on demands d_1 and d_2.

While the objective related to the maximization of profit is simple for mathematical formulation as the product of unit profit attributable to the path and the amount of the allocated load on it, the second objective of fairness requires some deeper consideration [6]. One way is to attach the rigid restrictions on the minimum requirements for a given path. This simple method does not give reliable results. It requires the knowledge of the decision maker about the minimum values of allocated resources. Unfortunately, it is difficult to estimate in the most cases. Several fair allocation schemes based on the concepts of equitable opti-

mization have been considered and analyzed, c.f. [7], [8]. These models are:

- max-min [2],
- lexicographic max-min [2], [9], [10],
- proportional fairness (PF) [11],
- ordered weighted averages (OWA) [12], [13],
- reference point method (RPM) [14].

The most important feature in each of those methods is taking into account impartiality and equitability in the preference model. Both properties are guaranteed by comparing ordered vectors making the original sequence of objective functions not relevant for optimization. During the implementation of the methods based on ordered outcomes one can take advantage of a problem that returns the k-th largest or the smallest value of the function of resource allocation on a set of requirements D [15]. For this purpose, binary variables z_{kd} and unlimited variable t_k have been introduced. The model, which allows to receive each further objective function values in descending order can be written as follows:

$$f(x)_k = \min t_k \,, \tag{1}$$

subject to:

$$t_k - y_d \geq -Cz_{kd}, z_{kd} \in \{0,1\}, \forall d \in D \,,$$

$$\sum_{j=1}^{m} z_{kd} \leq k-1 \,.$$

Such a formulation allows one to obtain the largest value for $k=1$ from the whole set of $f(x)$ values. Further, for any $k>1$ one gets the k-th value in non-increasing order. In this case formulation brakes $k-1$ restrictions using constant C with suitable large value (the largest achievement function value).
Similarly, can be determined successive values of $f(x)$ in non-decreasing order. The corresponding optimization model can be written as:

$$f(x)_k = \max t_k \,, \tag{2}$$

subject to:

$$t_k - y_d \leq Cz_{kd}, z_{kd} \in \{0,1\}, \forall d \in D \,,$$

$$\sum_{j=1}^{m} z_{kd} \leq k-1 \,.$$

The study is focused on OWA and the RPM models. Both methods allow to control the solution in their characteristic way, and allow to obtain results more or less fair. In determining the level of fairness, some abstract index has to be considered. It was also assumed, that in the case if for at least one of demand the allocated traffic load in the network has value of 0, then the solution is not fair. Further, fairness of solutions will become greater when the results are most aligned with each other. In statistics, this is represented by the so-called inequality measures [16]. Such measures are variance, standard deviation and kurtosis for example. Nonlinear dependencies complicate the possibility of their direct use in implementation of the large-scale network optimization model but on the other hand they can be used in the simple way to evaluate a final result of the test method.
Consider the outcome vectors set U, that is the set of revenue vectors for all achievable utility allocations. The quality of obtained result when selecting the method can be assessed by the ratio defining the loss of total revenue gained from the method maximizing the revenue disregarding fairness issues. This ratio is called the price of fairness (POF) [17] and it is defined by formula:

$$POF(U) = \frac{\max(U) - fair(U)}{\max(U)} \,, \tag{3}$$

where: $POF(U)$ – price of fairness $\max(U)$ – optimal solution in pure objective function maximization case $fair(U)$ – fair solution.

2. Mathematical Models

The problem will be analyzed on sample data obtained from the library SNDlib [18]. Exactly, the topology of the Polish backbone network has been chosen. The complete graph with nodes arranged and labeled arcs is shown in Fig. 2.

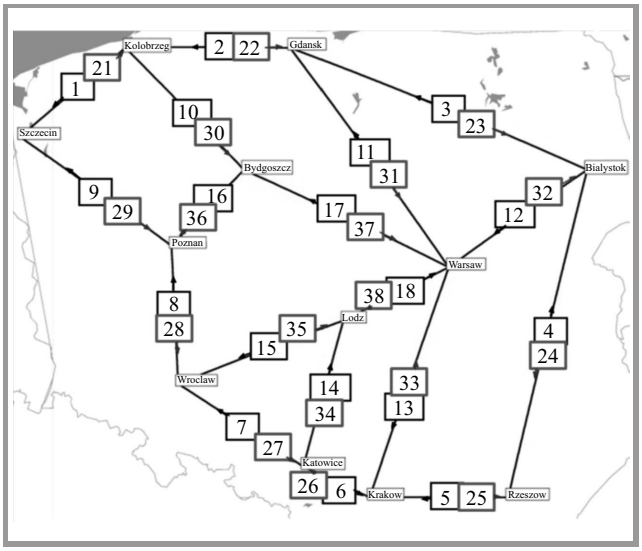


Fig. 2. Network topology of considered optimization problem.

Task of dimensioning is based on an allocation of the load on 10 pairs of source-destination demands. Pairs were selected in a way to represent a situation of overlapping paths to occur some links shared by them (Fig. 3). In order to ensure the possibility of paths bifurcation the network model is based in the node-link approach. This requires to represent the graph with an incidence matrix of vertices and arcs. Its coefficients are parameters a_{nl} and b_{nl}. For each

demand it was assigned the revenue value of the passage unit load by the demand. All of the values of variables are treat as integers. All the notations used in calculations are listed below:

- N – set of nodes (n_i – i-th node in network),
- L – set of arcs (l_i – i-th arc in network),
- P – vector of revenues per unit of capacity allocated on d-th demand (p_d – d-th demand unit revenue),
- D – set of demands between source-destination node pairs,
- C – vector of capacities of l-th arcs in the network (c_l – l-th arc's capacity),
- s_d – source assigned to d-th demand,
- e_d – destination assigned to d-th demand.

Auxiliary parameters are:

- d_{nl} – parameter having logical value which takes 1 in case of l-th arc comes out from n-th node and 0 in contrary case,
- b_{nl} – parameter having logical value which takes 1 in case of l-th arc comes into from n-th node and 0 in contrary case.

Used variables:

- h_d – allocated values of bandwidth on d-th demand between source and destination point,
- x_{ld} – value of bandwidth allocated on l-th arc used in d-th demand.

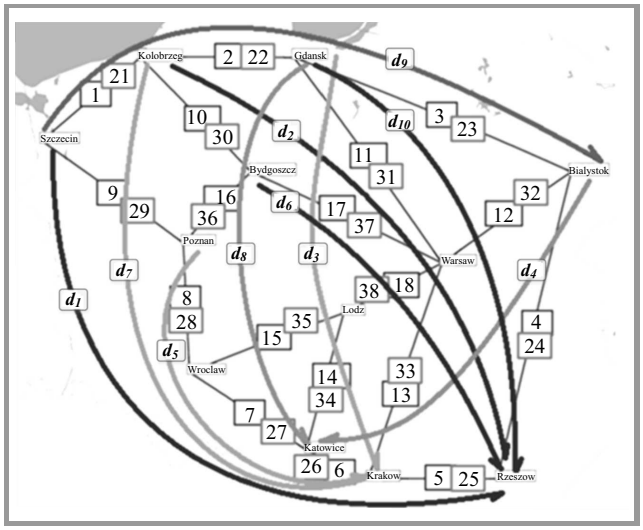


Fig. 3. Illustration of given demands of bandwidth allocation in assumed network topology.

Objective function:

$$\max \sum_{d \in D} h_d p_d \,, \tag{4}$$

subject to:

$$\sum_{l \in L} d_{sl} x_{ld} - \sum_{l \in L} b_{sl} x_{ld} = h_d, \quad \forall d \in D, s = s_d, \tag{5}$$

$$\sum_{l \in L} b_{el} x_{ld} - \sum_{l \in L} d_{el} x_{ld} = h_d, \quad \forall d \in D, e = e_d, \tag{6}$$

$$\sum_{l \in L} b_{nl} x_{ld} - \sum_{l \in L} d_{nl} x_{ld} = 0, \quad \forall d \in D, n \in N \setminus \{s_d, e_d\}, \tag{7}$$

$$\sum_{d \in D} x_{ld} \leq c_l, \quad \forall l \in L. \tag{8}$$

Equations above describe a basic node-link network model of the dimensioning problem. The main objective function (4) has been written for simple maximization problem of the total revenue. Next Eqs. (5) and (6) enforce equality of input and output throughout at each node. Limit of the maximum capacity of link is ensured by Eq. (8).
Cumulative model of the ordered weighted averages allows us to formulate the OWA optimization problem in a simple form of linear programming thus guaranteeing efficient computations. The method generates the equitable efficient solutions. Control parameters of the method are weights assigned to several achievement function values, which in each subsequent step of the optimization algorithm are ordered non-decreasing. Weights must be set among the input parameters methods in non-increasing order. Their number must be equal to the number of individual functions, which in this case refers to the amount of revenue from the allocation of a specific load value on the demand. Weighting the first significantly larger than any other impact on maximizing the value of the least attractive criterion function has been achieved. Assigning equal weights values determines solution comparable to the simple maximization of the total revenue, regardless of fairness. Taking advantages of Eq. (2), the OWA model can be written as the following linear program (LP):

$$\max \left(\sum_{i=1,\ldots,m} \overline{\omega}_k \eta_k \right), \tag{9}$$

where:

$$\eta_k = k t_k - \sum_{i=1}^{m} d_{ik} \,, \tag{10}$$

$$t_k - d_{ik} \leq f_i(x) \,, \tag{11}$$

$$d_{ik} \geq 0 \,, \tag{12}$$

$$\text{for } i,k = 1,\ldots,m \,.$$

The OWA method maximizes the sum of all ordered k-th lowest objective values with assigned weights (9).
The second analyzed method (RPM) uses the fuzzy intervals. The model takes into account in its design ranges of functions achievements that are most desired by the deci-

Table 1
Unit revenues for 11 data sets

d	ex1	ex2	ex3	ex4	ex5	ex6	ex7	ex8	ex9	ex10	ex11
1	200	200	80	50	110	70	200	120	60	50	100
2	50	50	110	120	70	80	70	70	140	120	140
3	150	150	110	140	130	60	10	130	100	130	100
4	100	50	70	140	110	110	80	110	60	50	70
5	60	60	120	50	70	200	140	50	60	200	200
6	200	200	120	90	60	120	50	80	100	120	140
7	50	200	50	80	200	110	100	120	200	100	70
8	150	70	50	200	100	90	90	200	100	70	70
9	100	100	120	50	50	50	300	100	70	130	100
10	60	60	140	50	100	200	50	120	50	80	200

sion maker, defined by their limits. The aspiration and the reservation levels (a_i and r_i). Using the features of fuzzy intervals allows assigning function values that do not necessarily belong to the predefined interval. It is solved by introducing additional factors responsible for the decrease (γ) "sorrow" and additional growth (β) "satisfaction" the decision-maker with the achieved value of the function, where $0 < \beta < 1 < \gamma$, see Eqs. (15), (16), and (17). Aspiration and reservation levels are the control parameters for this optimization method. In certain cases, these parameters can be given as the worst possible value and the best possible value, respectively. However, in most cases those control parameters are determined empirically on the basis of (or during) the problem analysis. The RPM model can be written as linear programming (LP) formulation:

$$\max \left(z + \varepsilon \sum_{i=1,\ldots,m} z_i \right), \tag{13}$$

subject to:

$$z \leq z_i\,, \tag{14}$$

$$z_i \leq \beta \frac{y_i - a_i}{a_i - r_i} + 1\,, \tag{15}$$

$$z_i \leq \frac{y_i - a_i}{a_i - r_i}\,, \tag{16}$$

$$z_i \leq \gamma \frac{y_i - a_i}{a_i - r_i}\,, \tag{17}$$

$$\text{for } i = 1 \ldots, m\,.$$

Value ε, used in Eq. (13), should be positive and less than 1. It defines how important for the decision-maker is additional improvement of the total revenue. Equation (14) allows variable z to get the minimum value from z_i for each $i = 1, \ldots, m$. This procedure uses in some part the max-min concept and guarantees the special treatment of the least attractive value in case of total system efficiency. It means how important for decision-maker is additional improvement of the solution.

3. Results

For implementations of the optimization models linear programming in the AMPL standard were used. The results were obtained using the GLPSOL solver and the GLPK as optimization package. The results are shown for eleven sets of income data, more precisely of given vector of revenues P. For each data set has been considered several cases of different control parameters, which affect problem solution from the equitable methods. The values of profit units were generated randomly for 10 demands for allocation of load between given pairs of vertices. They are presented in Table 1. It is expected that the most discriminated demand against the method of optimizing the total profit will be those for which the gain value assigned the least and share at least one arc to another demand. For example, given the first set of input data to the unequal treatment may occur for demand $d = 2$, 7, 5 and 10. Each of the eleven sets of input data were examined using three methods of optimization.

In the OWA method the values of weights are arranged in non-increasing order to guarantee the fairness properties. Each given weight refers to the successive value of the achievement function starting from the most "discrim-

Table 2
The OWA method control parameters (ω)

d	OWA(1)	OWA(2)	OWA(3)	OWA(4)	OWA(5)
1	10	10	10	10	10
2	10	1	10	10	9
3	10	1	10	10	8
4	10	1	10	10	7
5	10	1	10	1	6
6	9	1	10	1	5
7	1	1	10	1	4
8	10	1	10	1	3
9	10	1	10	1	2
10	9	1	10	1	1

Table 3
The RPM method control parameters (a, r)

d	RPM(1)		RPM(2)		RPM(3)		RPM(4)	
	a	r	a	r	a	r	a	r
1	6500	6000	11000	10000	11000	10000	6000	4000
2	6500	6000	11000	6000	11000	10000	6000	4000
3	6500	6000	11000	10000	11000	10000	6000	4000
4	6500	6000	11000	6000	11000	6000	6000	4000
5	6500	6000	11000	6000	11000	10000	6000	4000
6	6500	6000	11000	10000	11000	10000	6000	4000
7	6500	6000	11000	10000	11000	10000	6000	4000
8	6500	6000	11000	6000	11000	6000	6000	4000
9	6500	6000	11000	6000	11000	6000	6000	4000
10	6500	6000	11000	10000	11000	10000	6000	4000

Table 4
Solutions for the first group of input parameters

d	OWA(1)	OWA(2)	OWA(4)	OWA(5)	RPM(1)	RPM(2)	RPM(3)	RPM(4)
1	6400	5400	6600	20000	5400	9000	5400	5400
2	5050	5350	3700	1400	5350	550	5350	5350
3	6750	12600	6600	19950	9000	10050	10050	12600
4	12800	17600	15100	13500	15200	20000	15900	17600
5	6420	5340	6600	7140	6000	780	6360	5340
6	6400	5400	6600	20000	5400	9000	5400	5400
7	6400	5350	6300	1400	6000	10000	5350	5350
8	19800	12600	16350	18750	16200	9000	15150	12600
9	26800	27300	26700	20000	27300	25400	27300	27300
10	5100	5340	6600	1320	5340	8940	5340	5340
$\bar{x}$	10192	10228	10115	12346	10119	10272	10160	10228

inated". Table 2 summarizes considered OWA weighting schemes. For the RPM method such parameters are the limits of the range of values desired by the decision maker. Extremes of this range are the highest possible value and the worst possible values to achieve. Analyzed values of the control parameters are given in Table 3. For the first set of income parameters and input data the solutions are shown in details (Table 4 and Fig. 4). For the others configurations only basic statistics are presented.

As expected, methods maximizing the revenue unfairly, ignore demands, which are less attractive in case of this criterion. Those methods have returned solutions, which are unacceptable by the decision-maker taking into account the fairness criterion. Following Table 4, one can determine the values of loads of individual demands by dividing the objective functions by unit income from the given demand. Note that the values are relatively aligned with each other but the degree of fairness is fundamentally different. As mentioned, the results of Table 4 are also presented in the diagram (Fig. 4). On the horizontal axis mapped several solutions for the test methods. During the search for a solution one should be guided by the criterion of uniformity while simultaneously maximize the value of the total or average objective function. For some parameters, the OWA method returns a solution that assigns exactly the same load values as the RPM method. This is the case of situation where the value of the first weight stands out in relation to the remaining weights in the OWA method. Similar solution would be achieved when decision-maker has determined the appropriate low value of the bounds in the RPM algorithm as control parameters. These values are aiming to solve the max-min model, whose priority is to maximize the smallest value at first and then increase a total value of decision variables as much as possible. For non-zero value for the first weight and zero values for weights remaining, the OWA method returns a solution comparable to max-min solution. The OWA result in the fourth and fifth case can be considered as fair in some degree. This result is achieved for the distribution of weights where the first four are significantly larger while at the same time remaining values are lower – OWA(4). Slightly more efficient and fair solution is for linear decreasing weights – OWA(5).

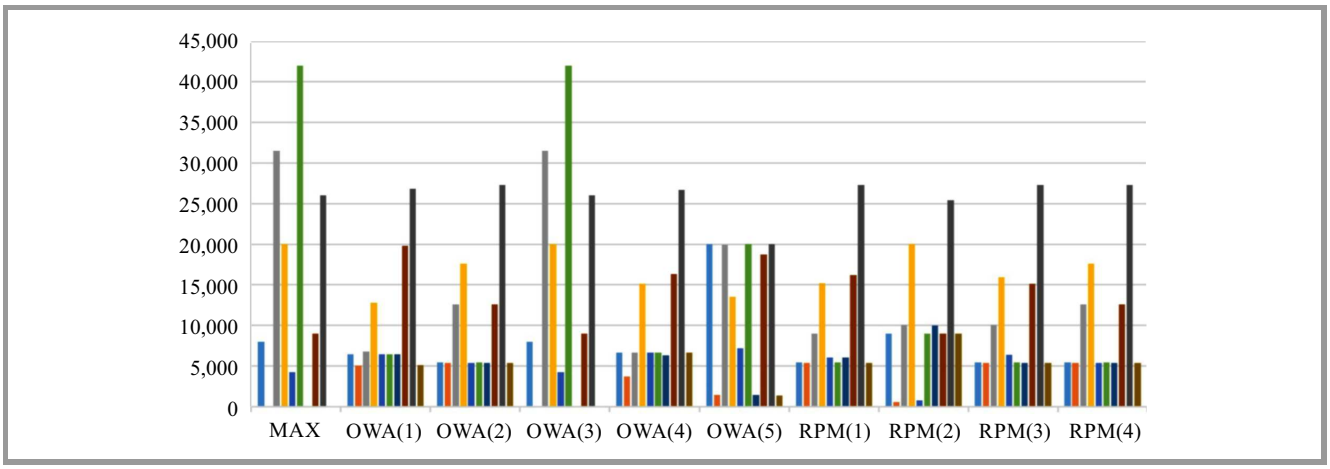


Fig. 4. Comparison of fair-optimization methods for the first set of income parameters. (See color pictures online at www.nit.eu/publications/journal-jtit)

Table 5
Calculated statistics for solutions obtained with several methods

Measure	MAX	OWA(1)	OWA(2)	OWA(3)	OWA(4)	OWA(5)	RPM(1)	RPM(2)	RPM(3)	RPM(4)
POF	0	0.2	0.19	0	0.22	0.18	0.24	0.28	0.27	0.23
$\bar{h}_d$	13758	10906	11032	13758	10643	11202	10362	9791	9921	10511
K	1.054	4.060	3.318	1.054	4.5053	2.431	3.4184	2.1772	4.552	3.874
σ	18730	9695	10333	18730	8580	8008	9014	7946	7606	9633
ϕ	0	20025	21690	0	12574	10854	23189	4079	21061	23343

The first index of quality of the analyzed methods is the price of fairness. Calculations were determined for the mean revenue value of each of eleven designing cases and described methods. Factor POF may, however, be interpreted in an ambiguous way. It does not include the value of their information on the degree of fairness of investigated method. For example, the best values of POF corresponds to MAX and OWA(3) cases which are completely unfair. It is difficult to say whether the method having the lower POF ratio is also less fair. Of course, the goal in designing efficient and fair method is to obtain the smallest possible values of POF. This index is inversely proportional to fairness and does not give any information about equity of objective functions values.

Another considered statistic is kurtosis. This measure is built on the fourth standardized moment of probability distribution and it takes a greater value, when more of the observations are placed around the mean value. This measure takes value 0 for the normal distribution. In addition, values of kurtosis close to 0 indicate the normal distribution of data sample. It follows that the decision-maker is interested in greater values of kurtosis. The analysis shows that for solutions of the pure maximizing model, kurtosis takes negative values. This affects the negative judgment in terms of fairness because it means that values of allocated loads are not uniform in high degree.

The basic statistic should also be a standard deviation which values have been calculated. This measure also determines the degree of distribution concentration, but it is less sensitive to the value of more deviating from the mean. This is because it is built on the second standardized central moment of probability distribution.

The above-mentioned basic statistics relating to the result set does not contain, however, the base fairness property. It is the assumption that the result of taking a value of 0 for at least one of the requirements should be defined as unfair. To challenge this own rate was introduced to determine the level of solutions fairness (19). It is the square root of the product of the minimum value, and the kurtosis of the sample. The higher the value, the method has higher qualities of fairness.

$$\phi = \min_{d \in D} \sqrt{h_d \cdot K} \tag{18}$$

Table 5 presents the mean values of described statistics gained from all the considered methods and each set of given control parameters from Table 1. In summary, the analysis of two selected fairness optimization methods cannot clearly point out which method is better. The OWA method is more intuitive and does not require knowledge of the achievements of the expected objective function. For properly selected weights, the decision-maker can get a solution with varying degrees of fairness. The value of the new-designed coefficient established to determine the degree of fairness of methods, which is averaged over 11 considered cases, speaks in favor of the reference point method. On the other hand, the POF index is clearly lower for the OWA method. Moreover, the OWA method allows the

decision-maker to obtain the suitable solution by assigning the control parameters – weights. In comparison to the reference point method, the OWA method can be controlled in a more friendly and intuitive way. For positive and decreasing weights, the OWA method allows to achieve result meeting high requirements for the criterion of fairness, and maximizing the load accumulated on paths. For equal weights in the OWA method, there is obtained solution identical to the simple maximization method. It can be simple used to determine the POF, which is one way to define quality of obtained solutions.

References

[1] W. Ogryczak and A. Wierzbicki, "On multi-criteria approaches to bandwidth allocation", *Control and Cybernet.*, vol. 33, pp. 427–448, 2004.

[2] W. Ogryczak, M. Pióro, and A. Tomaszewski, "Telecommunications network design and max-min optimization problem", *J. Telecommun. and Inform. Technol.*, no. 3, pp. 43–56, 2005.

[3] T. Ibarakiand and N. Katoh, *Resource Allocation Problems, Algorithmic Approaches*. Cambridge: MIT Press, 1988.

[4] M. Pióro and D. Medhi, *Routing, Flow and Capacity Design in Communication and Computer Networks*. San Francisco: Morgan Kaufmann, 2004.

[5] R. Denda, A. Banchs, and W. Effelsberg, "The fairness challenge in computer networks", in *QofIS 2000*, J. Crowcroft, J. Roberts, and M. Smirnov, Eds. *LNCS*, vol. 1922, pp. 208–220. Springer, 2000.

[6] J. Rawls and E. Kelly, *Justice as Fairness: A Restatement*. Cambridge: Harvard Univ. Press, 2001.

[7] W. Ogryczak, H. Luss, M. Pióro, D. Nace, and A. Tomaszewski, "Fair optimization and networks: A survey", *J. Appl. Mathem.*, vol. 2014, pp. 1–25, 2014 (doi: 10.1155/2014/612018).

[8] W. Ogryczak, "Fair optimization – methodological foundations of fairness in network resource allocation", in *Proc. IEEE 38th Ann. Int. Comp. Softw. & Appl. Conf. COMPSAC 2014*, Västerås, Sweden, 2014, pp. 43–48.

[9] H. Luss, "On equitable resource allocation problems: A lexicographic minimax approach", *Operation Research*, vol. 47, no. 3, pp. 361–378, 1999.

[10] J. Kleinberg, Y. Rabani, and E. Tardos, "Fairness in routing and load balancing", *J. Comput. Syst. Sci.*, vol. 63, no. 1, pp. 2–21, 2001.

[11] F. Kelly, A. Maulloo, and D. Tan, "Rate control for communication networks: shadow prices, proportional fairness and stability", *J. Oper. Res. Soc.*, vol. 49, no. 3, pp. 206–217, 1997.

[12] R. R. Yager, "On ordered weighted averaging aggregation operators in multicriteria decision making", *IEEE Trans. Sys., Man and Cyber.*, vol. 18, no. 1, pp. 183–190, 1988.

[13] R. R. Yager, J. Kacprzyk, and G. Beliakov, *Recent Developments in the Ordered Weighted Averaging Operators: Theory and Practice*. Springer, 2011.

[14] W. Ogryczak and B. Kozłowski, "Reference point method with importance weighted ordered partial achievements", *TOP*, vol. 19, no. 2, pp. 380–401, 2011.

[15] W. Ogryczak and A. Tamir, "Minimizing the sum of the k-largest functions in linear time", *Inform. Process. Lett.*, vol. 85, no. 3, pp. 117–122, 2003.

[16] M. Rothschild and J. E. Stiglitz, "Some further results in the measurement of inequality", *J. Economic Theory*, vol. 6, no. 2, pp. 188–204, 1973.

[17] D. Bertsimas, V. F. Farias, and N. Trichakis, "The price of fairness", *Operations Research*, vol. 59, pp. 17–31, 2011.

[18] S. Orłowski, R. Wessaly, M. Pióro, and A. Tomaszewski, "SNDlib 1.0 – survivable network design library", *Networks*, vol. 55, no. 3, pp. 276–286, 2009.

Grzegorz Zalewski works as specialist in Institute of Telecommunications in Warsaw in Advanced Informations Technologies Department. He got M.Sc. at Faculty of Transport of Warsaw University of Technology in 2005. He completed postgraduate studies of Programming Architecture and Engineering at Military University of Technology in 2014. At 2015 he began doctoral studies at Warsaw University of Technology at Faculty of Electronics and Information Technology in Warsaw in the domain of networks optimization models. Exactly he is interested in deploying fair methods in networks dimensioning.
E-mail: G.Zalewski@itl.waw.pl
National Institute of Telecommunications
Szachowa st 1
04-894 Warsaw, Poland

Włodzimierz Ogryczak is Professor of Computer Science and Director of the Institute of Control and Computation Engineering at the Warsaw University of Technology, Poland. He received both his M.Sc. (1973) and Ph.D. (1983) in Mathematics from Warsaw University, and D.Sc. (1997) in Computer Science from Polish Academy of Sciences. His research interests are focused on models, computer solutions and interdisciplinary applications in the area of optimization and decision making with the main stress on: multiple criteria optimization and decision support, decision making under risk, location and distribution problems. He has published four books and numerous research articles in international journals.
E-mail: wogrycza@ia.pw.edu.pl
Institute of Control and Computation Engineering
Warsaw University of Technology
Nowowiejska st 15/19
00-665 Warsaw, Poland

Paper

A Practical Approach to Traffic Engineering using an Unsplittable Multicommodity Flow Problem with QoS Constraints

Paweł Białoń

Department of Advanced Information Systems, National Institute of Telecommunications, Warsaw, Poland

Abstract—The paper presents a practical approach to calculating intra-domain paths within a domain of a content-aware network (CAN) that uses source routing. This approach was used in the prototype CAN constructed as a part of the Future Internet Engineering project outcome. The calculated paths must satisfy demands for capacity (capacity for a single connection and for aggregate connections using the given path are considered distinctly) and for a number of path-additive measures like delay, loss ratio. We state a suitable variant of QoS-aware unsplittable multicommodity flow problem and present the solving algorithm. The algorithm answers to the needs of its immediate application in the constructed system: a quick return within a short and fairly predictable time, simplicity and modifiability, good behavior in the absence of a feasible solution (returning approximately-feasible solutions, showing how to modify demands to retain feasibility). On the other hand, a certain level of overdimensioning of the network is explored, unlike in a typical optimization algorithm. The algorithm is a mixture of: (i) shortest path techniques, (ii) simplified reference-level multicriteria techniques and parametric analysis applied to aggregate the QoS criteria (iii) penalty and mutation techniques to handle the common constraints. Numerical experiments assessing various aspects of the algorithm behavior are given.

Keywords—multicriteria analysis, QoS-aware unsplittable multicommodity flow, traffic engineering.

1. Introduction

A practical approach to traffic engineering in a domain of the Content-Aware Network (CAN) with source routing is presented. The CAN network was a prototype built within the framework of the Future Internet Engineering project [1]. The project aimed at the construction of an architecture allowing a coexistence of various network techniques IP, circuit switching and post-IP, like CAN) on top of a common, virtualized equipment. A traffic engineering module computing content delivery paths satisfying Quality of Service (QoS) requirements within a CAN domain was necessary. Its construction was an interesting challenge, since the module had to be a part of an operational management system, thus it had specific demands, not usually satisfied by the existing relevant optimization algorithms. First, the module had to give any, perhaps by far non-optimal result within the time acceptable by the CAN administrator. On the other hand, a fair level of the network overdimensioning could be assumed, which is the usual case. Also, the constructed module and algorithm should have been easily expandable to encompass changes in the traffic engineering problem statement caused by a rapid development of the prototype.

Represent our network as directed graph (V,E) where $V \in \mathbb{N}$ is the set of nodes (identified with natural numbers) and $E \in \mathbb{N} \times \mathbb{N}$ is the set of arcs. Let $n = |V|$, $m = |E|$. The considered problem is then a variation of the unsplittable multicommodity flow problem with QoS constraints where commodities are defined by pairs: (relation, QoS class) with relation being a pair of different nodes: source and destination. We shall also discuss the possible extension of the problem with the constraints on maximum Protocol Data Units (PDUs) processed in a node within a second. Precisely, the problem is stripped a goal function, and is a feasibility problem rather than an optimization problem.

A commodity must be sent through a single path, due to the construction of the control plane. We avoid excess of the capacities of links. Also, the vector of $L \geq 1$ segment-additive measures of paths, like delay, error rate (when small), loss ratio, should not exceed the vector of demands connected with the given QoS class. The delay, loss ratio, or other additive measure for a given link may differ for different classes of services (CoS), which is determined by the queuing disciplines applied in the system.

1.1. Related Work

The problem of finding a path in a graph subject to multiple additive constraints, the multi-constrained path problem, is already NP-hard [2]. Thus, the same should be expected from our problem, containing that one. Actually, similar problems to ours cause a trouble to researches and their hardness (and their reluctance to distributed solving) ceases the proliferation of QoS technologies. Solving techniques for such problems traditionally use various polynomial-time approximations of them. Such approximations seem, however, aimed at obtaining a solution too precise for our needs at the expense of a too large solving time.

For example, in [3], a QoS-aware transportation planning problem (with a goal function representing the operator's

profit and with client demands elastic to the obtained QoS measures) is reduced to a fractional packing problem and treated using the Lagrangian relaxation technique of [4]. The authors obtain a $(1-\varepsilon)^{-2}(1+\varepsilon)^2$ – approximate solution within a $\mathcal{O}((\frac{1}{\varepsilon})^3(m+k)\log(m+k)mn^2\cdot(\frac{1}{\varepsilon})\log(m+k)+\log(nU))$ time, with U being the maximal ratio of link capacities. A more heuristic approach is presented in [5], for a delay-constrained routing problem, thus with $L=1$ but where a link delay can be a quite arbitrary function of the link traffic (we, in turn, assume this function constant). The main trick there was relaxing the ugly, non-convex delay constraints with the augmented lagrangian, the resulting subproblems were still non-convex but locally convex and could be approximately solved with local optimization techniques. This approach remains quite expensive in requiring optimization (mathematical programming) techniques while yielding only an approximate, local solution of a non-convex problem.

The complex problem of QoS multicommodity routing has been also treated with genetic algorithms. An interesting example is contained in [6], where the chromosomes encode some internal flows. The author tries to preserve the feasibility of chromosomes over the iterations. Genetic algorithms are not very sensitive to the choice of starting point but suffer from a too quick convergence that yields a solution far from the optimum. Therefore, the authors of [7] try to augment the genetic algorithm for a QoS multicast routing problem with a tabu-search technique, that has the opposite character: converges longer but depends of the starting point choice. In neither of the papers, however, very much can be precisely said about the solution quality and time, moreover, the experiments in [6] show an unsmooth, jumpy dependence of the solution time of problem sizes, while a predictable dependence is needed for our application.

An alternative to solving a QoS-constrained multicommodity problems is to allocate routing paths separately, i.e. solve a series of multi-constrained path (or: shortest path) problems that are, however, augmented to take care about leaving sufficient free link capacities for other paths. In the simple Widest-Shortest Path (WSP) approach [8], one picks the widest path between the shortest (simply in terms of hops number) paths from the origin to the destination in the subgraph built of links with capacities not less than the commodity demand. The symmetric Shortest-Widest Path approach is described in [9].

More sophisticated approaches involve more complex measures of bottlenecking potential of a path and rerouting, i.e. a recalculation of some paths if several paths coming through a link form a bottleneck – see [10]. Regarding routing a single QoS-constraints path (finding a multiconstraint path), which is an NP-hard problem, as said, and the solution methods are usually extensions of the Dijkstra shortest path method, which turn out to be variants of the Branch and Bound methods. They contain various accelerations, like fast closing trees (resulting in an approximate solution but of a controlled accuracy), or quite arbitrary reduction of the search space without a full control of the solution quality (TAMCRA, SAMCRA) – see [11], [12].

1.2. Proposed Approach

We propose a quick, rather rough yet effective heuristics, based on a consecutive allocating of paths for particular commodities (cf. Fig. 1). In this, we mimic a hypothetical manual traffic engineering. This is followed by a path rerouting phase, in case of the excess of the link capacities. In practice, however, this excess turns out to be marginal and the rerouting phase is short or even absent. This is important, because, in general, rerouting is a greedy operation, and it is difficult to design a rerouting-based algorithm of a provable low complexity. The path for the given commodity is generated as a shortest path in the appropriate source-sink relation with the link costs in the network graph defined as linear combinations of the link characteristics (delay, jitter, etc.) and also of some penalties for the current excess of the capacity of the link. The weights in the linear combination are, however, varied in a parametric experiment. Consequently, for a relation, many candidate paths are obtained.

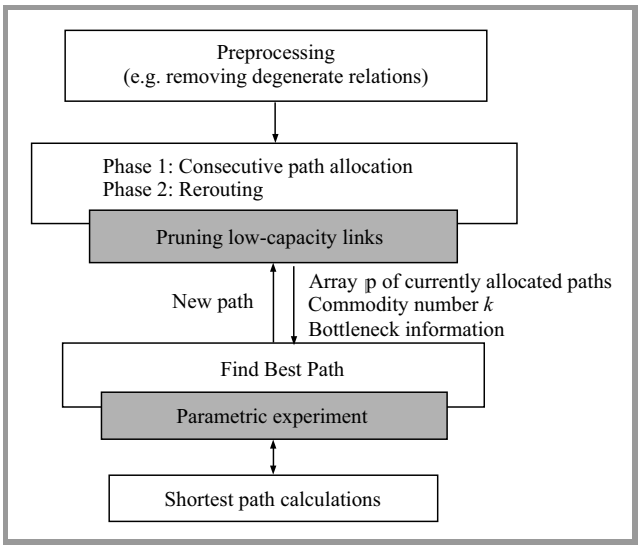


Fig. 1. Structure of the solving method.

The choice of the final path for the relation can be formed very elastically and may reflect various user preferences about the compromise between the particular QoS characteristics of the best path and also may take into account various potential heuristics to avoid link capacity excess in the further iterations of the algorithm. We have decided to use multicriteria technique (reference-level based [13]) to choose the best path. The overall simple and minimalist construction of the method allows its easy augmentation to follow even severe modifications to the solved problem. In developing new network techniques, the requirements from the traffic engineering module change very often. The price paid for the elasticity of our method is performing parametric experiments, which exhaustively search the space of weights. However, since the number of QoS characteristics

is usually low, the running time of the parametric experiments may be still moderate.

Our approach shares a relative computational simplicity with heuristics like SWP that allocate a path for the consecutive commodities and leaves room for other paths. Unlike these heuristics, it can be, however, considered a fully fledged method for solving a QoS-aware MCF problem, which looks at the whole set of commodities. Firstly, this is because of the existence of rerouting phase and secondly, because of the resolving of capacity conflicts of paths, which happens during the parametric experiments. In particular, the weights with which the bottlenecks contribute to the link weights when calculating the shortest path varies in the parametric experiment, unlike in [10], where it is fixed. Our approach is certainly a heuristics, but is computationally lighter than approaches like [4], [5] and has a highly predictable computation time. In addition, in Section 5 and in Appendix A we are able to show some partial possibilities of accessing the quality of obtained solution – in terms of the obtained additive path characteristics.

1.3. Mathematical Notation

We shall use the set membership operator $\in$ also to denote the presence of en element in a sequence. We shall have $\mathbb{R}_+ = [0,\infty)$, $\mathbb{R}_- = (-\infty,0]$, $\mathbb{N} = \{0,1,\ldots\}$, for $p \in \mathbb{R}^n$, $Y \subseteq \mathbb{R}^n$ $p+Y = \{p+y\colon y \in Y\}$, denote the convex hull of a set $A \in \mathbb{R}^n$ – by $\mathrm{conv}(A)$. A $C \in \mathbb{R}^n$ is a *cone* if $\forall c \in C$, $a > 0\, ac \in C$. We shall identify tuples of numbers (elements of $\mathbb{R}^n$) with column vectors.

2. Problem Origin

One of the Parallel Internets running simultaneously in the IIP system is the CAN network [14]. It uses its own transmission protocols in its interior, however, the users and the content storing servers connect to the network via TCP/IP access networks.

In the CAN, a user requests for a particular content (e.g. a video file), the network finds a server on which the content is stored and the content is transferred to the user via a constant (during the connection time) path between the access nodes controlling two access networks: that of the user and that of the content server. The transmission uses source routing, where the definition of the transmission path is stored in the frame header by the emitting node. By routing we mean the calculation of the paths.

The CAN network is divided into domains (Autonomous Systems, ASes). The connection path is set-up upon the connection request, by assembling intra-domain fragments of such paths (shortly: intra-domain paths), that are precalculated in each domain separately, for various possible external relations of the domain. The precalculation of intra-domain paths in the domain (called intra-domain routing) is the main subject of this paper and involves solving a mathematical programming problem.

Hence, in a domain (cf. Fig. 2), we need to compute paths for various CoS and various relations.

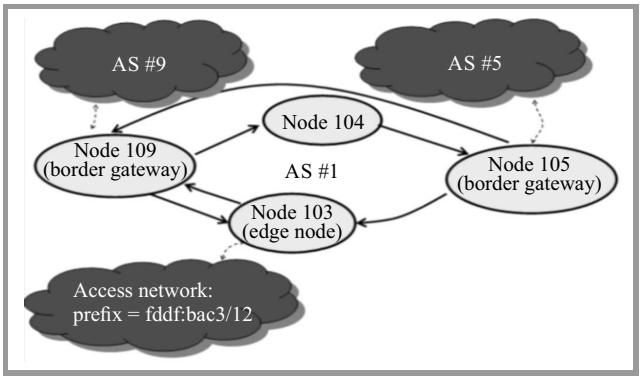


Fig. 2. An exemplary Parallel Internet CAN domain (AS) with $V = \{103,104,105,109\}$, $E = \{(103,109), (109,103), (104,105), (105,103), (109,104), (105,109)\}$, three external elements: two adjacent domains and one access network.

A relation is a pair of elements external to the domain (an external element is either an access network or an adjacent domain/AS, each external element has a unique controlling node in the domain – either a border gateway or an edge node, respectively). QoS demands for the intra-domain paths are given by the administrator for each relation.

3. Problem Statement

We shall sometimes identify network objects with their mathematical descriptions, e.g. identify nodes with their numbers. Our network is a directed graph $G = (V,E)$, where $V \subset \mathbb{N}$ is the nonempty set of nodes, $E \subseteq V \times V$ is the nonempty set of links. We use $n = |V|$, $m = |E|$.

We have the nonempty set $C \subseteq \mathbb{N}$ of classes of services and the number $L \geq 1$ of additive link/path characteristics like delay, loss ratio, etc.

Each link $e \in E$ has the associated capacity $\omega_e > 0$ and characteristics $\chi_{c,e,l} > 0$ for $c \in C$, $i \in \{1,\ldots,L\}$. These characteristics depend on the traffic but this dependence can be suppressed by taking values for some assumed maximum traffic. In traffic engineering we cannot control the actual future traffic intensities (we only calculate them using traffic demands estimates), thus cannot guarantee the values of the characteristics being functions of the traffic.

Note that the characteristics are indexed with a class of service, since different queue disciplines are set for different CoS, while the link capacities are common for all the CoS and it is the algorithm role to split the capacities between particular paths (thus between particular CoS).

We have the nonempty set $\{1,\ldots,K\}$ of commodities, actually describing relation-CoS pairs. For $k \in 1,\ldots,K$ let $\mathrm{start}(k)$ and $\mathrm{end}(k)$ be the be the source node and sink node for the commodity transfer, respectively, $c(k)$ be the class of service of the commodity. We assume $\mathrm{start}(k) \neq \mathrm{end}(k)$ holds[1]. There may be several commodities with the same

[1] Actually, relations between external elements controlled by the same node are possible. However, we can remove them from the considerations, since such relations yield degenerate, 0-link intra-domain paths.

start$(\cdot)$, end$(\cdot)$ and $c(\cdot)$, since they may refer to various relations with the same source and sink nodes (several external elements, i.e. adjacent domains or access networks can be controlled by the same node). Various relations can serve various subsets of classes of services, so the number of commodities may be lower than $|C|$ times the number of relations.
The following demands are defined by the administrator:

1. $\underline{\phi}_k > 0$ for $k = 1,\ldots,K$ – the QoS-required capacity of a path necessary for realizing a single connection for demand k;
2. ϕ_k (satisfying $\phi_k \geq \underline{\phi}_k$) for $k = 1,\ldots,K$ – the aggregated traffic (often referred as "traffic") from many simultaneous connections for commodity k. We use a static, deterministic model of traffic aggregation;
3. $\check{\chi}_{k,l} > 0$ for $k = 1,\ldots,K$, $l = 1,\ldots,L$ – maximum allowed values of the additive characteristics (delay, etc.) for the calculated intra-domain path for commodity k. The administrator sets these values bearing in mind the QoS requirements for the same characteristics for all the client-server paths, crossing several domains.

By a path p we shall mean a nonzero-element sequence $(p_1, p_2, \ldots p_q)$ of different numbers from V such that for all $i \in \{1,\ldots,q-1\}$ $(p_i, p_{i+1}) \in E$. For such a p for $e \in E$, we shall write $e \,\mathrm{on}\, p$ if $\exists k\ 1 \leq k < q$; $e = (p_j, pj+1)$, and $\mathrm{start}(p) = p_1$, $\mathrm{end}(p) = p_q$.
For commodity $k \in \{1,\ldots,K\}$, P^k will denote the set of possible paths for transferring the commodity k, i.e. such acyclic paths p that $\mathrm{start}(p) = \mathrm{start}(k)$, $\mathrm{end}(p) = \mathrm{end}(k)$.
The problem variables are $\mathbb{p}_i \in P^i$ for $i = 1,\ldots K$; $\mathbb{p}$ represents the intra-domain path for commodity i. We also use the vector notations: $\mathbb{p} = (\mathbb{p}_1,\ldots \mathbb{p}_K)$, $\phi = (\phi_1,\ldots,\phi_K)$. Variable $\mathbb{p}$ will be also the solving algorithm iterate. Let us define some functions:

1. $\phi_e(\mathbb{p},\phi) = \sum_{\substack{k=1,\ldots,K:\\ e \,\mathrm{on}\, \mathbb{p}^k}} \phi_k$
   for $e \in E$ – the total flow in link e;
2. $\chi_k(p) : P^k \mapsto \mathbb{R}^L$; $(\chi_k(p))_l = \sum_{e \in q} \chi_{c(k),e,l}$
   for $l = 1,\ldots L$ – vector of the additive characteristics of a potential path p for commodity k.

Our problem is defined as follows:

$$\text{Find } \mathbb{p} \in \{P^1,\ldots,P^K\} \tag{1}$$
satisfying
$$\underline{\phi}_k \leq \omega_e \text{ for } e \text{ on } \mathbb{p}_k,\ k = 1,\ldots,K \text{ (satisfaction of the QoS single connection capacity demand)} \tag{2}$$
$$\phi_e(\mathbb{p},\phi) \leq \omega_e \text{ for } e \in E \text{ (flow constraints of links)} \tag{3}$$
$$\big(\chi_k(\mathbb{p})\big)_l \leq \check{\chi}_{k,l} \text{ for } p \in P^k,\ k = 1,\ldots,K,\ l = 1,\ldots,L \text{ (additive QoS characteristics demands for paths).} \tag{4}$$

Additionally, we understand constraints (2) as hard (inviolable) since their violation would immediately violate some QoS demands of the assembled connection paths. Conversely, the remaining constraints are soft and could be possibly slightly violated if the algorithm cannot find a feasible solution. This setting is substantiated with the fact that these constrains anyway work with imprecise data: (3) – with the estimated traffic demands ϕ and (4) – with demands $\check{\chi}_{k,l}$, which are a kind of a quotas of some true QoS demands for a connection path assigned to the domain by an arbitrary decision of the administrator. They represent the maximum allowed contribution of the intra-domain path of our domain into the additive characteristics of the whole connection path.
Two modifications of the problem are considered:

Modification 1. We add the following constraints:

$$\mathbb{p}^i = \mathbb{p}^j \text{ for } (i,j) \in \{1,\ldots,K\} : \mathrm{start}(i) = \\ = \mathrm{start}(j) \wedge \mathrm{end}(i) = \mathrm{end}(j) \wedge c(i) = c(j). \tag{5}$$

In this way we require that paths for commodities with identical class of service, source and sink node should be transferred with the same path. This modification arose due to the limitations of the control plane in CAN, which distinguishes relations by pairs of source-sink nodes. Commodities coming from (or to) different domain external elements (access networks, neighboring domains) controlled by the same node and representing the same CoS cannot be properly distinguished.

Modification 2. We add the following constraints:

$$\varkappa_{c(k)} \sum_{\substack{K=1,\ldots,K:\\ e=(i,v),\\ e \,\mathrm{on}\, \mathbb{p}_k}} \phi_k + \varkappa_{c(k)} \sum_{\substack{k \in 1,\ldots,K:\\ \mathrm{start}(k) = v}} \phi_k \leq \xi_v \text{ for } v \in V, \tag{6}$$

where a parameter ξ_v denotes the Protocol Data Unit per second (PDU/s) throughput of node v, and a parameter $\varkappa_c$ denotes the size of a class c PDU, expressed in the used units of link capacity multiplied by one second. This modification expresses the limitations of the number of PDUs incoming in a second that the nodes can process.

4. Multicriteria Assessment Technique

Inside the algorithm, we shall assess some potential paths by several criteria that express the satisfaction of particular QoS demands, thus need a multicriteria assessment technique. Suppose we assess elements of set X with a vector quality function $Q : X \mapsto R^k$, where the higher $Q_i(\cdot)$, the better the satisfaction of the i-th criterion ($i = 1,\ldots, k$). Further assessments and comparisons of elements of X can be reduced to assessing and comparing the values of Q for them – points in the *space of attainable criteria* $Y = Q(X) \subseteq \mathbb{R}^k$.

Definition 1. For $y^1, y^2 \in \mathbb{R}^k$, y^1 *dominates* y^2 (in the Pareto sense), i.e. $(y^1 \succ y^2)$ if $\exists i \in \{1,\ldots,k\}\ y^1_i > y^2_i \wedge \forall j \in \{1,\ldots, k\} y^1_i > y^2)$.

Pareto dominance $\succ$ seems the only apparent comparison of points in Y but is only a partial order. A linear order can be obtained by scalarizing, i.e. comparing values of scalarizing function $S(q): Y \mapsto \mathbb{R}$ of point in Y. We will simplify the reference-level technique [13] and set $S = S^{\text{ref}} = S^{\text{ref}}_{\check{y},\bar{y}}$ where

$$S^{\text{ref}}_{\check{y},\bar{y}}(y) = \min_{i=1,\ldots m}(y_i - \check{y}_i)/(\bar{y}_i - \check{y}_i), \tag{7}$$

where we have the following *reference levels*: *reservation levels* $\check{y}_i$ for particular criteria (the values below that the relevant criteria should not deteriorate) and *aspiration levels* $\bar{y}_i > \check{y}_i$, here used for scaling purposes[2] ($i = 1,\ldots k$). S^{ref} is consistent with the Pareto dominance in the sense that if $a \succ b$ then $S(a) \geq S(b)$). This is also the property of *weighted summings*, more frequently used as scalarizing functions. Unlike with weighted summings, however, always all Pareto-nondominated (Pareto-optimal) elements of Y can be obtained as maximizers of $S^{\text{ref}}_{\check{y},\bar{y}}$ by a suitable choice of numbers $\check{y}_i$, $\bar{y}_i$ (assumed that the maximizers are unique for all choices of $\bar{y}_i$, $\check{y}_i$, which holds under the following regularity condition: $\forall q^1, q^2 \in Y \forall i \in \{1,\ldots,k\}\ q^1_i \neq q^2_i$, easily achievable for finite sets X by a suitable small random perturbation of Q). With $S^{\text{ref}}_{\check{y},\bar{y}}$ we have also a clear indication that all the criteria values y_i for some point in X (e.g. of a path) do not deteriorate below their reference levels ($\approx$ a path satisfies all the QoS constraints): $S^{\text{ref}}_{\check{y},\bar{y}}(y) \geq 0$.

Example 1. Let a path x be assessed by its bandwidth $\texttt{bandwidth}(x)$ and delay $\texttt{delay}(x)$. In our formalism, reasonably $y = (y_1, y_2) = \mathcal{Q}(x) = (\texttt{bandwidth(x)}, -\texttt{delay}(x))$, so both the outcomes y_1 and y_2 are maximized (the greater – the better). Let us have paths x_A, x_B, x_C with respective vectors of outcomes $y^A = (100, -3), y^B = (200, -2), y^C = (200, -1)$ – in some common units. Then

(i) $y^B \succ y^A$, since y^A is higher than y^B on all its coordinates,

(ii) y^A and y^C are not comparable in with Pareto order $\succ$: neither $y^A \succ y^B$ nor $y^B \succ y^A$.

Let us set reservation levels $\check{y} = (150, -4)$ and aspiration levels $\bar{y} = (400, -1)$. Then

(i) $S^{\text{ref}}_{\check{y},\bar{y}}(y^B) = \min((200-150)/(400-150), (-2--4)/(-1--4)) = 1/5$,

(ii) $S^{\text{ref}}_{\check{y},\bar{y}}(y^A) = \min((100-150)/(400-150), (-3--4)/(-1--4)) = -1/5$ and is negative, since the first coordinate of y^A is worse than its reservation level 150.

Note that since $y^B \succ y^A$, we have $S^{\text{ref}}_{\check{y},\bar{y}}(y^B) \geq S^{\text{ref}}_{\check{y},\bar{y}}(y^A)$.

[2]Particular criteria can have various typical values, be expressed in different units, thus should be made comparable. Note in (7), the i-th term in min (representing the satisfaction from fulfilling criterion i by y) becomes 0 when y_i is at its reservation level $\check{y}_i$ and 1 when y_i is at its aspiration level. Thus, in a sense, criterion i is normalized with $(\bar{y}_i - \check{y}_i)$ – cf. [13].

5. Solving Algorithm

5.1. Algorithm Statement

The main algorithm iterate will be $\mathbb{p} = (\mathbb{p}_1 1, \ldots, \mathbb{p}_K)$, where $p^i \in P^k$ for $i = 1,\ldots,K$; $\mathbb{p}$ is initially set to (NIL, NIL,…,NIL) and changed during the algorithm run.
Let us define some additional functions:

1. $\rho_e(\mathbb{p}, \phi)$ for $e \in E$ is the excess of the capacity of link e by the joint flows in the paths in $\mathbb{p}$ (in the few following definitions we shall assume path flows as given by ϕ) ; $\rho_e(\mathbb{p}) = \max\left(\left(\sum_{e \text{ on } \mathbb{p}^k, k=1,\ldots,K} \phi_k\right) - \omega_e, 0\right)$; we assume that no link belongs to a path being a NIL.

2. $\rho(\mathbb{p}) = \sum_{e \in E'} \rho_e(\mathbb{p})$ – the summary excess of the links capacity.

3. $\rho^-(k, \mathbb{p})$ where $k \in \{1,\ldots,K\}$, while we assume $p_k \neq \text{NIL}$ – is the measure of the contribution of the path $\mathbb{p}_k$ in the $\rho(\mathbb{p})$. We have $\rho^-(k,\mathbb{p}) = \rho(\mathbb{p}) - \rho((\mathbb{p}_1,\ldots,\mathbb{p}_{k-1},\text{NIL},\mathbb{p}_{k+1},\ldots,\mathbb{p}_K))$. Thus $\rho^-(k,\mathbb{p})$ is the decrease in $\rho(\mathbb{p})$ we would get by making $\mathbb{p}_k$ NIL by removing path $\mathbb{p}_k$ from the vector $\mathbb{p}$ of currently constructed paths.

4. $\rho^+(p,k,\mathbb{p})$ where $p \in P^k$, $k \in \{1,\ldots,K\}$, while we assume $p_k = \text{NIL}$ – is the measure of the potential of path p to increase the summary link capacity excess by storing p at the k-th position in $\mathbb{p}$. We have $\rho^+(p, k, \mathbb{p}) = \rho((\mathbb{p}_1,\ldots,\mathbb{p}_{k-1}p,\mathbb{p}_{k+1},\ldots,\mathbb{p}_K)) - \rho(\mathbb{p})$.

5. $\rho^+_e(e,k,\mathbb{p})$ where $e \in E$, $p \in P^k$, $k \in \{1,\ldots,K\}$, while we assume $p_k = \text{NIL}$ – is the measure of the contribution of path $\mathbb{p}_k$ to the excess of the capacity of link e. We have $\rho^+_e(p,k,\mathbb{p}) = \rho_e((\mathbb{p}_1,\ldots,\mathbb{p}_{k-1}p,\mathbb{p}_{k+1},\ldots,\mathbb{p}_K)) - \rho_e(\mathbb{p})$.

6. $\mathcal{Q}(p) = \mathcal{Q}_{k,E'}(p)$ (where $k \in \{1,\ldots K\}$ is the commodity number, $p \in P^k$, $E' \subseteq E$) is a scalar quality assessment function for path p for commodity k relative to subset E' of E; $\mathcal{Q}_{k,E'}(p) = -S^{\text{ref}}_{\check{y},\bar{y}}(-\chi_k(p))$, where $\check{y}_l = -\check{\chi}_{k,l}$, $\bar{y}_l = \check{y}_l + \sum_{e \in E'} \chi_{c(k),e,l}$ $(i = 1,\ldots L)$. The two minus signs serve to adjust the multicriteria apparatus from Section 4, which uses maximized criteria, to our minimized criteria (like path delay, path loss). Aspiration levels $\bar{y}_l$ are (quite arbitrarily) chosen to "scale" criterion i with the sum of the corresponding characteristics (delay, loss) over links in E' (cf. Section 4).

7. $\texttt{random(a,b)}$, where $a, b \in \mathbb{R}$, $a < b$ – returns a random value chosen under the uniform distribution on interval $[a,b]$,

8. $\texttt{randexpweightvector}()$ – returns $w/|w|$, where $w \in \mathbb{R}^{L+1}$, and each w_i is independently calculated as $\exp(10 \cdot \texttt{random}(0,1))$.

All the random choices in the algorithm are independent.

Algorithm 1 Parallel Internet CAN Traffic engineering algorithm

▷ Initialization:
$\mathbb{p}^k \leftarrow$ NIL for $k = 1,\ldots,K$.
▷ Phase 1
for all $k \in \{1,\ldots,K\}$ (in random order) **do**
  $E' \leftarrow \{e \in E:\ \omega_e \geq \underline{\phi}_k\}$ $V' \leftarrow \{v \in V:\ \exists w \in V:(v,w) \in E'\}$ ▷ Choose a subgraph of (V,E) with links of capacity not less than $\underline{\phi}_k$
  $\mathbb{p}_k \leftarrow$ FindBestPath(V',E',k)
end for
▷ Phase 2
$\mathtt{it2} \leftarrow 0$
repeat
  if $\Big(\big(\forall k \in \{1,\ldots,K\}, l \in \{1,\ldots,L\}\ \chi(\mathbb{p}_k)_l - \breve{\chi}_{k,l} \geq 0\big) \wedge \rho(\mathbb{p}) = 0\Big) \vee \mathtt{it2} \geq \Theta^{\mathrm{I}}(n,K)$ **then**
    return $\mathbb{p}$, $\breve{\phi}$
  end if
  $\mathtt{it2} \leftarrow \mathtt{it2}+1$
  $\mathtt{rhobefore} \leftarrow \rho(\mathbb{p})$ ▷ Try a mutation
  $\widetilde{K}$=SelectToChange(ntochange)
  $p_k \leftarrow$ NIL for $k \in \widetilde{K}$
  for $k \in \widetilde{K}$ (in random order) **do**
    $E' \leftarrow \{e \in E:\ \omega_e \geq \underline{\phi}_k\}$ $V' \leftarrow \{v \in V:\ \exists w \in V:(v,w) \in E'\}$ ▷ Choose a subgraph of (V,E) with links of capacity not less than $\underline{\phi}_k$
    $\mathbb{p}_k \leftarrow \mathtt{sparep}_k \leftarrow$ FindBestPath(V',E',k)
  end for
  if $\rho(\mathbb{p}) > \mathtt{rhobefore}$ **then**
    $\mathbb{p}_k \leftarrow \mathtt{sparep}_k$ for $k \in \widetilde{K}$ ▷ Withdraw mutation
  end if
until false
▷ Selects paths to be changed in the incoming mutation, randomly but with preferring those ps with high potential $\rho^-(\cdot,p)$ of decreasing $\rho(\mathbb{p})$ (heuristics)
function SelectToChange(numofpaths $\in \mathbb{N}$)
  $S \leftarrow \emptyset$
  $\mathtt{totalpathrho} \leftarrow \sum_{i=1}^K \rho^-(i,\mathbb{p})$
  repeat
    Choose randomly i from $\{1,\ldots,K\} \setminus S$
    if **random**$(0,1) < \Theta^{III}/K + \rho^-(i,p)/\mathtt{totalpathrho}$ **then** $S \leftarrow S \cup \{i\}$
    end if
  until $|S| = \mathtt{numofpaths}$
  return S
end function

The algorithm, for the problem without Modifications 1 and 2, is depicted as Algorithm 1. It consists of two phases. In phase 1, the paths for the commodities are computed by function FindBestPath that searches a path best in terms of both the additive characteristics (delay, jitter, etc.) and ρ^+, the potential of increasing the current total link capacity excess. The term "best" related to several criteria is understood in terms of a complex formula, involving the reference level technique. Function FindBestPath will be described in Subsection 5.2. If phase 1 does not find a feasible solution and it does not exhaust the iteration limit, phase 2 of the local solution improvement is executed. It iteratively tries to decrease the total link capacity excess by removing a few paths from $\mathbb{p}$ and then recompute these paths in random order (the order of computing paths for a set of commodities is essential, since one computed path influences the current function ρ^+, and the current ρ^+ influences the next computed path, and so on).

Modification 1 is easily taken into account in the realized management module. Problem with this Modification is reduced to the problem without the Modification with artificial commodities, each being an aggregate of the commodities with a particular source node-sink node pair. An aggregation of demands for commodities is also necessary; it is done by summing for the traffic demands, by taking maximum for the single-connection capacity demands, and by taking minimum for the additive characteristics demands. Tackling Modification 2 is discussed later but not implemented.

Function Θ^I and constant Θ^{III} are the algorithm parameters, they heuristically determine the construction of a mutation or the number of iterations in particular algorithm loops. The suggested defaults for these parameters are $\Theta^I(K) = 3\log(K+3)$, $\Theta^{III} = 0.1$.

Remark 1: Whenever for commodity k the algorithm constructs an empty E' the algorithm stops with the message for the administrator that there is no capacity-feasible (in terms of a single connection) path from node start(k) to node end(k) for the given CoS c. This message shows the direction of reengineering of the network.

5.2. The FindBestPath Function

Function FindBestPath(V',E',k) with $V' \subseteq V$, $E' \subseteq E$, $k \in \{1,\ldots,K\}$ returns a path:

$$\operatorname{arg\,lexmax}_{\substack{p \in P^k:\\ \forall v \in p\ v \in V',\\ \forall e \text{ on } p\ e \in E'}} \Big(\min(0, \mathscr{Q}_{k,E'}(p)), -\rho^+(p,k,\mathbb{p}), \mathscr{Q}_{k,E'}(p)\Big). \tag{8}$$

Here $\operatorname{arg\,lexmax}_{x \in X}(a_1(x), a_2(x), \ldots a_t(x))$ is an $x \in X$ that yields the lexicographically lowest sequence $(a_1(x), a_2(x),\ldots,a_t(x))$, where the lexicographical order of sequences is defined by $(c_1,c_2,\ldots,c_t) > (d_1,d_2,\ldots,d_t)$ if and only if $\big((c_1 < d_1) \vee (c_1 = d_1 \wedge c_2 > d_2) \vee \ldots (c_1 = d_1 \wedge \ldots c_{t-1} = d_{t-1} \wedge c_t > d_t)\big)$.

Function FindBestPath, a path for commodity k in the subgraph (V',E') of (V,E) is returned that, if possible:

- first of all, is feasible in terms of the additive QoS characteristics (satisfies constraints 4),
- secondly, contributes low to the total capacity infeasibility,

- lastly, when the two above condition can be satisfied, yields values of the additive characteristics as low as possible.

We try to satisfy the demands for additive characteristics before satisfying the capacity demands for the given traffic for commodities. This is natural, since the additive characteristic demands can be set quite precisely (they can follow from the QoS demands divided by the expected number of domains on the connection paths) while the traffic on commodities can be only a result of rough prognoses.
This presents an "ideal algorithm" with the "ideal" function FindBestPath that is hard to compute. Later we will show the "real" variant of the Algorithm 1 where this ideal function is approximated.
Note that the FindBestPath function implicitly depends on the current algorithm state, namely, on the array p of currently constructed intra-domain paths. Such an implicit dependence of functions on global variables will happen in our depiction of the algorithm.

5.3. Comments on the Algorithm

The ideal algorithm is a heuristics, greedy in that optimizes paths for single commodities. Thus, it cannot have a strict convergence proof. Nonetheless, it at least exhibits properties suggesting a reasonable approaching of some solution. The algorithm yields in each iteration a solution feasible in terms of path additive constraints provided that one exists and, additionally $\rho(p)$, connected with the excess of link capacities, decreases monotonically between the main iterations. The satisfaction of the single connection capacity demands is basically enforced by the construction of E'.

Remark 2: The algorithm yields a solution satisfying constraints (4) on the additive characteristics whenever such a solution exists. This is because all the paths in the algorithm are constructed due to (8), where whenever for commodity k a path $p \in P^k$ with a nonnegative $\mathscr{Q}_{k,E'}(p)$ exists, the argument maximum will be a path with a nonnegative $\mathscr{Q}_{k,E'}(p)$.

Remark 3: By construction, the algorithm produces in its Phase 2 a sequence of $\mathbb{p}$ monotonic in $\rho(\mathbb{p})$ (since a mutation that increases ρ is withdrawn). Note that $\rho(\mathbb{p})$ is zero if and only if all the link capacity constraints (3) are satisfied by $\mathbb{p}$.

A simple extension to take into account node throughput constraints is possible.

Remark 4: Problem Modification 2 could be tackled by the algorithm by adding the term

$$\sum_{k\in\{1,\ldots,K\}} \sum_{e \text{ on } \mathbb{p}_k} \xi_v^{\text{exc}} \tag{9}$$

in the definition of $\rho_e(\mathbb{p})$; here

$$\xi_v^{\text{exc}} = \max\left(0, \Big(\sum_{\substack{K=1,\ldots,K:\\ e=(i,v),\, e \text{ on } \mathbb{p}_k}} \phi_k + \sum_{\substack{k\in 1,\ldots,K:\\ \text{start}(k)=v}} \bar{\phi}_k \Big) \varkappa_{c(k)} - \xi_v \right)$$

is the throughput excess at node $v \in V$. This modification shall also update the descent definitions of ρ^+, ρ^- and ρ. Term (9) expresses the summary excess of a node throughput of both the end-nodes of the link. Also, with Modification 2, the commodities with degenerate relations (with the same source and sink node) are not negligible, since they load the nodes, but can be neglected with a simultaneous surrogate decrease of appropriate ξ_v.

5.4. Approximation of the FindBestPath Function

A strict realization of FindBestPath would be clearly a difficult numerical problem itself (it contains the well-known NP-complete multicriteria shortest path problem). In our real algorithm the function is approximated as depicted in Algorithm 2. Instead of searching the whole set of possible paths for a commodity P^k, we search the set of all possible shortest paths under a link cost being obtained by a different (but common for all the links) linear combinations of the additive link characteristics as well as of the link penalties ρ_e.

Algorithm 2 Approximation of function FindBestPath

function FindBestPath($V' \subseteq \mathbb{N}, E' \subseteq E, k \in \mathbb{N}$)
  $\bar{\omega} \leftarrow \sum_{e\in E'} \omega_e$
  $\bar{\chi}_l \leftarrow \sum_{e\in E'} \chi_{c(k),e,l}$ for $l = 1,\ldots,L$
  for $\texttt{itno} = 1,\ldots,\Theta^{II}(K)$ **do**
    $w \leftarrow \texttt{randexpweightvector}(1+\texttt{L})$
    $\texttt{Potentialpaths} \leftarrow \emptyset$
    for $e \in E'$ **do**
      $\mathfrak{c}[e] \leftarrow \sum_{l=1}^{L} w_l \bar{\chi}_{c(k)(k),e,l} / \bar{\chi}_l + w_{L+1}\rho_e(\mathbb{p})/\bar{\omega}$
▷ $\mathfrak{c}$ is an array of paths indexed with pairs of integers
      $\texttt{Potentialpaths} \leftarrow \texttt{Potentialpaths} \cup \{\texttt{Dijkstra}(V', E', c, \texttt{start}(k), \texttt{end}(k))\}$
    end for
  end for
  return $\arg\text{lexmax}_{p\in\texttt{Potentialpaths}} \Big(\min\big(0, \mathscr{Q}_{k,E'}(p)\big), -\rho^+(p,k,\mathbb{p}), \mathscr{Q}_{k,E'}(p) \Big)$
end function

Function $\texttt{Dijkstra}(V', E', c, \texttt{source}, \texttt{sink})$ returns a shortest path from $\texttt{source} \in V'$ to $\texttt{sink} \in V'$ in graph (V', E') (where $V' \in V$, $E' \in V' \times V'$) with link-weight mapping defined by array c (i.e., $c[e]$ is the weight of the link $e \in V'$) by calling the Dijkstra algorithm (see [15]). Function Θ^{II} is the algorithm parameter with the default value of the constant function of the value of 30.
For given commodity k and class of service c, the approximate variant of FindBestPath can access only a subset, call it $\underline{P}^k$, of the set P^k of paths available to the ideal variant. Namely, $\underline{P}^k$ is the set of paths available as shortest paths under some link weights that actually linearly combine the values of some characteristics of the link. The difference in the sets of available paths is essential. We can easily see it in terms of the supremum of the set of

values of $\mathscr{Q}_{k,E'}(p)$ with p running either of P^k and $\underline{P}^k$. The suprema may differ essentially, which might be easily shown to be equivalent to the well-known fact in the multicriteria analysis. In a set of variants we cannot in general find a Pareto-optimal variant by maximizing the weighted sum of the criteria values for the variants. In this equivalence, $\mathscr{Q}$ plays the role of the scalarizing function Q from Section 4. Fortunately, approximating Pareto-optimal variants with the mere weighting can be shown to introduce an error, measured in terms of Q, not greater than by the factor of $(\text{number of criteria}+1)$. This is the content of Theorem 1 in Appendix A. In translation to our example, it means that the maximal ratio of quality $\mathscr{Q}_{k,E'}$ of paths accessible to the real and ideal variants is not more than $(L+1)$. Of course, it is difficult to precisely calculate how this influence the quality of the solution yielded by our heuristics. However, the above observation gives some imagination about it. Consequently, we could use the number $(L+1)$ as an assessment of the rank of oversizing of the network (in terms of delay, jitter, etc.) necessary to compensate for the inaccuracy of the algorithm.
The practically important advantage of the real algorithm is that its time cost can be strictly assessed.

Remark 5: It is possible to have an implementation in which the references to the matrices elements cost $\mathscr{O}(1)$ and the `Dijkstra` implementation costs $\mathscr{O}(|E'|\log V')$ elementary operations (see [15]). We consider a call to `random` elementary. Even when there were always $V'=V$, $E'=E$, the cost of an iteration of phase 1 or phase 2 would be then dominated by the cost of $\Theta^{II}(K)$ calls to `Dijkstra` plus the cost $\mathscr{O}(\Theta^{II}(K)\cdot mK)$ of evaluating the arg lexmax in line 12 (we assume a reasonable implementation). Other sections of the algorithm would be clearly dominated in time by the above iterations.
Thus, the cost of the real algorithm is not greater than

$$\mathscr{O}\big(\Theta^{I}(n,K)\cdot\Theta^{II}(K)\cdot Km(K+\log n)\big). \tag{10}$$

Remark 6: It has been noticed in the literature that shortest paths (under some graph weights) in QoS-constrained Multicommodity Flow Problems already tend to be effective ducts for commodities also in the husbandry of available capacities. The algorithm constructs its solution as some shortest paths. Thus it may be often expected that the real algorithm finishes in phase 1 with $\mathbb{p}$ already feasible and phase 2 (in which link capacity violations are considered and decreased) makes 0 full iterations. In such a case, the run cost assessment reduces to

$$\mathscr{O}\big(\Theta^{II}(K)\cdot Km(K+\log n)\big). \tag{11}$$

Another formal issue must be noted.

Remark 7: Both the shortest path subproblems and argument maximum in (8), or in the corresponding condition in real can be ambiguous, and the algorithm chooses then any of the maximizing solutions. In scalarizing by function $\mathscr{Q}_{k,E'}$, it may lead to choosing a non-Pareto-optimal solution and in scalarizing by weighted summing, it may cause an impossibility to use Theorem 1. However, small random perturbation to the used link characteristics could rescind the ambiguities and it is the subject of further work.

6. Experiments

The goal of experiments was to verify the postulated properties of the algorithm: (i) the ability to quickly find a feasible solution under some existing overdimensioning of the network (also to examine the dependence of this time on the network size) and (ii) the ability to also quickly find a near-optimal solution when we shrink the resources a little.
The experiments have been run on topologies generated by the well recognized BRITE generator with a two-level hierarchy. Both the level of domains and the intra-domain level were generated due to the Waxman model, a probabilistic model of network growths. The problems have been created to reflect the the prototype CAN network in the IIP project, in particular, in its hierarchical structure and classes of service. Parameters, e.g. link capacities, have been given by hand reasonable values (when expressed in appropriate units), similar to that present in the project. Because of a high speed of modern network devices, delays were modeled as induced only by propagation, i.e. proportionally to the physical link length. Many parameters were set to the defaults taken by the authors of BRITE.
The domain number zero of the generated domains was always taken to construct the problem. The commodities were constructed as follows. The relations were established in all pairs of different domains adjacent to domain 0 (access networks were absent for the generation simplicity). Two classes of service, 1 and 2 (interpretable as 1 – best effort, 2 – premium) were served in each relation.
The algorithm with its defaults settings of Θ^{I}, Θ^{II} and Θ^{III} and with the extension for Modification 1 was implemented in C++ as a part of the CAN management module. The implementation of `Dijkstra` used C++ `Sets` to emulate heaps, and we may expect it to cost $\mathscr{O}(|E'|\log|V'|)$ elementary operations. The algorithm implementation included several small optimizations, e.g. avoiding unnecessary repetitions of invocations of some code fragments for unchanged data.

6.1. Key Experiment Parameters

The key experiment parameters were following:

- number of nodes n in the problem,
- the demand on the capacity of a single connection for all relations: for CoS 1 – `capacity1`, for CoS 2 – `capacity2`,
- the demand on the aggregated traffic for all relations – for CoS 1 – `traffic1`, for CoS 2 – `traffic2`,

- the demand on the path delay for all relations: for CoS 1: `delay1`, for CoS 2: `delay2`,
- the demand on the path loss ratios for all relations: for CoS 1: `loss1`, for CoS 2: `loss2`.

Several series of experiments were performed. Each series of experiments consisted in changing the value of one the above parameters while the remaining of them remained constant.
In each experiment, according to the values of these key parameters, a topology was generated by BRITE and a problem was constructed based on this topology. The random number generator of BRITE was always initialized with the same (default) values so two generations of topologies with the same parameters yielded identical topologies and problems).

6.2. Other Experiment Parameters

Some other BRITE parameters (`RT_N`, `AS_N`, `RT_m`, `RT_m` and `RT_HS` `BWIntraMin` – compare [16]) and problem parameters were following in a particular experiment:

1. Number of nodes in each domain `RT_N` $= n = 30$;
2. Number of domains `AS_N` $= 10$;
3. Approximate domain neighbors count `AS_m` $= 5$. In all the experiments, domain 0 turned out to have exactly 5 neighbors, this yields the number of relations equal to $5 \cdot (5-1) = 20$ and the number of commodities $K = 2 \cdot 20 = 40$;
4. The length of the square the nodes locations to be generated within `RT_HS` $= 300$;
5. The link capacities $\omega_e = 30$ for $e \in E$, thus `BWIntraMin` was set to 30;
6. The number of additive characteristics $L = 2$ (1 refers to delay, 2 to loss ratio)
7. The delay $\chi_{c,e,1}$ of link $e \in E$ for $c \in C$ was taken as $1/300$ of the distance of the endpoint nodes of link e; the distribution of this distance depends on `RT_HS`.
8. The loss ratio $\chi_{c,e,2}$ of link $e \in E$ for $c \in C$ was always set to 0.005.
9. Demands: $\underline{\phi}_k =$ `capacity1`, $\phi_k =$ `traffic1` $\check{\chi}_{k,1} =$ `delay1`, $\check{\chi}_{k,1} =$ `loss1` for $k \in i\{1,\ldots,K\}$, $c(k) = 1$; $\underline{\phi}_k =$ `capacity2`, $\phi_{k,2} =$ `traffic2` $\check{\chi}_{k,1} =$ `delay1`, $\check{\chi}_{k,2} =$ `loss2` for $k \in \{1,\ldots,K\}$ for $k \in \{1,\ldots,K\}$, $c(k) = 2$;

Other BRITE parameter settings were the the distribution defaults taken from the exemplary `TD_ASWaxman_RTWaxman.conf` file, other problem parameter settings were done according to the described construction of the problem from the topology.

6.3. Feasibility Limits

We shall establish the approximate "problem feasibility limit" values of some key parameters that describe demands – `traffic1`, `traffic2`, `delay1`, `delay2`, `loss1`, `loss2`, i.e. for a particular key parameter, we shall assess its best value when we obtain a feasibility problem, assumed the other demands are set loosely and essentially do not intervene. We shall do it in a heuristic reasoning and in performed experiments (described later) in which we gradually increase particular demands observing when the solver falls in troubles with obtaining a feasible solution. The established approximate limits are:

1. 1.25 for `delay1` or `delay2`,
2. $4 \cdot 10^{-5}$ for `loss1` or `loss2`,
3. 15 for `traffic2` (assumed `traffic1` is small).

The heuristic reasoning starts with delays. The node locations are randomly selected from the square of the side of 300 in BRITE (since `RT_HS`=300). Thus, roughly, we can expect that a maximum distance of the source-sink pair of nodes for some commodity is about 300 (remember that there are only 5 adjacent domains to our domain, thus at most 5 sink or source nodes. We cannot expect the extreme case that some two of them are situated at the both sides of a diagonal, i.e. at the distance of $300\sqrt{2}$). If some intra-domain path of this commodity were straight-line, the delay would be, according to the settings explained above, 1/300 of the length of this path, i.e. about 1. As any such a path is rather a segment line, we can expect the minimum possible delay on an intra-domain for this commodity be some more than 1, perhaps between 1 and 2.
Now consider traffic demands. Let us account only for the traffic demand for one CoS, say, CoS 2, and assume `traffic1` is negligibly small. The capacity demands will be always set lower in the experiments, than the respective traffic demands, thus can be neglected as well. In a typical case, each of the external domains is connected to our domain by a separate border gateway node in domain (because there are sufficiently many nodes in our domain). Thus there are 4 intra-domain paths starting at one border gateway node (they lead to the four remaining external domains). According to the setting `RT_m`=3, this node has 3 adjacent nodes in its domain, and it has to dispatch this incoming traffic firstly into three links, each of capacity of 30. This seems to be the bottleneck, the distribution of the traffic within the domain should be easier. The paths demands are equal and the paths cannot be split, so some link has to conduct two paths. Thus the traffic demand `traffic2` should not exceed a number about 15. We have described the bottleneck for ingress traffic. A symmetric bottleneck will clearly appear on egress traffic on some border gateway node but it yields a similar traffic limit.
The limit demands on loss ratios are more difficult to reason about, thus we left their derivation entirely to experiments. We only mention that these limits are connected with the

minimum hop number of a path in a relation (since all the links have the same loss ratio). Since the nodes are interconnected quite randomly in BRITE, the minimal hop length of a path should not highly grow with the growth of the number n of nodes. Hence, the feasibility limit of `loss1` or `loss2` should not depend essentially on n. We derive them for two different ns, for certainty.

6.4. Construction of Experiments

The default values for the key parameters taken in the series of experiments were following: $n = 30$, `capacity1` = 0.005, `capacity2` = 0.5, `traffic1`=1, `traffic2`=4 `delay1` = = 3, `delay2`=3, `loss1`=10^{-4}, `loss2`=10^{-4}. That were set loosely, i.e. far from the limits of problem feasibility.
The series of experiments consisted in changing selected key parameters from the defaults while the remaining key parameters were kept equal to their defaults. The following series were present:

1. Changing `delay2` – from 0.75 to 2 with step 0.25. One goal of this series was to observe the heaviness of the reaction of the solver computation time and the solution infeasibility on breaking feasibility limits while the other demands are set loosely. A second goal was to examine the values of these feasibility limits experimentally.

2. Changing `traffic2` – from 10 to 2 with step 2. The goals were analogous to that of series 1.

3. Changing `loss2` – from 10^{-4} to $6 \cdot 10^{-4}$ with step 10^{-4}, with analogous goals.

4. Changing `loss2` also from 10^{-4} to $6 \cdot 10^{-4}$ with step 10^{-4} but for $n = 100$ nodes (and the remaining key parameters set to the defaults, as before).

5. Changing the number n of nodes: experiments for $n = 10$, 30, 100, 300, 1000, to examine the influence of the number of nodes on the computation time under a large network overdimensioning. The feasibility limits should not depend much on n. The heuristic reasoning about them does not depend essentially on n. Some extra experiments, not presented here, also indicate this.

6. Changing n; experiments for n=10, 20, 100, 300, 1000 as well, however, with `delay1=delay2`=1.75, `loss1=loss2`=$6 \cdot 10^{-4}$, `traffic1`=1, `traffic2`=9. This series brings more demands closer to the feasibility limits, keeping them far from the limits respectively by the factor about 1.5 (or 1/1.5 for traffic demands). Note that the constraints induced by particular demands are not independent. Thus setting all of them to their feasibility limits would probably give an infeasible problem. Thus, with the settings of this series, we are even closer to the feasibility limits than "by the factor of 1.5" and we present a harder problem to the solver.

   The setting of `delay1` `delay2`, `loss1`, `loss2` are quite clear. Setting `traffic1`=3 and `traffic2`=7 gives the sum of `traffic1` and `traffic2` about 10 but the `traffic1` is not quite negligible (one must, however, remember that that now the traffic in a relation can be essentially split into two paths, realizing two CoS and thus the heuristic reasoning about the feasibility limits alters and we get slightly more distant from these limits).

7. Changing n; experiments for $n = 10$, 20, 100, 300, 1000 as well, however, with `delay1=delay2` = = 1.5, `loss1=loss2` = $4.5 \cdot 10^{-4}$, `traffic1` = 1, `traffic2` = 11.5. This series brings even tighter demands, distant from their limits by the factor 1.1–1.2.

6.5. Experiment Results

The experiments were done on a Dell PC with the Pentium 4 2.8 GHz CPU and with 1 GB RAM, under the Fedora Linux.
For a final solution $(\mathbb{p}^\star, \phi^\star)$, (where $p^\star \in \{P^1, \ldots, P^K\}$, $\phi^\star \in \mathbb{R}^n$ we define its traffic infeasibility – as the excess of the link capacity by the found intra-domain paths and its delay (loss) infeasibility – as the summary violation of delay (loss) over all the commodities: "traffic inf."=$\rho(\mathbb{p})$,

$$\text{"delay inf."} = \sum_{k=1}^{K} \max\left(\left(\sum_{e \text{ on } \mathbb{p}_k^\star} \chi_{c(k),e,1} \right) - \breve{\chi}_{k,1}, 0 \right),$$

$$\text{"loss inf."} = \sum_{k=1}^{K} \max\left(\left(\sum_{e \text{ on } \mathbb{p}_k^\star} \chi_{c(k),e,2} \right) - \breve{\chi}_{k,2}, 0 \right).$$

The results of experiments are shown in Tables 1 through 4. The dependence the computation time on the number n

Table 1
Influence of `delay2` (series 1)

`delay2`	Time [s]	Traffic inf.	Delay inf.	Loss inf.
0.75	3.67	0	3.48	0
1	3.62	0	1.46	0
1.25	1.23	0	0	0
1.5	1.21	0	0	0
1.75	1.25	0	0	0
2	1.21	0	0	0

Table 2
Influence of `traffic2` (series 2)

`traffic2`	Time [s]	Traffic inf.	Delay inf.	Loss inf.
10	1.22	0	0	0
12	1.26	0	0	0
14	1.23	0	0	0
16	3.72	4	0	0
18	3.64	18.2	0	0
20	3.62	30.2	0	0
22	3.62	42.2	0	0

Table 3
Influence of `loss2`

`loss2`	Time [s]	Traffic inf.	Delay inf.	Loss inf.
$n = 30$ (series 3)				
0.00001	3.63	0	0	0.00034
0.00002	3.66	0	0	0.00008
0.00003	3.65	0	0	0.00002
0.00004	1.2	0	0	0
0.00005	1.25	0	0	0
0.00006	1.22	0	0	0
$n = 100$ (series 4)				
0.00001	13.21	0	0	0.00038
0.00002	13.27	0	0	0.00014
0.00003	13.19	0	0	0.00004
0.00004	4.41	0	0	0
0.00005	4.43	0	0	0
0.00006	4.44	0	0	0

Table 4
Influence of n for a varying tightness of the demands

n	Time [s]	Traffic inf.	Delay inf.	Loss inf.
Series 5				
10	0.4	0	0	0
30	1.26	0	0	0
100	4.42	0	0	0
300	15.28	0	0	0
1000	60.6	0	0	0
Series 6*)				
10	0.4	0	0	0
30	1.22	0	0	0
100	4.42	0	0	0
300	15.38	0	0	0
1000	62.09	0	0	0
*) `delay1=delay2` = 1.75, `loss1=loss2` = $5 \cdot 10^{-4}$, `traffic1` = 1, `traffic2` = 9)				
Series 7**)				
10	0.4	0	0	0
30	1.42	0	0	0
100	4.42	0	0	0
300	45.78	8.5	0	0.000365
1000	180.63	6.5	0	0.000305
**) `delay1=delay2` = 1.5, `loss1=loss2` = $4.5 \cdot 10^{-4}$, `traffic1` = 2, `traffic2` = 11.5)				

of nodes for various demand settings is also illustrated in Fig. 3 (unless mentioned the key parameters have their default values).

The solver proved able to solve the problem even for a domain with a thousand of nodes within a time fully acceptable for an off-line management. Feasible solutions were returned in a similar time when the network overdimensioning was large and when many of the demands were situated close the problem feasibility limits, i.e. the network overdimensioning was small.

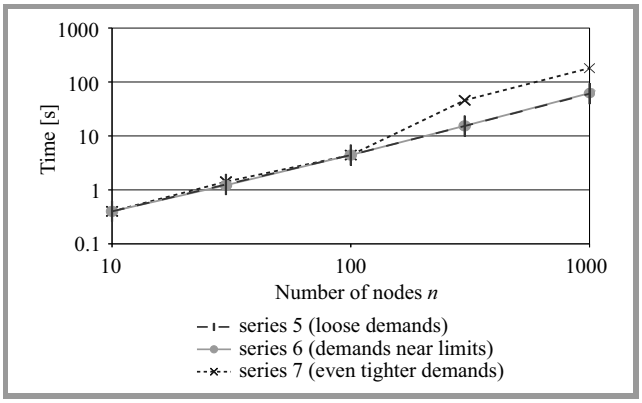


Fig. 3. Influence of n for a varying tightness of the demands.

The practical dependence of computation time on n was slightly more than linear. This is consistent with the theoretical value assumed the solution is already found in phase 1. Note (11) with the default Θ^I, Θ^{II}, with constant K and $m \sim n$ yields the solution time that depends on n like $O(n \log n)$. Another reason why the time grew slightly quicker than linearly was that the realization of some arrays (C++ Maps) raised a nonconstant array element access time.

When the demands were set so tightly that the solver could not obtain a feasible solution (so phase 2 was present), the computation time did not grow much, which could be expected by the construction of the stopping criterion for phase 2. The growth was about 3–4 times through the experiments and the time remained pretty acceptable in terms of its absolute values.

In the experiments where particular demands were gradually tightened, the solution infeasibilities responded with a gradual growth. Anyway, traffic, loss and delay infeasibilities (whose definitions use summing over commodities) were not big values compared with the applied shrinks in `delay2`, `loss2` or `traffic2` multiplied by the number of commodities (40). In series 7, the final infeasibilities that appeared for big n values were neither large in such a view. The experimentally obtained feasibility limits were 14–16 for traffic a demand (for one CoS, assumed the traffic demand for the second class is small), 1–1.25 for a delay demand, $3 \cdot 10^{-4} \ldots 4 \cdot 10^{-4}$ for a loss demand (the latest – for two different ns). This was consistent with the outcome of our heuristic reasoning about the limits and substantiated the previously described settings for the limits taken in the experiments.

7. Conclusions

The presented practical approach to the QoS-aware traffic engineering based on a small level of network overdimen-

sioning proved efficient in the experiments. Unlike sophisticated optimization algorithms, our heuristics most often exhibits a computation time a little-over-linear in the number of nodes and is able to tackle a thousand node network within a pretty-acceptable time. It behaves well when a feasible solution cannot be found.

Appendix A

Quality of the Weight-based Path Scalarization

Lemma 1. We have a nonempty finite set $Y \subset \mathbb{R}^k_-$. Let P be the set of nondominated (Pareto-optimal) points of Y: $P = \{y \in Y : \neg\exists z \in Y\, z \succ y\}$. Let W be the set of maximizers of weighted sum scalarizing functions: $W = \{w \in Y : \exists v \in \mathbb{R}^k_+, v \neq 0\, w \in \mathrm{Arg\,xmax}_{y\in Y} v^\top y\}$. Then $\forall p \in P\ \big(p \in W \vee \exists w^\star \in W\, w^\star \succ p\big)$.

Proof. By contradiction, we assume the negation of the claim : $\exists p \in P\ \big((p+\mathbb{R}^k_+) \cap \mathrm{conv}\,(W) = \emptyset\big)$. So there exists a hyperplane separating the convex sets $p+\mathbb{R}^k_+$ and $\mathrm{conv}\,(W)$, and since $p+\mathbb{R}^k_+$ is a (shifted) cone, the hyperplane can be chosen so as to contain the cone origin, p. I.e, $\exists s \in \mathbb{R}^k, s \neq 0, C \in \mathbb{R}\ \big((\forall x \in p+\mathbb{R}^k_+, s^\top x + C \geq 0) \wedge s^\top p + C = 0 \wedge \forall y \in \mathrm{conv}\,(W)\, s\top y + C < 0\big)$. Vector s cannot have a negative coordinate (if s_i were negative, then $p+\mathfrak{e}_i$, which is in $p+\mathbb{R}^k_+$, would give the negative value of our separating function, i.e. $s^\top(p+\mathfrak{e}_i)+C<0$ would hold; $\mathfrak{e}_i$ means the i-th versor). Thus the true sentence $\forall_{w\in W}\, s^\top w \leq s^\top p$ contradicts, by the definition of W, to $p \notin W$. ■

Theorem 1. We have a finite set $Y = \{y^1, \ldots, y^r\} \subset \mathbb{R}^k_-$ (with $r \geq 1$). Let $W = \{w^1, \ldots, w^m\}$ (with $r \geq 1$), $W = \{y \in Y : \exists v \in \mathbb{R}^k_+, \neq 0\, y \in \mathrm{Arg\,xmax}_{y\in Y} v^\top y\}$ be the set of weighted-sum maximizers of Y. Let $P = \{P^1, \ldots, P^n\}$ (with $n \geq 1$), $P = \{y \in Y : \neg\exists z \in Y\, z \succ y\}$ be the set of Pareto-optimal points of Y (note that both W and P must be nonempty by definition). Then for each $p \in P$ there exists $w \in W$ such that

$$\forall i = 1, \ldots, k\ |\omega_i| \leq (k+1)|p_i|. \tag{12}$$

Proof. Take any $p \in P$. If $p \in W$, the claim is obvious, so further assume $p \notin W$. By Lemma 1 there exists $\hat{w} \in \mathrm{conv}\,(W)$ such that $\hat{w} \succ p$. By Carathéodory's Theorem $\hat{w}$ is a convex combination of at most $k+1$ extremal points of $\mathrm{conv}\,(W)$. But each extremal point of $\mathrm{conv}\,(W)$ is in W, so $\hat{w}$ is a convex combination of at most $k+1$ points of W: $\hat{w} = \alpha_1 v^1 + \ldots + \alpha^{k'} v_{k'}$ with $1 \leq k' \leq k+1$, $\alpha_j \geq 0$, $\alpha \neq 0$, $\sum_j \alpha_j = 1$, $v^i \in W$. For some $j^\star$ there must be $\alpha_{j^\star} \geq 1/(k')$. Thus, bearing in mind that all v_i^j are nonpositive, for each $i \in \{1, \ldots, k\}$ $\hat{w}_i \leq (1/k') \cdot v_i^{j\star}$, thus also $\hat{w}_i \leq 1/(k+1) v_i^{j\star}$, $v_i^{j^\star} \geq (k+1) \cdot \hat{w}$ and, since $w \succ p$, $v_i^{j\star} \geq (k+1) p_i$. ■

Acknowledgments

The author would like to thank the cooperators from the Future Engineering Project, especially Prof. Wojciech Burakowski, Dr. Andrzej Bęben from Warsaw University of Technology, Dr. Janusz Granat and Dr. Paweł Olender form the National Institute of Telecommunications in Warsaw for the extensive discussions on the requirements and problem formulation.

This work was funded by the European Union, European Funds 2007–2013, under contract number POIG.01.01.02-00-045/09-00 "Future Internet Engineering" and by the National Institute of Telecommunications (Poland) Grants 06300013 through 06300016.

References

[1] W. Burakowski, H. Tarasiuk, A. Bęben, and G. Danilewicz, "Virtualized network infrastructure supporting co-existence of Parallel Internets", in *Proc. 13th ACIS Int. Conf. Softw. Engin., Netw. and Parallel & Distrib. Comput. SNPD 2012*, Kioto, Japan, 2012, pp. 679–684 (doi: 10.1109/SNPD.2012.67).

[2] A. Iwata, R. Izmailov, D.-S. Lee, B. Sengupta, G. Ramamurthy, and H. Suzuki, "ATM routing algorithms with multiple QOS requirements for multimedia internetworking", *IEICE Trans. Commun.*, vol. E79-B, no. 8, pp. 999–1006, 1996.

[3] G. Tsaggouris and C. Zaroliagis, "QoS-aware Multicommodity Flows and Transportation Planning", in *6th Workshop Algorithmic Methods and Models for Optimization of Railways (ATMOS'06),* R. Jacob and M. Müller-Hannemann, Eds. *OASIcs – OpenAccess Series in Informatics*, Technical Report ARRIVAL-TR-030. Schloss Dagstuhl–Leibniz-Center for Informatics, Dagstuhl Publishing, Germany, 2006.

[4] N. Garg and J. Könemann, "Faster and simpler algorithms for multicommodity flow and other fractional packing problems", in *Proc. 39th Ann. Symp. Foundat. of Comp. Sci. FOCS 1998*, Palo Alto, CA, USA, 1998, pp. 300–309.

[5] C. Duhamel and A. Mahul, "An augmented lagrangean approach for the QoS constrained routing problem", Research Report LIMOS/RR07-15, Université Blaise-Pascal, Aubiére, France, 2007 [Online]. Available: http://limos.isima.fr/IMG/pdf/rr-07-15.pdf

[6] M. Ghatee, "QoS-based cooperative algorithm for integral multicommodity flow problem", *Comp. Commun.*, vol. 34, no. 7, pp. 835–846, 2011.

[7] A. M. Allakany, T. M. Mahomud, K. Okurama, and M. R. Girgis, "Multiple constraints QoS multicast routing optimization algorithm based on Genetic Tabu Search algorithm", *ACSIJ Adv. in Comp. Science: an Int. J.*, vol. 4, issue 3, pp. 118–125, 2015.

[8] G. Apostopoulos, D. Williams, S. Kamat, R. Guerin, A. Orda, and T. Przygienda, "QoS routing mechanisms and OSPF extensions", RFC2676, 1999 [Online]. Available: https://tools.ietf.org/html/rfc2676

[9] J. Wang and J. Crowcroft, "QoS routing for supporting multimedia applications", *IEEE J. Selec. Areas in Communi.*, vol. 14, no. 7, pp. 1228–1234, 1996.

[10] Y. Wang and Z. Wang, "Explicit routing algorithm for internet traffic engineering", in *Proc. 8th Comp. Commun. and Netw.*, Boston, MA, USA, pp. 582–588, 1999.

[11] R. G. Garroppo, S. Giordano, and L. Tavanti, "A survey on multi-constrained optimal path computation: Exact and approximate algorithms", *Computer Networks*, vol. 54, no. 17, pp. 3081–3107, 2010.

[12] A. Kuipers, "Quality of Service routing in the Internet. Theory, complexity and algorithms", Ph.D. thesis, Delft University, Delft University Press, Delft, 2014.

[13] A. P. Wierzbicki, M. Makowski, and J. Weesels, Eds., *Model-Based Decision Support Methodology with Environmental Applications*, Dordrecht, Netherlands: Kluwer Academic Publishers, 2000.

[14] A. Bęben, Ed., "Specification of Parallel Internet Content Aware Network (version 2)", The IIP project, Warsaw, Poland, Report 31.01.2012, Task Z2.6.

[15] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, 2nd ed. MIT Press and McGraw-Hill, 2001 (1990).

[16] A. Medina, A. Laghina, I. Matta, and J. Byers, "BRITE: Universal Topology Generation from a User's Perspective", Boston University, Boston, 2001, user manual" [Online]. Available: http://www.cs.bu.edu/brite/publications/usermanual.pdf

Paweł M. Białoń has been with the National Institute of Telecommunications. He received his Ph.D. in Automatic Control and Robotics from Warsaw University of Technology in 2013. His scientific interests include decision support and optimization with applications in telecommunications and data mining.

E-mail: P.Bialon@itl.waw.pl
Department of Advanced Information Systems
National Institute of Telecommunications
Szachowa st 1
04-894 Warsaw, Poland

Paper

Heavy Gas Cloud Boundary Estimation and Tracking using Mobile Sensors

Mateusz Krzysztoń and Ewa Niewiadomska-Szynkiewicz

Institute of Control and Computation Engineering, Warsaw University of Technology, Warsaw, Poland
Research and Academic Computer Network (NASK), Warsaw, Poland

Abstract—This paper addresses issues concerned with design and managing of monitoring systems comprised of mobile wireless sensing devices (MANETs). The authors focus on self-organizing, cooperative and coherent networks that maintain a continuous communication with a central operator and adopt to changes in an unknown environment to achieve a given goal. The attention is focused on the development of MANET for heavy gas clouds detection and its boundary estimating and tracking. Two strategies for constructing the MANET are described, in which sensors explore the region of interest to detect the gas cloud, create temporary network topology and finally, cover the cloud boundary, and track the moving cloud. The utility and efficiency of the proposed strategies has been justified through simulation experiments.

Keywords—deployment strategies, heavy gas cloud boundary tracking, MANET, mobile ad hoc network, mobility models, sensor networks.

1. Introduction

The management of emergency activities such as guiding people out of dangerous areas and coordinating rescue teams is characterized by uncertainty regarding both the source of danger and the availability of useful resources. Depending upon the scale and nature of the incident, people involved in a crisis may suffer from limited situational awareness. Situational awareness is a state of being aware of what is happening in an area of interest and understanding how information, events, and actions impact objectives. Inadequate situational awareness has been identified as a primary factor leading to human error in emergency situations, with grave consequences. Therefore, there is a huge demand for effective situational awareness systems that must gather data in a timely manner in order to create an evolving image of the emergency at hand, ultimately generating a holistic view of the emergency to be used by authoritative decision makers and emergency services. As emergency situations are chaotic in nature, data sources are usually dispersed throughout geographical areas due to dynamic nature of the disaster, situational awareness becomes a complex, distributed processing problem where innovative techniques need to be employed in order to effectively monitor and neutralize the threat.

In this paper the attention is focused on the effectively aiding with emergency situations caused by release of toxic gas. Extremely dangerous are heavy gas clouds formed by gas heavier than air (e.g. chlorine, nitrogen or sulfur dioxide). These clouds are usually created due to a natural phenomena (e.g. volcano eruption) or as a result of terrorist attack and military action. Furthermore, great amount of toxic substances are transported and stored by industries. Despite high safety standards gas tankers crashes, in which dangerous substance is released to the atmosphere, occur from time to time [1]–[3]. In general, in case of environmental disasters the extensive monitoring of the area of interest is necessary to manage the evacuation of people from a disaster zone, track the propagation of a given cloud, measure the level of contamination and finally, neutralize the cloud. As gas clouds are dispersed throughout geographical areas the innovative techniques need to be employed in order to effectively monitor and neutralize the disaster.

Mobile wireless ad hoc networks (MANETs) can significantly enhance the capability to investigate contaminated areas, in particular detect and track heavy gas clouds. In general, MANETs are comprised of wireless mobile devices (network nodes) that can dynamically and freely self-organize into temporary network topologies that can change rapidly and adopt to the changing environment [4]. Nodes communicate wirelessly and share the same radio channel. The devices located within their transmission range can communicate directly without the need for an established infrastructure and centralized administration. For communicating with devices located beyond the transmission range, a node needs to use intermediate nodes to relay messages hop by hop. Thus, in general, routes between mobile nodes may include multiple hops.

Advanced monitoring systems can be created by wireless sensors mounted on mobile platforms, i.e. unmanned vehicles, mobile robots or drones, and moved to desirable positions. Authors have developed two three-phase strategies for constructing MANETs, in which mobile devices, equipped with gas sensors and radio transceivers, explore the region of interest to detect a gas cloud, create preliminarily network topology, estimate a boundary of this cloud and track it maintaining the permanent communication with the central operator (base station). Such a sensing system can successfully support the management of emergency activities.

The paper is organized as follows. In Section 2 the problems and approaches to development of MANETs for dynamic processes sensing are investigated and discussed. In Section 3 a formal statement of a network and gas cloud propagation models is provided. All phases of creation of MANET for a gas cloud boundary estimation and tracking are discussed in Section 4. Two algorithms for such MANETs development are described in Sections 5 and 6. The results of performance evaluation of these algorithms are described and discussed in Section 7. The paper is concluded in Section 8.

2. Related Work

Large-scale heterogeneous wireless ad hoc networks are becoming a technological cornerstone for many important applications in today's society. These collections of autonomous and distributed nodes capable of sensing, communication, processing and self-organization are emerging as a new era of intelligent information-driven paradigms. Ad hoc networks are used in many applications such as surveillance systems, environment monitoring and unmanned space explorations. On the other hand, the deployment of these networks in industrial environments is generating tremendous streams of daily data and qualities which describe the operation, condition, performance and status of a wide range of equipment. This represents an additional large volume of data to explore, the need for more efficient and scalable data analysis methods and raises additional challenges on real-time stream data processing, distribution and storage. Furthermore, nodes of ad hoc networks are often small battery powered devices, which means their power source is limited. The network's throughput is also limited. Thus, various approaches to energy saving are considered, i.e. temporary deactivating selected nodes [5]–[8], decreasing number and size of transmitted messages [6], [7]. Moreover, poor deployment of sensor devices may lead in small coverage of a region of interest. The influence of poor placement of devices on network reliability, stability and availability is discussed in [9].

Another problem is the dynamic nature of sensing phenomena. Therefore, recently a lot of effort is put into movement-assisted deployment systems [10], [11]. Endowing sensors with mobility significantly expands capabilities of monitoring and tracking systems. Mobility allows to detect lacks of deployment objectives, improve coverage and communication connectivity even decreasing number of employed sensing devices. A large number of measurement targets can be handled with smaller number of migrating sensors. On the other side it is obvious that mobility implies an additional complexity layer. Paths on which vehicles carrying sensors can move to desired destination have to be calculated [12], [13], and internode communication has to be managed to imply connectivity among the working set of devices and a base station. Numerous strategies and approaches to global connectivity maintenance by network composed of autonomous mobile devices have been developed and described in the literature [14]–[16]. Presented algorithms enable to create network topologies with different characteristics (size, nodes' degree, etc.). Another problem is to discover redundant links in a sensing network that could be removed [17] or to indicate the region where the extra nodes should be supplied to restore the global connection [18], [19]. The description of numerous examples of monitoring systems built by static and mobile sensors can be found in literature, e.g. real time monitoring system for nuclear plant [20], mobile systems for environmental monitoring [21] and exploring unknown areas [22], [23]. In emergency situations mobile wireless devices can be used to establish new communication infrastructure for rescue teams [24], [25]. The system for firefighters that allows to conduct audio and video conference during rescue actions is described in [26]. The MANET-based communication infrastructure for telemedicine service is described in [27]. Kulla e*t al*. describe in [28] the application of MANET to maintain a permanent communication with a single robot that explores inside of a building in emergency scenario.

A significant attention in the recent years is focused on the application of mobile ad hoc networks for detecting and boundary tracking of phenomena clouds. Phenomena clouds are characterized by nondeterministic, dynamic variations of shapes, sizes, direction, and speed of motion along multiple directions. The phenomena cloud detection and tracking require more reliable techniques that can accurately adapt to the dynamics of a given phenomena, and should not limit to simple and well-defined shapes of clouds. In [5] a framework for environmental boundary estimation and tracking by considering the boundary as a hidden Markov model with separated observations collected from multiple sensing devices is presented. Based on the data collected from sensors and prior knowledge of the dynamic model of boundary evolvement the optimization problem is formulated. The boundary is estimated by solving this problem for prediction and current observation of a given phenomena.

The simpler but still challenging problem is to create mobile system for heavy gas clouds monitoring. In this paper authors focus on a heavy gas clouds boundary detection and tracking. Clouds created by heavy gas are very dangerous for human beings. They can move close to the ground for significant time at high level of gas concentration. In the significant number of works on a gas cloud, boundary detection is calculated based on estimated distribution of phenomena concentration [29]–[32]. It is assumed that concentration decreases smoothly to the boundary, which is inadequate for scenarios with heavy gas for few reasons. Firstly, the dynamics of a heavy gas cloud is very fast. Secondly, gas sensors can measure the gas concentration only at a given point. Furthermore, lower concentration can indicates a boundary or any obstacle in a working space. Therefore, the application of networks created by mobile

sensing devices that can dynamically self-organize into coherent topologies is a viable solution for heavy gas clouds monitoring.

3. Problem Formulation and Sensing System Modeling

3.1. Model of Sensing MANET

Let us consider a network that comprises N autonomous mobile platforms (unmanned vehicles or mobile robots) D_i, $i = 1,\ldots,N$ equipped with heavy gas detectors and radio transceivers that can create a sensing system in a two-dimensional workspace W with self-configuring capabilities. The objective is to deploy all devices to achieve the optimal sensing of boundaries of a given gas cloud to estimate a size of this cloud, and minimize the energy usage for carrying sensors. All devices can dynamically change their positions and the role in the network according to a current knowledge about the environment and the positions of all other devices in a network. Furthermore, it is assumed that all measurements can be transmitted to the central operator (base station) any time. Hence, the permanent communication with the base station has to be maintained.

In general, the design of self-organizing networks that can freely organize into temporary topologies is challenging problems. The development of applications relying on mobile devices and wireless communication protocols can be greatly simplified by the use of modeling and simulation tools. Therefore, authors have developed and investigated a simulation-based method to design and develop the MANET for heavy gas clouds detection, its boundary estimation and tracking. In presented approach the utility and efficiency of proposed sensing devices deployment strategies are evaluated through simulations.

In simulation-based designing the model of a system considered has to be created and implemented. Authors formulated a mathematical model of proposed network, modeling both radio signal proposed propagation and movement of all network nodes. In our model all network nodes are solid bodies with an arbitrary shape. In order to simplify the description of the system each network node is modeled by a polygon with its reference point $\mathbf{c}^i = [x^i, y^i]$, which is the location of the device (exactly its antena). The radio coverage region of each node is a disc of a radius r_t centered at the transmitter (exactly at the reference point $\mathbf{c}^i$ in case of D_i). The commonly used long-distance path loss model described in [33] was used for estimation of signal degradation with a given distance, and calculation of the internode distance d_{ij} in time t. In this research all sensing devices could be forced to move in advisable direction with the speed $v \in [v_{min}, v_{max}]$ while forming in time t a dynamic multi-hop network $\mathscr{G} = (\mathscr{V}, \mathscr{E})$ defined as follows:

$$\mathscr{V} = \{D_i, i = 1,\ldots,N\}, \quad (1)$$

$$\mathscr{E} = \{(D_i, D_j), d_{ij} \leq r_t, i, j = 1,\ldots,N, i \neq j\}, \quad (2)$$

where (D_i, D_j) denotes a bidirectional link between a pair of nodes D_i and D_j that can be enabled or disabled in time due to node mobility, d_{ij} is the Euclidean distance between these nodes.

In presented study all devices D_i are autonomous agents that collaborating create a sensing network. Thus, the aim of each device is to reach the target point in a workspace that is defined by $\mathbf{c}_g^i = [x_g^i, y_g^i]$. To ensure permanent network connectivity motion trajectory calculated for each D_i depends on the positions of all other network devices D_j, $j = 1,\ldots,N$, $j \neq i$ in the workspace W.

3.2. Model of Heavy Gas Cloud Propagation

To perform simulations with a sensing system for a heavy gas cloud monitoring it is necessary to model propagation of such cloud. The models of heavy gas dispersion are divided into several categories based on different criteria. Three main groups: empirical, research and engineering models are distinguished in [34]. Empirical models are developed based on environmental measurements and laboratory experiments. Mathematical models – formulated by sets of partial differential equations dependent on time and three space coordinates – provide complete and detailed description of the physical process of a heavy gas dispersion [34]. However, mathematical models require the estimation of numerous parameters and their application is usually limited to obstacle-free sensing area. The trade off are engineering models that are widely used in practical applications.

In the research, which results are presented in this paper, a simple engineering model described in [35] – the box model – was used to simulate heavy gas clouds propagation. The summary of this model is presented below. The heavy gas cloud is modeled as a uniform cylinder with dynamics described by a set of three linear ordinary differential equations:

$$\frac{d\bar{\mathbf{c}}_c}{dt} = v_c, \quad (3)$$

$$\frac{dr}{dt} = v_f, \quad (4)$$

$$\frac{dm_a}{dt} = \rho_{air}(\pi r^2)v_t + \rho_{air}(2\pi rh)v_e, \quad (5)$$

where $\bar{\mathbf{c}}_c = [x_c, y_c]$ denotes the position of the centre of a cloud, v_c, v_f, v_e, v_t denote following velocities: transport, gravitational and entrainment for edge and top of a cloud. r is the radius of a cloud, h its height and m_a is the entrained mass. ρ_{air} denotes the air density.

The Eq. (3) describes the spreading of the centre of a cloud, Eq. (4) the puff horizontal spreading influencing the cloud radius. Mass conservation is described by the formula (5).

The gravitational velocity v_f is calculated for a given standard gravity g. The height of a cloud h, cloud and air

densities – ρ_c and ρ_{air} are calculated according to the following formula:

$$v_f = C_F \sqrt{\frac{g(\rho_c - \rho_{air})h}{\rho_{air}}}, \tag{6}$$

where C_F denotes the Froude number of the front (for dense gas models typically $C_F = 1.1$ [35]).
The relationship between the edge entrainment velocity v_e and the gravitational velocity is described as follows:

$$v_e = \alpha v_f, \tag{7}$$

where $\alpha \in [0.6, 0.9]$ (see [34]).
Finally, the entrainment velocity for top of a cloud can be calculated due to the equation

$$v_t = u_* \left(\frac{\kappa}{1 + \beta \frac{g(\rho_c + \rho_{air})h}{\rho_{air} u_*^2}} \right), \tag{8}$$

where $\kappa = 0{,}4$ denotes the von Karman constant [34], u_* the friction velocity [36], β the parameter (suggested value $\beta = 0.125$ [37]), ρ_c the current cloud density.
To calculate displacement of a cloud its density ρ_c and height h have to be determined. They depend on the concentration z of gas in a cloud. The value of z dynamically changes due to cloud mixing with an ambient air. It can be calculated due to the formula

$$z = \frac{\frac{m_0}{M}}{\frac{m_0}{M} + \frac{M_a}{M_{air}}}, \tag{9}$$

where m_0 is a mass of contaminant gas, M and M_{air} the molar weights of the gas and air respectively.

The relation between the gas concentration and its density notable influences a cloud dynamics. This relation is affected by many factors. In this research authors neglected chemical reactions and occurrence of any aerosol formations in the cloud. Mixing of gas with ambient air was the only source of density change – the density of gas was calculated according to the following formula

$$\rho_c = \rho_{air} \left(\frac{1 + z\frac{M - M_{air}}{M_{air}}}{1 + \frac{z\Delta H_0}{\left((1-z)M_{air} q_p^{air} + z M q_p\right) T_{air}}} \right), \tag{10}$$

where ΔH_0 denotes the enthalpy difference between the release material at the source and ambient conditions, q_p and q_p^{air} are specific heat capacities of gas and air respectively. T_{air} is the temperature of an ambient air.
Then, the height of a cloud h was computed

$$h = \frac{V}{\pi r^2}, \quad V = \frac{m}{\rho_c}, \tag{11}$$

where V is the volume of a cloud.

The presented model was employed to simulate a gas dispersion in a flat area without obstacles. The Euler method was used to solve set of Eqs. (3)–(5). In general, this model is valid until the occurrence of one of two conditions [34]:

- the difference between the density of cloud and air is less than a small assumed value,
- the growth of a cloud radius in single step is small enough.

3.3. Model for Motion Trajectory Computing

The goal of mobility model is to describe the movement of all devices of a sensing network $\mathscr{G}$ in the workspace W, i.e., how their location, velocity, and acceleration change over time. The main problem addressed in many recent publications on MANETs is a high impact of the mobility of network devices on the overall network performance and connectivity. The mobility models should resemble the real life movements of all network nodes. Moreover, they should be appropriately reflected in simulations, which can be used to support design and management of a given network $\mathscr{G}$. A number of less and more detailed and accurate mobility models have been introduced, tested and implemented in various mobile networks. The survey and discussion of the taxonomies of mobility models and main directions to mobility modeling are provided in [12].
In the research presented in this paper the mobility model that resembles a collision-free movement of a group of mobile wireless devices is used. The model was adapted to coherent and cooperative network topologies construction. The algorithm for motion trajectories calculation and results of performance evaluation are described and discussed in [13]. This mobility model incorporates two techniques, the concept of an artificial potential and the concept of a particle-based mobility schemes. The artificial potential field can be viewed as a landscape where the mobile devices move from a high-value state to a low-value state. Thus, the artificial potential function, which value can be viewed as energy has to be defined for each network device. It is constructed as a sum of repulsive and attractive potentials. Its value depends on Euclidean distances between a given device and all other devices in a sensing network $\mathscr{G}$ and the distance to the target position and obstacles in the workspace W. Moreover, in the concept of a particle-based mobility each network device, is considered as a self-driven moving particle, and is characterized by a sum of forces, describing its desire to move to the target position, avoiding collisions with other devices and obstacles and maintaining continuous connectivity with the network head.
In a system formed by only one mobile device or set of non-cooperating devices moving in the workspace without obstacles authors can explicitly calculate the optimal position of each device (coordinates of its reference point $\mathbf{c}^i$) – the location close to its target destination $\mathbf{c}_g^i$. In presented case study the collaboration between network devices is required to explore a gas cloud, tackle its boundary and maintain communication with a network head. Therefore, the motion trajectory of each mobile device D_i de-

pends on the positions of all sensors located in its transmission radio range, i.e. neighboring nodes from the set $S_i = \{D_j : (D_i, D_j) \in \mathscr{E}, j = 1,\ldots,N, j \neq i\}$. In the adopted mobility model to calculate a new position of the device D_i the following optimization problem has to be solved

$$\min_{\mathbf{c}^i} \left[U^i = U^i_g + \sum_{D_j \in S_i, j \neq i} U^i_j = \right.$$
$$\left. = \varepsilon_g \left(\frac{\overline{d}^i_g}{d^i_g} - 1 \right)^2 + \sum_{D_j \in S_i, j \neq i} \varepsilon_j \left(\frac{\overline{d}^i_j}{d^i_j} - 1 \right)^2 \right]. \tag{12}$$

In the above formulation the performance measure – artificial potential function U^i consists of the potential U^i_g between D_i and its target g and a sum of potentials between D_i and D_j, $j \in S_i$. $\varepsilon_g \geq 0$ and $\varepsilon_j \geq 0$ denote weighting factors determining the importance of, respectively the goal g and the device D_j. d^i_g and d^i_j are real Euclidean distances, between $\mathbf{c}^i$ and respectively, $\mathbf{c}_g$ and $\mathbf{c}_j$ after a network transformation. $\overline{d}^i_g$ and $\overline{d}^i_j$ are the reference distances between $\mathbf{c}^i$ and respectively, $\mathbf{c}_g$ and $\mathbf{c}_j$ (calculated due to a current signal strength measurement). The final network topology depends on a target point location, and the established values of the reference distances $\overline{d}^i_g$ and $\overline{d}^i_j$ and weighting factors ε_g, ε_j in Eq. (12).

4. MANET for Gas Cloud Boundary Tracking – a Design Process

The investigated computing scheme for creating a MANET for a moving heavy gas cloud estimation of a cloud size and boundary consists of three phases:

1. Working space exploration.
2. Gas cloud detection.
3. Optimal deployment of sensing devices and a gas cloud boundary tracking.

In all listed phases network devices dynamically change their positions in W, thus at each timestep t the position of each network node in W is updated. The permanent connectivity with the central operator of the system is maintained.

Phase 1 – working space exploration. In the exploration phase the aim of the performance of a team of N mobile sensors D_i, $i = 1,\ldots,N$ that create a network $\mathscr{G}$, is to search for a heavy gas cloud in W. The device D_1 denotes the head H of this network. The network head is responsible for maintaining the connectivity with the base station using, e.g. a satellite connection. Moreover, it is assumed that all other devices D_i, $i = 2,\ldots,N$ enable the continuous wireless communication with H. Thus, for each pair of nodes (D_i, H) exists at least one path composed of links from $\mathscr{E}$ in time t. These devices move and follow the node H. The displacements of all network nodes are calculated according to the mobility model (12) for $U^i_g = U^i_j$, $j = i+1$, $i = 1,\ldots,N-1$ and $\overline{d}^i_j \leq r_t$. U^i_j denotes the potential between D_i and its successor.

Phase 2 – gas cloud detection. Let us assume that the gas cloud was detected in W in a given time t by several sensors – nodes of the network $\mathscr{G}$. These sensors create a subnetwork located inside the cloud $\mathscr{G}' = (\mathscr{V}', \mathscr{E}')$ and exchange information with the network $\mathscr{G}$ head H using multi-hop connections. The messages broadcasted by nodes $D_i \in \mathscr{G}'$ contain information about their current positions in the workspace W. It is assumed that each network node is equipped with the tool for location calculation.
After collecting messages from established number of sensing devices H estimates the location of the gas cloud center $\mathbf{c}_c$ (a centroid of $\mathscr{G}'$) based on data received from $D_i \in \mathscr{G}'$.

$$\mathbf{c}_c = \frac{\sum_{D_i \in \mathscr{V}'} \mathbf{c}^i}{|\mathscr{V}'|}. \tag{13}$$

H estimates the initial reference distance to the centroid $\overline{d}_c = \max_{D_i \in \mathscr{V}'} d^i_c + w_1$, where $w_1 > 0$ denotes a distance margin and d^i_c a distance between c_c and c^i. Next, H distributes both $\mathbf{c}_c$ and $\overline{d}_c$ across the whole network $\mathscr{G}$.

Phase 3 – sensing devices optimal deployment. The aim is to surround the most of the detected gas cloud by sensors and track its boundary. In general, in presented computing schemes the construction of MANET for cloud boundary tracking is composed of following steps executed repetitively:

- data exchange between the head of MANET and all other sensing devices,
- a gas cloud centroid update,
- attraction of sensing devices inside the gas cloud,
- connectivity maintenance and redundant network nodes detection,
- optimal displacements of network nodes calculation.

All sensing devices with positions outside the gas cloud are attracted by the gas cloud centroid. They are forced to move to the region covered by the cloud. Their new positions are calculated solving the optimization problem (12) for $\mathbf{c}^i_g = \mathbf{c}_c$ and $\overline{d}^i_g = \min_{D_i \in \mathscr{V}'} \overline{d}^i_c$, $i = 1,\ldots,N$.
Next, each sensing device estimates its own position and the optimal displacements for all nodes are calculated. Two computing schemes – centralized and distributed – have been developed for calculating the optimal positions of all devices and create the optimal network topology for a given gas cloud boundary tracking.

5. Centralized Algorithm for Sensing Devices Deployment

Let us assume that the goal is to create sensing system for regular cloud boundary detecting and tracking by sensor devices equipped with the same quality radio transceivers. Authors establish as a target point in Eq. (12) the centroid of a gas cloud calculated based on preliminary cloud exploration, i.e. $\mathbf{c}_g^i = \mathbf{c}_c$, $i = 1,\ldots,N$ i provided. Furthermore, the same similar value of $\overline{d}_g^i = \overline{d}_c$ for all D_i and values of $\overline{d}_j^i$ slightly smaller than the transmission range $\overline{d}_j^i \leq r_t$, $i, j = 1,\ldots,N$ is provided.
The mobility model (12) induces all devices to move in the advisable direction to cover the region of interest by the coherent network of sensing devices. The objective is to track and estimate the boundary of the cloud, not to explore the inside of this cloud. Therefore, some modifications to the model (12) have been proposed. To surround most of the cloud authors have to elbow all devices, repulse from the centroid $\mathbf{c}_c$, and force them to move and take positions on the cloud boundary. Hence, the number of neighboring nodes for i-th device (a set S_i) should be reduced to two. Two neighboring nodes are enough to maintain permanent connectivity with the network head H. To create the optimal topology for cloud boundary tracking the redundant nodes have to be detected, removed from the set S_i and shifted away. The following procedure for detecting and removing redundant links has been developed. The inspirations came from [17], [38], [39]. Let us define two coverage regions for the i-th transceiver: safe (cov_s^i) and critical (cov_c^i):

- cov_s^i denotes a disc of a radius r_t^s, $r_t^s < r_t$ centered at the transmitter.
- cov_c^i denotes a set of points with distance d_j^i to $\mathbf{c}^i$ satisfying the condition $r_t^s \leq d_j^i \leq r_t$.

We assume that all nodes located in cov_c^i can be critical for maintaining connectivity with the i-th node and the special attention should be paid on the calculation of their displacements.
The information about the current status of each node is provided by the network head H. Next, the set $C_i(t)$ of critical neighbours of the i-th node every timestep t is created. The network head H removes the link (i, j) from $\mathscr{E}(t)$ and creates a new graph $\mathscr{G}^*$. Next, the laplacian matrix L^* is determined:

$$L^* = \Delta^* - A^*, \tag{14}$$

where $A^* = (a_{ij}^*)$ denotes the adjacency matrix of the graph $\mathscr{G}^*$. $a_{ij}^* = 1$ if $(D_i, D_j) \in \mathscr{E}^*$ and 0 otherwise, $\Delta^* = diag(\sum_{j=1}^{n} a_{ij}^*)$. The eigenvalues λ_i^* of the matrix L^* are calculated and sorted in ascending order

$$\lambda_1^* \leq \lambda_2^* \leq \ldots \leq \lambda_N^*. \tag{15}$$

Due to [17] the graph $\mathscr{G}^*(t)$ is connected for $\lambda_2^* \geq 0$. It means that the node j-th does not influence the connectivity – it is redundant and can be removed from the set $S_i(t)$. Otherwise, the j-th node is critical and can not be removed from the set C_i. To preserve connectivity all devices $D_j \in C_i \neq \emptyset$, $j = 1,\ldots,N$ are attracted to D_i. They are forced to move and take position in the region cov_s^i.
Finally, each device computes its new position in the workspace W. Depending on the position of the node two phases are distinguished. In case of $D_j \in C_i$ the node D_j is the critical one for connectivity maintenance, and is attracted to D_i. New position of the j-th node is calculated solving the optimization problem (12) for $U^j = \sum_{D_m \in C_j, m \neq j} U_m^j$.
After moving all critical nodes to the safe regions and ensuring the network connectivity new positions of all nodes are calculated to detect and track the boundary of the cloud.

6. Distributed Algorithm for Sensing Devices Deployment

In centralized deployment all calculations are performed by the network head H based on data gathered from all other network nodes. The main drawback of such computing

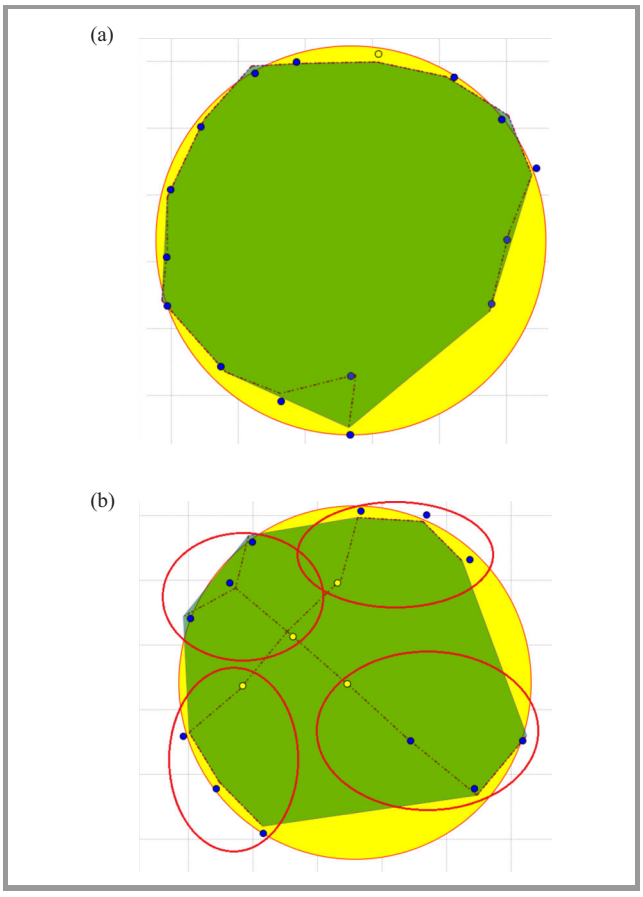


Fig. 1. Sensing network topologies: (a) centralized deployment, (b) distributed deployment, $k = 4$. (See color pictures online at www.nit.eu/publications/journal-jtit)

scheme is a significant amount of messages that have to be exchanged among all devices (nodes' positions, updated $\mathbf{c}_c$ and $\overline{d}_c$, connectivity messages, etc.). Furthermore, it is impossible to surround a large gas cloud by limited number of devices with low quality transceivers. Nodes tend to create *half ring* topology (Fig. 1a), which causes unbalanced communication load – the closer the head H the node is, the more messages has to relay. The solution is a network composed of heterogeneous devices and division of a set of devices $\mathscr{V}$ into K separated clusters of devices:

$$\mathscr{V}_1 \cup \mathscr{V}_2 \cup \ldots \cup \mathscr{V}_K = \mathscr{V} \tag{16}$$

$$\mathscr{V}_1 \cap \mathscr{V}_2 \cap \ldots \cap \mathscr{V}_K = \emptyset \tag{17}$$

In each cluster $\mathscr{V}_k$, $k = 1, \ldots, K$ a device equipped with the most powerful transceiver is nominated for a cluster head $H_k \in \mathscr{V}_k$. The network head H belongs to this group. Only cluster heads are responsible for maintaining a permanent connectivity with H. Devices from the cluster $\mathscr{V}_k$ create a sensing subnetwork $\mathscr{G}_k$. Thus, to maintain the connectivity within a network the following requirements have to be satisfied:

- a permanent connectivity inside each subnetwork $\mathscr{G}_k$ has to be maintained,
- a permanent connectivity between all cluster heads has to be maintained.

Each device repetitively calculates its new position in the workspace W. The following optimization problem, that is a modified version of the problem (12), is solved by the i-th device that is a member of the mth cluster, $D_i \in \mathscr{V}_m$:

$$\begin{aligned} \min_{\mathbf{c}^i} \Bigg[U^i &= U^i_g + \sum_{D_j \in S_i, D_j \in \mathscr{V}_m} U^i_j + \sum_{k \in IC_m} U^i_k \\ &= \varepsilon_g \left(\frac{\overline{d}^i_g}{d^i_g} - 1 \right)^2 + \sum_{D_j \in S_i, D_j \in \mathscr{V}_m} \varepsilon_j \left(\frac{\overline{d}^i_j}{d^i_j} - 1 \right)^2 \\ &\quad + \sum_{k \in IC_m} \varepsilon_k \left(\frac{\overline{d}^i_k}{d^i_k} - 1 \right)^2 \Bigg], \end{aligned} \tag{18}$$

where IC_m is a set of indexes of two closest neighboring clusters of m-th cluster that contains D_i, defined as:

$$IC_m = \left\{ \arg\min_{\mathscr{V}_j \neq \mathscr{V}_m} \sphericalangle(\mathscr{V}_m, \mathscr{V}_j) \right\} \cup \left\{ \arg\max_{\mathscr{V}_j \neq \mathscr{V}_m} \sphericalangle(\mathscr{V}_m, \mathscr{V}_j) \right\} \tag{19}$$

$$\sphericalangle(\mathscr{V}_m, \mathscr{V}_j) = \begin{cases} \arccos \frac{\overrightarrow{\mathbf{c}_c\mathbf{c}_m} \cdot \overrightarrow{\mathbf{c}_c\mathbf{c}_j}}{|\mathbf{c}_c\mathbf{c}_m| \cdot |\mathbf{c}_c\mathbf{c}_j|} & \overrightarrow{\mathbf{c}_c\mathbf{c}_m} \times \overrightarrow{\mathbf{c}_c\mathbf{c}_j} \geq 0 \\ 2\Pi - \arccos \frac{\overrightarrow{\mathbf{c}_c\mathbf{c}_m} \cdot \overrightarrow{\mathbf{c}_c\mathbf{c}_j}}{|\mathbf{c}_c\mathbf{c}_m| \cdot |\mathbf{c}_c\mathbf{c}_j|} & \overrightarrow{\mathbf{c}_c\mathbf{c}_m} \times \overrightarrow{\mathbf{c}_c\mathbf{c}_j} < 0 \end{cases} \tag{20}$$

$$\mathbf{c}_m = \frac{\sum_{D_i \in \mathscr{V}_m} \mathbf{c}^i}{|\mathscr{V}_m|}. \tag{21}$$

The idea of selecting the closest clusters is illustrated in Fig. 2. In the presented example D_i belongs to the cluster $\mathscr{V}_4$. The set IC_m contains indexes of clusters $\mathscr{V}_1$ and $\mathscr{V}_3$.

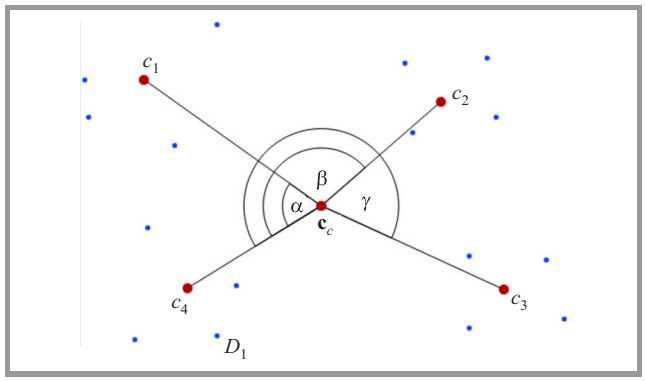


Fig. 2. Illustration of two closest clusters selection; angles to be considered in Eq. (19): $\sphericalangle(\mathscr{V}_4, \mathscr{V}_1) = \alpha$, $\sphericalangle(\mathscr{V}_4, \mathscr{V}_2) = \beta$, $\sphericalangle(\mathscr{V}_4, \mathscr{V}_3) = \gamma$.

Node D_i will be forced to move to such position in which the distance to centroids of clusters $\mathscr{V}_1$ (point $\mathbf{c}_1$) and $\mathscr{V}_3$ (point $\mathbf{c}_3$) are similar. Hence, D_i will be repulsed from the centroid of the closer cluster ($\mathscr{V}_1$) and will be attracted by the further cluster ($\mathscr{V}_3$).

To ensure even distribution of clusters the distance $\overline{d}^i_m$ is defined as an average distance between two clusters with indexes from IC_m increased by a distance margin w_2 (slightly greater than 0)

$$\overline{d}^i_m = \frac{\sum_{k \in IC_m} \overline{d}^i_k}{2} + w_2, \qquad w > 0, \tag{22}$$

where $\overline{d}^i_k$ is the real Euclidean distance between $\mathbf{c}^i$ and $\mathbf{c}_k$.

Figure 1a shows a network topology created according to centralized computing scheme. The results of distributed computing scheme, i.e. four clusters with ring-marked cluster heads are presented in Fig. 1b. It can be observed that in topologies created according to the distributed strategy the cluster heads are located inside the cloud serving as higher-level communication layer.

7. Case Study Results and Performance Evaluation

A numerous simulation experiments were conducted in order to present the efficiency of proposed approaches for design of MANET for detecting and boundary tracking of heavy gas cloud. All experiments were performed using the MobAsim framework for mobile ad hoc networks simulation described in [13].

7.1. Simulation Scenarios

The following emergency situation was simulated. A tank crash caused an instantaneous release of chlorine gas and environmental damage. The goal was to detect, surround and suppress a chlorine gas cloud. The emergency team

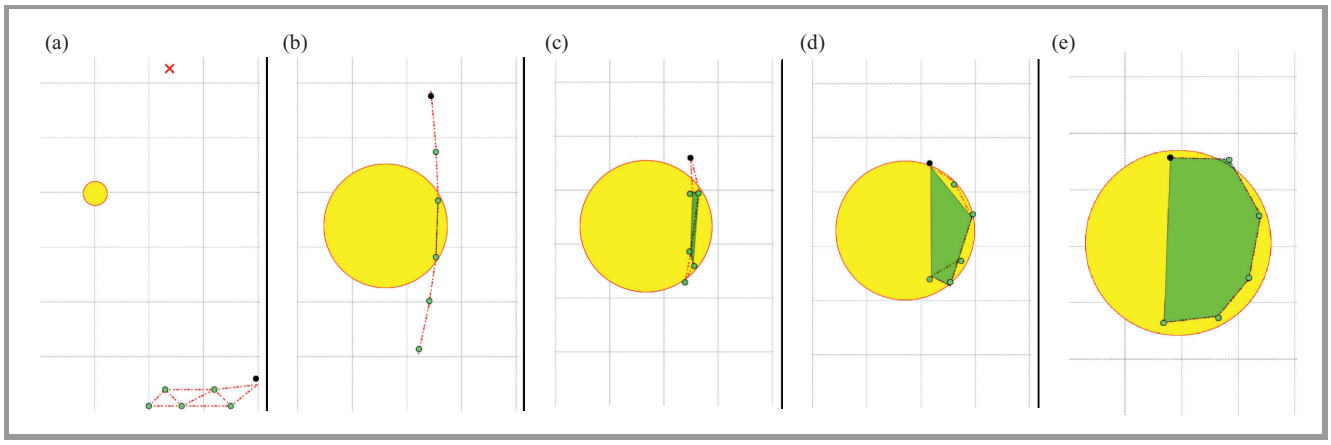


Fig. 3. Initial, temporal and final topologies of the MANET for heavy gas cloud boundary tracking.

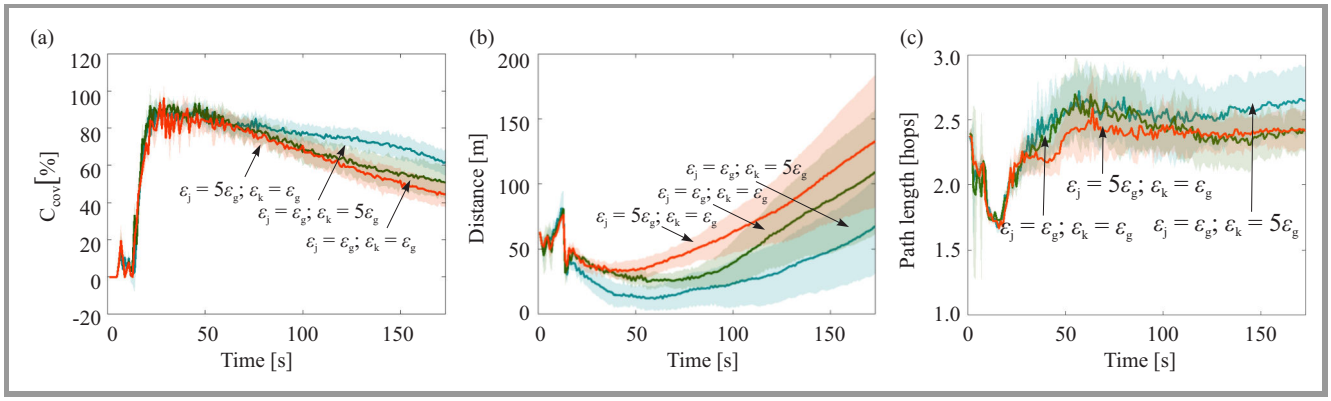


Fig. 4. Quality of network topologies for various values of parameters ε_j and ε_k: (a) average coverage rate, (b) distance between estimated and real centroid of a cloud, (c) average path between a node and a network head.

comprised of self-organized wireless mobile devices carrying punctual gas sensors was employed to perform this task.

Various topologies of sensing networks created using centralized and decentralized strategies were evaluated and compared according to the following criteria:

1. The percent of a gas cloud coverage by a given MANET
$$C_{cov} = \frac{cov_{\mathscr{G}}}{cov_{GC}} \cdot 100\%, \tag{23}$$
where C_{cov} is the percent of a surface of a gas cloud detected by MANET, cov_{GC} denotes a real surface of the gas cloud, $cov_{\mathscr{G}}$ an area of a polygon with boundary discovered by all sensing devices (the network $\mathscr{G}$);
2. The distance between the centroid of detected cloud $\mathbf{c}_c$ and the centroid of the real cloud $\overline{\mathbf{c}}_c$;
3. The average path length between each node and a network head H.

7.2. Illustration of the Deployment Process

The steps of sensing network comprised of six devices creation process are illustrated in Fig. 3a-e. The initial topology and the location of released gas cloud are presented in Fig. 3a. The black node represents the head of a network. In the exploration phase the head was forced to the randomly selected direction, while other nodes followed him. After detecting the gas cloud (Fig. 3b) all nodes located outside the cloud were forced to move inside the cloud. They were attracted by the estimated centroid of the cloud. The preliminary sensing topology was created (Fig. 3d). Finally, the devices self-organized themselves to cover the most of the boundary of the cloud and were tracking this boundary. The final topology is presented in Fig. 3e.

7.3. Distributed and Centralized Deployment

In the first series of experiments the distributed scheme was applied to generate sensing network topology. The goal was to tune the number of clusters and parameters ε_g, ε_j, ε_k in (18). The set of devices was divided into four groups ($k = 4$) and ε_g was set to 1000. The topologies for various values of ε_j and ε_k were compared. The results are presented in Fig. 4. It can be seen that the best results were obtained for $\varepsilon_k > \varepsilon_j$. The exemplary final topologies are depicted in Fig. 5.

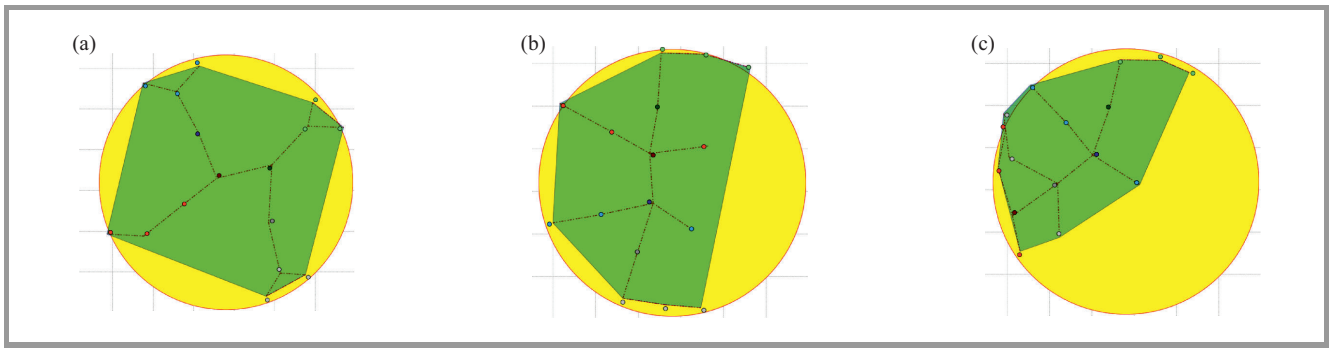


Fig. 5. MANET topologies ($t = 180$, $K = 4$) for various values of parameters: (a) $\varepsilon_j = \varepsilon_g$ and $\varepsilon_k = 5\varepsilon_g$, (b) $\varepsilon_j = \varepsilon_g$ and $\varepsilon_k = \varepsilon_g$, (c) $\varepsilon_j = 5\varepsilon_g$ and $\varepsilon_k = \varepsilon_g$.

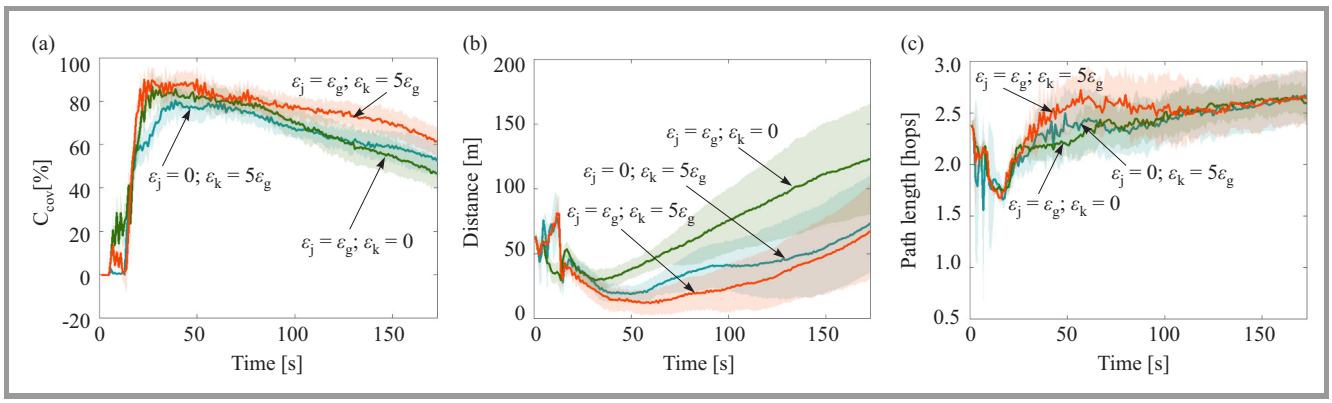


Fig. 6. Quality of network topologies for various values of parameters ε_j and ε_k: (a) average coverage rate, (b) distance between estimated and real centroid of a cloud, (c) average path between a node and a network head.

Then, two series of experiments for $\varepsilon_j = 0$, $j = 1,\ldots,|\mathcal{V}_k|$ and $\varepsilon_k = 0$, $k = 1,\ldots,K$ were conducted, respectively. The results are presented in Fig. 6. In general, it was observed that the accuracy of the cloud centroid detection was much better when interactions between clusters were taken into account in calculation process, i.e. $\varepsilon_k > 0$. Moreover, repulsion within a cluster (i.e. $\varepsilon_j > 0$) increased network coverage. Exemplary final topologies calculated for $\varepsilon_j = 0$ or $\varepsilon_k = 0$ are presented in Fig. 7.

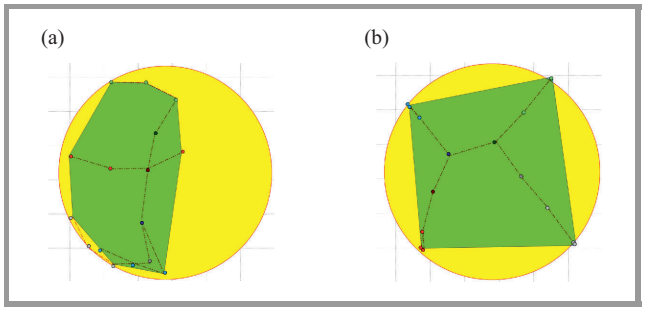


Fig. 7. MANET topologies ($t = 180$, $K = 4$) for various values of parameters: (a) $\varepsilon_j = \varepsilon_g$ and $\varepsilon_k = 0$, (b) $\varepsilon_j = 0$ and $\varepsilon_k = 5\varepsilon_g$.

Next, the influence of number of clusters on the efficiency of sensing network system was tested. The results for various number of clusters are presented in Fig. 8. Comparison of topologies generated for different values of K are shown in Fig. 9. In general, the simulation results confirm the assumption that the number of clusters should be tuned to the total number of sensing devices. In case of small set of devices the number of clusters should be limited.

Finally, the distributed deployment strategy was compared with the centralized one. Figure 10 presents values of criteria defined in Subsection 7.1 obtained for both approaches. The application of distributed algorithm significantly shortened the average path length between nodes and network head. It should be pointed that the shorter path length and the aggregation of transmitted data by cluster heads reduce the communication cost. The final coverage of a gas cloud was similar both in centralized and distributed computing schemes.

8. Summary and Conclusions

Modern sensing systems can be created by sensors mounted on mobile platforms, i.e., unmanned vehicles, mobile robots or drones, moved to desirable positions. It is obvious that mobility implies an additional complexity layer. However, the complexity of sensing systems design, implementation

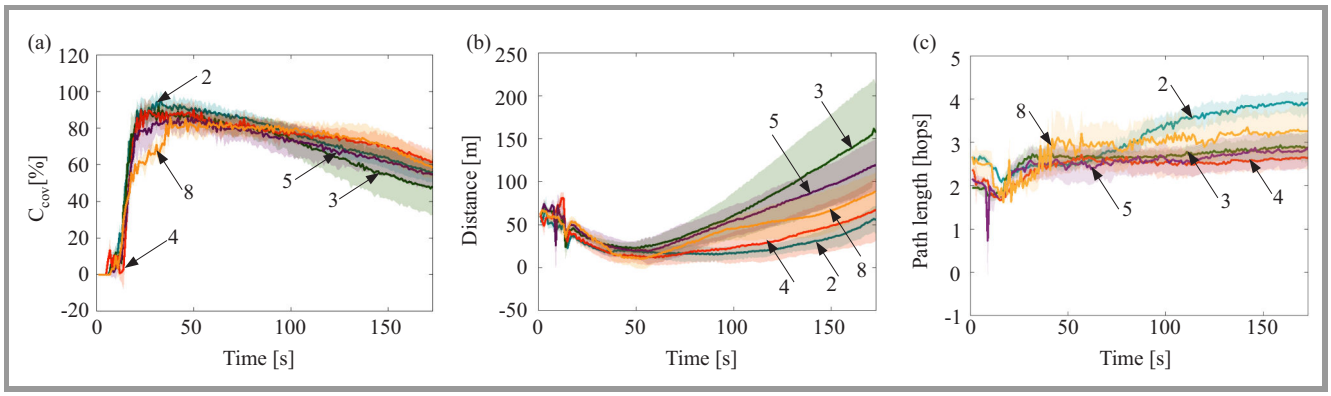


Fig. 8. Quality of network topologies for various number of clusters, $\varepsilon_j = \varepsilon_g$ and $\varepsilon_k = 5\varepsilon_g$: (a) average coverage rate, (b) distance between estimated and real centroid of a cloud, (c) average path between a node and a network head.

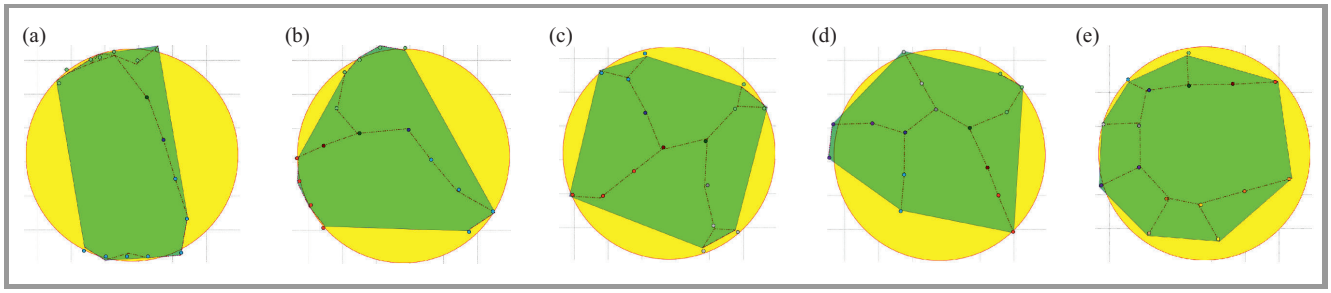


Fig. 9. MANET topologies ($t = 180$) for various number of clusters: (a) $K = 2$, (b) $K = 3$, (c) $K = 4$, (d) $K = 5$ and (e) $K = 8$.

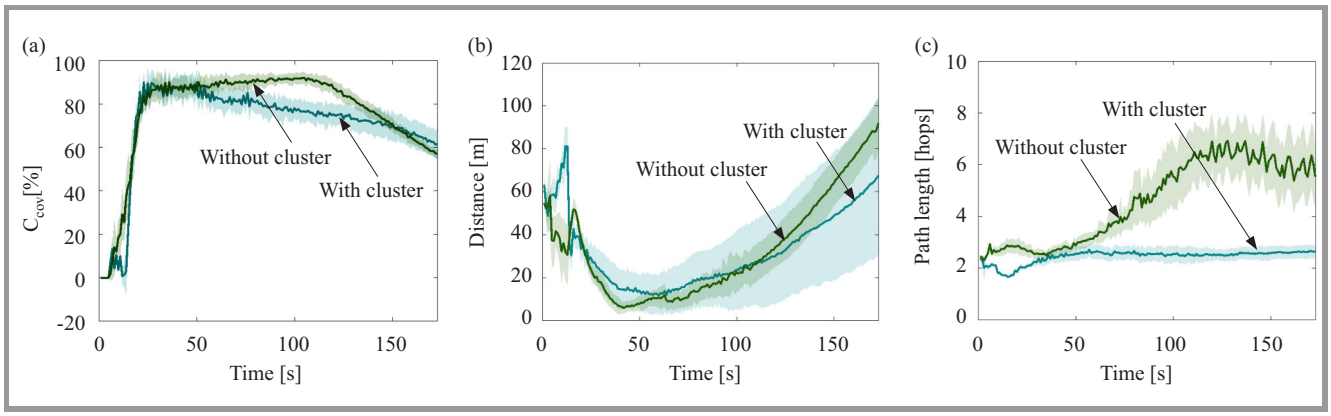


Fig. 10. Comparison of centralized and distributed deployment strategies.

and management is compensated by a number of benefits. Endowing network nodes with mobility drastically expands sensing networks capabilities. Mobility allows to detect lacks of deployment objectives, improve coverage and communication connectivity even decreasing number of employed sensing devices. A large number of measurement targets can be handled with smaller number of migrating sensors.

In this paper two computing schemes for construction of mobile sensing system for heavy gas cloud detection and boundary tracking are described. These schemes utilize centralized and distributed strategies for calculating the desired positions of all sensing devices in a region of interest. Both developed algorithms were implemented in the simulation platform and verified through extensive simulation experiments. The presented case study shows that presented algorithms can be successfully used to design self-configuring and coherent networks for monitoring and tracking purposes. Moreover, the efficiency of monitoring can be increased by enabling clustering methods.

References

[1] R. Jones, B. Wills, and C. Kang, "Chlorine gas: An evolving hazardous material threat and unconventional weapon", *Western J. of Emerg. Medicine: Integrat. Emerg. Care with Population Health*, vol. 11, no. 2, pp. 151–156, 2010.

[2] C. C. Yockey, B. M. Eden, and R. B. Byrd, "The McConnell missile accident. Clinical spectrum of nitrogen dioxide exposure", *JAMA*, vol. 244, no. 11, pp. 1221–1223, 1980.

[3] N. B. Charan, C. G. Myers, S. Lakshminarayan, and T. M. Spencer, "Pulmonary injuries associated with acute sulfur dioxide inhalation", *Am. Rev. Respir. Dis.*, vol. 119, no. 4, pp. 555–560, 1979.

[4] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, *Mobile Ad Hoc Networking*. Wiley, 2004.

[5] M. T. Thai, R. Tiwari, R. Bose, and A. Helal, "On detection and tracking of variant phenomena clouds", *ACM Trans. Sen. Netw.*, vol. 10, no. 2, pp. 34:1–34:33, 2014.

[6] K. Jung-Hwan, K. Kee-Bum, H. C. Sajjad, C. Min-Woo, and P. Myong-Soon, "Energy-efficient tracking of continuous objects in wireless sensor networks", in *Ubiquitous Intelligence and Computing*, H. Jin, L. T. Yang, and J. J.-P. Tsai, Eds. Springer, 2008, pp. 323–337.

[7] S. Duttagupta, K. Ramamritham, and P. Ramanathan, "Distributed boundary estimation using sensor networks", in *Proc. IEEE Int. Conf. Mob. Adhoc & Sensor Syst. MASS 2006*, Vancouver, Canada, 2006, pp. 316–325.

[8] H. Hong, J. Lee S. Oh, and S. H. Kim, "A chaining selective wakeup strategy for a robust continuous object tracking in practical wireless sensor networks", in *Proc. 27th IEEE Int. Conf. Adv. Inform. Netw. & Appl AINA 2013*, Barcelona, Spain, 2013, pp. 333–339.

[9] T. Aurisch and J. Tölle, "Relay placement for ad-hoc networks in crisis and emergency scenarios", in *Proc. Inform. Systems and Technology Panel Symposium IST-091*, Bucharest, Romania, 2009, vol. 11.

[10] G. Y. Keung, Q. Zhang B. Li, and H. D. Yang, "The target tracking in mobile sensor networks", in *Proc. Global Telecommun. Conf. GLOBECOM 2011*, Houston, TX, USA, 2011, pp. 1–5.

[11] E. Niewiadomska-Szynkiewicz and A. Sikora, "Simulation-based evaluation of robot-assisted wireless sensors positioning", in *Progress in Automation, Robotics and Measuring Techniques*, R. Szewczyk, C. Zieliński, and M. Kaliczyńska, Eds. Springer, 2015, pp. 181–190.

[12] R. R. Roy, *Handbook of Mobile Ad Hoc Networks for Mobility Models*. Springer Science & Business Media, 2010.

[13] E. Niewiadomska-Szynkiewicz, A. Sikora, and J. Kołodziej, "Modeling mobility in cooperative ad hoc networks", *Mob. Netw. and Appl.*, vol. 18, no. 5, pp. 610–621, 2013.

[14] T. Facchinetti, G. Franchino, and G. Buttazzo, "A distributed coordination protocol for the connectivity maintenance in a network of mobile units", in *Proc. 2nd Int. Conf. Sensor Technol. & Appl. SENSORCOMM'08*, Cap Esterel, France, 2008, pp. 764–769.

[15] Z. Kan, L. Navaravong, J. M. Shea, E. L. Pasiliao, and W. E. Dixon, "Graph matching-based formation reconfiguration of networked agents with connectivity maintenance", *IEEE Trans. Control Netw. Syst.*, vol. 2, no. 1, pp. 24–35, 2015.

[16] R. K. Williams and G. S. Sukhatme, "Constrained interaction and coordination in proximity-limited multiagent systems", *IEEE Trans. on Robot.*, vol. 29, no 4, pp. 930–944, 2013.

[17] N. Michael, M. M. Zavlanos, V. Kumar, and G. J Pappas, "Maintaining connectivity in mobile robot networks", in *Experimental Robotics*, O. Khatib, V. Kumar, and G. Pappas, Eds. Springer, 2009, pp. 117–126.

[18] A. Konak, G. E. Buchert, and J. Juro, "A flocking-based approach to maintain connectivity in mobile wireless ad hoc networks", *Appl. Soft Comput.*, vol. 13, no. 2, pp. 1284–1291, 2013.

[19] S. Hauert, L. Winkler, J. C. Zufferey, and D. Floreano, "Ant-based swarming with positionless micro air vehicles for communication relay", *Swarm Intelligence*, vol. 2, no. 2–4, pp. 167–188, 2008.

[20] R. Lin, Z. Wang, and Y. Sun, "Wireless sensor networks solutions for real time monitoring of nuclear power plant", in *Proc. 5th World Congr. Intell. Control & Autom. WCICA 2004*, Hangzhou, China, 2004, vol. 4.

[21] A. Vasiliou and A. A. Economides, "MANETs for environmental monitoring", in *Proc. Int. Telecommun. Symp. ITS 2006*, Fortaleza, Ceara, Brazil, 2006, pp. 813–818.

[22] T. P. Lambrou and C. G. Panayiotou, "Collaborative event detection using mobile and stationary nodes in sensor networks", in *Proc. 3rd Int. Conf. Collabor. Comput.: Networking, Applications & Worksharing CollaborateCom 2007*, New York, NY, USA, 2007, pp. 106–115.

[23] K. Young-Duk, Y. Yeon-Mo, K. Won-Seok, and K. Dong-Kyun, "On the design of beacon based wireless sensor network for agricultural emergency monitoring systems", *Comp. Stand. & Interf.*, vol. 36, no. 2, pp. 288–299, 2014.

[24] Y.-N. Lien, H.-C. Jang, and T.-C. Tsai, "A MANET based emergency communication and information system for catastrophic natural disasters", in *Proc. 29th IEEE Int. Conf. Distrib. Comput. Syst. Worksh. ICDCS Workshops'09*, Montreal, Canada, 2009, pp. 412–417.

[25] Y.-N. Lien, L.-C. Chi, and C.-C. Huang, "A multi-hop walkie-talkie-like emergency communication system for catastrophic natural disasters", in *Proc. 39th Int. Conf. Parallel Process. Worksh. ICPPW 2010*, San Diego, CA, USA, 2010, pp. 527–532.

[26] M. Aloqaily, S. Otoum, and H. T. Mouftah, "A novel communication system for firefighters using audio/video conferencing/subconferencing in standalone manets", in *Proc. 5th Int. Conf. Comp. Sci. & Inform. Technol. CSIT 2013*, Amman, Jordan, 2013, pp. 89–98.

[27] J. C. Kim *et al.*, "Implementation and performance evaluation of mobile ad hoc network for emergency telemedicine system in disaster areas", in *Proc. Annual Int. Conf. IEEE Engin. in Medicine & Biology EMBC 2009*, Minneapolist, MN, USA, 2009, pp. 1663–1666.

[28] E. Kulla, R. Ozaki, A. Uejima, H. Shimada, K. Katayama, and N. Nishihara, "Real world emergency scenario using MANET in indoor environment: Experimental data", in *Proc. 9th Int. Conf. on Complex, Intell., & Softw. Intensive Syst. CISIS 2015*, Blumenau, Brazil, 2015, pp. 336–341.

[29] Z. Jin and A. L. Bertozzi, "Environmental boundary tracking and estimation using multiple autonomous vehicles", in *Proc. 46th IEEE Conf. Decision & Control*, New Orleans, LA, USA, 2007, pp. 4918–4923.

[30] D. Marthaler and A. L. Bertozzi, "Collective motion algorithms for determining environmental boundaries", in *SIAM Conf. on Applications of Dynamical Systems*, Snowbird, UT, USA, 2003.

[31] I. Triandaf and I. B. Schwartz, "A collective motion algorithm for tracking time-dependent boundaries", *Mathem. & Comp. in Simulation*, vol. 70, no. 4, pp. 187–202, 2005.

[32] S. Srinivasan, "Contour estimation using collaborating mobile sensors", in *Proc. Worksh. Dependability Issues in Wirel. Ad Hoc Netw. & Sensor Netw. DIWANS'06*, Los Angeles, CA, USA, 2006, pp. 73–82.

[33] T. S. Rappaport, *Wireless Communications – Principles and Practice*, 2nd ed. Prentice Hall, 2001.

[34] M. T. Markiewicz, "Mathematical modeling of heavy gas atmospheric dispersion over complex and obstructed terrain", *Archiv. of Environm. Protect.*, vol. 36, no, 1, pp. 81–94, 2010.

[35] M. Nielsen, "Dense gas dispersion in the atmosphere", Tech. Rep. Risø-R-1030(EN), Risø National Laboratory, Roskilde, Denmark, Sept. 1998.

[36] H. W. M. Witlox, "The HEGADAS model for ground-level heavy-gas dispersion-I. Steady-state model", *Atmospheric Environ.*, vol. 28, no. 18, pp. 2917–2932, 1994.

[37] R. E. Britter and J. E. Simpson, "Experiments on the dynamics of a gravity current head", *J. Fluid Mechan.*, vol. 88, no. 2, pp. 223–240, 1978.

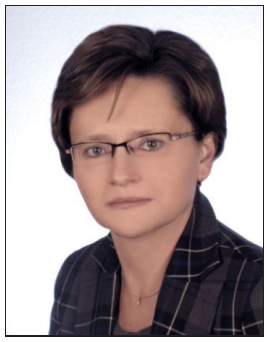
[38] S. S. Ponda, L. B. Johnson, A. N. Kopeikin, H.-L. Choi, and J. P. How, "Distributed planning strategies to ensure network connectivity for dynamic heterogeneous teams", *IEEE J. Selec. Areas in Commun.*, vol. 30, no. 5, pp. 861–869, 2012.

[39] P. D. Hung, M. T. Pham, T. Q. Vinh, and T. D. Ngo, "Self-deployment strategy for a swarm of robots with global network preservation to assist rescuers in hazardous environments", in *Proc. IEEE Int. Conf. Robot. & Biomimetics ROBIO 2014*, Bali, Indonesia, 2014, pp. 2655–2660.

Mateusz Krzysztoń received M.Sc. in Computer Science from the Cracow University of Science and Technology (2013). Currently he is a Ph.D. student at the Warsaw University of Technology. Since 2016 with Research and Academic Computer Network (NASK). The author and co-author of several conference papers. His research area focuses on mobile ad hoc networks, decision support systems and machine learning.

E-mail: mateusz.krzyszton@gmail.com
Institute of Control and Computation Engineering
Warsaw University of Technology
Nowowiejska st 15/19, 00-665 Warsaw, Poland

E-mail: mateuszkr@nask.pl
Research and Academic Computer Network (NASK)
Kolska st 12
01-045 Warsaw, Poland



Ewa Niewiadomska-Szynkiewicz received her D.Sc. in 2005 and Ph.D. in 1995. She is a Professor of control and computer engineering at the Warsaw University of Technology and head of the Complex Systems Group. She is also the Director for Research of Research and Academic Computer Network (NASK). The author and co-author of three books and over 160 journal and conference papers. Her research interests focus on complex systems modeling, optimization and control, computer simulation, parallel computation, computer networks and ad hoc networks. She was involved in a number of research projects including EU projects, coordinated the Groups activities, managed organization of a number of national-level and international conferences.

E-mail: ens@ia.pw.edu.pl
Institute of Control and Computation Engineering
Warsaw University of Technology
Nowowiejska st 15/19
00-665 Warsaw, Poland

E-mail: ewan@nask.pl
Research and Academic Computer Network (NASK)
Kolska st 12
01-045 Warsaw, Poland

Paper

Variable-Weight Optical Code Division Multiple Access System using Different Detection Schemes

Saleh Seyedzadeh[1], Majid Moghaddasi[2], and Siti B. A. Anas[2]

[1] *Integrated Lightwave Research Group, Department of Electrical Engineering, University of Malaysia, Kuala Lumpur, Malaysia*
[2] *Wireless and Photonics Research Center of Excellence, Department of Computer and Communication Systems Engineering, University Putra Malaysia, UPM Serdang, Malaysia*

Abstract—In this paper a Variable Weight OCDMA (VW-OCDMA) system using KS code with Direct Decoding (DD), Complementary Subtraction (CS) and AND subtraction detections is proposed. System performance is analyzed using mathematical approximation and software simulation. In mathematical analysis, the effects of Phase-Induced Intensity Noise, shot noise and thermal noise are taken into account. Bit Error Rate of different users is plotted as a function of received optical power per chip with varying the bit rates and number of active users. It has been shown that for different bit rates and number of users, system using DD has better performance than the system applying CS and AND detection. Using DD scheme, the number of active users are 100 while this value is 27 and 25 in case of using CS and AND detection, respectively, when the received optical power per chip is –10 dBm.

Keywords—AND detection, direct detection, QoS differentiation, spectral amplitude coding, variable-weight OCDMA.

1. Introduction

Recently, Optical Code Division Multiple Access (OCDMA) system has been considered for fiber optic communication as it provides asynchronous access, privacy, secure transmissions and service differentiation capability in metro network where applications such as video streaming and voice over IP require different amount of bandwidth portion [1]. In OCDMA system each user has a unique signature code, which distinguishes one user from the others. OCDMA systems have also received attention in optical sensor networks [2], [3] and free space optical communication [4].

Among the advantages of OCDMA systems, the ability to support application with various data rates and Quality of Service (QoS) requirements made it an attractive solution for metro networks as it deals with heterogeneous traffic [5]. Physical layer QoS was achievable using OCDMA by several means such as varying weight [6]–[8], length [9], [10] or both weight and length [11]. QoS differentiation with fixed weight and varying the number of existing users in matrix construction was also represented [12], [13].

Spectral Amplitude Coding (SAC) system has been considered as a candidate to provide QoS by varying the code weights for different users [14]. This is due to the fact that SAC does not require a complicated protocol or control. Wavelength components of optical pulses are encoded at the spectral encoder by obstructing or transmitting specific wavelength components in accordance of a signature code. In receiver side a sort of filters are deployed to extract the desired signal for each user. SAC was first introduced by Zaccarin and Kavehrad [15], which eliminates the Multiple Access Interference by applying the right detection techniques. Experimental demonstration of QoS differentiation using SAC-OCDMA for three different services have been recently reported [16].

Three SAC detection techniques had been developed to decode the users' data, which are Direct Decoding (DD) [17], Complementary Subtraction (CS) detection [15] and AND subtraction detection [18].

VW-SAC system is proposed in this paper and comparison of such system using three different detection techniques is presented. VW-SAC supports service differentiation by varying the wavelength components where users with higher priority are assigned higher weights in order to have lower Bit Error Rate (BER).

First VW-OCDMA system is described in detail and VW-code construction is demonstrated. Then AND subtraction, CS and DD techniques are explained in terms of their architecture and mathematical representation. Numerical analysis is proposed to calculate approximate Signal-to-Noise Ratio (SNR) and BER of users of different weights. Finally, results are presented to evaluate the performance of the proposed system based on number of active users, received optical power and bit rate.

2. System Description

The architecture of a VW-SAC OCDMA system for k number of users with code weight of w is depicted in Fig. 1. For simplification purpose, only a pair of transmitter and receiver is shown.

At the transmitter side, power from a broadband source (BBS) spectrum is split among k users. A series of fiber Bragg gratings (FBGs) filter different wavelengths of $\lambda_1, \ldots, \lambda_w$ from the spectrum to form the different signature code with weight of w.

A Mach-Zehnder modulator (MZM) is used to modulate the users' binary data, which formed as Non-Return-to-Zero

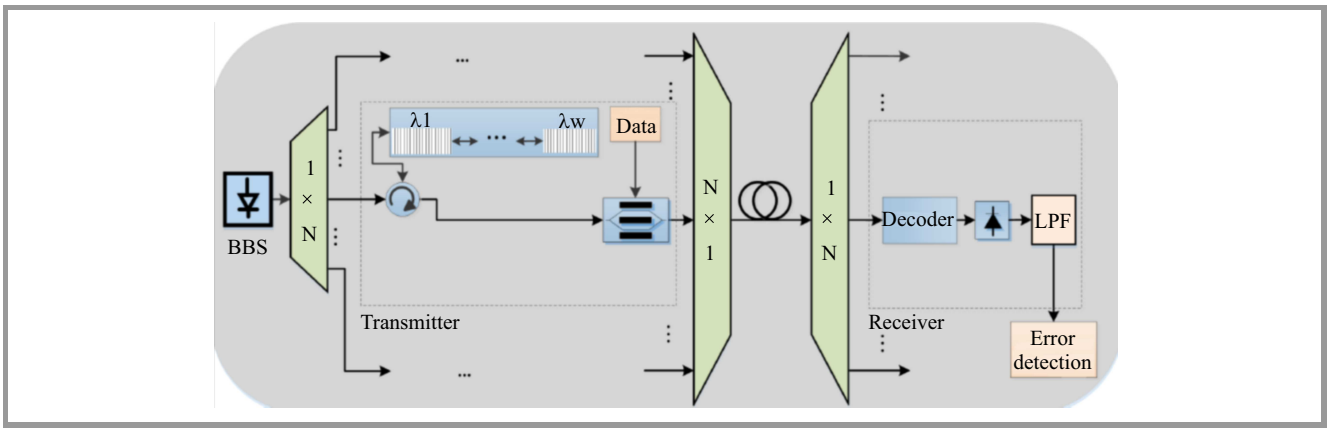


Fig. 1. Architecture of a VW-SAC OCDMA system.

(NRZ) signal to the optical carrier. Modulated signals from all users are then combined using a power combiner, and transmitted over the single mode fiber (SMF) based on ITU G652.

At the receiver part, one of the detection techniques developed for SAC-OCDMA may be applied to extract the desired data for each user. FBGs were used to filter the signals for all detection techniques. Each technique will be discussed in detail subsequently.

Among different codes developed for service differentiation in SAC-OCDMA systems are Integer Lattice OOC (IL-OOC) [6], Variable Weight Random Diagonal (VW-RD) [19] and Variable Weight code using Khazani-Syed (VW-KS) code [5]. In this analysis, VW-KS is used due to its ability to maintain a tolerable code length compared to others.

Table 1
Comparison of different variable weight codes properties

Code	No. of code weights	No. of users	Code length	$R_{\max}$
IL-OOC	4 $\{5,4,3,1\}$	49	28	7
VW-RD	4 $\{6,5,4,3\}$	50	74	5
VW-KS	4 $\{8,6,4,2\}$	50	168	1

Table 1 presents the advantages and disadvantages of VW-KS against its counterparts in terms of code design. In terms of codes performance, the evaluation in terms of mathematical analysis will be presented and elaborated in Fig. 6 of Section 5, subsequently. In this example all code families support 50 users with four different weights. IL-OOC and VW-RD has shorter code length as compared to VW-KS code, however $R_{\max}$ can reach up to 7 and 5, respectively, which might lead to poor Multiple Access Interference (MAI) cancelation. Although VW-KS has longer code length than IL-OOC and VW-RD, yet it guarantees the maximum cross-correlation of 1 between different users.

Three weights of 6, 4 and 2 are used to support QoS in VW-OCDMA system which can be referred to voice, data and video signals, respectively.

3. SAC OCDMA Detection Techniques

The detection techniques AND, CS and DD are described in detail in this section. These three techniques will then be mathematically analyzed and the results are compared.

3.1. AND Subtraction Technique

AND subtraction uses balanced detection to eliminate the effect of MAI. In this technique, two decoders are required in a single receiver, which are the upper and lower decoders. The upper decoder detects the desired code, $x(\lambda)$ while the lower decoder detects binary logical AND of desired and interfering code, $x(\lambda) \cap y(\lambda)$, with $y(\lambda)$ being the interferer signal of other codes having overlapping chip with desired user.

3.2. Complementary Subtraction Detection

Most conventional SAC systems deploy CS using balanced detection as well as AND. In this technique, the upper decoder has the same structure as the encoder at the transmitter side $x(\lambda)$, while the lower decoder is the complement of the upper decoder $\bar{x}(\lambda)$. The decoded signals are then detected by a balanced receiver, which performs MAI cancellation.

3.3. Direct Decoding Technique

DD is another subtraction technique, developed for SAC systems, where it only deploys one decoder unlike AND detection, which reduces the number of filters and receiver complexity.

DD only detects the non-overlapping code of the desired signal, which can be represented by $x(\lambda) - x(\lambda) \cap y(\lambda)$.

4. VW-Code Construction

VW-KS code will be explained as it is adopted in this research. This code was developed based on the single

weight KS code [20]. Firstly, a brief description of KS code and its construction is presented, then variable weight implementation are described in detail.

4.1. Khazani-Syed Code

KS code is based on matrix construction, where the two sub-codes $A = [110]$ and $B = [011]$ are used to construct the basic matrix. The structure of this code is causing that the cross-correlation R between each pair of different users' codes is zero or one, which results in reduction of MAI effect.
The size of basic matrix C_B for KS code $(K \times N)$ is depending on the code weight W $(W = 2,4,6,\ldots)$, where K and N are the number of users and code length respectively. Construction of basic matrix for KS code is summarized as following steps [21]:

1. Fill the first row with sub-code A until number of chips equal to W.
2. Starting from second row, diagonally fill the matrix with sub-code B until last existing column.
3. Fill the empty spaces with zeros.
4. Repeat steps 1 to 3 staring from the second user until all code sequences get their weight.

The combination of every three columns needs to be $[1\,2\,1]$ in order to be assured that the R_{xy} of one between each pair of codes will be obtained. An example of KS code construction with code weight of 4 is depicted in Fig. 2. It is seen that with code weight of 4, number of users and code length are 3 and 9 respectively.

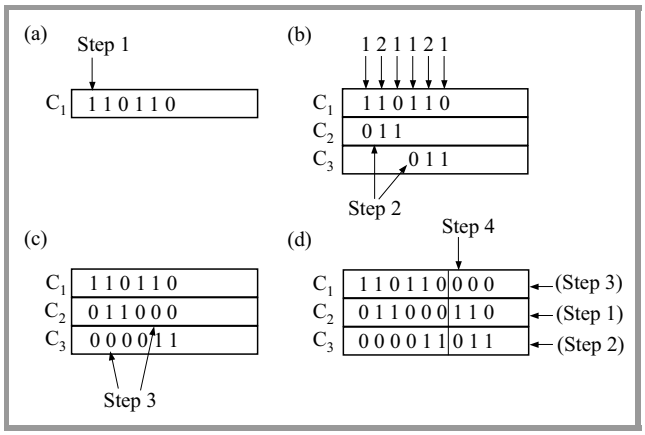


Fig. 2. Construction of KS [20].

The number of rows K_B, also known as basic number of users and number of columns N_B or basic code length are calculated by following equations:

$$K_B = \frac{W}{2} + 1 \tag{1}$$

and

$$N_B = 3\sum_{i=1}^{\frac{W}{2}} i. \tag{2}$$

Using mapping technique, a large number of users K can be obtained from basic matrix C_B. This is carried out by repeating the basic matrix diagonally by M times, where M is the mapping sequence. This increases the maximum number of users by MK_B. The new large matrix resulted from applying mapping technique is

$$C(M) = \begin{bmatrix} C_{B,1} & 0 & 0 & 0 \\ 0 & C_{B,2} & 0 & 0 \\ 0 & 0 & C_{B,3} & 0 \\ 0 & 0 & 0 & C_{B,4} \end{bmatrix},$$

where $C_{B,m}$ is C_B at the m-th mapping sequence, $m = 1,2,\ldots,M$.

Each 0 is a sequence of zeros with the same size of C_B and $C(M)$ is the code at certain mapping number, M. Mapping of the basic matrix, C_B of weight two is depicted in Fig. 3, with $M = 3$.

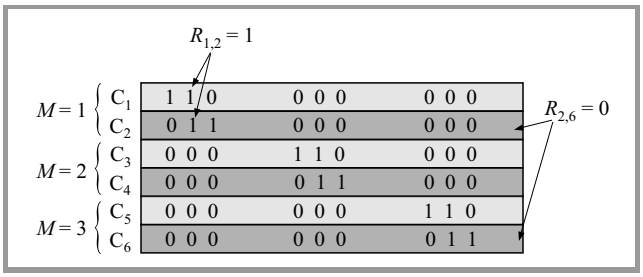


Fig. 3. Mapping process of KS code of weight 2 using $M=3$ [20].

In the mapped matrix, as shown in the Fig. 3 the cross-correlation between each pair of users within the same mapping sequence is one; in the meantime, R_{xy} between two distinct codes in different mappings is zero.
The maximum number of users, $K_{\max}$ and the corresponding code length, $N_{\max}$ obtained with mapping sequence, M can be derived as follow

$$K_{\max}(M) = M\left(\frac{W}{2}\right) \tag{3}$$

and

$$N_{\max}(M) = 3M\sum_{i=1}^{\frac{W}{2}} i \tag{4}$$

Mapping sequences, M needed for any specific number of users, $K(M)$ is given by

$$M = \left\lceil \frac{K(M)}{\frac{W}{2}} \right\rceil. \tag{5}$$

4.2. Construction of Variable Weight KS Code

A mapping technique can be used to combine users of different service requirements. In this method, codes of different weights is ordered so that the R_{xy} of one is obtained.

This method is using the mapping techniques, which was used for extension of single weight KS code. However, in the VW-code each mapping sequence is devoted for a specific weight. Hence, the number of supportable users of a specific weight should first to be determined to generate sufficient codes. These generated codes of specific weight will later be mapped together to form a set of codes with variable weights. The general form of the constructed variable weight code, C_V is given by

$$C_V = \begin{bmatrix} C_{W_1,M_1} & 0 & 0 & 0 \\ 0 & C_{W_2,M_2} & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & C_{W_J,M_J} \end{bmatrix}.$$

C_{W_j,M_j} is the specific group of codes generated from the j-th weight and mapping, and J is the number of different weights in a system with $j = 1,2,\ldots,J$. Each 0 is a sequence of zeros with the same size of C_{W_j,M_j}.

5. Mathematical Analysis of VW-OCDMA System

In mathematical analysis, the effects of Phase-Induced Intensity Noise (PIIN), shot noise and thermal noise is considered. The noise variance of a photocurrent due to the detection of an ideally unpolarized thermal light, which is generated by spontaneous emission, can be written as [22]:

$$\langle I^2 \rangle = \langle I_{shot}^2 \rangle + \langle I_{PIIN}^2 \rangle + \langle I_{thermal}^2 \rangle , \tag{6}$$

where I_{shot} denotes the shot noise, I_{PIIN} represents the PIIN and $I_{thermal}$ is the thermal noise. The coherence time of the thermal source, τ_c is given by [23]:

$$\tau_c = \frac{\int_0^\infty G^2(v)dv}{\left[\int_0^\infty G^2(v)dv\right]^2}, \tag{7}$$

where $G(v)$ is the source power spectral density (PSD). The crosstalk from adjacent optical channels is ignored as chips spacing is assumed to be sufficiently wide [24]. This method gives an upper bound for the system performance [23], means the simulation and hardware results must be better than the numerical results calculated with this method.

This analysis is made with the following assumptions:

- each power spectral component has identical spectral width,
- each user receives equal power per chip at the receiver,
- each bit stream from each user is synchronized.

The PSD of the received signals can be written as [25]:

$$r(v) = \frac{P_{sr}}{\Delta v} \sum_{k=1}^{K} d_k \sum_{i=1}^{N} c_k(i)\Pi(i) , \tag{8}$$

where P_{sr} is the effective power of source at receiver, Δv is the bandwidth of optical source, K and N are number of users and code length respectively, d_k is the information bit of k-th active user which is either "1" or "0" ($d_k \varepsilon 0,1$), $c_k(i)$ is the i-th element of the k-th KS code sequence and $\Pi(i)$ is a function defined as:

$$\begin{aligned} \Pi(i) &= u\left[v - v_0 - \frac{\Delta v}{2N}(-N+2i-2)\right] - \\ &\quad - u\left[v - v_0 - \frac{\Delta v}{2N}(-N+2i)\right] = \\ &= u\left[\frac{\Delta v}{2N}\right], \end{aligned} \tag{9}$$

and $u[v]$ is the unit step function expressed as:

$$u[v] = \begin{cases} 1, & v \geq 0 \\ 0, & v < 0 \end{cases}. \tag{10}$$

The following subsections explain and expand the analysis with respect to three different detection schemes, AND, CS and DD schemes.

5.1. AND Subtraction Detection

The VW-KS code properties for upper and lower arms of AND subtraction technique can be written as:

$$\sum_{i=1}^{N} c_k(i)c_l(i) = \begin{cases} W_k, & k = l \\ 1, & k \neq l, W_k = W_l \\ 0, & k \neq l, W_k \neq W_l \end{cases} \tag{11}$$

and

$$\sum_{i=1}^{N} c_k(i)(c_l(i) \cdot c_k(i)) = \begin{cases} W_k/2, & k = l \\ 1, & k \neq l, W_k = W_l \\ 0, & k \neq l, W_k \neq W_l \end{cases} \tag{12}$$

respectively, where W_k is the weight of k-th user. The number of users with same weight in a basic matrix, K_{B_W} is given by

$$K_{B_W} = \frac{W}{2} + 1 . \tag{13}$$

Substituting Eqs. (11) and (12) in (8) and integrating them results into the total power incident at the upper and lower photodetectors, PIN 1 and PIN 2, respectively which can be written as:

$$\begin{aligned} \int_0^\infty G_1(v)dv &= \int_0^\infty \left[\frac{P_{sr}}{\Delta v} \sum_{k=1}^{K} d_k \sum_{i=1}^{N} c_k(i)c_l(i) \times \right. \\ &\quad \left. \times \left\{ u\left[\frac{\Delta v}{N}\right] \right\} \right] \mathrm{d}v = \\ &= \frac{P_{sr}}{N} \left(W_k d_l + \sum_{\substack{k=1 \\ k \neq l}}^{K} d_k \right) \end{aligned} \tag{14}$$

and

$$\int_0^\infty G_2(v)dv = \int_0^\infty \left[\frac{P_{sr}}{\Delta v} \sum_{k=1}^{K} d_k \sum_{i=1}^{N} c_k(i)(c_l(i)\times \right. \\ \left. \times c_k(i))) \times \left\{ u\left[\frac{\Delta v}{N} \right] \right\} \right] \mathrm{d}v = \\ = \frac{P_{sr}}{N} \left(\frac{W_k}{2} d_l + \sum_{\substack{k=1 \\ k \neq l}}^{K} d_k \right). \tag{15}$$

Let I_1 and I_2 be the photocurrent at PIN 1 and PIN 2, respectively. The photocurrent I, therefore, is given by:

$$I = I_1 - I_2 = \Re \left[\int_0^\infty G_1(v) - \int_0^\infty G_2(v) \right] = \frac{\Re P_{sr} W_k}{2N_v} d_l, \tag{16}$$

where $\Re = \eta e/hv$ is the photodiode responsivity. Here η is quantum efficiency, e is the electron charge, h is Planck's constant, and v is the central frequency of optical source's spectra. k in Eq. (16) represents the desired user, with respect to the occurrence of other users of different weights. Users of different weights is denoted by $j = 1,2,\ldots,J$ where J is the total number of different weights in the system and N_v is the code length of variable weight users defined as [21]:

$$N_v = \sum_{j-1}^{J} N_{B_j} m_j, \tag{17}$$

where N_{B_j} and m_j is the number of user in basic matrix and the number of sequence with weight j.
The noise power of shot noise can be written as:

$$\left\langle I_{shot}^2 \right\rangle = 2eB(I_1 + I_2) = \\ = 2eB\Re \left(\int_0^\infty G_1(v) + \int_0^\infty G_2(v) \right) = \\ = \frac{5eB\Re P_{sr} W_k}{N_v}, \tag{18}$$

where B is half of the bit rate, which denotes the noise-equivalent electrical bandwidth of the receiver.

In order to calculate the variance of PIIN, the mean squared power of both PIN 1 and PIN 2 is first obtained by integrating $G_1^2(v)$ and $G_2^2(v)$, such as [23]:

$$\int_0^\infty G_1^2(v)dv = \int_0^\infty \left[\frac{P_{sr}}{\Delta v} \sum_{k=1}^{K} d_k \sum_{i=1}^{N} c_k(i)c_l(i) \times \right. \\ \left. \times \left\{ u\left[\frac{\Delta v}{N} \right] \right\} \right]^2 \mathrm{d}v = \\ = \frac{P_{sr}^2}{\Delta v N} \sum_{i=1}^{N} \left\{ c_l(i) \left[\sum_{k=1}^{K} d_k c_k(i) \right] \times \right. \\ \left. \times \left[\sum_{m=1}^{K} d_m c_m(i) \right] \right\} \tag{19}$$

and

$$\int_0^\infty G_2^2(v)dv = \int_0^\infty \left[\frac{P_{sr}}{\Delta v} \sum_{k=1}^{K} d_k \sum_{i=1}^{N} c_k(i)(c_l(i) \cdot c_k(i)) \times \right. \\ \left. \times \left\{ u\left[\frac{\Delta v}{N} \right] \right\} \right]^2 \mathrm{d}v = \\ = \frac{P_{sr}^2}{\Delta v N} \sum_{i=1}^{N} \left\{ c_l(i) \cdot c_k(i) \left[\sum_{k=1}^{K} d_k c_k(i) \right] \times \right. \\ \left. \times \left[\sum_{m=1}^{K} d_m c_m(i) \right] \right\}. \tag{20}$$

In VW-KS code when all users are transmitting bit 1, the code sequence c_k can be approximated as:

$$\sum_{k=1}^{K} c_k \approx \frac{1}{N_v} \sum_{j=1}^{J} K_j W_j. \tag{21}$$

Using approximation in Eq. (21), the variance of PIIN can be written as:

$$\left\langle I_{PIIN}^2 \right\rangle = B\Re \left(\int_0^\infty G_1^2(v) + \int_0^\infty G_2^2(v) \right) \cong \\ \cong \frac{5B\Re P_{sr}^2 W_k}{2\Delta v N_v^2} \sum_{j=1}^{J} K_j W_j. \tag{22}$$

The thermal noise is given as:

$$\left\langle I_{thermal}^2 \right\rangle = \frac{4K_b T_n B}{R_L}, \tag{23}$$

where K_b is Boltzmann's constant, T_n is received noise temperature and R_L represents the receiver load resistor.

Noting that the probability of sending bit 1 at any time for each user is $\frac{1}{2}$, the SNR of the VW-KS system deploying AND technique for users with weight k can be expressed as:

$$SNR_k = \frac{(I_1 - I_2)^2}{\langle I^2 \rangle} = \\ = \frac{\frac{\Re^2 P_{sr}^2 W_k^2}{4N_v^2}}{\frac{5eB\Re P_{sr} W_k}{N_v} + \frac{5B\Re P_{sr}^2 W_k}{4\Delta v N_v^2} \sum_{j=1}^{J} K_j W_j + \frac{4K_b T_n B}{R_L}}. \tag{24}$$

Therefore, using Gaussian approximation, the BER of users with weight k for a multiple weight system is given by

$$P_{e_k} = \frac{1}{2} erfc \left(\sqrt{\frac{SNR}{8}} \right). \tag{25}$$

5.2. Complementary Subtraction Detection

The correlation properties of the VW-KS code based on CS detection scheme users can be written as:

$$\sum_{i=1}^{N} c_k(i)c_l(i) = \begin{cases} W_k, & k = l \\ 1, & k \neq l, W_k = W_l \\ 0, & k \neq l, W_k \neq W_l \end{cases} \tag{26}$$

and

$$\sum_{i=1}^{N} c_k(i)\bar{c}_l(i) = \begin{cases} 0, & k=l \\ W_k-1, & k\neq l, W_k = W_l \\ W_l, & k\neq l, W_k \neq W_l \end{cases}. \tag{27}$$

In order to achieve proper cancelation of MAI, the complement cross-correlation $\sum_{i=1}^{N} c_k(i)\bar{c}_l(i)$ is needed to be multiplied by $1/W_k - 1$. This is because weight of the complement signal (27) is $1/W_k - 1$ times of the actual signal (26) when c_k is different with c_l.

Therefore, the subtraction can be written as:

$$\begin{aligned} \sum_{i=1}^{N} c_k(i)c_l(i) - \frac{1}{W_k-1}\sum_{i=1}^{N} c_k(i)\bar{c}_l(i) = \\ = \begin{cases} W_k, & k=l \\ 0, & k\neq l, W_k = W_l \\ 0, & k\neq l, W_k \neq W_l \end{cases}. \end{aligned} \tag{28}$$

Equation (28) shows that a strong autocorrelation of the intended user's code weight W_k is obtained. The MAI is also eliminated as the weight zero is attained when the code sequences is unmatched.

The total power incident at the upper photodetector PIN 1 is calculated in (14). PIN 2 can be derived by substituting Eq. (27) in Eq. (8) as

$$\begin{aligned} \int_0^{\infty} G_2(v)dv = \int_0^{\infty}\left[\frac{1}{W_k-1}\frac{P_{sr}}{\Delta v}\sum_{k=1}^{K} d_k \sum_{i=1}^{N} c_k(i)\times\right. \\ \left.\times\big(c_l(i)\cdot c_k(i)\big)\left\{u\left[\frac{\Delta v}{N}\right]\right\}\right]\mathrm{d}v = \frac{P_{sr}}{N}\left(\sum_{\substack{k=1\\k\neq l}}^{K} d_k\right). \end{aligned} \tag{29}$$

Let I_1 and I_2 be the photocurrent at PIN 1 and PIN 2, respectively. Therefore, the photocurrent I is given by:

$$\begin{aligned} I = I_1 - I_2 = \Re\left[\int_0^{\infty} G_1(v) - \int_0^{\infty} G_2(v)\right] = \\ = \frac{\Re P_{sr} W_k}{N_v} d_l. \end{aligned} \tag{30}$$

The variance of shot noise in the photocurrent can be calculated as:

$$\begin{aligned} \left\langle I_{shot}^2 \right\rangle = 2eB(I_1+I_2) = \\ = 2eB\Re\left(\int_0^{\infty} G_1(v) + \int_0^{\infty} G_2(v)\right) = \\ = \frac{4eB\Re P_{sr} W_k}{N_v}. \end{aligned} \tag{31}$$

The mean squared power of PIN 1 is obtained in Eq. (19) and the mean squared power of PIN 2 is calculated by integrating $G_2^2(v)$:

$$\begin{aligned} \int_0^{\infty} G_2^2(v)dv = \int_0^{\infty}\left[\frac{1}{W_k-1}\frac{P_{sr}}{\Delta v}\sum_{k=1}^{K} d_k\sum_{i=1}^{N} c_k(i)\bar{c}_l(i)\times\right. \\ \left.\times\left\{u\left[\frac{\Delta v}{N}\right]\right\}\right]^2 \mathrm{d}v = \\ = \frac{P_{sr}^2}{(W_k-1)^2\Delta v N}\sum_{i=1}^{N}\left\{\bar{c}_l(i)\left[\sum_{k=1}^{K} d_k c_k(i)\right]\times\right. \\ \left.\times\left[\sum_{m=1}^{K} d_m c_m(i)\right]\right\}. \end{aligned} \tag{32}$$

Using approximation Eq. (21), power of PIIN can be written as:

$$\begin{aligned} \left\langle I_{PIIN}^2 \right\rangle = B\Re\left(\int_0^{\infty} G_1^2(v) + \int_0^{\infty} G_2^2(v)\right) \cong \\ \cong \frac{B\Re P_{sr}^2}{\Delta v N_v^2}\sum_{j=1}^{J} K_j W_j\left(\frac{3}{2}W_k + \frac{W_k}{2(W_k-1)} + \right. \\ \left. + \frac{\sum_{j=1}^{J} K_j W_j - (\frac{W_k}{2}+1)}{(W_k-1)^2}\right). \end{aligned} \tag{33}$$

Noting that the probability of sending bit 1 at any time for each user is $\frac{1}{2}$, SNR of system using CS can be written as:

$$\begin{aligned} SNR_k = \frac{(I_1-I_2)^2}{\langle I^2\rangle} = \\ = \frac{\frac{\Re^2 P_{sr}^2 W_k^2}{N_v^2}}{\frac{4eB\Re P_{sr} W_k}{N_v} + \frac{B\Re P_{sr}^2}{2\Delta v N_v^2}\sum_{j=1}^{J} K_j W_j\left(\frac{3}{2}W_k + \frac{W_k}{2(W_k-1)}\right) + \frac{4K_b T_n B}{R_L}} \end{aligned} \tag{34}$$

BER of users can be calculated by substituting SNR_k in Eq. (34) into Eq. (25).

5.3. Direct Decoding

DD scheme only detects the non-overlapping spectra using a single receiver, thus only half of the weight assigned for a particular user is detected ($\frac{W}{2}$). It is assumed that $c_k(i)$ denotes the i-th element of the k-th KS code sequence, therefore the code properties for the KS code using this technique can be written as:

$$\sum_{i=1}^{N} c_k(i)c_l(i) = \begin{cases} W_k/2, & k=l \\ 0, & k\neq l \end{cases}. \tag{35}$$

Using the same mathematical analysis as in Subsection 5.1 the PSD at the input of the photodetector $G_{dd}(v)$ can be expressed as:

$$G_{dd}(v) = \frac{P_{sr}}{\Delta v}\sum_{k=1}^{K} d_k\sum_{i=1}^{N} c_k(i)c_l(i)\times\left\{u\left[\frac{\Delta v}{N}\right]\right\}. \tag{36}$$

Therefore, the photocurrent of the desired user's signal is

$$I_{dd} = \Re \int_0^{\infty} G_{dd}(v)\mathrm{d}v = \frac{\Re P_{sr} W_k}{2N_v} d_l \,. \tag{37}$$

Since only the non-overlapping chip is filtered for DD technique, PIIN is negligible. The total noise here is considered to be only the sum of shot noise and thermal noise such as:

$$\langle I^2 \rangle = 2eBI_{dd} + \frac{4K_b T_n B}{R_L} = \frac{eB\Re P_{sr} W_k}{N_v} + \frac{4K_b T_n B}{R_L} \,. \tag{38}$$

Noting that the probability of sending bit 1 at any time for each user is $\frac{1}{2}$, the SNR of the VW-KS system deploying DD technique for users with weight k can be expressed as

$$SNR_k = \frac{(I_{dd})^2}{\langle I^2 \rangle} = \frac{\dfrac{\Re^2 P_{sr}^2 W_k^2}{4N_v^2}}{\dfrac{eB\Re P_{sr} W_k}{2N_v} + \dfrac{4K_b T_n B}{R_L}} \,. \tag{39}$$

BER of users can be derived using Eq. (25).

6. Results and Discussion

The parameters used in mathematical analysis are listed in Table 2, as published by other researchers [18], [23].

Table 2
Typical parameters used in the analysis

Symbol	Parameter	Value
η	Photodetector quantum efficiency	0.6
Δv	Linewidth of broadband source	3.75 THz
P_{sr}	Received optical power	–10 dBm
B	Electrical bandwidth	622 MHz
λ_0	Operating wavelength	1550 nm
T_n	Receiver noise temperature	300 K
R_l	Receiver load resistor	1030 Ω
e	Electron charge	$1.6 \cdot 10^{-19}$ C
h	Planck's constant	$6.66 \cdot 10^{-34}$ Js
K_b	Boltzmann's constant	$1.38 \cdot 10^{-23}$ J/K

In all analyses, the number of active users with different weights are almost the same, i.e. each service (voice, data and video) has the same portion of total users.
Figure 4 illustrates the probability of error for users with different weights versus number of active users using IL-OOC, VW-RD and VW-KS, respectively, where CS is applied as detection technique. The SNR equation for multi-wavelength IL-OOC and VW-RD are extracted from [26], [27] and [19], [28], respectively. It is shown that even the code weights of VW-KS users (8, 6 and 2) are less than IL-OOC and VW-RD (22, 13 and 5), KS still outperform them. This shows that although the code length of KS code families are longer than others, performance of the code is better due to smaller cross-correlation.

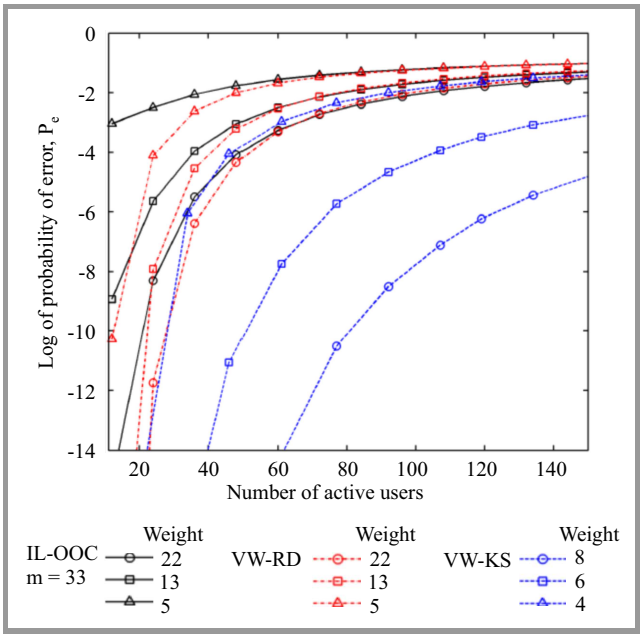


Fig. 4. Probability of error versus number of users for different code families.
(See color pictures online at www.nit.eu/publications/journal-jtit)

Figure 5 shows the probability of errors for users with different weights versus number of active users, employing CS, AND and DD techniques. The total code length is increased by the increase of total number of users in the system, which reduces BER of all users. Moreover, performance of system deploying AND and CS is decreased

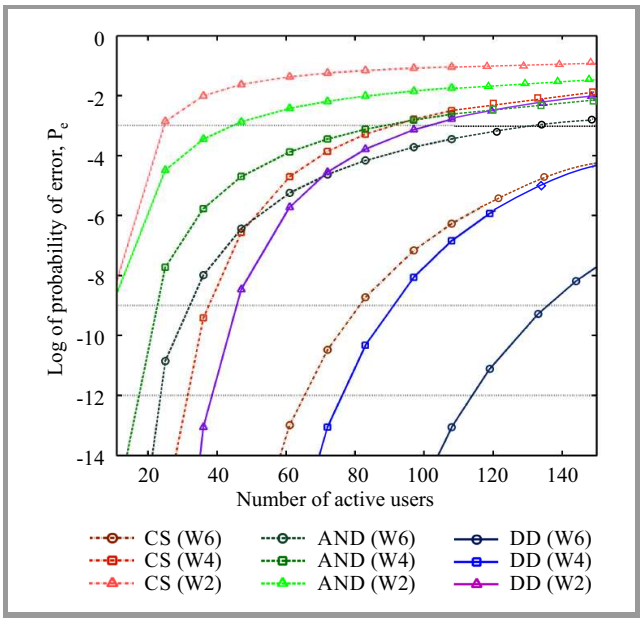


Fig. 5. Probability of error versus number of users.

further because of PIIN which have significant effect for lower weights. It is shown that performance of system deploying DD is much better than the system with AND and CS. The performance of users with different weights is much more differentiated employing DD technique. With reference to the BER of 10^{-3}, 10^{-9} and 10^{-12} for voice, data and video, respectively, the maximum number of active users that can be supported in a VW-OCDMA is 27, 25 and 100 deploying CS, AND and DD, respectively.

Figure 6 illustrates the probability of error as a function of probe optical received power per chip when number of active users is 11 and bit rate is 1.25 Gb/s. The number of users with weight 6, 4 and 2 is 4, 3 and 4, respectively and the total code length is 33. Figure 6 reveals that performance of systems with AND and CS detections is limited even with increase of received optical power. This is due to the PIIN noise, as performance of system with DD dramatically increases with gaining more power because DD detects only non-overlapping signals and avoid the PIIN.

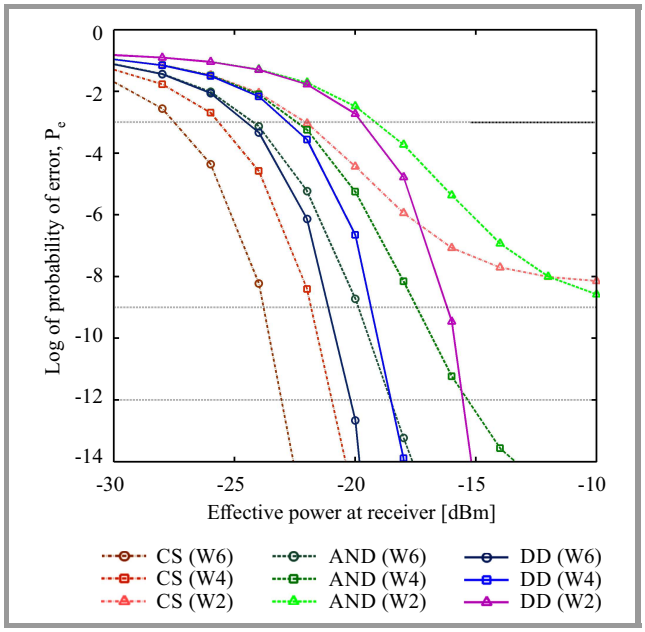


Fig. 6. Probability of error versus effective power per chip at receiver.

Figure 7 shows the plot of probability of error for the system using DD detection versus number of simultaneous users for bit rates of 2.5, 5 and 10 Gb/s, where P_{sr} is –10 dBm. It is shown in Figs. 5 and 7 that the number of supportable users for VW-OCDMA system using DD technique is 46, 30, 24 and 20 for bit rates of 1.25, 2.5, 5 and 10 Gb/s, respectively, for BER of 10^{-9} and all users with different weights.

Performance of a VW-OCDMA system with 11 active users is also analyzed using OptiSystem version 11 simulation software. The performance of system is investigated based on received optical power. In software simulation

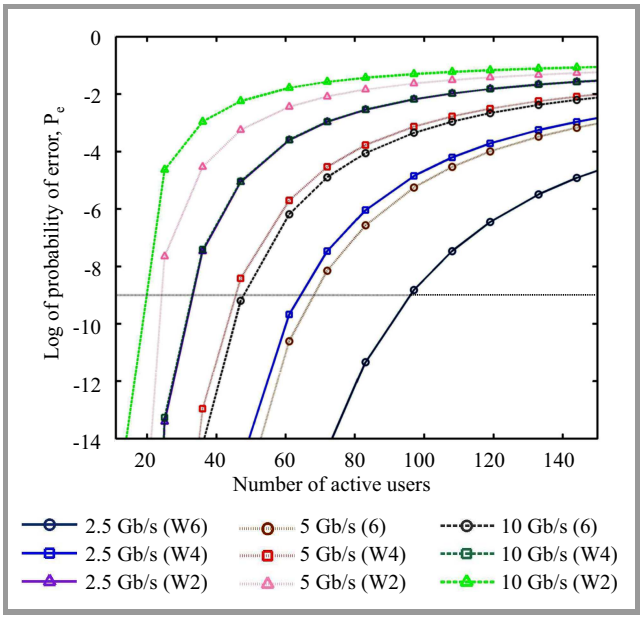


Fig. 7. Probability of error versus number of active users for different bit rates for DD technique.

the parameters used are the same as parameters used in numerical analysis. The chip spacing is chosen as 0.8 nm to avoid crosstalk between channels.

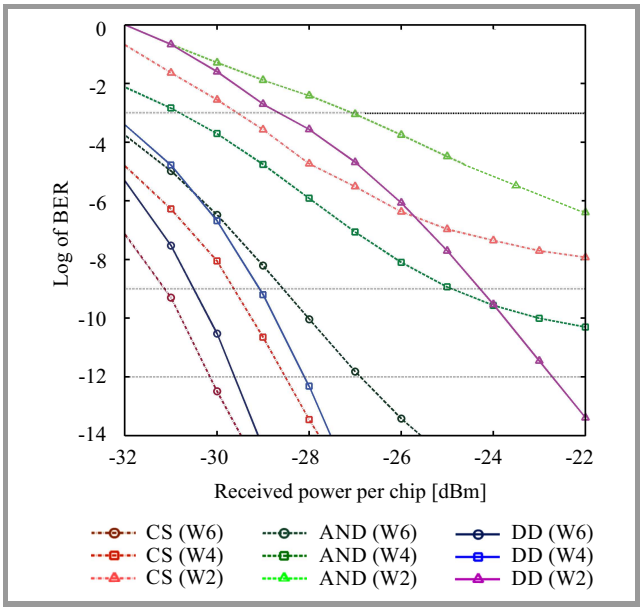


Fig. 8. BER versus effective power per chip at receiver.

Figure 8 shows the BER of users with different weights for the CS, AND and DD techniques. As mentioned, mathematical analysis approximates the upper bound for system performance. The simulation results proves this fact and also supports the numerical analysis. As depicted in Fig. 8, DD outperforms the other detections using balanced receiver in which PIIN significantly reduces the system performance.

7. Conclusion

In this paper performance of a VW-OCDMA system using AND, CD and DD techniques was numerically analyzed and compared to simulation result. Effects of different parameters including number of users, optical received power and bit rate was investigated. It has been shown that performance of system employing DD technique is much better than system with CS and AND subtraction. The obtained results showed that when received power per chip is –10 dBm, system deploying DD can support up to 100 users while this amount is 25 and 27 for the system with CD and AND detections, respectively. The difference between number of supportable users using CS, AND and DD becomes further differentiated by the increase of received power. VW-OCDMA with DD technique with reduced complexity and number of filters offers a great potential in service differentiation in physical layer.

Acknowledgment

The work described in this paper is funded by Research University Grant Scheme (RUGS) of Universiti Putra Malaysia. The authors would like to thank all those who have contributed towards the success of this project.

References

[1] H. Ghafouri-Shiraz and M. M. Karbassian, *Optical CDMA Networks: Principles, Analysis and Applications*. Wiley-IEEE Press, 2012.

[2] A. Noura, S. Seyedzadeh, and S. Anas, "Simultaneous vibration and humidity measurement using a hybrid WDM/OCDMA sensor network", in *Proc. 4th IEEE Int. Conf. Photon. ICP 2013*, Melaka, Malaysia, 2013, pp. 163–165.

[3] A. Taiwo, S. Seyedzadeh, S. Taiwo, R. Sahbudin, M. Yaacob, and M. Mokhtar, "Performance and comparison of fiber vibration sensing using SAC-OCDMA with direct decoding techniques", *Optik – Int. J. for Light and Electron Optics*, vol. 128, no. 17, pp. 4803–4806, 2014.

[4] T. Ohtsuki, "Performance analysis of atmospheric optical PPM CDMA systems", *J. Lightw. Technol.*, vol. 21, no. 2, pp. 406–411, 2003.

[5] S. Anas, T. Quinlan, and S. Walker, "Service differentiated drop code unit for metro ring optical networks", *IET Optoelec.*, vol. 4, no. 1, pp. 46–50, 2010.

[6] I. Djordjevic, B. Vasic, and J. Rorison, "Multi-weight unipolar codes for multimedia spectral-amplitude-coding optical CDMA systems", *IEEE Commun. Lett.*, vol. 8, no. 4, pp. 259–261, 2004.

[7] N. Nasaruddin and T. Tsujioka, "Design of strict variable-weight optical orthogonal codes for differentiated quality of service in optical CDMA networks", *Comp. Netw.*, vol. 52, no. 10, pp. 2077–2086, 2008.

[8] S. Seyedzadeh, R. Sahbudin, A. Abas, and S. Anas, "Weight optimization of variable weight OCDMA for triple-play services", in *Proc. 4th IEEE Int. Conf. on Photon. ICP 2013*, Melaka, Malaysia, 2013, pp. 99–101, 2013.

[9] S. Maric, O. Moreno, and C. Corrada, "Multimedia transmission in fiber-optic LANs using optical CDMA", *J. Lightw. Technol.*, vol. 14, no. 10, pp. 2149–2153, 1996.

[10] W. Kwong, "Design of multilength optical orthogonal codes for optical CDMA multimedia networks", *IEEE Trans. Commun.*, vol. 50, no. 8, pp. 1258–1265, 2002.

[11] W. Kwong and G.-C. Yang, "Multiple-length multiple-wavelength optical orthogonal codes for optical CDMA systems supporting multirate multimedia services", *IEEE J. Selec. Areas in Commun.*, vol. 22, no. 9, pp. 1640–1647, 2004.

[12] M. H. Kakaeea, S. Seyedzadeh, H. A. Fadhil, S. B. Ahmad Anas, and M. Mokhtar, "New dynamic technique for SAC-OCDMA system", in *Proc. 4th IEEE Int. Conf. Photon. ICP 2013*, Melaka, Malaysia, 2013, pp. 120–122.

[13] M. H. Kakaee, S. Seyedzadeh, H. Adnan Fadhil, S. Barirah Ahmad Anas, and M. Mokhtar, "Development of multi-service (MS) for SAC-OCDMA systems", *Optics & Laser Technol.*, vol. 60, pp. 49–55, 2014.

[14] P. R. Prucnal, *Optical Code Division Multiple Access: Fundamentals and Applications*. CRC Taylor & Francis, 2006.

[15] D. Zaccarin and M. Kavehrad, "An optical CDMA system based on spectral encoding of LED", *IEEE Photon. Technol. Lett.*, vol. 5, no. 4, pp. 479–482, Apr. 1993.

[16] S. Seyedzadeh, G. A. Mahdiraji, R. K. Z. Sahbudin, A. F. Abas, and S. B. A. Anas, "Experimental demonstration of variable weight SAC-OCDMA system for QoS differentiation", *Opt. Fiber Technol.*, vol. 20, no. 5, pp. 495–500, 2014.

[17] M. K. Abdullah, F. N. Hasoon, S. Aljunid, and S. Shaari, "Performance of OCDMA systems with new spectral direct detection (SDD) technique using enhanced double weight (EDW) code", *Optics Commun.*, vol. 281, no. 18, pp. 4658–4662, 2008.

[18] R. Sahbudin, S. Aljunid, M. Abdullah, M. B. A. Samad, M. Mahdi, and M. Ismail, "Comparative performance of hybrid SCM SAC-OCDMA system using complementary and AND subtraction detection techniques", *The Int. Arab J. of Inform. Technol.*, vol. 5, no. 1, pp. 61–65, 2006.

[19] H. A. Fadhil, S. Aljunid, and R. Badlisha, "Triple-play services using random diagonal code for spectral amplitude coding OCDMA systems", *J. of Optical Commun.*, vol. 30, no. 3, pp. 155–159, 2009.

[20] S. Ahmad Anas, M. Abdullah, M. Mokhtar, S. Aljunid, and S. Walker, "Optical domain service differentiation using spectral-amplitude-coding", *Opt. Fiber Technol.*, vol. 15, pp. 26–32, no. 1, 2009.

[21] M. Abdullah, S. Aljunid, S. Anas, R. Sahbudin, and M. Mokhtar, "A new optical spectral amplitude coding sequence: Khazani-Syed (KS) code", in *Proc. 5th Int. Conf. Inform. & Commun. Technol. ICICT 2007*, Dhaka, Bangladesh, 2007, pp. 266–278.

[22] Z. Wei, H. Shalaby, and H. Ghafouri-Shiraz, "Modified quadratic congruence codes for fiber Bragg-grating-based spectral-amplitude-coding optical CDMA systems", *J. Lightw. Technol.*, vol. 19, no. 9, pp. 1274–1281, 2001.

[23] E. Smith, R. Blaikie, and D. Taylor, "Performance enhancement of spectral-amplitude-coding optical CDMA using pulse-position modulation", *IEEE Trans. Commun.*, vol. 46, no. 9, pp. 1176–1185, 1998.

[24] L. Chao, "Effect of laser diode characteristics on the performance of an SCM-OFDM direct detection system", *IEE Proc. J. Optoelectron*, vol. 140, no. 6, pp. 392–396, 1993.

[25] C.-C. Yang, J.-F. Huang, and S.-P. Tseng, "Optical CDMA network codecs structured with M-sequence codes over waveguide-grating routers", *IEEE Photon. Technol. Lett.*, vol. 16, no. 2, pp. 641–643, 2004.

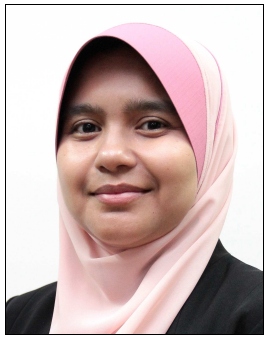
[26] I. Djordjevic and B. Vasic, "Novel combinatorial constructions of optical orthogonal codes for incoherent optical CDMA systems", *J. Lightw. Technol.*, vol. 21, pp. 1869–1875, 2003.

[27] I. Djordjevic, B. Vasic, and J. Rorison, "Design of multiweight unipolar codes for multimedia optical CDMA applications based on pairwise balanced designs", *J. Lightw. Technol.*, vol. 21, no. 9, pp. 1850–1856, 2003.

[28] H. A. Fadhil, S. Aljunid, and R. Ahmad, "Performance of random diagonal code for OCDMA systems using new spectral direct detection technique", *Opt. Fiber Technol.*, vol. 15, no. 3, pp. 283–289, 2009.

Saleh Seyedzadeh received his B.Sc. degree in Software Engineering from SUT, Iran (2008) and M.Sc. degree in the area of optical communication system from University Putra Malaysia, Malaysia (2013). Currently he is a researcher at Department of Electrical Engineering, University of Malaya and member of Integrated Lightwave Research Group (ILRG). His research interests include optical CDMA, quality of service in optical networks, optical hybrid modulation, and optical sensors.
E-mail: s.seyyedzadeh@gmail.com
Integrated Lightwave Research Group
Department of Electrical Engineering
University of Malaysia
Jalan University
50603 Kuala Lumpur, Malaysia

Majid Moghaddasi received the M.Sc. degree in Communication and Computer Engineering from National University of Malaysia in 2011. From 2012 he been a member of Wireless and Photonic Networks Research Center (WiPNET) in the Department of Computer and Communication Systems Engineering of Universiti Putra Malaysia (UPM) and worked as a research assistant. His research interests include optical CDMA, free-space optics, optical networks, and computer networks.
E-mail: majidmoghaddasi@ieee.org
Wireless and Photonics Research Center of Excellence
Department of Computer
and Communication Systems Engineering
University Putra Malaysia
UPM Serdang
Malaysia



Siti Barirah Ahmad Anas obtained her Ph.D. in 2009 from University of Essex specializing in optical CDMA. She received an M.Sc. from Universiti Putra Malaysia (2003) and a B.Eng. from University of Strathclyde (1999). She is currently an Associate Professor in the Faculty of Engineering, UPM. Her research interests include optical communication and networks.
E-mail: barirah@upm.edu.my
Wireless and Photonics Research Center of Excellence
Department of Computer
and Communication Systems Engineering
University Putra Malaysia
UPM Serdang
Malaysia

Paper

Concept for a Measurement Management System for Access Service to the Internet

Janusz H. Klink[1], Maria J. Podolska[2], and Tadeus Uhl[3]

[1] *Wrocław University of Technology, Wrocław, Poland*

[2] *Office of Electronic Communications, Warsaw, Poland*

[3] *Maritime University of Szczecin, Szczecin, Poland*

Abstract—This paper describes the problems associated with the provision of quality of service over an access connection to the Internet, i.e. the Internet Access Service (IAS). The paper has something of an overview character. Following a comprehensive introduction to the subject of "Changing Network Technologies" the paper focuses on the topic "Quality of IAS" in the light of regulatory directives of the European Parliament and the latest recommendations of ITU-T and ETSI. The focus will then shift to "Measurement Points and Measurement Scenarios for Determining QoS". This topic will be described in detail and illustrated with several graphics. The final chapter has a pronounced scientific character and contains, among other things, a suggestion for a so-called Measurement Management System (MMS) to aid the design, execution and evaluation of efficient, automatic QoS measurements in networks.

Keywords—Internet, Measurement Management Systems, Quality of Service.

1. Introduction

There is no denying that the store and forward technique has become tremendously popular throughout the telecommunications market since the turn of the century. Little by little, it has managed to oust older switching technologies. So it is not surprising that many network providers have announced their intention to pull out of ISDN [1] and ATM [2] in the near future. The success of the new technology is no doubt due to the flexibility of its redesign of packet switching. It allows for a high degree of flexibility in modern digital network architecture and management. The World Wide Web also uses this switching technique in the form of its datagram concept. The Internet Protocol (IP) [3] used in the network layer supports packet switching splendidly, and modern mobile wireless networks use packet switching as well. At the heart of these networks are transport platforms that also operate according to the TCP/IP [4] protocol stack. It is impossible to imagine modern digital networks without store and forward technology. Internet works according to the "best effort" principle. Although it is very flexible, it does have a number of drawbacks. The packets are transported through the network along the best routes available at any given time (according to whichever metric is used). There are no confirmation mechanisms on this level, which means that lost packets will not be resent. Nor is there any content control (apart from the information in the header). Any errors that occur will be propagated and will accumulate towards the receiver's end. This can have a substantial effect on quality of service (QoS). It is often the case in IP-based networks that bottlenecks occur in various places. This means that in overloaded areas individual packets must be stored for a considerable time to be handled at a later time, and this causes significant end-to-end delays. An overload situation also means that the interarrival times of individual packets that belong to a single communication (in a word: jitter) can vary enormously. Jitter, too, can have a negative influence on QoS. If, during real-time communication, large jitter values cannot be redressed in the jitter buffers, additional packet losses will occur, and QoS will deteriorate even more. So it is evident that IP-based networks are flawed by multiple impairment parameters that can influence QoS.

A major aim in modern networks is to keep the customer happy. As the guru of American management, William Deming, once so aptly put it: "Quality is what satisfies, or even excites, the end user". To achieve this aim, the quality of service provided by the network must be constantly monitored, and corrective measures must be taken the instant it shows signs of decreasing significantly. It would be best if the continuous measurement of QoS values that this assumes could be done discretely and automatically. That is by no means an easy task for either network providers or national regulatory authorities.

The issue of QoS has received much attention in Brussels in recent years with negotiations leading to the enactment of the Communications Package in November 2009. It contains two eminently important directives: Directive 2009/136/EC [5] and Directive 2009/140/EC [6], that have been designed to ensure network neutrality and transparency throughout the telecommunications market of the European Union. With the publication of these Directives the Member States of the EU committed themselves to implementing them, as it turns out, however, with widely differing quantities of vigour from one country to the next. In November 2012, Poland's regulatory authority

UKE [7] launched an initiative called "QoS Memorandum". In April 2013 Germany's regulatory authority BNetzA [8] created a forum for the "Promotion of Transparency in End-Customer Markets and Measurement Methods". These two steps aimed to stake out boundary conditions for ensuring transparency and network neutrality on the telecommunications market within the respective country.

These two initiatives have been put into practice in both countries: in 2014 the UKE in Poland and the BnetzA in Germany both published official calls for tenders to establish Monitoring and Measuring Systems for evaluating QoS at IAPs. The calls for tender closed at the end of 2014 and contracts have been awarded to selected firms. In Poland the first measurement system (with the features outlined above) already went into operation in the summer of 2015 and its performance is now undergoing tests, of course under the supervision of the contractor UKE. The same is due to happen in Germany in the second half of 2015.

There are a number of companies on the telecommunications market offering systems that measure QoS in networks. Here are some examples: Nextragen [9], Opticom [10], Empirix [11], Ixia [12], NetIQ [13], IpLabel [14], Telchemy [15], Shenick [16], VoIP Future [17] and Systemics [18]. Surfing the Internet will reveal a number of open systems and/or software solutions with which the actual transmission rate in last-mile downlinks and uplinks can be measured. Here are a few examples: Measurement Lab (M-Lab) [19], Broadband Speedchecker [20], Wireshark [21]. Any appraisal of an open measuring system or a software solution will focus on its reliability, specifically: on its credibility. At the time of writing there are hardly any systems which allow the user to configure, implement and audit measurements of QoS. In a nutshell: there are no MMSs. Any such MMS should have to be designed to measure impairment parameters in networks and yield service-specific QoS values yet all the while remain unobtrusive, operating discretely somewhere in the network. It is of utmost importance that such measuring systems should be compatible primarily with existing standardised, service-specific QoS measurement methods. For only then are objective and comparable measurements possible. Furthermore, any statistical analysis of measurement results must take the rules defined in ITU-T and ETSI Recommendations into account. So it is patently clear that any MMS will be an extremely complex structure which takes many factors and circumstances into account. The authors, given their experience in all matters concerning the subject of QoS, will endeavour to develop and appraise in the course of this paper a concept for a universally applicable MMS. The latest initiatives of EU research projects (e.g. Leone [22] and mPlane [23]) also have this aim, as does the organisation IETF, which is at present working on a framework for the Large-scale Measurement of Broadband Performance (LMBP) [24].

The study will begin with a presentation of the Access Service to the Internet within the context of the regulatory framework in Europe (Section 2). Following that there will be a brief presentation of the existing measurement points and measurement scenarios that are typical of networks; special attention will be paid to ITU-T- and ETSI Recommendations (Section 3). A further Section 4 will be devoted to the main topic of this paper, namely the development of an MMS with the focus on a workable layout design of the system. The paper will conclude with a summary and an outlook on areas of future work in Section 5.

2. Access Service to the Internet

The Body of European Regulators for Electronic Communications (BEREC) has prepared on behalf of the European Commission a consultation process (finished on 28th April 2014) and launched the report "Monitoring the quality of Internet Access Services in the context of net neutrality" [25]–[26] and the report "Guidelines for quality of service in the scope of net neutrality" [27]. These documents will grant National Regulatory Authorities (NRAs) improved capacity to perform regulatory assessments of potential degradation of service. Furthermore, transparency enables end users to compare Internet Access Service (IAS) offers and hence strengthen the demand side of the market. It is therefore essential to have appropriate quality monitoring tools to implement the recommendations drawn from earlier studies in this area. The main goal of this report is to establish a basis for the creation of Internet access service quality monitoring systems covering two main use cases (see Fig. 1):

- Case A – providing transparency on the quality of the Internet access service for end users,
- Case B – regulatory supervision through monitoring the quality of the Internet access service with regard to potential degradation of service.

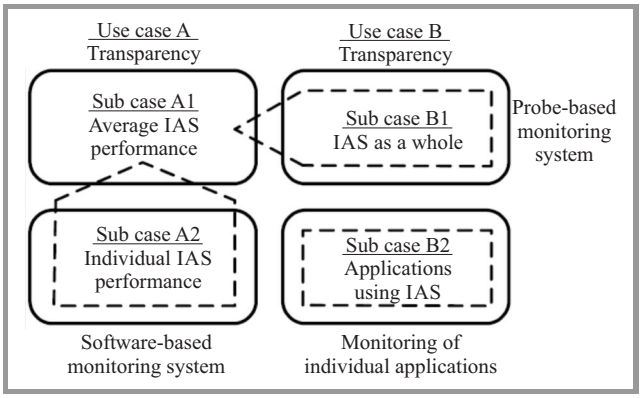


Fig. 1. Measurement systems vs. use cases.

When considering Case A there are two options:

- Sub Case A1 – average IAS performance,
- Sub Case A2 – individual IAS performance.

BEREC recommends implementing end user transparency measurements in a user-friendly manner. A software-based measurement agent download to end user equipment can be sufficient, provided that measurement results are validated by collecting additional end user information. Regarding aggregated results, BEREC recommends – for reasons of cost-effectiveness and user-friendliness – that averaging (based on data gathered from all participating users) should be performed based on crowd-sourcing.
When considering Case B there are two options:

- Sub Case B1 – degradation of IAS as a whole,
- Sub Case B2 – applications using IAS.

Measurements for monitoring the quality of IAS as a whole will typically be conducted in one of two ways. The NRA could either use a controlled system, e.g. with hardware probes that measure the systems of a preselected panel of specialists, or a less controlled system with software agents and a crowd-sourced user base. When evaluating potential degradation of IAS as a whole, BEREC recommends that such measurements are conducted over time to allow trend analysis to be performed. Measurement results need to be assessed in the light of technical progress and market evolution, with the goal of evaluating potential effects such as the provision of specialised services at the expense of IAS.
When it comes to monitoring applications using IAS, BEREC recommends the use of appropriate tools to measure the performance of individual applications (can also be used for transparency; use Case A) and also exploring the use of passive measurements. Leveraging applied to information from the measurement systems of content and applications providers (CAPs) and other complementary methods could also be considered. Measurement results obtained by these methods will need to be assessed by experts with regard to reasonable and unreasonable traffic management, in order to detect degradation of individual applications that are using IAS.
In CEPT's ECC report 195 [28], the following quality metrics have been selected: upload and download speeds, delay, delay variation, packet loss ratio, and packet error ratio. The criteria CEPT used to choose the relevant standard were primarily based on ETSI Guide EG 202 057 [29], ITU-T Recommendations Y.1541 [30] and G.1010 [31].
Quality assurance of measurement results and regulatory assessment of the results require deep understanding of the underlying complexities of Internet communications, and of monitoring methodologies. It is expected that this understanding will need to develop over time, and the exchange of experience among NRAs to foster convergence of practices, and participation in and contribution to standardization activities are good strategies for harmonization in this area. Especially when it comes to gaining experience in assessing degradation of service, BEREC recommends that NRAs collaborate to develop a common regulatory practice. Harmonization of evaluation of potential degradation of IAS as a whole, typically at the expense of specialized service, and assessment of degradation of individual applications, are both of utmost importance.
It is recommended that BEREC conduct a feasibility study for a potential future opt-in monitoring system before it contemplates pursuing the implementation of a full-blown measurement system. This would draw upon the proposed quality monitoring approach described above, containing as it does recommended measurement parameters and methods. The system should be designed in a way that allows additional measurement scenarios to be integrated smoothly into existing national systems. Such a study should also consider the effect of the dissemination of knowledge among NRAs and further development of best practices. This should accelerate harmonization of measurement methodologies and increase competence in the field of quality monitoring in the context of net neutrality.
There are three different types of regulatory approaches to implementing a quality monitoring system:

Traditional regulation – the quality monitoring system may be implemented and managed by the NRA itself or by an independent measurement provider commissioned by a public procurer. Given a sufficient legal basis, the NRA may also impose a system of quality monitoring on the ISPs.

Co-regulation – under certain circumstances, NRAs may find it appropriate to establish joint regulator-stakeholder organs rather than simply imposing implementation on ISPs. Under such a scheme, cooperation with stakeholders may be useful for meeting specific needs or regulatory objectives, or both. Examples would be: (i) system development by independent research institutions; (ii) conducting measurement campaigns with the help of consumer organizations; (iii) publishing results on third-party comparison websites.

Self-regulation – finally, under certain circumstances, NRAs may decide to leave deployment of measurement systems to market forces, and promote self-regulatory initiatives for the implementation of relevant measurement methods, and the publication of monitoring results, through moral suasion. For instance, NRAs may launch education and information campaigns to increase consumers' awareness of the availability and use of measurement tools, while inviting ISPs to make user-friendly tools available to their customers. Here, the NRA may have some influence, but does not control the methodology of the quality monitoring system, supervise its implementation or manage the generated data.

For the purpose of harmonization, BEREC recommends that an evolutionary strategy is pursued in which harmonization itself is viewed as a multi-stage process that encompasses the following:

Stage 1 – convergence of metrics and methods,

Stage 2 – sharing and comparison of measurement results,

Stage 3 – harmonization of cross-border measurements.

3. Measurement Points and Measurement Scenarios in a Focus of ITU-T and ETSI Recommendations

An enormous number of difficulties are connected with the quality of services provided to end users via IP networks. One of them is the issue of Internet access. Physically, it is a combination of different connections and services needed to establish a functioning Internet access. Each of them can be treated as a separate service described by its own quality parameters. On the other hand, inexperienced users do not usually understand the term "Internet access" as an access in the true sense of the word, i.e. the provision of a physical connection to the network [29]. Users normally understand Internet access to mean access to the end-to-end services available on the Internet. To them, a purely physical access to the Internet has no practical meaning beyond the provision of the possibility of using the various services, e.g. e-mail and Web browsing, and applications available in the network. So Internet access is generally understood as a platform that provides access to Internet services. From the technical point of view, however, the primary meaning of term Internet access should be understood as the physical and logical access to the core of the network, including all functionalities needed to enable the user to establish a connection to further entities in the Internet and to run the advanced services [29].

This section presents the main issues connected with specifying the measurement scenarios, locating the points at which the measurements can be performed, and identifying the parameters that affect quality of service. Simply put, this section says "what, how and where" measurements should be made to provide operators, Internet Service Providers and users with a thorough knowledge of quality of service.

Specifying the proper measuring points is quite a serious issue because Internet access is no longer provided by a single network or service provider as was once the case with traditional voice communication in public switched telephone networks (PSTNs). Normally, a user gains indirect access to the public Internet via an Internet Access Point (IAP). There is a transit network between user terminal and IAP. This is usually the public telecommunications network (PTN) but it might also be a wired or wireless local area network (LAN/WLAN). Therefore, the overall quality of services (or, in general, Internet access) is a combination of the performance of all elements involved in the connection.

The measurements can be divided into two groups: so-called "in-net" and "over-the-top" (OTT) measurements. The first case covers the Internet service provider's area - the area on which it acts. OTT measurements are more closely related to the user's perspective, i.e. the way he perceives the quality of service. In the context of net neutrality, performance of individual applications is also important because it can be used to detect potential degradation of the quality of the Internet access service.

ECC Report [28] specifies a list of technical quality parameters that could be used to make a technical evaluation of IAS. Many NRAs or other national institutions agree that the list is too long and consider it to be too complicated and incomprehensible to the average user. Thus, they propose the selection of a subset of parameters to the same ends. There is no consensus on which set of parameters would be best. So, after consulting an abundance of documents [28]–[30] and points of view, the EEC has proposed a list of minimum technical parameters that take their influence on the most popular Internet applications into account.

The following quality metrics have been selected: data transmission rate, delay, delay variation, packet loss ratio, and packet error ratio. Table 1, based on ECC Report 195 [28], illustrates popular services, and the relevance of the network performance parameters to the performance or quality of those services, or both. In the following table, the relevance ranges from "–" (irrelevant) to "+++" (very relevant).

Table 1
Relevance of network impairment parameters to various applications

Service	Data transmission speed		Delay	Delay variation	Packet loss	Packet error
	Down-stream	Up-stream				
Browse (text)	++	–	++	–	+++	+++
Browse (media)	+++	–	++	+	+++	+++
Download file	+++	–	+	–	+++	+++
Transactions	–	–	++	–	+++	+++
Streaming media	+++	–	+	–	+	+
VoIP	+	+	+++	+++	+	+
Gaming	+	+	+++	++	+++	+++

The first parameter presented in Table 1 is data transmission rate (or shorter: transmission rate). It was selected because it is probably the most relevant parameter; it is self-evident, and mentioned in virtually every Internet Service Provider's offer. Moreover, it can be measured on the network layer (in-net measurements) and can be compared with values obtained on the application level (OTT measurements). It is defined as the data transmission rate that is achieved separately for downloading and uploading specified test files between a remote Web site and a user's terminal equipment [29]. The next parameter is delay, defined as half the time (in ms) that is needed for an ICMP packet to reach a valid IP address. This parameter is also easy to understand and has an influence on many applications available over the Internet. It is already being used by many NRAs, operators and web-based speed meters.

For some applications the delay variation is relevant. It is therefore the third parameter selected for measurements. The exact definition of this parameter can be found in [30], [32]. Losing information is another parameter that can be relevant to some applications. IP packets can some-

times be dropped due to a small buffer size or poor radio connection although values for the transmission rate, delay, and delay variation remain good enough. UDP-based applications such as Voice over IP could not work properly in such conditions if it were not for compensation techniques operating on the application level. This phenomenon can be quantified and described by packet loss ratio, which is the ratio of total lost IP packets occurrences to the total number of packets in the population under examination [32]. This parameter can also be measured on the network layer and compared with results obtained on the application level.

The last, but not least, parameter that has been selected as relevant to many applications is the IP packet error ratio, sometimes called packet error ratio. It is defined as the ratio of total faulty IP packet occurrences to the total of successful IP packet deliveries plus faulty IP packet occurrences within a population of interest.

In conclusion, it should be noted that the transmission rate of IAS is the most popular parameter, being the one that end users understand best. It is also used by the operators as a basis for evaluating of the Internet Access Service. Each of the other four equally important parameters addresses a particular quality feature. Thus, IAS can only be comprehensively described by using all of them, including the transmission rate.

Usually, the values of the parameters being measured vary considerably throughout the course of a measurement procedure. So, questions arise as to how the final values can be calculated (the average, minimum, maximum, or perhaps another) and which of them are really important. It seems that the average value is very important for all the parameters: it gives general information. But in the case of transmission rate the minimum value can be very relevant, especially for the end user. Most Internet applications require certain transmission rates, i.e. certain minimum values. Figure 2 presents a generic overview of the elements, network sections and interfaces of the IAS according to ETSI and CEPT documents [28]. Users can be connected to the various Internet Service Providers via access/aggregation networks, using wired or wireless connections. Communication over the Internet requires data interchange over different National and International eXchange Points (NXPs and IXPs). QoS management is therefore a very demanding issue. Moreover, mapping the quality of service of particular network sections according to the Quality of Experience (QoE), i.e. quality as perceived by the user, is quite complicated and requires clear specification of interfaces between these networks. Specification of the interfaces, as presented in Fig. 2, allows so-called "in-net" measurements to be made with which operators and service providers could then examine their own networks to verify their conformity with specifications and minimal service requirements.

Three "in-net" evaluation methods seem to be relevant to measurements connected with IAS quality assessment. The methods all revolve around examination of the access network, the ISP network and sometimes the network connections to national or international exchange points (NXP or IXP). The names of these methods (also see Fig. 3) are listed below:

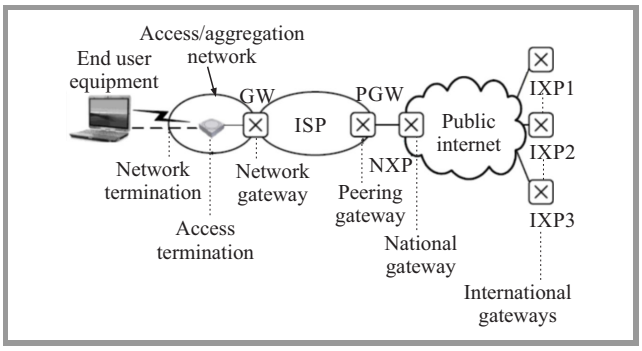


Fig. 2. Generic overview of elements and network sections of private end user IAS.

- QoS evaluation within the ISP leg,
- QoS evaluation between Network Termination Point (NTP) and NXP(s),
- QoS evaluation between NTP and IXP(s).

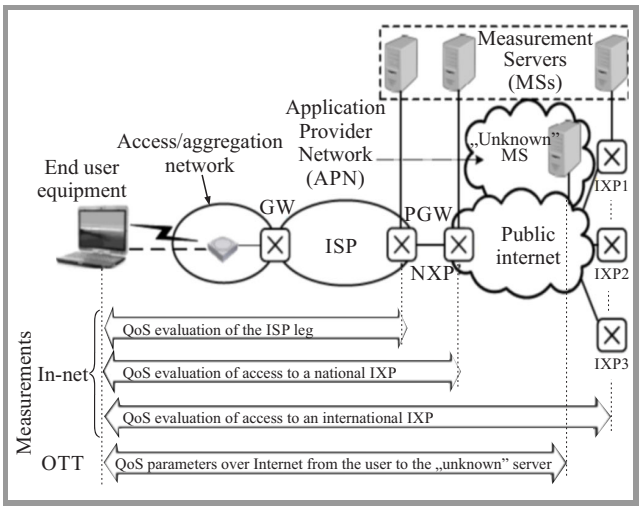


Fig. 3. Internet Access Service QoS evaluation.

According to ETSI [29], the access network is the most essential for the assessment of the ISP leg. To assess the access network only, the test server should be located as near as possible to the gateway (GW) between the access network and the ISP network. If the quality of the entire ISP leg is to be evaluated, the test server should be placed inside the ISP network, near the public Internet interface (PGW in Fig. 3). For a QoS evaluation of the section up to a national Internet Exchange Point, the test server should be located at the NXP. This set-up should make it possible to compare the QoS of access to the NXP of different ISPs within a specific country. Any such evaluation must be done in the light of the set of QoS parameters specified by

the NRA of that country. To compare Internet Access Services using different ISPs, a central test server is necessary to establish comparable measurement results.
The bottleneck of the ISP's network, besides the Access leg, lies within the interconnection points, where capacity is usually insufficient. Therefore, the comparability of measurements of the different Internet Access Services can only be achieved if all ISPs being examined are connected to the central measuring point in the same way. To guarantee objectivity it is recommended that such measurements should be performed by a third-party measuring organization (NRA itself or other relevant national institution or independent organization) using suitable hardware tools, software clients or web-based applications. This scenario reflects far more accurately the performance of the IAS as it is perceived by the user than does the "ISP leg scenario" described above. So the results obtained for the QoS of the IAS will come far closer to its QoE values. If QoS evaluation is to be performed on the access to an international Internet eXchange Point, it should be noted that such IXPs might not be a single physical entity. Nevertheless, the results of the measurements should be collected using one – and only one – analysis system capable of encompassing all points.
Finally, the measurement scenarios should also specify the times at which the measurements are made. In general, measurements should be schedules so as not to fall in periods of low or high traffic, let alone peak hours. To obtain representative values within a short time, measurements should be performed continuously, but due to extraneous circumstances (primarily money and pressure of time) the observations might quite reasonably be limited to specific times depending on user behavior.
When accessing the services or applications available in the global network users perceive the quality of access provided by the IAS as a whole. Therefore, the second approach to evaluation, called "over the top" evaluation, has been proposed. It reflects most faithfully users' perception of service quality. It can be performed using a third-party server located in the Application Provider Network, which allows users to conduct end-to-end measurements between their own terminal equipment and a so-called "unknown" application-specific server (see Fig. 3).

4. Concept for a Measurement Management System

The Measuring Management System (MMS) designed for quantifying Quality of Service (QoS) in modern digital networks encompasses four elements:

- organization,
- information,
- communication,
- function.

The element Organization describes the components of the Measuring Management System, such as a manager, agent, etc., and their inter-relationship. The arrangement of these components leads to different types of architecture; this will be discussed at a later stage. The element Information is concerned with the structure and storage of measuring management information. The information is stored in a database called Management Information Base (MIB). The ISO standardized the Structure of Management Information (SMI) to define the syntax and semantics of management information stored in the MIB. The element Communication deals with the process of communicating management data between agent and manager. It is concerned with the transport protocol, with the application protocol and with commands and responses issued and transported between peers. The last element, Function, addresses the measuring management applications that reside in the node management station (NMS). The following function areas are possible:

- configuration – e.g. address of agents, number of measurement sessions, address of sessions, measurement duration, number of repetitions, type of measurement techniques, location of stored measurement information,
- performance – e.g. establishing connections, synchronizing measurement clients, QoS measurement, building of records,
- fault indication – checking availability, route tracing, and generating test functions.

The architecture of the intended MMS is shown in Fig. 4.

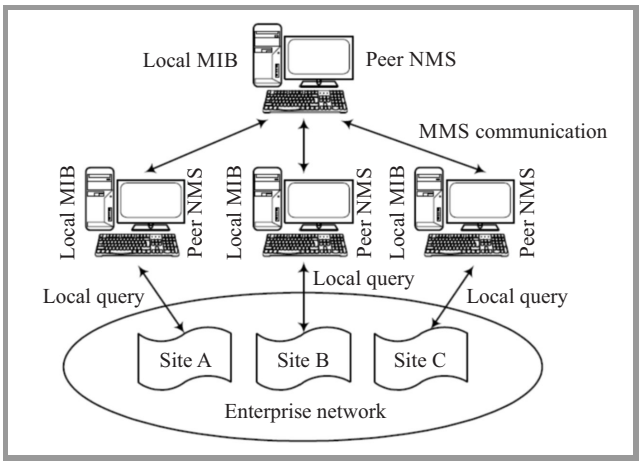


Fig. 4. Architecture of the Measuring Management System.

In a distributed network, a decentralized architecture is more appropriate, with a local NMS at each site. These distributed NMSs can act in a client-server architecture in which one NMS (Manager) acts as master server and the others as clients (Agents). The clients send their data to the master server for centralized storage. An alternative is to have all distributed NMSs bear equal responsibility,

each with its own manager databases, so that management information is distributed over the peer NMSs.
Communication between the components in the MMS is done by way of an application layer protocol Simple Network Management Protocol (SNMP). Three versions of this protocol are currently available: V.1 (RFC 1155-7, 1988), V.2 (RFC 1351-3, 1993) and V.3 (RFC 3410-18, 2002). This protocol is well known; it is commonly implemented in such network components as routers and gateways and is thus routable. This proves to be a huge advantage in practice especially when MMS is used in hybrid network structures (with multiple gateways). SNMP utilises the User Datagram Protocol (UDP) and communicates via ports 161 and 162. It is based on an exchange of messages. There are three common types of message:

- GET – enables the management station to retrieve the value of MIB objects from the agent,
- SET – enables the management station to set the value of MIB objects at the agent,
- TRAP – enables the agent to notify the management station of significant events.

A MIB is used to store the structured information representing measuring elements and their attributes. The structure itself is defined in a standard called Structure of Management Information (SMI) which defines the types of data that can be used to store objects, the names of these objects and how they are encoded for transmission via a network. Each object assumes a unique identifier, the so-called Object Identifier (OID). Assignment of OIDs is organized strictly hierarchically. As the above example shows, it is possible, using such a type of OID, to define private objects that can be used in a MIB. They must be requested from Internet Assigned Numbers Authority (IANA) from the standards groups or from the producers of QoS measurement systems.
The MMS manager is usually a standalone workstation, but it might also be implemented under several operating systems. It includes a collection of software called Measuring Management Application (MMA). The MMA includes a user interface to allow authorized MMS agents to manage the measuring system. It responds to user commands issued throughout the network. The agents are measuring management software modules. They respond to requests for information and requests for action from the MMS manager, such as polling, and can provide the manager with important but unsolicited information, such as traps. All management information about a particular agent is stored in the management information base at that agent. An agent might keep track of the following:

- number of measurement sessions,
- address of measurement session,
- type of service,
- kind of measurement method,

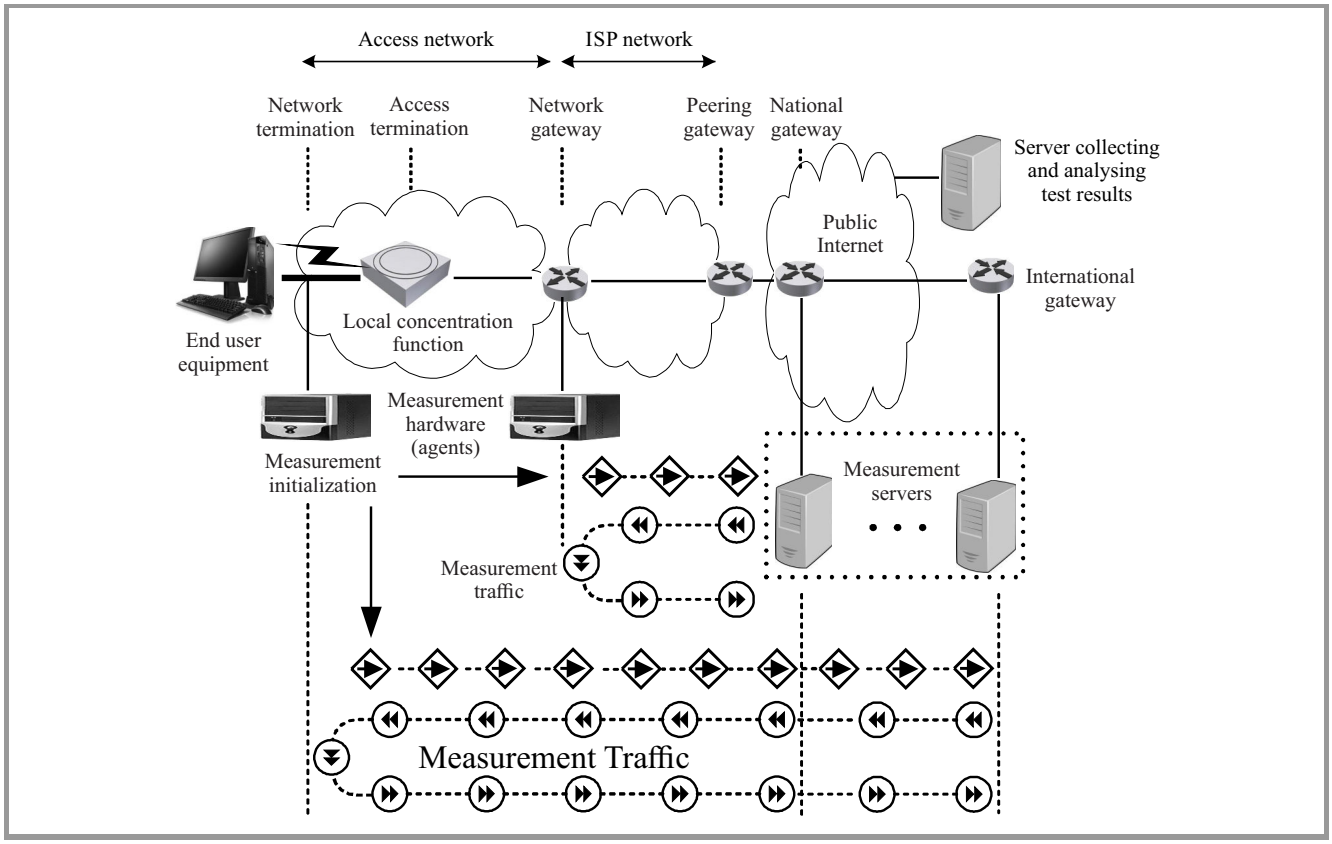


Fig. 5. Measuring Management System implementation.

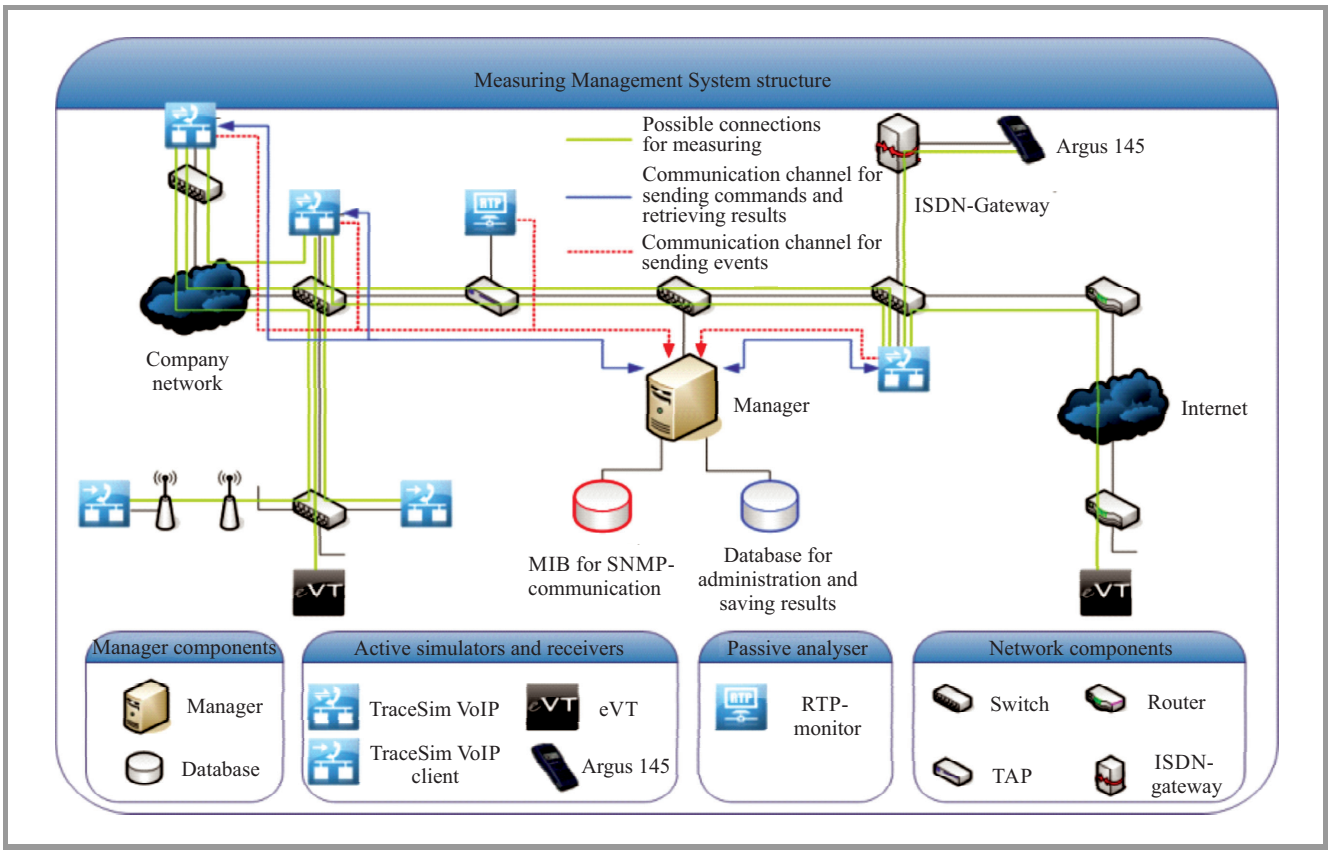


Fig. 6. Architecture of the implemented MMS for QoS in VoIP.

- data and duration of measurement session,
- QoS value for measurement session,
- error indication.

The management entity is also referred to as the manager or NMS. It is responsible for soliciting information from the agent. Such solicitations are based on very specific requests. The manager processes the retrieved information in a number of ways. It can be logged for later analysis, displayed using a graphing utility, or compared with preconfigured values to verify whether a particular condition has been met. Figure 5 presents an example of an implementation of MMS in a real network.

It can be seen that the MMS system consists of several measurement hardware units (Agents) located at characteristic termination points (connected at the interfaces between different network portions) or at node management stations (i.e. the measurement servers in Fig. 5) located in the network core and connected to national or international gateways respectively, or to both. Location of the NMS depends on which portion of the network is to be tested. When testing Internet Service Access within the national network (i.e. within one country) the MMS should be connected to the ISP peer gateway or national gateway. The second solution is recommended for testing and comparison of IAS performed by different ISPs. A measurement scenario must be initialized before measurement traffic can be sent. A special hardware unit with dedicated measurement software plays the role of the agent of the MMS, while measurement servers constitute an NMS. Standard messages, like GET, SET and TRAP, allow the retrieval of MIB values from the agents, the setting of values or notification of important events to the management.

Figure 6 shows the first implementation of a Measuring Management System for QoS in VoIP (designed in compliance with the concept presented above), developed at the Flensburg University of Applied Sciences [33]. The system has a centralized architecture. The manager acts as master and the agents as clients. The manager has two databases: MIB for SNMP communication and SQL for administration and saving results.

The agents contain the measurement systems by the company Nextragen Flensburg, i.e. Trace_View_VoIP, Trace_Sim_VoIP and RTP-Monitor [9]. The agents will be configured by the manager automatically. They send the measurement results back to the manager. It saves and evaluates them. An administrator can access the SQL database any time to view the results obtained.

The tests have confirmed the functionality of the MMS in this configuration, and the new MMS has subsequently been included in the company Nextragen's range of products [9] and is available on the telecommunications market as one of the components of the Trace_Sim_VoIP tool. Using the tool's option EMP (Extended Measurement Plan) it is possible to define the distributed node management sta-

tion (NMS) as an independent measuring node and have it function as one. This provides a platform for identifying bottlenecks and for making reconfigurations accordingly. In the course of time, however, the new MMS has been shown to have two shortcomings: 1) The system's throughput is low and 2) encoding is only done on a pretty primitive level. So the company Nextragen is busy on an even newer, more efficient MMS based on its own high-performance communications protocol coupled with more sophisticated encoding. The latest developments take into account the latest recommendations of both the EU workgroup [23] and the IETF [24].

5. Conclusion and Outlook

This paper has discussed extensively the problems associated with the provision of quality of service of an Internet access connection, i.e. the Internet Access Service. It started with a detailed presentation of the most recent developments in network technologies and emphasised the importance of QoS. It also contained detailed descriptions of the latest activities of the European Parliament and the Council of Europe affecting network neutrality and transparency. It introduced and illustrated with several graphics the measurement points and measurement scenarios that have been based on the recommendations of ITU-T and ETSI and the EU workgroups BEREC and PTTRIS to determine the QoS in networks. The final chapter defined a concept for the so-called MMS and described it in detail. The concept takes account of the recommendations of international standardization organizations and the most important European telecommunications workgroups. The concept is therefore tailor-made for the real world.

One particularly important initiative affecting Internet Access Service QoS evaluation must be mentioned. In 2010 the European Commission contracted the company SamKnows with the identification of the chief impairment parameters in the IP networks of EU member states. So a massive measuring project was called into life that took three years to complete. For the purposes of this study 8,582 households across the European Union were given a specially configured hardware device (SamKnows Whitebox), which runs a series of purpose-built tests to measure every aspect of Internet performance. The final report is available [34] and includes a comprehensive explanation of the project, the purpose, the test methodology and the analysis of performance against key indicators across the EU. The analysis in this report is based on data collected in the month of October 2014. SamKnows continues to look for volunteers to participate in studies throughout Europe. Participants can sign up at www.samknows.eu.

Several member states of the European Union: Poland, Lithuania, Germany, Greece, France and Austria for instance (see Appendix to [26]) have already taken the initiative, implementing MMSs and using them regularly to determine the QoS in IAS. In Poland a new system called NKP (Measurement & Control Tool) [7] went into operation 2015 and it is designed for control of broadband networks built with EU funds. In 2016, it will be built a system for customers as a mechanism monitoring certified to evaluate the service access to the Internet. A similar MMS has been in operation in Germany since early 2016 [35]. This all goes to show that the issue of QoS in Europe's networks is not only being taken seriously, practical steps to assure QoS are also actually being taken.

The examination of QoS in IAS discussed in this paper is to be extended to cover any and all real-time and non-real-time applications available in the modern Internet of Things. Further types of efficient MMSs are needed and will have to be designed and produced. For only through using such MMSs can transparency and network neutrality be achieved throughout the communications market. This will present a major challenge to Internet engineers.

References

[1] ITU-T Recommendations concerning ISDN [Online]. Available: http://www.itu.int/rec/T-REC-I/e

[2] ITU-T Recommendations concerning ATM [Online]. Available: http://members.tripod.com/atm_protocols/PtoP/list.html

[3] IETF Recommendation 791 (IP protocol version 4) [Online]. Available: https://tools.ietf.org/html/rfc791

[4] IETF Recommendation 793 (TCP protocol) [Online]. Available: http://www.ietf.org/rfc/rfc793.txt

[5] Directive 2009/136/EC of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (hereinafter: Citizens' Rights Directive). (Official Journal EU L 337/11, 25 November 2009.

[6] Directive 2009/140/EC of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services (hereinafter: Better Regulation Directive). (Official Journal EU L.337/37, 25 November 2009.

[7] Office of Electronic Communications (UKE) Poland [Online]. Available: http://www.uke.gov.pl

[8] Bundesnetzagentur (BNetzA) for Electricity, Gas, Telecommunications, Post and Railway Germany [Online]. Available: http://www.bundesnetzagentur.de/cln_1931/DE/Home/home_node.html

[9] Company Nextragen [Online]. Available: http://www.nextragen.de

[10] Company Opticom [Online]. Available: http://www.opticom.de

[11] Company Empirix [Online]. Available: http://www.empirix.com

[12] Company Ixia [Online]. Available: http://www.ixiacom.com

[13] Company NetIQ [Online]. Available: http://www.netiq.com

[14] Company Ip-label [Online]. Available: http://www.ip-label.fr

[15] Company Telchemy [Online]. Available: http://www.telchemy.com/index.php

[16] Company Shenick [Online]. Available: http://www.shenick.com

[17] Company VoIP Future [Online]. Available: http://www.voipfuture.com

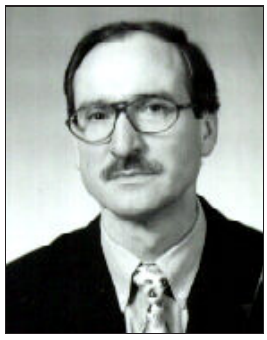
[18] Company Systemics [Online]. Available: http://www.systemics.com.pl

[19] M-Lab consortium [Online]. Available: http://www.measurementlab.net

[20] Tool Broadband speedchecker [Online]. Available: http://www.broadbandspeedchecker.co.uk/compare_broadband.aspx
[21] Protocol analyzer Wireshark [Online]. Available: http://www.wireshark.org
[22] Project Leone – from global measurements to local management [Online]. Available: http://www.leone-project.eu/leone
[23] Project mPlane – an Intelligent Measurement Plane for Future Network and Application Management [Online]. Available: http://www.ict-mplane.eu
[24] Project lmap – Large-Scale Measurement of Broadband Performance [Online]. Available: https://tools.ietf.org/wg/lmap
[25] BEREC, A framework for quality of service in the scope of net neutrality, Document no. BoR (11) 53, 2011 [Online]. Available: http://berec.europa.eu/doc/berec/bov.bov11_53_qualityservice.pdf
[26] BEREC, Monitoring quality of Internet access services in the context of net neutrality, Document no. BoR (14) 117, 2014.
[27] BEREC, Guidelines for quality of service in the scope of net neutrality, Document no. BoR(12) 131, 2012.
[28] ECC Raport 195 [Online]. Available: http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP195.PDF
[29] ETSI EG 202 057 [Online]. Available: https://www.google.de/#q=ETSI+Guide+EG+202+057
[30] ITU-T Recommendation Y.1541 [Online]. Available: https://www.itu.int/rec/T-REC-Y.1541/en
[31] ITU-T Recommendation G.1010 [Online]. Available: https://www.google.de/#q=ITU-T+Recommendation+G.1010
[32] ITU-T Recommendation Y.1540 [Online]. Available: https://www.google.de/#q=ITU-T+Recommendation+Y.1540
[33] H. Jürgensen, "Entwurf und Implementierung eines Measurement Management Systems (MMS)", M.Sc. thesis, Flensburg University of Applied Sciences, Germany, September 2009 (in German).
[34] "Quality of Broadband Services in the EU", Final report, European Commission, October 2014, internal (SamKnows Limited) identification contract number: 30-CE-0392545/00-77.
[35] Broadband measurement in Germany [Online]. Available: https://breitbandmessung.de

Janusz Klink received his M.Sc. and Ph.D. in Telecommunications from Wrocław University of Technology in 1994 and 2000, respectively. Since 1994 he has worked as an Assistant and since 2000 as an Assistant Professor at the Institute of Telecommunications and Acoustics, Wrocław. In 2013 he started to work for Department of Telecommunications and Teleinformatics (since 2007 as Head of Telecommunication Networks Laboratory) at the Faculty of Electronics of the Wrocław University of Technology. His main activities concentrate on the following areas: telecommunication networks, signalling protocols, traffic engineering, quality of service and quality of experience. He is an author or co-author of 14 chapters in books, over 60 papers and 70 reports on the subject of telecommunications networks, services and quality of service.
E-mail: janusz.klink@pwr.edu.pl
Wrocław University of Technology
Janiszewskiego st 9
50-372 Wrocław, Poland

Maria Jolanta Podolska received the M.Sc. in Electronic in Wrocław University of Technology and the Ph.D. in Telecommunications in National Institute of Telecommunications in 2000. From 1983 to 2007 she has carried out research related to objective assessment of voice quality in telecommunications networks in National Institute of Telecommunications in Warsaw. From 2008 she is chief expert in the Office of Electronic Communications (the Polish Regulatory Authority) in the Department of Monitoring and she has provided many projects related to the assessment of the quality of broadband networks. In the years 2014–2015 supervised the execution and implementation of the project Measurement and Control Tool for the technical evaluation of broadband networks built with EU funds. She is a member of the working group BEREC acting on behalf of the European Commission, which deals issues of net neutrality and quality of broadband networks. She is an author and co-author of numerous scientific publications on the regulation and assessment of the quality of telecommunication services.
E-mail: m.podolska@uke.gov.pl
Office of Electronic Communications
Kasprzaka st 18/20
01-211 Warsaw, Poland



Tadeus Uhl received his M.Sc. in Telecommunications from the Academy of Technology and Agriculture in Bydgoszcz, Poland, in 1975, his Ph.D. from Gdańsk University of Technology, Poland, in 1982, and his D.Sc. from the University of Dortmund, Germany, in 1990. Since 1992 he has worked as Professor at the Institute of Communications Technology, Flensburg University of Applied Sciences, Germany, and in addition since 2013 as Professor at the Institute of Transport Engineering, Maritime University of Szczecin, Poland. His main activities cover the following areas: traffic engineering, performance analysis of communications systems, measurement and evaluation of communication protocols, QoS and QoE in Triple Play Services, Ethernet and IP technology. He is author or co-author of three books and some 130 papers on the subjects of LAN, WAN and NGN.
E-mail: t.uhl@am.szczecin.pl
Maritime University of Szczecin
Henryka Pobożnego st 11
70-507 Szczecin, Poland

Paper

Stackelberg Security Games: Models, Applications and Computational Aspects

Andrzej Wilczyński[1,2], Agnieszka Jakóbik[2], and Joanna Kołodziej[2]

[1] *AGH University of Science and Technology, Cracow, Poland*
[2] *Tadeusz Kościuszko Cracow University of Technology, Cracow, Poland*

Abstract—Stackelberg games are non-symmetric games where one player or specified group of players have the privilege position and make decision before the other players. Such games are used in telecommunication and computational systems for supporting administrative decisions. Recently Stackleberg games became useful also in the systems where security issues are the crucial decision criteria. In this paper authors briefly survey the most popular Stackelberg security game models and provide the analysis of the model properties illustrated in the realistic use cases.

Keywords—Bayesian games, game theory, leadership, Nash equilibrium, normal form games, security games, Stackelberg equilibrium, Stackelberg games.

1. Introduction

Game theory is the formal, mathematical methodology for analyzing interactions between intelligent players: people, corporations, software agents, or making decisions robots. The theory is useful for solving problems in many disciplines, from economics, business, and law, public policy to telecommunication. Game theory provides the tools for determining optimal behavior in competitive environments. Formally, *a game refers to all the situations involving two or more intelligent individuals making rational decisions* [1]. The players are making decisions consistently to obtain the assumed target. The player is considered intelligent, if he knows the game rules and can make decisions based on his knowledge.

The basic examples of game theoretical modeling include the simulations of the competitive processes in economics, political science, psychology, or biology. The players are interest groups, politicians, or competing animal species. Computer science uses game theory during modeling multiagent systems, online algorithms or processes in computer networks [2].

Game theory is also useful in the cases where security is important: in everyday life and security of the large-scale IT systems such as computational grids and clouds. The airport police behavior as one side of the conflict playing against thieves or terrorists was modeled. Randomizing schedules for patrolling, checking, or monitoring is typical outcome of the models [3].

In this paper, authors focus on Stackelberg security models, where one or group of players are the privilege in the game. They play first, and the rest of the players follow the leader(s) and make their decisions based on the leader's actions. Such games can be a good proposal for supporting the decisions in the cloud systems, where security remains a challenging research and engineering task. The existing Stackelberg models related to the security aspects in high performance computing telecommunication and transportation systems are surveyed and the models properties from the implementation perspective are analyzed. The effectiveness of the models has been justified in realistic use cases.

The paper is organized as follows. In Section 2 the basic definitions and backgrounds of the game-theoretical models are explained together with the definition of the generic Stackelberg game. In Sections 3 and 4 the secure Stackelberg game is defined and the most popular Stackelberg security models are reviewed. The computational and implementation aspects of the analyzed Stackelberg models are discussed in Section 5. In Section 6 the realistic use cases for Stackelberg security games are presented. Section 7 concludes the paper.

2. Game Theory – Backgrounds and Game Models

Game theoretical models are very useful in the formal analysis of task, data and information management and decision-like processes in highly distributed large-scale computational environments mainly because of the strict mathematical formalism. Although, there are many types of games and also many formal models of such games, the most commonly used and known is the *normal-form game model* introduced by Tadelis *et al.* [4] as follows:

Normal-form game consists of three sets: players, strategies and payoff functions specified for each player in order to define the solution of the game for each combination of the players' actions.

Formally, the n-player normal game Γ_n can be defined by the following rule:

$$\Gamma_n = (N, \{S_i\}_{i\in N}, \{Q_i\}_{i\in N}) \,, \tag{1}$$

where:

- $N = \{1,\ldots,n\}$ is the set of players,
- $\{S_1,\ldots,S_n\}$ ($card\ S_i \geq 2; i = 1,\ldots,n$) is the set of strategies for the players,
- $\{H_1,\ldots,H_n\}; H_i : S_1 \times \cdots \times S_n \to \mathbb{R}; \forall_{i=1,\ldots,n}$ is the set of payoff functions of the players.

The strategy of the player in the game can be defined as a plan of actions of that player to make the game beneficial for him. Two classes of strategies are defined, namely pure strategies and mixed strategies [4].

Definition 1. Pure strategy of the player i is the deterministic plan of player's actions during the game. The set of all pure strategies specified for player i is denoted by S_i. A profile of pure strategies in the n-players game Γ_n is defined by the following vector of the players' strategies:

$$s = [s_1, s_2, \ldots, s_n], s_i \in S_i; (i = 1,2,\ldots,n). \tag{2}$$

Such strategy profile can be defined for any combination of the players' pure strategies in the game Γ.

Definition 2. Let us denote by $S_i = s_{i1}, s_{i2}, \ldots, s_{im}$ the finite set of m pure strategies of the player i. Let us also denote by ΔS_i the simplex over S_i. ΔS_i is the set of all probability distributions over S_i.
The mixed strategy of player i is denoted by $\sigma_i \in S_i \subset \Delta S_i$ and is defined as follows [4]:

$$\sigma_i = \{\sigma_i(s_{i_1}), \sigma_i(s_{i_2}), ..., \sigma_i(s_{i_m})\}, \tag{3}$$

where $\sigma_i(s_i)$ is the probability that the player i plays according to the strategy s_i.

One can conclude from the above definition that $\sigma_i(s_i) \geq 0$ for all $i = 1,\ldots N$ and

$$\sigma_i(s_{i_1}) + \sigma_i(s_{i_2}) + \ldots + \sigma_i(s_{i_m}) = 1\,. \tag{4}$$

It can be also observed that the mixed strategy becomes pure if $\sigma_i(s_{i_j}) = 1$ for some j $\sigma_i(s_{i_k}) = 0$ for all $k \neq j$.
In the mixed strategy model, the decisions of each player are randomized according to the probability distribution $\sigma_i(s_i)$. In such a case, the payoffs are also non-deterministic.

Definition 3. Tadelis *et al.* [4] the expected payoff of player i in 2-players game is defined as:

$$H_i(s_i, \sigma_{-i}) := \sum_{s_{-i} \in S-i} \sigma_{-i}(s_{-i}) H_i(s_i, s_{-i})\,, \tag{5}$$

where $H_i(s_i, s_{-i})$ is the payoff function calculated for the player i. It is assumed in that game, that player i chooses the pure strategy $s_i \in S_i$ and his opponents plays the mixed strategy $\sigma_{-i} \in \Delta S_{-i}$.

Similarly:

Definition 4. The expected payoff of player i when he chooses the mixed strategy $\sigma_i \in \Delta S_i$ and his opponents plays the mixed strategy $\sigma_{-i} \in \Delta S_{-i}$ is defined in the following way:

$$H_i(\sigma_i, \sigma_{-i}) = \sum_{s_i \in S_i} \sigma_i(s_i) H_i(s_i, \sigma_{-i}) =$$
$$= \sum_{s_i \in S_i} \Big(\sum_{s_{-i} \in S_{-i}} \sigma_i(s_i)\sigma_{-i}(s_{-i}) H_i(s_i, s_{-i}) \Big)\,. \tag{6}$$

The main aim of each player during the game it to maximize his expected payoff by defining the optimal strategy. The most commonly encountered concept of the game solution is an equilibrium point defined as follows:

Definition 5. An n-dimensional vector $(\bar{s}_1,\ldots,\bar{s}_n)$ of strategies is called an equilibrium point or Nash equilibrium, if:

$$H_i(\bar{s}_1,\ldots,\bar{s}_n) = \max_{s_i \in S_i} H_i(\bar{s}_1,\ldots,\bar{s}_{i-1}, s_i, \bar{s}_{i+1},\ldots,\bar{s}_n)$$
$$\text{for all } i = 1,\ldots,n\,. \tag{7}$$

The Nash equilibrium [5] can be interpreted as a steady state of the play of a strategic game, in which each player holds correct expectations concerning the other players' behaviors. If the strategies chosen by all players are Nash equilibrium, no player is interested in changing his strategy.
An n-vector $\bar{H} = \big(H_1(\bar{s}_1,\ldots,\bar{s}_n),\ldots,H_n(\bar{s}_1,\ldots,\bar{s}_n)\big)$ is called a value of the game. The strategies $(\bar{s}_1,\ldots,\bar{s}_n)$ are the pure strategies (see Def. 1). It means that they are never changed during the game.
Some equilibrium points cannot be accepted as solutions of the game. It is usually required that the solution should not satisfy the following condition:

Definition 6. An n-dimensional vector of strategies $(\hat{s}_1,\ldots,\hat{s}_n)$ is Pareto non-optimal, if there exists another n-vector $(\check{s}_1,\ldots,\check{s}_n)$, for which the following two conditions hold:

$$\forall_{i \in \{1,\ldots,n\}}\ H_i(\hat{s}_1,\ldots,\hat{s}_n) \leq H_i(\check{s}_1,\ldots,\check{s}_n)\,, \tag{8}$$

$$\exists_{i \in \{1,\ldots,n\}}\ H_i(\hat{s}_1,\ldots,\hat{s}_n) < u_i(\check{s}_1,\ldots,\check{s}_n)\,. \tag{9}$$

One can say that the n-vector $(\check{s}_1,\ldots,\check{s}_n)$ dominates $(\hat{s}_1,\ldots,\hat{s}_n)$.
It can be observed, that vector $(s_1,\ldots,s_n)$ cannot be accepted as the solution of the game, if it is Pareto non-optimal (even if it is the Nash equilibrium).

2.1. Minimization of the Game Multi-loss Function

The problem of detecting the Nash equilibrium of a finite strategic non-cooperative game can be also formulated as a global optimization problem with loss instead of payoff functions.
Let us define a set of loss (cost) functions for the players:

$$\{Q_1,\ldots,Q_n\}; Q_i : S_1 \times \cdots \times S_n \to \mathbb{R}; \forall_{i=1,\ldots,n}\,. \tag{10}$$

Each player tends to the minimization of his loss function in the game, which is equivalent with the maximization of

the payoff function. Let us define a set of *players' response functions* $\{r_i\}_{i=1,\ldots,n}$; $r_i : S_1 \times \cdots \times S_n \to \mathbb{R}$ where:

$$r_i(\hat{s_i}) = \arg\min_{s_i \in S_i} \{Q_i(s_1, \ldots, s_n)\}, \tag{11}$$

where $\hat{s_i} = (s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$. The response function defines an optimal strategy for the player.

We can define now *a multi-loss function* $Q : S_1 \times \cdots \times S_N \to \mathbb{R}$ for the game by the formula:

$$Q(s_1, \ldots, s_n) = \sum_{i=1}^{n} \left[Q_i(s_1, \ldots, s_n) - \min_{s_i \in S_i} Q_i(s_1, \ldots, s_n) \right]. \tag{12}$$

Note that the multi-loss function has non-negative values. In such a case, the Nash equilibrium is the result of the global minimization of the function Q. The players' strategies are called the decision variables and the players' loss functions are called players' objective functions.

It follows from the definition of the function Q that is needed to minimize first the loss functions of the players and then to compute the values of the multi-loss function. Thus the detection procedure of the Nash equilibrium is a parallel algorithm composed of two cooperated units:

- **main unit** – which solves the problem of global minimization of the function Q,
- **subordinate unit** – which solves the problems of minimization of the players' loss functions Q_i.

The subordinate unit could be a parallel algorithm designed for the numerical optimization of the real functions of several variables.

2.2. Stackelberg Games

In all game scenarios considered in the Section 2, it was assumed that the games are symmetric. It means that all players have the same privileges and knowledge about the game conditions and the other players' strategies and actions. However, that assumption may never occur in the real situations, where usually there is a player (or group of players) with the deeper knowledge of the game conditions. Cloud administrators and local cloud service providers can be good examples of the realistic potential players in non-symmetric resource allocation decision making game model. In grid and cloud computing, Stackelberg games are the most popular non-symmetric game models used for supporting the decisions of various system users.

In Stackelberg game [6], one user acts as a *leader* and the rest are his *followers*. The leader may keep his strategy fixed while the followers react independently subject to the leader's strategy. Formally, the N-players Stackelberg game can be defined as two-level game model, where the players act sequentially as follows: (i) the leader is the only player active at the first level, he chooses his best-response strategy; (ii) at the second level, the followers react rationally to the leader's action. It means that they try to minimize their game cost functions subject to the leader's choice. Finally, the leader updates his strategy to minimize the total game cost.

The solution of the Stackelberg game is called *Stackelberg equilibrium*. In such a case, each follower observes the leader's strategy x and responds with strategy $f(x) : x \to y$ that is optimal with respect to his expected payoff. Two types of Stackelberg equilibrium points can be defined, namely Strong Stackelberg Equilibrium (SSE) and Weak Stackelberg Equilibrium (WSE). SSE assumes that the follower breaks ties in favor of the defender. It means that he chooses his optimal strategy, which is also optimal from the leader's perspective. WSE assumes that the follower chooses the worst strategy from the leader's perspective [7]. Formally, both scenarios can be defined in the following way:

Definition 7. A pair of strategies $\big(x, f(x)\big)$ is defined as Strong Stackelberg Equilibrium if the following conditions are satisfied [7]:

1. The leader plays his best-response strategy:

$$H_l\big(x, f(x)\big) \geq H_l\big(x', f(x')\big), \tag{13}$$

   for all leader's strategies x'.

2. The follower plays his best-response strategy:

$$H_f\big(x, f(x)\big) \geq H_f(x, y'), \tag{14}$$

   for all follower's strategies y'.

3. The follower breaks ties in favor of the leader:

$$H_l\big(x, f(x)\big) \geq H_l(x, y'), \tag{15}$$

   for all optimal follower's strategies y'.

2.3. Bayesian Stackelberg Games

In Bayesian Stackelberg Game, the *type* of player must be specified for each of N players. In two players game, there is only *one leader type*, although there are multiple follower types, denoted by $l \in L$. Authors define the probability p^l that a follower of type l will appear in the game. The leader does not know the follower's type. For each player type (leader or follower) n, there is a set of strategies σ_n and a utility function of the game $Q_n : L \times \sigma_1 \times \sigma_2 \to \mathbb{R}$, which is usually defined as the game cost function of the given player n [8].

Bayesian game can be transformed into a normal-form game using Harsanyi transformation. Let us assume there are two follower types 1 and 2. Type 1 will be active with probability α, and follower type 2 will be active with proba-

Table 1
Payoff tables for a Bayesian Stackelberg game with 2 follower types

	c	d	c'	d'
a	2.1	4.0	1.1	2.0
b	1.0	3.2	0.1	3.2

Table 2
Harsanyi transformed payoff table

	cc'	cd'	dc'	dd'
a	$2\alpha+(1-\alpha),1$	$2,\alpha$	$4\alpha+(1-\alpha),(1-\alpha)$	$4\alpha+2(1-\alpha),0$
b	$\alpha,(1-\alpha)$	$\alpha+3(1-\alpha),2(1-\alpha)$	$3\alpha,2\alpha+(1-\alpha)$	$3,2$

bility $1-\alpha$. A chance node must be specified for Harsanyi transformation. That node is required for the specification of the follower's type. It transforms the leader's incomplete information regarding the follower into an imperfect information game. In the transformed game, the leader still has two strategies while there is a single follower type with four $(2\cdot 2)$ strategies [8]. That scenario is illustrated in Tables 1 and 2.

3. Security Stackelberg Games

Decision processes of users, administrators and resource owners in high performance computational systems are very complex especially in the case, where security and data protection are the important decision criteria. Game models and Stackelberg games in particular, can be very useful in supporting such difficult decisions. The game models used in security applications are called *security games*.
Security game is a game between defender and attacker. The attacker may pick any target from the target set:

$$Targets = \{t_1,\ldots,t_n\}. \tag{16}$$

The defender may cover targets by available resources from the set of resources:

$$Resources = \{r_1,\ldots,r_K\}. \tag{17}$$

Tambe *et el.* [9] defined the compact security game model. In this model, all resources are identical and may be assigned to any target and payoffs depend only on the identity of the attacked target and whether or not it is covered by the defender.
Any security game represented in this compact form can also be represented in normal form. The attack vector A maps directly to the attacker's pure strategies, with one strategy per target. For the defender, each possible allocation of resources corresponds to a pure strategy in the normal form. A resource allocation maps each available resource to a target, so there are *n Choose m* ways to allocate m resources to n targets [9].
Let us denote the defender utility if t_i is attacked when it is covered by $U_d^c(t_i)$, and defender utility if t_i is attacked when it is uncovered by $U_d^u(t_i)$, and attacker utility $U_a^c(t_i)$ and $U_a^c(t_i)$, respectively. Then, during the game, it is assumed that adding the resource to cover targets benefits the defender and operates to the detriment of attacker:

$$U_d^c(t_i)-U_d^u(t_i)>0, U_a^u(t_i)-U_a^c(t_i)>0. \tag{18}$$

For each resource r_i there is a subset S_i of of the schedules S that r_i can cover. The example of such a situation is marshal's fly tours. In security game, the defender may play best-response strategy, however, it depends on the attacker's behavior.
In normal representation of security game, the attacker's pure strategy is specified as a set of targets. The attacker's mixed strategy is defined by the following vector $\mathbf{a}=[a_1,\ldots,a_n]$ representing the probability of attacking the targets. The defender's pure strategy is defined by the coverage vector $\mathbf{d}\in\{0,1\}^n$, where d_i represents if target t_i is covered or not. Let us denote by $D\in\{0,1\}^n$ the set of possible coverage vectors, and by $\mathbf{c}$ the vector of coverage probabilities. The defender's mixed strategy C is defined as the vector of probabilities of playing each $\mathbf{d}\in D$. For strategy C, the defenders utility is defined as:

$$U_d(C,a)=\sum_{i=1}^{n} a_i\left(c_iU_d^c(t_i)+(1-c_i)U_d^u(t_i)\right), \tag{19}$$

and attacker's utility is defined in the following way:

$$U_a(C,a)=\sum_{i=1}^{n} a_i\left(c_iU_a^c(t_i)+(1-c_i)U_a^u(t_i)\right). \tag{20}$$

In symmetric security games, the Nash equilibrium can be also estimated. In such a case, the defender plays his best-response strategy C, such that for any other strategy C', his utility is the most beneficial:

$$U_d(C,a)>U_d(C',a). \tag{21}$$

The attacker plays also his best-response strategy a, such that for any other strategy a', his utility is the most beneficial:

$$U_a(C,a)>U_a(C,a'). \tag{22}$$

The game model, in which the defender makes his decision first and attacker chooses his strategy based on the results of the defender's action, is called *security Stackelberg game*. In that game, $g(C)=\mathbf{a}$ is the attacker response function. Strong Stackelberg Equilibrium (SSE) can be found by:

- the defender plays the best-response strategy C, such that $U_d(C,g(C))>=U_d(C',g(C'))$ for all C',
- the attacker plays the best-response strategy C, such that $U_a(C,g(C))>=U_a(C,g'(C))$ for all g',C,
- the attacker breaks ties optimally for the leader: $U_d(C,g(C))>=U_d(C,\tau(C))$ for all C, where $\tau(C)$ is the set of followers best responses to C.

The basic version of the game assumes that utility functions are common knowledge. In SSE (see Def. 7), the

attacker must know the defender's utility, in order to compute his own strategy. In Nash equilibrium, the attacker does not follow the defender's actions. In real life applications, defender does not know the attacker's utility function and the game may be defined by using the Bayesian model. The assumption that attacker responds optimally (selects the best-response strategy) may not happen either (imperfect follower case) [10].

4. Secure Stackelberg Game-based Models

In this section, the most popular Stackelberg security game models are surveyed. Presented models were selected due to the increasing limitations on resources and growing attackers' number, incorporating uncertainty about the optimal behavior of attackers, uncertainty about the observation possibility.

4.1. DOBSS Model

Paruchuri *et al.* in [11] considered the Bayesian Stackelberg security game for one leader, multiple independent followers and the situation when the leader does not know the follower type. For leader strategy vector $x = [x_1, \ldots, x_n] \in [0,1]$ represents the proportion of times when pure strategy $i = 1, \ldots, n$ was chosen. The authors proposed the algorithm for finding the optimal mixed strategy for the leader, under the assumption that the follower (attacker) knows this mixed strategy choosing his own. The authors defined the following two utility matrices for the leader $U_d^{i,j} = R_{i,j}$ and attacker $U_a^{i,j} = C_{i,j}$. It is assumed that the leader plays pure strategy i and attacker plays pure strategy j.
Let us denote by $q = [q_1, \ldots, q_n] \in \{0,1\}$ the mixed strategy for the follower, X – leader pure strategies index set, and by Q – the pure follower's strategy indexes. The algorithm is implemented in the following steps (one follower is considered):

- for fixed leader strategy X the follower solves the linear problem to find his optimal response:

$$\max_{q} \sum_{j \in Q} \sum_{i \in X} C_{i,j} x_i q_j \,, \tag{23}$$

  with constraints that means that every pure strategy is possible:

$$\sum_{j \in Q}^{q_j >= 0} q_j = 1 \,; \tag{24}$$

- the leader finds the strategy x that maximizes his utility, under the assumption that the follower used optimal response $a(x)$:

$$max_q \sum_{i \in X} \sum_{j \in Q} R_{i,j} q(x) x_i \,, \tag{25}$$

  with assumption that each pure strategy is possible:

$$\sum_{i \in X}^{x_i \in [0,1]} x_i = 1 \,. \tag{26}$$

The authors proposed also the model for multiple followers, with specified recognition probability of the follower's type. Let us denote by $U_d^{i,j,l} = R_{i,j}^l$ and $U_a^{i,j,l} = C_{i,j}^l$ the utility matrices of the leader's respectively. Leader plays pure strategy i and attacker plays pure strategy j, and the follower type is l. Let us also denote by p^l the probabilities of playing with the follower of type l. The solution of such a game can be defined as quadratic programming problem (specified for the leader) with the following distribution over the follower type p^l:

$$\max_{x,q,a} \sum_{i \in X} \sum_{l \in L} \sum_{j \in Q} p^l R_{i,j}^l q_j^l x_i \,, \tag{27}$$

with the following leader's and follower's strategies:

$$\sum_{i \in X}^{x_i \in [0,1]} x_i = 1 \,, \sum_{j \in Q}^{q_j^l \in [0,1]} q_j^l = 1 \,. \tag{28}$$

It can be observed that $q_j^l = 1$ only for a strategy that is optimal for follower l:

$$0 =< \left(a^l - \sum_{i \in X} C_{i,j} x_i <= (1 - q_j^l) M\right), \tag{29}$$

where M is the fixed large positive number, and $a \in \mathbf{R}$.

In the above models, the players are completely rational (they play according to the concrete calculated strategy) and followers can follow the leader's strategy. The quadratic problem given by Eqs. (27)–(29) may be linearized by defining the new variables $z_{i,j}^l := x_i q_j^l$.

4.2. BRASS, BOSS and MAXMIN Models

Pita *et al.* in [12] proposed three mixed-linear program algorithms for solving the Bayesian Stackelberg games. They considered the following two game scenarios:

- bounded rationality of the followers scenario – the leader cannot be sure that he will play the game according to the calculated strategy with the selection ε-optimal response strategy – the follower may choose any response,
- uncertainty scenario – the recognition of the leader's strategy by the follower can be incorrect.

In the first case, the problem of solving the game was defined as the following BRASS linear programming problem:

$$\max_{x,q,h,a,\gamma} \sum_{l \in L} p^l \gamma^l \,, \tag{30}$$

where the leader's and follower's strategies can be specified as:

$$\sum_{i \in X}^{x_i \in [0,1]} x_i = 1 \,, \tag{31}$$

allowing to select more than one policy per follower type

$$\sum_{j \in Q} q_j^l >= 1, \sum_{j \in Q} h_j^l = 1 \,, \tag{32}$$

and the condition that ensure that $q_j^l = 1$ only for a strategy that is optimal for follower l:

$$0 =< \left(a^l - \sum_{i \in X} C_{i,j} x_i <= (1 - h_j^l)M\,, \tag{33}$$

$$\varepsilon(1 - q_j^l) =< a^l - \sum_{i \in X} C_{i,j}^l x_i <= \varepsilon + \left(1 - q_j^l\right)M\,, \tag{34}$$

$$(1 - q_j^l)M + \sum_{i \in X} R_{i,j}^l x_i >= \gamma_l\,, \tag{35}$$

where $h_j^l =< q_j^l$, $h_j^l, q_j^l \in \{0,1\}$, for the fixed large positive number M and $a \in \mathbf{R}$.

In the uncertainty scenario model (BOSS), developed by Jain *et al*. [12], the follower may not change the optimal calculated strategy, but deviate from it. Instead of x_i, the follower plays $x_i + \delta_i$.

The authors proposed also the third MAXMIN model, which is a simple combination of BRASS and BOSS models. The main aim in this model is to maximize the minimal reword γ irrespective of the followers' action:

$$\max_{\gamma} \sum_{l \in L} p^l \gamma^l\,, \tag{36}$$

where the leader's and follower's are defined in the following way:

$$\sum_{i \in X}^{x_i \in [0,1]} x_i = 1\,, \tag{37}$$

$$\sum_{i \in X}^{x_i \in [0,1]} R_{i,j}^l x_i >= \gamma^l\,. \tag{38}$$

4.3. COBRA Models

Pita *et al*. in [12] defined following three game models: (i) COBRA(0, ε) model (bounded rationality), (ii) COBRA(α, 0) model (observational uncertainty), and (iii) COBRA(α, ε) model as the combination of (i) and (ii). Parameters α and ε are two main parameters of the games. For the real leader's strategy x and follower's strategy x', the problem of solving the game is defined as the linear problem $x_i' = \alpha(1/|X|) + (1\alpha)x_i$. The value of α=1 indicates the player's behavior in the situation of no knowledge about the other strategies – any strategy is uniformly probable. For $\alpha = 0$ (full information available), $x_i' = x_i$ is the optimal strategy played by the follower. For $\alpha = 1$, $x_i' = (1/|X|)$ is the probability of playing the strategy x_i'.

Using that model, the following problem as the game solution was formulated:

$$\max_{x,q,h,a,\gamma} \sum_{l \in L} p^l \gamma^l\,, \tag{39}$$

under the following constrains:

$$\sum_{i \in X}^{x_i \in [0,1]} x_i' = 1, \sum_{j \in Q} q_j^l >= 1, \sum_{j \in Q} h_j^l >= 1\,, \tag{40}$$

$$0 =< (a^l - \sum_{i \in X} C_{i,j} x_i' <= (1 - h_j^l)M\,, \tag{41}$$

$$\varepsilon(1 - q_j^l) =< a^l - \sum_{i \in X} C_{i,j}^l x_i <= \varepsilon\,, +(1 - q_j^l)M\,, \tag{42}$$

$$(1 - q_j^l)M + \sum_{i \in X} R_{i,j}^l x_i >= \gamma_l\,, \tag{43}$$

where $x_i' = \alpha(1/|X|) + (1\alpha)x_i$, $h_j^l =< q_j^l$, $h_j^l, q_j^l \in \{0,1\}$, for M being the large positive number, and $a \in \mathbf{R}$.

4.4. ORIGAMI Model

Kiekintveld *et al*. in [13] defined the model in which the attack set can be computed directly for the attacker in order to cover target benefits of defender and for the detriment of attacker. Let us denote by C the coverage vector for the defender selected the optimal strategy, and by c_t the probabilities that t-th target is covered. It is assumed, that including any additional target to the attack set cannot increase the players' payoffs in the equilibrium states of the game. Using indifference equation if $U_a(C) = x$ then:

$$c_t >= \frac{x - U_a^u(t_i)}{U_a^c(t_i) U_a^u(t_i)}\,, \tag{44}$$

for each target t_i, such that

$$U_a^u(t_i) > x\,. \tag{45}$$

In the algorithm defined for solving the ORIGAMI game models, the target has maximal $U_a^u(t_i)$, and the attack set is updated in each algorithm iteration for decreasing $U_a^u(t_i)$. After each update of the attack set, the coverage of each target is updated to reach the indifference of attacker payoffs in the attack set.

4.5. SU-BRQR Model

Nguyen *et al*. in [14] modified the standard Stackelberg security model by introducing the following subjective utility function:

$$a_i = w_1 c_i + w_2 U_a^u(t_i) + w_3 U_a^c(t_i)\,, \tag{46}$$

where w, w_2, w_3. The optimal strategy is calculated as follows:

$$\max_{c} \sum_{i=1}^{n} \frac{e^{(w_1 c_i + w_2 U_a^u(t_i) + w_3 U_a^c(t_i))}}{\sum_{j'=1}^{n} e^{(w_1 c_j + w_2 U_a^u(t_j) + w_3 U_a^c(t_j))}} \cdot \ldots \tag{47}$$

$$\ldots \cdot \left(c_j U_a^c(t_j) + (1 - c_j) U_a^u(t_j)\right)\,,$$

where

$$\sum_{i=1}^{n} c_t <= K, \quad 0 =< c_t <= 1\,.$$

In this model, the adversary has his own preferences according to the importance of the rewords, penalties, and probabilities. The authors recommended the maximum like-

hood estimation method for estimating the game parameters w_1, w_2, w_3.

4.6. Eraser-C Model

Tsai *et al*. in [15] tried to simplify the standard security Stackelberg game model. In their model, the payoffs depend on the structure of the coverage set (the attacked target can be its element or not). In this model the actions of the players are defined by the targets instead of coverage sets.

4.7. ASPEN Model

Jain *et al*. in [16] considered large, arbitrary schedules in the Stackelberg security game. The main idea of their model is to represent strategy space for defender using column generation, subcompositions into smaller problems, and a technique for searching the space of attacker strategies. The solution is dedicated for large number of defenders of different types.

4.8. GUARDS Model

Bo An *et al*. in [17] defined the model for massive scale games with hundreds of heterogeneous security activities, reasoning over different kind of potential threats. They considered the situation when the defender has the possibility of protecting targets by different heterogeneous security activities for each potential target, and an adversary can execute heterogeneous attacks on a target. In addition, the defender is able to allocate more than one resource for covering a given target. Moreover, the authors defined the defender's uncertainty regarding the payoff values of the attacker, and uncertainty in the attackers' observation of the defender's strategy. Pita *et al*. proposed model for heterogeneous security activities for each target and heterogeneous threats for each target.

4.9. Multiple SSE Case

Tambe *et al*. in [18] defined the game scenario, where the attacker deviates from optimal strategy, with unknown capability constraints that may restrict the attack set. Authors introduced equilibrium refinement algorithm. In the case of multiple SSE states, the developed algorithm is able to choose the robust equilibrium for the most efficient utilization of the available resources. The idea is based on the fact that if the vector of coverage $c = [c_1, \ldots, c_n]$ generates the SSE, then it is possible to find another SSE by reducing coverage of targets outside the attack set. The authors defined the maximum attack set (MSSE) as:

$$M = \{t \in Target\ s : U_a^u(t) >= U_a(c,a)\}. \qquad (48)$$

They proved that any security game could not have two maximum attack sets with different attack sets. The authors sorted target set using the values of utility function $U_a^u(t)$ in the following way:

$$Target\ s_{sorted} = \{t_1, \ldots, t_n\}. \qquad (49)$$

The authors also developed the concrete algorithm for computing the unique maximum attack set. It starts with $M = t_1$ and generates new targets in each iterated loop (Algorithm 1).

Algorithm 1: Computing the unique maximum attack set

```
i ← 0, M ←, Target s_sorted
while i <= n do
  if M = Target s_sorted then return M
  j ← i+1, M' ← M ∪ {t_j}, Target s_sorted
      while j > n and U_a^u(t_{j+1} = U_a^u(t_j)) do
        M' ← M' ∪ {t_{j+1}}, j++
      end do
if Condition C1 is true or C2 is violated for attack set M'
then return M
  M ← M', i ← j
end do
```

The following conditions were defined for the above model:

- C1 – $\sum_{t \in M} c_t <= m$,
- C2 – $c_t <= 1$ for each $t \in M$.

4.10. Multi-step Attack MILP Model

Vorobeychik *et al*. in [19] considered the game scenario when each attack may be realized in many steps and to be completed it requires an arbitrary number (h) of such steps. Mixed integer linear programming (MILP) formulation for defender was proposed by discretizing the time unit interval defender probabilities was spited into L intervals. Authors proposed $d_{i,j,l}$ as the binary variables such equals 1 indicates a particular discrete probability choice $p_l \in [0,1]$ for $l = 1 \ldots, L-1$ with $p_0 = 0$ and $P_L = 1$, such that only one chose is possible, that is $\sum_l d_{i,j,l} = 1$. Based on this idea, new set of variables $w_{i,j,l} = d_{i,j,l} v_j$ was introduced, where v_j is the expected attacker value of starting in state j. The model includes the probability that a target j is visited in exactly t steps, starting from i and the probability that j is visited in $1 \ldots h$ steps.

5. Computational Aspects

All secure Stackelberg game models surveyed in the previous section can be solved by the global optimization of the game utilization function (loss or game payoff) in the same way it was defined in Section 2 for the generic game models. Such global optimization problems for Stackelberg security games can be defined usually as special cases of mixed-integer linear problems (MILP) or mixed-integer-quadratic programming problems (MIQP). Depending on the type of the game, such problems are of different computational complexity (Table 3). Such complexity can be expressed by the number of control variables (strategies), the number of leaders and followers and the number of

uncertainty parameters in the game, which are estimated by using the likelihood methods.

Table 3
The characteristics of surveyed Stackelberg models

Reference	Size	Value examined
[17]	5 / 20	Runtime, memory usage
[12]	50 / 200	Runtime, memory usage
[13]	3 / 8	Defender expected utility
[14]	9 / 24	Defenders expected utility
[20]	3 / 3	Pure strategies behavior
[12]	3 / 10	Runtime, expected rewards
[14]	3 / 10	Runtime
[11]	2 / 14	Runtime, speed up

The following theorem was proof according to the computational complexity of the problem [5]. In 2-player normal-form games, an optimal mixed strategy to commit to can be found in polynomial time using linear programming, in 3-player normal-form games, finding an optimal mixed strategy to commit to is NP-hard. Moreover, finding an optimal mixed strategy to commit to in 2-player Bayesian games is NP-hard, even when the leader has only a single type and the follower has only two actions.

5.1. Equilibrium Points

SSE and NE equilibrium states (defined in Section 2) are the typical solutions for Stackelberg and non-cooperative symmetric games. In Stackelberg security game, there is however, the third type of equilibrium state, which can be the most beneficial solution of such game in many practical applications.
Let us denote by $\Omega_{NE} :=$ a set of strategies played for reaching the Nash equilibrium, and by $\Omega_{SSE} :=$ a set of strategies for reaching strong Stackelberg equilibrium.

Definition 8. For a defender's mixed strategy C and attacker's best response strategy $E(C) = \max_{i=1}^{n} U_a(c,t_i)$, a set of defender's minimax strategies is defined as:

$$\Omega_M := \{C : E(C) = E^*\}, \tag{50}$$

where $E^* = \min_C E(C)$ is the minimum of attacker's best response utilities over all defender's strategies.

The following relations among these three types of equilibrium states can be specified:

- in a security game the set of defenders minimax strategies is equal to the set of defenders NE strategies, that is $\Omega_M = \Omega_{NE}$,
- if C is the SSE strategy in a security game that satisfies the property that for any recourse and any subset of a schedule is also a possible schedule then $\Omega_{SSE} \subset \Omega_M = \Omega_{NE}$.

Solving MILP and MIQP problems may be done by one of traditional methods: simplex method, interior-point methods, Conic linear programming, descent methods, conjugate direction methods or Quasi-Newton methods [21]. In addition a lot of new methods were developed recently, from among them: relaxation method [22], Dantzig-Wolfe decomposition [23], primal nested-decomposition method [24].

5.2. Time of Solution Finding

All the Stackelberg security game models presented in Section 3 cannot be compared to each other in the straightforward way, because they differ according to the assumptions. A simple summative analysis have been performed with runtime, memory usage expected utility values, strategies behavior and speed up as the main criteria. The results of such analysis are presented in Table 4. The time that is necessary for computing proper strategies depends on the characteristics of the machine that was used for computation.
We can conclude from conducted simple analysis of the surveyed Stackelberg game models that the strategy space may exponentially increase with the number of security activities, attacks, resources, and the time necessary for finding the game solution.

Table 4
The time a for finding solution to the maximum problem

Reference/model	Time [min]	Size [targets]
[17]	8.2	250
[12]	116	200
[13] DOBSS	4.5	20
[13] ERASER	10.5	3000
[13] ORIGAMI	10.2	3500
[12] COBRA	7.5	8 followers
[12] DOBSS	11	8 followers
[14] BOSS	16.5	200
[11]	16.5	4

6. Use Cases

Stackelberg security games have been successfully implemented in realistic large-scale IT systems for supporting the system management and users and administrators decisions. In this section the most interesting use cases for such game models are reported.
The most spectacular implementation of the security Stackelberg game model is the security system at the Los Angeles International Airport. Randomizing schedules in such systems for monitoring the system performance is a critical issue. The main reason for that is the importance of the knowledge about the possible patrolling that may cause terrorist attacks. This use case was realized as a software-assistant multi-agent system called ARMOR (Assistant for Randomized Monitoring over Routes). This model supports the administrators and users decisions

about the location of the checkpoints in the physical environment or canine patrol routes. The decision model is based on the Bayesian Stackelberg games, in which the optimal mixed strategy is generated for the leader (patrol) and the follower (terrorist) may know this mixed strategy when choosing his own strategy in the game [9].

The next example of the practical Stackelberg game is the strategic security allocation system in transportation networks (IRIS) used by Federal Air Marshal Service (FAMS). In transportation networks with hundreds thousands of vehicles, police has to create patrolling schedules in order to ensure safety. Aggressors can observe the law-enforcement patterns and try to exploit generated schedule. IRIS systems use the fastest known solver for this class of security games, namely ERASER-C [9].

Another Stackelberg use case is the United States Transportation Security Administration system (TSA). The transportation systems are very large and protecting them requires many personnel and security activities. System supported the decisions how properly divide resources between layers of security activities. In this type of game, TSA acts as a defender who has a set of targets to protect, a number of security activities and a limited number of resources. The name of dedicated software system is Game-theoretic Unpredictable and Randomly Deployed Security (GUARDS) [9].

There are many applications of game theory in communications and networking. Using a variety of tools from game theory, there was possible to find new solutions in areas related to cellular and broadband networks such as uplink power control in CDMA networks, resource allocation in OFDMA networks, deployment of femtocell access points, IEEE 802.16 broadband wireless access, and vertical handover in heterogeneous wireless networks [25].

7. Conclusions

Security Stackelberg games presented in this paper are very promising tools for modeling the data and user managements, as well as supporting complex decision processes in competitive computational environments with possible conflicts of interests of the users and system administrators and service and resource providers. All surveyed models were based on the realistic characteristics of the systems, namely existing limitations in access to the resources, uncertainty about follower types, non-optimal behavior of the players or limited knowledge of the opponents' actions and strategies. Increasing the efficiency of the game model is strictly connected with the increase of the calculated number of parameters in the game and equations to solve in the game optimization models, which makes of course the all implementation of such models more complex.

Although, all optimization problems related to solving the presented Stackelberg security games are NP-hard, the practical use cases reported in this paper show the high potential practical benefits of using the presented games in transportation systems in USA. It makes such models a potential efficient tool for supporting the complex decisions in large-scale cloud environments, which will be the next step of authors' research on security aspects in cloud computing.

References

[1] R. B. Myerson, *Game Theory: Analysis of Conflict*. Harvard University Press, 1991).

[2] N. Nisan *et al*., Ed., *Algorithmic Game Theory*. Cambridge University Press, 2007.

[3] J. Pita *et al*., "Using game theory for Los Angeles Airport security", *Artif. Intell*., vol. 30, no. 1, pp. 43–57, 2009 (doi: http://dx.doi.org/10.1609/aimag.v30i1.2173).

[4] S. Tadelis, *Game Theory: An Introduction*. Princeton University Press, 2013.

[5] J. F. Nash, "Equilibrium points in *n*-person games", *Proc. of the National Academy of Sciences of the United States of America*, vol. 36, no. 1, pp. 48–49, 1950.

[6] B. von Stengel and S. Zamir, "Leadership with commitment to mixed strategies", Tech. Rep. LSE-CDAM-2004-01, CDAM Research Report, 2004 [Online]. Available: http://www.cdam.lse.ac.uk/Reports/Files/cdam-2004-01.pdf

[7] J. Gan and B. An, "Minimum support size of the defender's strong Stackelberg equilibrium strategies in security games", in *Proc. AAAI Spring Symp. on Appl. Computat. Game Theory*, Stanford, CA, USA, 2014 [Online]. Available: http://www.ntu.edu.sg/home/boan/papers/AAAISS14b.pdf

[8] P. Paruchuri *et al.*, "Efficient Algorithms to Solve Bayesian Stackelberg Games for Security Applications", in *Proc. 23rd Nat. Conf. on Artificial Intelligence AAAI'08*, Chicago, IL, USA, 2008, vol. 3, pp. 1559–1562.

[9] M. Tambe, *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned*, 1st ed. Cambridge University Press, 2011.

[10] D. Korzhyk, Z. Yin, C. Kiekintveld, V. Conitzer, and M. Tambe, "Stackelberg vs. Nash in security games: an extended investigation of interchangeability, equivalence, and uniqueness", *J. Artif. Intell. Res*., vol. 41, no. 2, pp. 297–327, 2011.

[11] M. Jain *et al.*, "Bayesian Stackelberg games and their application for security at Los Angeles international airport", *ACM SIGecom Exchan.*, vol. 7, no. 2, article no. 10, 2008 (doi: 10.1145/1399589.1399599).

[12] J. Pita, M. Jain, M. Tambe, F. Ordoñez, and S. Kraus, "Robust solutions to Stackelberg games: Addressing bounded rationality and limited observations in human cognition, *Artif. Intell*., vol. 174, no. 15, pp. 1142–1171, 2010, (doi.org/10.1016/j.artint.2010.07.002).

[13] R. Yang, C. Kiekintveld, F. Ordoñez, M. Tambe, and R. John, "Improving resource allocation strategies against human adversaries in security games: An extended study", *Artif. Intell.*, vol. 195, pp. 440–469, 2013 (doi: 10.1016/j.artint.2012.11.004).

[14] A. Tambe and T. Nguyen, "Robust resource allocation in security games and ensemble modeling of adversary behavior", in *Proc. 30th Ann. ACM Symp. Appl. Comput. SAC'15*, Salamanca, Spain, 2015, pp. 277–282 (doi: 10.1145/2695664.2695686).

[15] J. Tsai, S. Rathi, C. Kiekintveld, F. Ordoñez, and M. Tambe, "IRIS – A tool for strategic security allocation in transportation networks", in *Proc. 8th International Conference on Autonomous Agents and Multiagent Systems AAMAS 2009*, Budapest, Hungary, 2009, vol. 2, pp. 1327–1334.

[16] M. Jain, E. Kardes, C. Kiekintveld, F. Ordoñez, and M. Tambe, "Security games with arbitrary schedules: A Branch and price approach", in *Proc. 24th AAAI Conf. on Artif. Intell. AAAI-10*, Atlanta, GE, USA, 2010, pp. 792–797.

[17] B. An, J. Pita, E. Shieh, M. Tambe, C. Kiekintveld, and J. Marecki, "GUARDS and PROTECT: next generation applications of security games", *SIGecom Exch.*, vol. 10, no. 1, pp. 31–34, 2011 (doi: 10.1145/1978721.1978729).

[18] B. An, M. Tambe, F. Ordoñez, E. A. Shieh, and C. Kiekintveld, "Refinement of strong Stackelberg equilibria in security games", in *Proc. 25th AAAI Conf. on Artif. Intell.*, San Francisco, CA, USA, 2011 [Online]. Available: www.aaai.org/OCS/index.php/AAAI/AAAI11/paper/view/3461/3928

[19] J. Letchford and Y. Vorobeychik, "Computing optimal security strategies in networked domains: a cost-benefit approach", in *Proc. 11th Int. Conf. on Autonom. Agents and Multiagent Syst. AAMAS'12*, Valencia, Spain, 2012, vol. 3, pp. 1303–1304.

[20] J. B. Clempner and A. S. Poznyak, "Stackelberg security games: Computing the shortest-path equilibrium", *Expert Syst. with Applications*, vol. 42, no. 8, pp. 3967–3979, 2015 (doi: 10.1016/j.eswa.2014.12.034).

[21] D. G. Luenberger and Y. Ye, *Linear and Nonlinear Programming*, 3rd ed. Springer, 2008 (doi: 10.1007/978-0-387-74503-9).

[22] M. Held, R. M. Karp, and P. Wolfe, "Large scale optimization and the relaxation method", in *Proc. of the ACM Annual Conference ACM'72*, Boston, MA, USA, 1972, vol. 1, pp. 507–509 (doi: 10.1145/800193.569964).

[23] J. Rios, "Algorithm 928: A general, parallel implementation of Dantzig-Wolfe decomposition", *ACM Trans. Mathem. Softw.*, vol. 39, no. 3, article no. 21, 2013 (doi: 10.1145/2450153.2450159).

[24] J. K. Ho and R. P. Sundarraj, "Distributed nested decomposition of staircase linear programs", *ACM Trans. Mathem. Softw.*, vol. 23, no. 2, pp. 148–173, 1997 (doi: 10.1145/264029.264031).

[25] Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, *Game Theory in Wireless and Communication Networks*, 1 ed. Cambridge University Press, 2012.

Andrzej Wilczyński is an Assistant Professor at Cracow University of Technology and Ph.D. student at AGH University of Science and Technology. The topics of his research are multiagent systems and cloud computing.

E-mail: and.wilczynski@gmail.com
AGH University of Science and Technology
Mickiewicza av 30
30-059 Cracow, Poland

Tadeusz Kościuszko Cracow University of Technology
Warszawska st 24
31-155 Cracow, Poland

Agnieszka Jakóbik (Krok) received her M.Sc. in the field of stochastic processes at the Jagiellonian University, Poland and Ph.D. degree in the field of neural networks at Cracow University of Technology, Poland, in 2003 and 2007, respectively. She is an Assistant Professor at Cracow University of Technology. Her main scientific interests are cryptography, cloud systems, including cloud security, big data systems, modeling and simulation using artificial intelligences.

E-mail: agneskrok@gmail.com
Faculty of Physics, Mathematics and Computer Science
Tadeusz Kościuszko Cracow University of Technology
Warszawska st 24
31-155 Cracow, Poland

Joanna Kołodziej is an Associate Professor in Department of Computer Science of Cracow University of Technology. She is a vice Head of the Department for Sciences and Development. She serves also as the President of the Polish Chapter of IEEE Computational Intelligence Society. She published over 150 papers in the international journals and conference proceedings. She is also a Honorary Chair of the HIPMOS track of ECMS. The main topics of here research is artificial intelligence, grid and cloud computing, multiagent systems.

E-mail: jokolodziej@pk.edu.pl
Faculty of Physics, Mathematics and Computer Science
Tadeusz Kościuszko Cracow University of Technology
Warszawska st 24
31-155 Cracow, Poland

Paper

Application of Recurrent Neural Networks for User Verification based on Keystroke Dynamics

Paweł Kobojek and Khalid Saeed

Faculty of Mathematics and Information Sciences, Warsaw University of Technology, Warsaw, Poland

Abstract—Keystroke dynamics is one of the biometrics techniques that can be used for the verification of a human being. This work briefly introduces the history of biometrics and the state of the art in keystroke dynamics. Moreover, it presents an algorithm for human verification based on these data. In order to achieve that, authors' training and test sets were prepared and a reference dataset was used. The described algorithm is a classifier based on recurrent neural networks (LSTM and GRU). High accuracy without false positive errors as well as high scalability in terms of user count were chosen as goals. Some attempts were made to mitigate natural problems of the algorithm (e.g. generating artificial data). Experiments were performed with different network architectures. Authors assumed that keystroke dynamics data have sequence nature, which influenced their choice of classifier. They have achieved satisfying results, especially when it comes to false positive free setting.

Keywords—biometrics, GRU networks, keystroke dynamics, LSTM networks, recurrent neural networks, user verification.

1. Introduction

The problem of verification is most often solved by assigning some kind of a password, which should only be known to a given user and consists of finite sequence of characters. When the user provides this password, a party responsible for confirmation of an identity may tell whether the user is whom he claims, he is (based on an assumption that only the real user knows the password). However, such approach is not free from drawbacks. For example, there has to be some kind of a mechanism to handle a situation in which the user forgets his or her password. Moreover, traditional passwords can be broken with brute force method if only attacking person has enough time and computation power (and, of course, there are no other protections against it). Also, if the user stores the password somewhere else than in his or her own brain it has to be somehow secured as well. Alternative to this method is using a biometrics-based security.

Keystroke dynamics is a field within behavioral biometrics, which concerns humans typing patterns on a keyboard. It turns out that the way a user writes on a keyboard is one of his or her unique characteristics. Back in 1980s, the first work was done in order to develop an algorithm which could identify a user based on this trait [1]. Many experiments were performed which have shown it is a good indicator of identity [1]–[4].

In order to describe mathematically a typing pattern we first need to acquire specific data from the user. This data consists of a timestamp of the moment of pressing and/or leaving the button. Next, different measurements out of this can be computed, e.g. [5]:

- dwell time – time between moment of pressing and moment of leaving the button,
- flight time – time between pressing (or leaving) subsequent keys.

A user who types the text can make mistakes, which means that vectors representing different samples may differ in length.

In the next step, data is passed to some kind of a model, which task is to answer the question whether examined user is the one who he claims to be. This model may be anomaly detection system or classifier. Popular approach is to use algorithms based on database of samples. In this case, new sample is compared with those already in database in order to find similarity.

The algorithm consists of two parts: way of acquiring data along with features extraction and a model, which verifies/identifies the sample. Designing new solutions may affect both of these modules.

The accuracy may be influenced even by a way of acquiring data from a user as well as it nature. In the most basic approach, sample describing the user simply consists of timestamps mentioned earlier (from which dwell/flight time is computed). Besides this, it is sometimes useful to measure other values, e.g. eye motion. Humans often either follow their fingers with their eyes or look straight at the monitor. Taking this behavior into consideration may enhance classification accuracy. Mobile devices are supplied with additional sensors like gyroscope or accelerometer. Information from these sensors was proven useful [6]–[8]. [9] shows thoughts about authorization specific for mobile devices with focus on using biometrics techniques including keystroke dynamics. In addition to all these information, there is also meaningful signal in errors made by the user along with the way they correct them (e.g. by using *delete* vs. *backspace*).

For some applications, using only keystroke dynamics may not be accurate enough because of strict regulations. Even

in such situation, it can be used as a valuable support for traditional data. Such approaches increase security and combined accuracy may be high enough to be used even in healthcare [10]. Such methods may be extended by even more biometrics techniques, e.g. face recognition [11].

As it was stated before, keystroke dynamics data may also find applications when it comes to user identification. In this paper this problem is reduced to of multiclass classification, i.e. each user is represented by a class. In this case, we usually have limited user count. This work focuses on verification because in a problem it tries to solve the user is already identified by his or her email address. Identification problem was broadly described in [12] along with proposed algorithm.

1.1. State of the Art Algorithms

Looking at the problem as an anomaly detection problem, statistical methods based on some kind of distance are often used. In standard approach, having some data set (let us treat every sample as a vector) we find its center, which is also a vector. This is a training phase. In testing phase on the other hand, the task is to tell that whether given vector (test sample) is an anomaly or not. In order to answer this question distance between center and test sample has to be computed. The distance may be classic Euclidean distance as well as something more sophisticated i.e. Manhattan distance. This simple algorithm can be further modified e.g. by applying distance norming. In *Filtered Manhattan* algorithm, after finding the center at first all samples, which are too far from it, are removed and then new center point is computed. Similar group of algorithms are those based on k-nearest neighbors idea. In this case, instead of designating a center point and comparing input with it, we find k (in particular, $k = 1$) closest, in terms of defined distance, samples. In this case, usually an *anomaly score* as distance from their center is computed. Another interesting approach is using fuzzy sets. In such sets each object belongs (to some degree) to ranges. The anomaly score is then computed as an average lack of belonging. The approach, which is most similar to the idea presented in this work, is probably one-class SVM. However, such a classifier is trained only on positive class (in opposition to this work's algorithm).

More thorough description of those algorithms (with references to exhaustive descriptions) can be found in [13]. Results of [13] are benchmark for results achieved by the algorithm described in this paper.

When it comes to multiclass classification with keystroke dynamics, the multiple classifiers were tested: HMM, SVM, k-nearest neighbors, and neural networks [14]. Presented algorithm does not solve multiclass classification problem. Nevertheless, with slight modification it could be trained for such problems as well. On the other hand, algorithms mentioned in this paragraph could be used as binary classifiers and replace the proposed one.

1.2. Algorithm Evaluation Methods

An important thing to consider is the evaluation of proposed algorithms. Let us introduce the following terms:

- True Positive Rate (TPR) or hit-rate $\frac{TP}{TP+FN}$,
- False Positive Rate (FPR) $\frac{FP}{FP+TN}$, informs about the probability of accepting an impostor,

where: TP – number of true positives, TN – number of true negatives, FP – number of false positives, FN – number of false negatives.

Besides standard accuracy or error measure, when it comes to keystroke dynamics (and also in other fields of biometrics) two more measures are often used to evaluate algorithms:

- Equal Error Rate (EER) – value for a threshold in which FPR and miss rate1 – TPR are equal,
- Zero-miss rate – FPR value for which TPR = 1 (no false positive errors).

Both these values can be easily read from ROC curve. Figure 1 shows sample ROC curve along with mentioned points marked on it. The values can be read from x axis of these points.

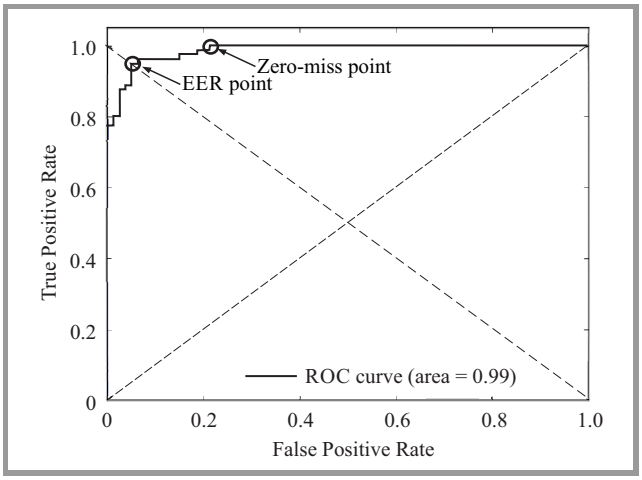


Fig. 1. Sample ROC curve (from the results of this research) with EER and zero-miss points marked.

1.3. Problems with Algorithms and Authors' Proposition

Some of the mentioned algorithms are based on assumption that we have some database of patterns for a user. In the moment when a new sample appears, we need to go through the whole database and find similarities (k-nearest neighbors is an example of this approach). Note that the keystroke dynamics is a behavioral feature, thus it changes with time more than physiological traits. When it comes to keystroke dynamics problem, maintaining a static database for a given user may end up with gradually decreasing accuracy. One of the solution, which comes to mind, is adding new samples. Unfortunately, the side effect of this approach

is the growing need of memory of such a system. This disadvantage, combined with a big number of users may result in memory consumption as the main drawback. When it comes to multiclass classification, there is a need to add new class with each new user.

Another problem of these algorithms is the fact, that they treat input as a vector. Intuitively it seems that numbers representing the sample from a human are more like a sequence, i.e. there is some relation between them. As usual in machine learning problems – it is hidden and unknown. Because mentioned algorithms do not treat data as a sequence, some information natural to them must be encoded artificially. As an example, let us say that the user has mistaken and then corrected the errors. In case of sequence, such information is directly encoded in its length, because errors and corrections require more keystrokes.

Algorithms, which are described and compared in [13], reach relatively low accuracy when it comes to the situation where the threshold was set to avoid false positive errors (zero-miss). The best presented algorithm in this setting (*k*-nearest neighbors with Mahalanobis distance) achieved 0.468 zero-miss rate. In a problem of access control, this would mean the situation in which probability of rejecting a genuine user is close to 0.5.

A problem for which the presented algorithm could be useful is creating a centralized system serving authentication based on a way the user types his or her email address. Thus, the email along with the biological characteristic of a human being would be the only ID in the Internet and necessity of using multiple long passwords would disappear. Services of such a system could be used by external services which could supply it with sufficient information, i.e. keystroke dynamics data plus email address and in return get the information whether the user is verified or not.

Having all this in mind, the presented algorithm is a subject of more constraints. First, it should authenticate potentially everyone in the Internet. Given the enormous number of Internet users (almost 3 billion in 2014 [15]), infinite scalability in terms of user count have to be assumed, which cannot be constrained by the algorithm.

Such a system could potentially be used to grant the access to many services using the same one identification way. The most important feature of such a system is definitely securing resources from unauthorized people. Ignoring this problem would result not only in not solving the problem in which a user has one password to many accounts and someone has accessed it, but could even make it worse. It seems better to reject a genuine user from time to time than to accept the attacking one. The designed algorithm should thus focus on minimizing (ideally eliminating) false positive errors, which means accepting wrong user. Eliminating such errors should be a goal even at the cost of big drop in accuracy.

The proposed algorithm was designed with all that features in mind. Thus, the most important goals are scalability in terms of user count and high accuracy without false positive errors.

2. The Algorithm

2.1. General Idea and Motivation

The standard approach in a keystroke dynamics based verification is using anomaly detectors. Presented approach is different. It uses a binary classifier (recurrent neural networks). Data from the genuine user are positive and from the other people – negative. A big disadvantage, which may appear in readers mind, is the requirement of negative data for training phase. Some thoughts about it along with ways of mitigating this issue were described in latter sections.

In order to choose good classifier it is worth to consider the nature of a problem. First property of the examined data is they do not seem to be a vector describing some physical phenomenon or object (like images, where every element of a vector contains information about specific pixel). As it was stated before, it is assumed that data has a sequence nature. It is worth noting though, that there are no strict proofs of that. However, for some people it seems intuitive, because of (among other reasons) keyboard arrangement. This assumption has influenced the choice of a classifier.

2.2. Recurrent Neural Networks

Due to assumed sequence nature of input data authors have decided to use recurrent neural networks. These networks naturally operate on sequences. Plain recurrent neural networks are very simple (compared to other neural network architectures) models. They differ from feed forward networks in the way of processing input – here it is processed in a step-by-step manner. At step t the network receives x_t as input and having knowledge about state from last step h_{t-1} it computes its output according to the formulas (1) and (2). W_{hh}, W_{xh} and W_{hy} are matrices of network parameters.

$$h_t = tanh(W_{hh} \cdot h_{t-1} + W_{xh} \cdot x_t) \tag{1}$$

$$y = W_{hy} \cdot h_t \tag{2}$$

Unfortunately, in its simplest form, recurrent neural networks are very hard to train due to the problem known as exploding or vanishing gradient [16], [17]. However, there are modified architectures of recurrent neural networks, which solve this problem.

2.3. LSTM

Long Short-Term Memory (LSTM) networks along with training algorithm were proposed in 1997 in the paper [16] in order to solve mentioned problem of vanishing gradient. They are successfully used in many fields, especially when data is sequential, e.g. natural language processing, speech recognition, machine translation, image captioning [18] or even bioinformatics [19].

Core idea behind LSTM network is inclusion of a so-called cell state. It is a vector, which simply stores information, thus it is a kind of memory. This vector is passed through computation steps – modified or not. At each step the network can write or remove some information to/from the

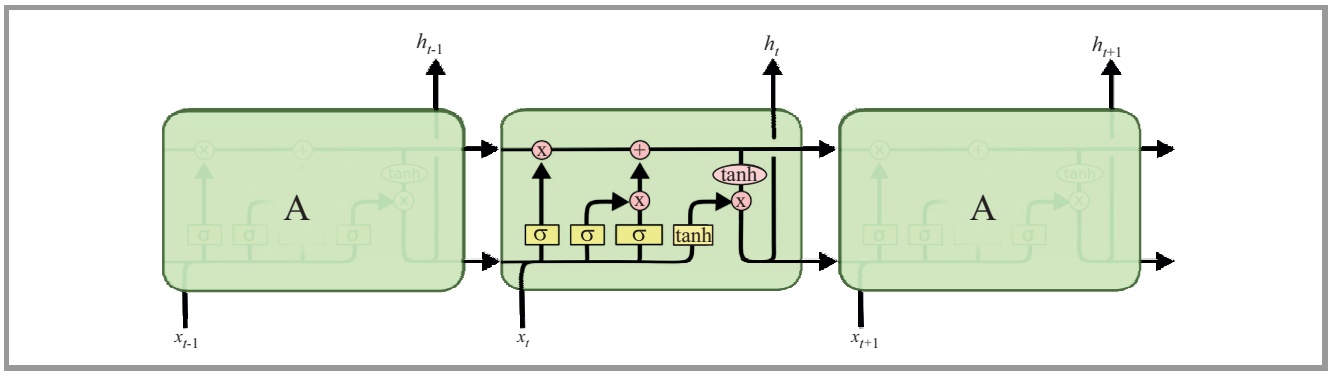


Fig. 2. LSTM computation in time.

memory. It is done using so-called gates. At each computation step the input and the cell state from previous step first go to the forget gate. The way it operates is very simple – it is a plain sigmoidal layer known from neural networks. To be more precise, its output is computed with formula:

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f) \tag{3}$$

where:

- σ – sigmoid function $\left(\sigma(x) = \frac{1}{1+e^{-x}}\right)$,
- W_f, b_f - weight matrix and bias of forget gate,
- h_{t-1} - output from previous step,
- x_t - input in current step.

The vector resulting from this gate tells how much information should be forgotten and how much should be remembered. Degree of this "forgetting" is controlled by the value of sigmoid function which is in range $[0,1]$: 0 means forget everything, 1 means remember everything.

Next is the input gate. Input data along with the output from the previous step are used twice in this gate: in the sigmoid layer (similar to forget gate) and in another layer with hyperbolic tangent as activation. Results of these layers are going to be used in order to create a vector, which is then added to the cell state. This step is described by formulas:

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i), \tag{4}$$

$$\tilde{C}_t = tanh(W_C \cdot [h_{t-1}, x_t] + b_C). \tag{5}$$

After computing these 3 values they can be used to update the cell state. This computation is shown by equation:

$$C_t = f_t \cdot C_{t-1} + i_t \cdot \tilde{C}_t, \tag{6}$$

where: C_t is the cell state at the moment t. f_t is computed from Eq. (3), i_t from Eq. (4), $\tilde{C}_t$ from Eq. (5). Current memory value is first multiplied by an output from forget gate which potentially erases some information and then new information is added. The final LSTM result from the current step is computed not only from the input and the state but also from the cell state. This is described by following formulas:

$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o), \tag{7}$$

$$h_t = o_t \cdot tanh(C_t). \tag{8}$$

Final result of this computation is some real value from range $[0,1]$ if the network is last layer of the model. If it is inner layer then it returns the whole sequence containing all values of h computed in "for" loop. If network is the last layer then its output is compared with the threshold, which determines the final class.

Figure 2 shows how the mentioned computations are performed in time [20].

2.4. GRU

Gated Recurrent Units (GRUs) were introduced in 2014 [21]. They are a similar to LSTM. What is different is that instead of two gates – forget and input gate, GRUs have only one – update gate. Another difference and simplification lies in fact, that GRUs do not have separate memory (cell state). The memory is associated with the state from previous step. Network computation is described by formulas:

$$z_t = \sigma(W_z \cdot [h_{t-1}, x_t]), \tag{9}$$

$$r_t = \sigma(W_r \cdot [h_{t-1}, x_t]), \tag{10}$$

$$\tilde{h}_t = tanh(W \cdot [r_t \cdot h_{t-1}, x_t]), \tag{11}$$

$$h_t = (1 - z_t) \cdot h_{t-1} + z_t \cdot \tilde{h}_t. \tag{12}$$

Merged gates output is z_t vector. It is used for both forgetting and remembering.

As in LSTM, output is a real number from range $[0,1]$ if network is last layer of a model. Otherwise, it returns sequence consisting of every h values computed in "for" loop. The final model output is then compared with the threshold in order to determine the class.

Figure 3 presents diagram with GRU cell [20].

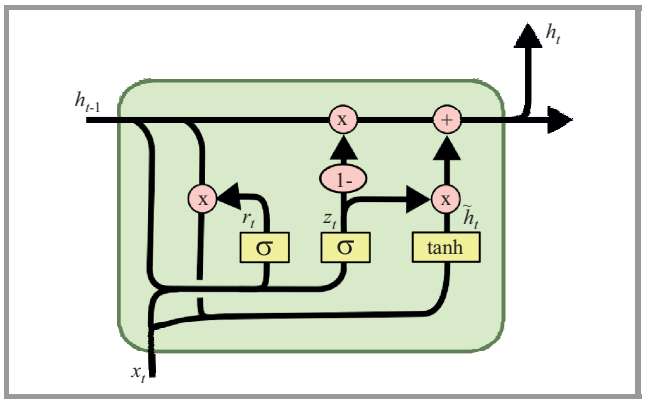


Fig. 3. GRU diagram.

2.5. Training

LSTM and GRU were trained by standard Back Propagation Through Time (BPTT) algorithm [22]. It is used to compute cost function derivative required for optimization algorithm, i.e. Adam optimizer in this case [23]. Networks were trained for 100 epochs, and cost is described by function:

$$C = -\frac{1}{n}\sum_{x}\left[y\ln a + (1-y)\ln(1-a)\right], \qquad (13)$$

where: n – samples count, x – single element, y – expected label for x, a – actual label for x.
Figure 4 shows an example loss over iterations graph.

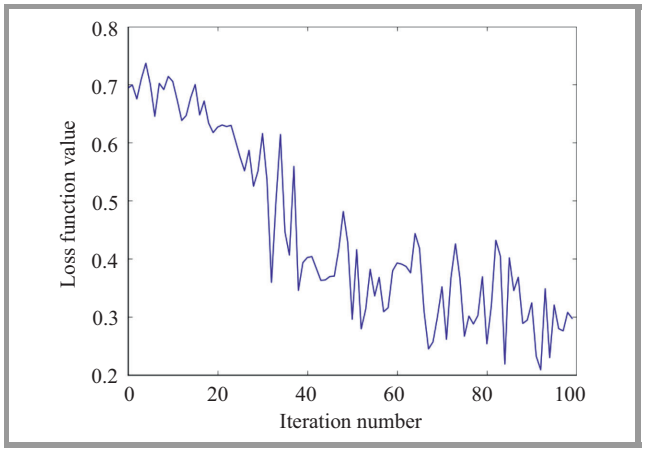


Fig. 4. An example graph showing loss value over iterations.

2.6. Small Training Set and Lack of Negative Data

As it was mentioned earlier, serious drawback of the presented algorithm is a need for negative data during the training phase. In real life applications, requiring user to type his address several times is already an inconvenience for him. Forcing other people to type, this address would be even harder. One of possible solutions could be using neural network as one-class classifier. In such a case, the model would be trained only on positive data, which is easier to acquire. Such methods are successfully applied for SVM classifiers [13] to solve verification problem. Unfortunately, the conducted experiments had not shown any good results with recurrent neural networks.
Another approach, which was tested, is generation of artificial negative data. From every positive sample authors got a negative by adding a random (with normal distribution, several values of standard deviation were tested) noise to it. The classifier was trained on positive and artificially created negative data and then evaluated only on real data.
Another problem is the size of a training set. Deep neural networks are models in which there are enormous number of parameters, which has to be adjusted during the training, thus they require big amount of data. Training for much iteration with small dataset tends to overfit. Unfortunately, in this case asking the user to type an address several hundred times would clearly be impractical. In this work, authors' dataset has only over a dozen samples for each user. Because of that, the authors had to apply regularization techniques in order to avoid overfitting.
It is worth mention that the challenges may not be a problem in some real applications. Large email services, e.g. Google Gmail, have (or might have) access to a large amount of data about address typing. Positive data could come from successful login or typing own email. Negative data on the other hand could be extracted from other people who type email of a given user in order to send him a message. In such a case, there would be no need to generate artificial data.

2.7. False Positive Errors Minimalization

As it was mentioned earlier, one of the challenges for the designed algorithm is the minimalization of false positive errors.
A standard approach is to select the acceptance thresholds. By increasing its value, number of samples classified as positive should decrease. Hopefully, first to drop will be samples classified as positive with low likelihood, which are potentially false positive errors. The idea to eliminate such errors is then to increase the threshold until every false positive error is gone on training set.
Unfortunately, networks tend to classify with a very high likelihood. Thus selecting the threshold, which eliminates unwanted errors will definitely decrease total accuracy, because it has to be pretty high, so many genuine samples are rejected.
The question arouses – why LSTM and GRU models tend to return high numbers even if they mistake? These models are very sophisticated and are based on strong type of neural networks (so-called deep neural networks) and are used for high dimensional problems like image recognition [24]. Compared to such problems, the presented task has much smaller dimensionality, which is probably a reason why network overfits.
There are different methods of regularization, which help to mitigate the problem of overfitting [25]. One of them, used in this work is dropout.

2.8. Dropout

Dropout was introduced by researchers from University of Toronto [26] as a regularization technique for deep neural networks. The idea behind it is to remove some random group of neurons along with connections during training phases. Since those random groups are different at each step, it prevents neurons from learning to copy other neurons, which in turn makes them better at approximating desired output. This is often compared to ensemble models, which is training several models and making them vote. Dropout is fully described in [26].

2.9. Tested Architectures

Several neural network architecture were trained and tested as classifiers. Architecture which was satisfying on chosen test, dataset turned out to be too weak for benchmark dataset (see results in Section 4) so it had to be adjusted. The tested architectures are shown in Figs. 5–8, where:

- LSTM – single LSTM cell,
- GRU – single GRU cell,
- Dropout – adding regularization using dropout,
- LR – sigmoid layer,
- Embedding – mapping value to vector space.

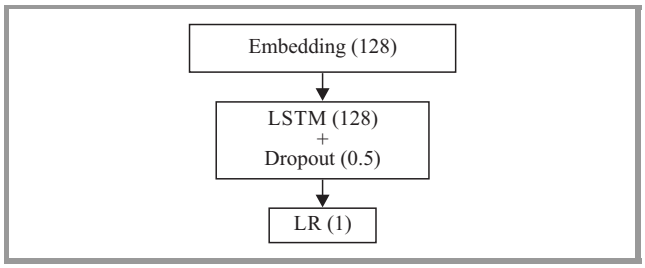


Fig. 5. Network embedding and one LSTM layer.

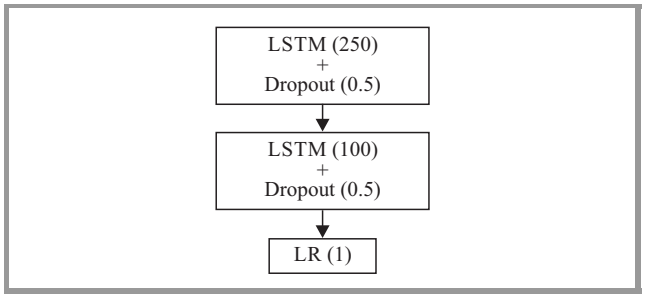


Fig. 6. Network structure with two LSTM layers.

Moreover, networks in Figs. 5 and 6 were trained with and without dropout, which turned out to have major influence on results. Process of architecture selection was empirical, which means that many architectures have been tested and hyperparameters based on results were adjusted.

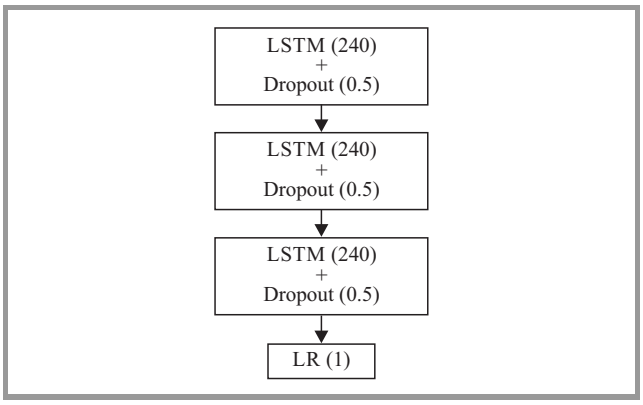


Fig. 7. Network with three LSTM layers (it was tested only on benchmark set).

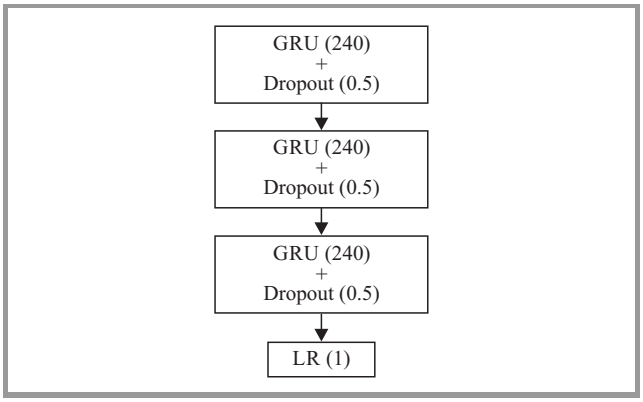


Fig. 8. Network with three GRU layers (it was tested only on benchmark set).

3. Datasets

3.1. Authors' Dataset

In order to conduct experiments we prepared own dataset. To achieve this task a website gathering keystroke data was used. The recording software was implemented as a student project by Albert Wolant. Every user was asked to type his address 5 times and type other addresses once. Nine students have taken part in this experiments, but due to low quality of some data (e.g. copy-paste method), samples batch from 3 people was rejected. Final dataset consisted of data from 6 people ranging from 12 to 20 samples each. It is worth mentioning that samples include information about mistakes made by typists.

3.2. Benchmark Dataset

Because the dataset described in previous section has only few samples, in addition a benchmark dataset available on the website was used [27]. This site provides exhaustive description of this set and acquiring method. This dataset was used by its authors to compare anomaly detectors [13]. It consists of data gathered from 51 typists, each has typed the same phrase 400 times. Even though it was created

for anomaly detectors, it turned out to be very valuable for presented algorithm. Because users typed the same phrase (to be more precise – same password), it is possible to create a dataset for each user containing this user's samples as positive data and all other samples as negative. The problem here is that in such case there are 50 times as many negative as positive data. Classifier trained on such data will most likely tend to classify new samples as negative. It would also give false impression of high accuracy [28]. Because only small part of test data would be positive, so just classifying everything as negative gives high accuracy. With this problem in mind, authors decided to balance positive and negative data. For every user, only 400 random samples from other users were chosen as negative. Eventually, 51 sets were obtained (one for every user) containing 800 samples each: 400 hundred positive, 400 negative.
One drawback of this set is that it is cleared from mistakenly typed samples. Thus, there is no information about frequency of errors done by a user.
It should be clearly stated, that since this set was not used in its direct shape and that evaluation methods were different from those used by its authors results of this research cannot be directly compared to original results achieved by authors in [13].

4. Experiments and Results

For both (own and benchmark) datasets the different but not disjoint sets of models have been tested. In addition, a scenario in which negative data is artificial was also included in test process. In this case was tested and compared with *k*-nearest neighbors' classifier.
In order to achieve repeatability of experiments, they were all performed with the same random number generator seed.

4.1. Authors' Dataset

Due to small size of this set, a non-standard evaluation has been employed (by "standard" we mean dividing set for training, validation and test sets). This is why leave-n-out-cross-validation with $n = 1$ [29] is used. In this validation with ($n = 1$) the one model for every dataset element was trained. This selected element acts as one element test set. The model is trained on the rest of the set. This means, having n elements in a set, n models should be trained. Then the model computation on this selected element is performed. The total accuracy is an average computed from all those results.

4.1.1. Model with one LSTM Cell and Embedding

For this model, the total accuracy for all users reached only 58%. Table 1 shows results for all users. Note that because of validation type, single sample is included multiple times here. FP-free thresholds cell shows score when acceptance thresholds were chosen to eliminate false positive errors on training set. Because total accuracy was low, we got rid of embedding layer in favor of another LSTM cells.

Table 1
Results for all users

	Accepted	Rejected
Genuine user	359	138
Impostor	164	72
	Threshold 0.5	FP-free thresholds
Accuracy	0.58	0.55

Table 2
Results for all users

	Accepted	Rejected
Genuine user	456	41
Impostor	75	161
	Threshold 0.5	FP-free threshold
Accuracy	0.85 (0.88)	0.52 (0.8)

4.1.2. Model with two LSTM Cells

This model was tested in two versions – with and without dropout. Table 2 shows its accuracy. The numbers in parentheses relate to models with dropout.
The accuracy of LSTM model with 2 cells is satisfying. The dropout's influence on results is clear, especially if false positive free thresholds are used. By only adding dropout, the accuracy raised from 0.52 to 0.8. Unfortunately, the size of this dataset is small and the evaluation method had negative impact on results. Hence, it is hard to judge the algorithm quality by this data only. Despite this problem, those results hold some value, because in real life applications of verification based on keystroke dynamics usually only have small datasets are available.

4.2. Benchmark Set – Limited Data

Benchmark dataset, as it was described earlier, contains more data (in terms of both user count and samples per user). It is thus more reliable when it comes to the algorithm evaluation. Samples in this dataset contain more than just dwell-time. However, because only dwell-time was recorded in author's dataset, first study was performed only including this measure.

4.2.1. Model with two LSTM Cells

This is the same model, which turned out to be good enough for our custom dataset. This time, only version with dropout was tested as it achieved better results. Results are presented in Tables 3 and 4.
Unfortunately, model with two LSTM cells, even though it performed well on small dataset, does not give satisfying

Table 3
Results on benchmark dataset for two LSTM cells

	Threshold 0.5	FP-free
Average accuracy	0.759	0.59
Maximum	0.975	0.994
Minimum	0.4875	0.5
Standard deviation	0.101	0.1344

Table 4
Results on benchmark dataset for two LSTM cells

EER	0.227 (0.094)
Zero-miss rate	0.764 (0.221)

results on benchmark dataset. We have then made it more complex by adding one more LSTM cell as well as increasing the total number of neurons. This model has achieved results presented in Tables 5 and 6.

Table 5
Accuracy on benchmark dataset for model with three LSTM cells

	Threshold 0.5	FP-free
Average accuracy	0.764	0.61
Maximum	0.9875	0.9875
Minimum	0.5187	0.5
Standard deviation	0.114	0.1399

Table 6
Benchmark dataset results for three model with three LSTM layers

EER	0.219 (0.106)
Zero-miss rate	0.747 (0.221)

4.2.2. Model with Three LSTM Cells

In this case results are only slightly better than previous. It seems like simply increasing complexity of this model is not enough. Therefore, we decided to try again, swapping LSTM cells with GRU equivalents.

4.2.3. Model with Three GRU Cells

Results of experiments with this model (Tables 7 and 8) are comparable with those achieved on own dataset. However, if we compare it with results achieved by author's dataset, proposed algorithm would be placed 8th in terms of EER and 6th when it comes to zero-miss rate. Especially zero-miss rate is high which we would like to minimize.

4.3. Benchmark Dataset – All Data

As it was mentioned earlier, original dataset contains more than just dwell-time. Authors decided to try testing proposed algorithm using all data provided by the dataset. Achieved results are presented in Table 9. Only measures, which are easily comparable with algorithms presented in [13] are shown.

Table 7
Accuracy on the benchmark dataset for model with three GRU cells

	Threshold 0.5	FP-free
Average accuracy	0.83	0.68
Maximum	0.9875	0.9875
Minimum	0.5	0.5
Standard deviation	0.099	0.1397

Table 8
Benchmark dataset results for three model with three GRU layers

EER	0.150 (0.087)
Zero-miss rate	0.613 (0.260)

Table 9
Models results on benchmark dataset with all data

Model	EER	Zero-miss rate
LSTM 2 cells	**0.136 (0.176)**	0.379 (0.314)
LSTM 3 cells	0.165 (0.191)	**0.333 (0.282)**
GRU 3 cells	0.224 (0.319)	0.389 (0.325)

The results are significantly better than those which only included dwell time. In addition, the best model here is the one built with 3 LSTM cells.

4.4. Artificially Generated Data

One of the most important disadvantages of the algorithm is the need of negative data during training. In this work the method of artificial generation of negative data based on positive samples have been tested. Proposed algorithm was to *k*-nearest neighbor classifier. In total 417 different combinations of distance definition, number of neighbors and standard deviation of the normal distribution used for negative data generation was tested. It is worth noting that the algorithm is used as a classifier and not as an anomaly detector. The algorithm presented in this work has achieved results shown in Tables 10 and 11.

Table 10
Accuracy for data with artificial negative samples

Model	Accuracy threshold 0.5	Accuracy FP-free
LSTM 2 cells	0.622 (0.094)	0.562 (0.094)
LSTM 3 cells	0.633 (0.106)	0.561 (0.100)
GRU 3 cells	0.629 (0.093)	0.707 (0.101)

Table 11
EER and zero-miss rate for data with artificial negative samples

Model	EER	Zero-miss rate
LSTM 2 cells	0.441 (0.336)	0.598 (0.303)
LSTM 3 cells	0.768 (0.219)	0.592 (0.291)
GRU 3 cells	0.527 (0.402)	0.597 (0.334)

For a comparison, best result of k-nearest neighbor was for $k = 1$ and dice distance and it was 58%.

A similar experiment was also conducted on author's dataset. In this case, the best k-nearest neighbor algorithm accuracy was 87% while neural networks achieved 100% accuracy. However, this cannot be used as an argument for high accuracy of the model, because experiments on the larger dataset have not confirmed such high accuracy. The question is, however, why artificial data has actually increased accuracy (using only real data 80% accuracy was achieved). The reason is probably that without artificial data, the dataset was imbalanced in terms of negative to positive samples ratio, which made the network to be more eager to answer with class, which was overrepresented in the training set. Since we generated one artificial sample for each positive, this gave us the perfectly balanced set.

Unfortunately, presented method of generating artificial data turned out to be not very effective. The accuracy is significantly lower compared to training with only real (positive and negative) data. However, as was expected, recurrent neural networks performed generally better than k-nearest neighbor classifier.

5. Conclusions and Algorithm Evaluation

Compared to results from authors of the benchmark dataset, achieved best result (EER 0.136) would be on 7th place in terms of EER for total 14 places. It is equal to the one achieved by filtered Manhattan algorithm, yet its standard deviation is better: 0.083 compared to 0.176. The presented algorithm performed better than other neural networks tested by authors.

However, zero-miss rate is more interesting. The best result achieved by authors of [13] is 0.468. In this research the best result is 0.333, a lot better, however, those results cannot be directly compared, because of different nature of algorithms – this work shows binary classifier, authors of the mentioned paper tested anomaly detectors, different training method and different evaluation method. Despite that, presented algorithm performed well in terms of zero-miss rate and lets us recommended it as valuable when it comes to such a case. It is worth reminding, that high accuracy without false positive errors was one of the main objectives of the designed algorithm. It is worth noting, that the big leap in accuracy was caused by including additional data (both flight and dwell time). As it turned out, this had more influence than classifier architecture.

Another important feature, which was required from the algorithm, was scalability in terms of user count. Because for each user we train separate classifier, there is no problem with too many similar classes – each model is binary classifier trained for a given individual. Because neural networks are based on parametric models, they require the access to samples database only in the training phase. Thus, the increasing sample count for the user will not increase the size of the model when it comes to memory usage. Each model requires about 3.5 MB. This seems reasonable size (1 million users would require 3.5 TB of disk space). Therefore, the objective of unconstrained scalability is achieved.

We have stated the hypothesis that input data are sequences, and not just vectors and that a valuable signal comes from this information. Because recurrent neural networks are the natural choice for sequences processing, it could have direct impact on the accuracy. However, we cannot say with strong belief that this statement is more than just hypothesis. If our results were significantly better then others, it would be the strong evidence for it.

Unfortunately, the algorithm is not free from flaws. Most of them, however, were known at the beginning of the work. We have tried to mitigate the problem by generating artificial negative data. Results were admittedly better than k-nearest neighbors, yet they are noticeably worse than those achieved by the same model with access to real negative data. Perhaps, there is a method of generating better data, but further studies are needed here.

Certain drawback of the algorithm is how much time it requires to be fully trained. Neural networks are complicated models with a large number of parameters, so it requires time to adjust them. On a typical desktop 2.9 GHz Intel Core i5 CPU training and evaluating most sophisticated models took about 8 hours, which means about 10 minutes per user (there were 51 typists in benchmark dataset). Even if this seems quick, it is very long time compared to many anomaly detectors, which often only require one pass through the database. 10 minutes is a big issue for so-called continuous verification, i.e. constant monitoring of keyboard usage in order to detect impostors. However, training time directly depends on the dataset size. In this case, for each user we had 640 samples. Acquiring this number of samples (with assumption that exactly half of them are negative) requires time and has to be finished before training. Having said that, 10 minutes becomes less significant. Nevertheless, full training and evaluation requires 8 hours, which makes the hyperparameters adjustment a tougher task.

Paper [30] presents LSTM networks used as anomaly detectors. By incorporating this idea, we could use the same evaluation method as it was used in [13], which introduced benchmark dataset. This would allow us direct comparison. Moreover, it would solve the problem of negative data

requirement. Results achieved in the mentioned work give hope for increase of usability if those models for keystroke dynamics in the future.

References

[1] R. Gaines, W. Lisowski, S. J. Press, and N. Shapiro, "Authentication by keystroke timing: some preliminary results", R-2526-NSF RAND Report, RAND Corporation, Santa Monica, CA, USA, May 1980.

[2] F. Monrose and A. D. Rubin, "Keystroke dynamics as a biometric for authentication", *Future Gener. Comp. Syst*., vol. 16, pp. 351–359, 2000.

[3] R. Joyce and G. Gupta, "Identity authorization based on keystroke latencies", *Commun. of the ACM*, vol. 33, no. 2, pp. 168–176, 1990.

[4] D. Mahar, R. Napier, M. Wagner, W. Laverty, R. Henderson, and M. Hiron, "Optimizing digraph-latency based biometric typist verification systems: Inter and intra typists differences in digraph latency distributions", *Int. J. Human-Comp. Stud*., vol. 43, no. 4, pp. 579–592, 1995.

[5] P. R. Dholi and K. P. Chaudhari, "Typing Pattern Recognition Using Keystroke Dynamics", in *Mobile Communication and Power Engineering*, Vi. V. Das and Y. Chaba, Eds. *Communications in Computer and Information Science*, vol. 296, pp. 275–280. Springer, 2012.

[6] G. Ho, "TapDynamics: Strengthening User Authentication on Mobile Phones with Keystroke Dynamics", Tech. Rep., Stanford University, San Francisco, CA, USA, 2014.

[7] Y. Deng and Y. Zhong, "Keystroke dynamics advances for mobile devices using deep neural network", in *Recent Advances in User Authentication Using Keystroke Dynamics Biometrics*, Y. Zhong and Y. Deng, Eds. Science Gate Publishing, 2015, vol. 2, pp. 59–70.

[8] C. Giuffrida, K. Majdanik, M. Conti, and H. Bos, "I sensed it was you: Authenticating mobile users with sensor-enhanced keystroke dynamics", in *Detection of Intrusions and Malware, and Vulnerability Assessment*, S. Dietrich, Ed. *LNCS*, vol. 8550, pp. 92–111. Springer, 2014 (doi: 10.07/978/3-319-08509-8_6).

[9] M. Rogowski, K. Saeed, M. Rybnik, M. Tabędzki, and M. Adamski, "User authentication for mobile devices", in *Computer Information Systems and Industrial Management*, K. Saeed, R. Chaki, A. Cortesi, and S. Wierzchoń, Eds. *LNCS*, vol. 8104, pp. 47–58. Springer, 2013.

[10] T. Bhattasali and K. Saeed, "Two Factor Remote Authentication in Healthcare", in *Proc. 3rd Int. Conf. Advan. in Comput., Commun. & Inform. ICACCI 2014*, Delhi, India, 2014, pp. 380–386.

[11] T. Bhattasali, K. Saeed, N. Chaki, and R. Chaki, "Bio-authentication for layered remote health monitor framework", *J. Medical Inform. & Technol.*, vol. 23, no. 1, pp. 131–139, 2014.

[12] M. Rybnik, P. Panasiuk, K. Saeed, and M. Rogowski, "Advances in the keystroke dynamics: the practical impact of database quality", in *Computer Information Systems and Industrial Management*, A. Cortesi, N. Chaki, K. Saeed, and S. Wierzchoń, Eds. *LNCS*, vol. 7564, pp. 203–214. Springer, 2012 (doi: 101007/978-3-642-33260-9_17).

[13] K. S. Killourhy and R. A. Maxion, "Comparing anomaly detectors for keystroke dynamics", in *Proc. 39th Annual IEEE/IFIP Int. Conf. Dependable Syst. & Netw. DSN 2009*, Lisbon, Portugal, 2009, pp. 125–134.

[14] Y. Deng and Y. Zhong, "Keystroke Dynamics User Authentication Based on Gaussian Mixture Model and Deep Belief Nets", *ISRN Sig. Process*., vol. 2013, article ID 565183, 2013 (doi: 10.1155/2013/565183).

[15] "ICT Facts and Figures" 2005, 2010, 2014, Telecommunication Development Bureau, International Telecommunication Union (ITU), 24 May 2015.

[16] S. Hochreiter and J. Schmidhuber, "Long short-term memory", *Neural Computat*., vol. 9, no. 8, pp. 1735–1780, 1997.

[17] Y. Bengio, P. Simard, and P. Frasconi, "Learning long-term dependencies with gradient descent is difficult", *IEEE Trans. on Neural Netw*., vol. 5, no. 2, pp. 157–166, 1994.

[18] W. Zaremba, I. Sutskever, and O. Vinyals, "Recurrent Neural Network Regularization", in *Proc. Int. Conf. on Learn. Representat. ICLR 2015* San Diego, CA, USA, 2015 [Online]. Available: https://arxiv.org/pdf/1409.2329.pdf

[19] S. K. Sønderby, C. K. Sønderby, H. Nielsen, and O. Winther, "Convolutional LSTM Networks for subcellular localization of proteins", in *Algorithms for Computational Biology*, A.-H. Dediu, F. Hernández-Quiroz, C. Martín-Vide, and D. A. Rosenblueth, Eds. *LNCS*, vol. 9199, pp. 68–80. Springer, 2015.

[20] C. Olah, "Understanding LSTM Networks", Aug. 27, 2015 [Online]. Available: http://colah.github.io/posts/2015-08-Understanding-LSTMs/ (accessed on Aug. 9, 2016)

[21] K. Cho, F. Bougares, H. Schwenk, D. Bahdanau, and Y. Bengio, "Learning phrase representations using RNN Encoder-decoder for statistical machine translation", in *Proc. of the Conf. on Empir. Methods in Natural Language Process. EMNLP 2014*, Doha, Qatar, 2014, pp. 1724–1734.

[22] P. J. Werbos, "Backpropagation through time: What it does and how to do it", *Proc. of the IEEE*, vol. 78, no. 10, pp. 1550–1560, 1998.

[23] D. P. Kingma and J. L. Ba, "Adam: A Method for stochastic optimization", in *Proc. Int. Conf. on Learn. Representat. ICLR 2015* San Diego, CA, USA, 2015 [Online]. Available: https://arxiv.org/pdf/1412.6980v8.pdf

[24] A. Graves, M. Liwicki, S. Fernandez, R. Bertolami, H. Bunke, and J. Schmidhuber, "A novel connectionist system for unconstrained handwriting recognition", *IEEE Trans. Pattern Anal. & Mach. Intellig.*, vol. 31, no. 5, pp. 855–868, 2009.

[25] A. Ng, "Feature selection, L1 vs. L2 regularization, and rotational invariance", in *Proc. 21st Int. Conf. on Machine Learn. ICML'04*, Banff, Canada, 2004.

[26] N. Srivastava *et al.*, "Dropout: A simple way to prevent neural networks from overfitting", *J. of Mach. Learn. Res.*, vol. 15, no. 1, 1929–1958, 2014.

[27] K. Killourhy and R. Maxion, "Keystroke Dynamics – Benchmark Data Set", Carnegie Mellon University, Pittsburgh, PA, USA [Online]. Available: http://www.cs.cmu.edu/∼keystroke/ (accessed on May 27, 2016).

[28] H. He and E. A. Garcia, "Learning from imbalanced data", *IEEE Trans. on Knowl. & Data Engin.*, vol. 21, no. 9, pp. 1263–1284, 2009.

[29] J. Schneider, "Cross Validation", Carnegie Mellon University, Pittsburgh, PA, USA [Online]. Available: https://www.cs.cmu.edu/∼schneide/tut5/node42.html (accessed on May 27, 2016).

[30] P. Malhotra, L. Vig, G. Shroff, and P. Agarwal, "Long short term memory networks for anomaly detection in time series", in *Proc. of European Symp. on Artif. Neural Netw., Computat. Intellig. and Machine Learning ESANN 2015*, Bruges, Belgium, 2015.

Paweł Kobojek received the M.Sc.degree in the field of Computer Science from Warsaw University of Technology in 2016. His scientific interests are mainly focused on Bioinformatics and Artificial Intelligence and its applications in biometrics and language processing.

E-mail: PawelKobojek@gmail.com
Faculty of Mathematics and Information Sciences
Warsaw University of Technology
Koszykowa st 75
00-662 Warsaw, Poland

Khalid Saeed is a B.Sc., M.Sc., Ph.D. and D.Sc. degrees holder. He is a Computer Science full professor (Biometrics, Image Analysis and Processing) at Białystok University of Technology. He also works with the Faculty of Mathematics and Information Sciences, Warsaw University of Technology. He was with AGH Krakow in 2008–2014. He has published more than 200 publications and edited 27 books, journals and conference proceedings, 11 text and reference books. He received 19 academic awards. Mr. Khalid Saeed is a member of more than 15 editorial boards of international journals and conferences. He is an IEEE Senior Member and has been selected as IEEE Distinguished Speaker for 2011–2017. He is the editor-in-chief of International Journal of Biometrics with Inderscience Publishers.

E-mail: k.saeed@mini.pw.edu.pl
Faculty of Mathematics and Information Sciences
Warsaw University of Technology
Koszykowa st 75
00-662 Warsaw, Poland

Paper

Cross-spectral Iris Recognition for Mobile Applications using High-quality Color Images

Mateusz Trokielewicz[1,2] and Ewelina Bartuzi[1]

[1] *Biometrics Laboratory, Research and Academic Computer Network, Warsaw, Poland*
[2] *Institute of Control and Computation Engineering, Warsaw University of Technology, Warsaw, Poland*

Abstract—With the recent shift towards mobile computing, new challenges for biometric authentication appear on the horizon. This paper provides a comprehensive study of cross-spectral iris recognition in a scenario, in which high quality color images obtained with a mobile phone are used against enrollment images collected in typical, near-infrared setups. Grayscale conversion of the color images that employs selective RGB channel choice depending on the iris coloration is shown to improve the recognition accuracy for some combinations of eye colors and matching software, when compared to using the red channel only, with equal error rates driven down to as low as 2%. The authors are not aware of any other paper focusing on cross-spectral iris recognition is a scenario with near-infrared enrollment using a professional iris recognition setup and then a mobile-based verification employing color images.

Keywords—biometrics, cross-spectral, iris recognition, mobile technologies, smartphones.

1. Introduction

1.1. Iris Biometrics

In the recent decades, biometric authentication and identification of humans has received considerable interest as a fast, safe, and convenient way of replacing password, token, or key-based security measures. One of the most accurate biometric methods is iris recognition, whose concept was first conceived by British ophthalmologists Safir and Flom [1] and later patented and implemented by Daugman [2], [3]. The iris, a part of the uvea, is located at the back of the anterior chamber of the eye, protected from the outside environment by eyelashes, tear film, the cornea and the aqueous humor. Its usefulness as a biometric identifier is attributed to the intricate patterns of the trabecular meshwork found in the front part of the organ. These patterns are developed in the embryonic stage and have low genotype dependence, thus providing enough unique features for high confidence classification. Iris texture is also believed to be exceptionally stable in time and virtually impossible to alter without inflicting extensive damage to the eye.

1.2. Cross-Spectral Iris Recognition

Iris recognition biometric systems are usually taking advantage of images collected using near-infrared (NIR) illumination. This is due to certain light absorption properties of melanin – the pigment, to which the iris attributes its appearance. While the absorption is significant for light from the visible spectrum, it is almost negligible for higher wavelengths. Higher reflectance enables good visibility of iris texture details even for highly pigmented (dark) irises. For this reason most commercial iris cameras collect images under illumination from the 700–900 nm wavelength range. However, with the recent shift in consumer computing towards mobile devices, visible light and cross-spectral iris recognition has received considerable attention.
This study aims at analyzing cross-spectral performance of the state-of-the-art iris recognition methods when applied with visible spectrum and near-infrared images. To our best knowledge, this is the first analysis of such kind incorporating high quality, flash-illuminated visible light iris images obtained using a mobile phone, which are then matched against NIR-illuminated enrollment samples. If good performance of the recognition methods can be achieved, it could pave the way for low-effort, real world applications, such as user authentication on a mobile device, which would serve as a remote verification terminal complementing a typical enrollment setup employing a NIR camera. We envisage a scenario, in which the enrollment stage is performed using a professional NIR setup for purposes such as government-issued IDs, travel documents, etc. Then, mobile authentication could be performed using a phone or a tablet whenever user deems it necessary. As of August 2016, there are only three iris recognition enabled mobile phones with the capability to obtain iris images in near infrared: Fujitsu NX F-04G ([4], available only in Japan), Microsoft Lumia 950 and 950XL ([5], employing Windows Hello iris-based authentication, currently in beta) and Samsung Galaxy Note 7 [6]. Due to this limited availability of NIR iris scanning equipment in mobile devices, a possibility of cross-spectral iris matching using color images is explored. Therefore, this paper offers three main contributions:

- evaluation of cross-spectral iris comparisons in a mobile recognition scenario,

- analysis of how the eye color influences cross-spectral iris matching,
- selection of the most efficient RGB channel depending on the eye color in order to optimize cross-spectral iris matching.

This paper is organized as follows: Section 2 presents an overview of the current state-of-the-art research related to this topic. Section 3 offers a brief explanation how the iris color in the human eye is determined. Multispectral database of iris images, data subset creation in respect to the eye color, and image preprocessing using selective RGB channel grayscale transformation are described in Section 4. Experimental methodology and software tools are characterized in Section 5, while Section 6 presents an overview of results. Finally, relevant conclusions are drawn in Section 7.

2. Related work

Probably the first systematic study devoted to multispectral iris biometrics was this of Boyce *et al*. [7], in which authors studied the reflectance response of the iris tissue depending on the spectral channel employed: red, green, blue, and infrared. Results of matching performance evaluation across channels and wavelengths are reported with the conclusion that decreases in matching accuracy is smallest in spectral channels that are closest to each other wavelength-wise. Technique for improving the recognition accuracy by employing histogram equalization in the CIE L*a*b color space is shown. Authors also present insight on how iris recognition could benefit from multispectral fusion in both segmentation and matching domains. Park *et al*. [8] explored fusing multispectral iris information as a countermeasure against spoofing. Iris features extracted from images acquired almost simultaneously both in low wavelength band and in high wavelength band are fused together in an attempt to create a method that would differentiate between real and counterfeit samples without compromising the recognition accuracy. Spectral variations found in real images obtained under different illumination conditions are said to offer enough variability to achieve this.

Ross *et al*. [9] were the first to investigate multispectral iris recognition using wavelengths longer than 900 nm, proving that images obtained in the range of 900–1400 nm can offer iris texture visibility good enough for biometric applications. At the same time, authors argue that the iris is able to give different responses as different wavelengths, which could prove useful for improving segmentation algorithms. Intra- (i.e. between images obtained in the same wavelength) and inter-spectral (i.e. between images obtained in two different wavelengths) genuine and impostor comparisons were generated. This revealed that despite inter-spectral genuine comparison distributions being shifted towards relevant impostor distributions, nearly perfect separation between genuine and impostor distributions can be achieved with the use of multispectral fusion at the score level.

Burge *et al*. [10] studied the iris texture appearance depending on the eye color combined with light wavelength employed for imaging. A method of approximating NIR image from visible light image is presented, together with multispectral iris fusion designed to create a high confidence image that would improve cross-spectral matching accuracy. Zuo *et al*. [11] attempted to predict NIR images from color images using predictive image mapping, to compare them against the enrolled typical NIR image. This method is said to outperform matching between NIR channel and red channel by roughly 10%.

Recently, advancements have also been made in the field of visible light iris recognition applications in more practical scenarios, including mobile devices – smartphones and tablets. Several databases have been released, including the UPOL database of iris images obtained using an ophthalmology device [12], the UBIRISv1 database, representing images obtained using Nikon E5700 camera and the UBIRISv2 database, which gathers images captured *on-the-move* and *at-a-distance* [13], [14]. These databases represent images obtained in very unconstrained conditions, and therefore usually of low quality. Recently, we have published the first available to researchers database of high quality iris images: the Warsaw-BioBase-Smartphone-Iris dataset [15], which comprises images obtained with iPhone 5s phone with embedded flash illumination (available online at [16]).

Challenges related to visible light iris recognition were extensively studied by Proenca *et al*., including the amount of information that can be extracted from such images [17], possible improvements to the segmentation stage [18], and methods for image quality assessment to discard samples of exceptionally poor quality [19]. Santos *et al*. explored possible visible light illumination setups in the search for optimal solution for unconstrained iris acquisition [20]. Segmentation of noisy, low quality iris images was also studied by Radu *et al*. [21] and Frucci *et al*. [22]. Raja *et al*. explored visible spectrum iris recognition using a light field camera [23] and white LED illumination [24]. They also investigated a possibility of deploying iris recognition onto mobile devices using deep sparse filtering [25] and K-means clustering [26], reporting promising results such as EER as low as 0.31% when visible spectrum, smartphone-obtained images are used for recognition. The feasibility of face and iris biometrics implementations in mobile devices was also studied by De Marsico *et al*. [27]. Our own experimentations devoted to this field of research have shown that intra-wavelength visible spectrum iris recognition is possible when high-quality, color iris images obtained using a modern smartphone are used with the existing state-of-the-art methods, which are typically designed for NIR images [15], [28].

3. Anatomical Background of Iris Color

The iris consists of two major layers: the outer stroma, a meshwork of interlacing blood vessels, collagen fibers,

and sometimes melanin particles, and the inner epithelium, which connects to the muscles that control the pupil aperture. The epithelium itself contains dark brown pigments regardless of the observed eye color. The eye color perceived by the human observer depends mainly on the amount of melanin that can be found in the stroma. The more melanin in the stroma, the darker the iris appears due to absorption of incoming light by melanin. Blue hue of the iris, however, is attributed to light being scattered by the stroma, with more scattering occurring at higher frequencies, hence the color blue. This phenomenon, called the Tyndall effect, is similar to Rayleigh scattering and occurs in colloidal solutions, where the scattering particles are smaller than the scattered light wavelengths. Green eye color, on the other hand, is a result of combining these two phenomena (melanin light absorption and Tyndall scattering) [29].

4. Multispectral Database of Iris Images

For the purpose of this study a multispectral database of iris images has been collected, comprising NIR-illuminated images of standard quality (as recommended by ISO/IEC standard regarding biometric sample quality [30]) and high quality images obtained in visible light. 36 people presenting 72 different irises participated in the experiment. IrisGuard AD100, a two-eye NIR iris recognition camera, has been employed to capture six NIR-illuminated images (480×640 pixel bitmaps). Color images were acquired using the rear camera of Apple iPhone 5s (8-megapixel, JPG-compressed), with flash enabled. Data acquisition with a phone produced at least three images for each eye. In total, 432 near-infrared images acquired by a professional iris recognition camera and 272 color photos taken with a mobile phone were collected.

Images were then divided into three separable groups in respect to the eye color: the blue eyes subset, the green eyes subset, and the brown/hazel eyes subset, comprising 32 blue eyes, 18 green eyes and 22 brown, hazel or mixed-color eyes, respectively. Commercially available iris recognition software is typically built to cooperate with data compatible with the ISO/IEC standard specification. Color images were thus cropped to VGA resolution (640×480 pixels) and then converted to grayscale using selective RGB channel decomposition. Red, green, and blue channel of the RGB color space were extracted separately for each of the three eye color groups. Figure 1 presents sample images obtained using both cameras employed in this study, together with images extracted from each of the three RGB channels.

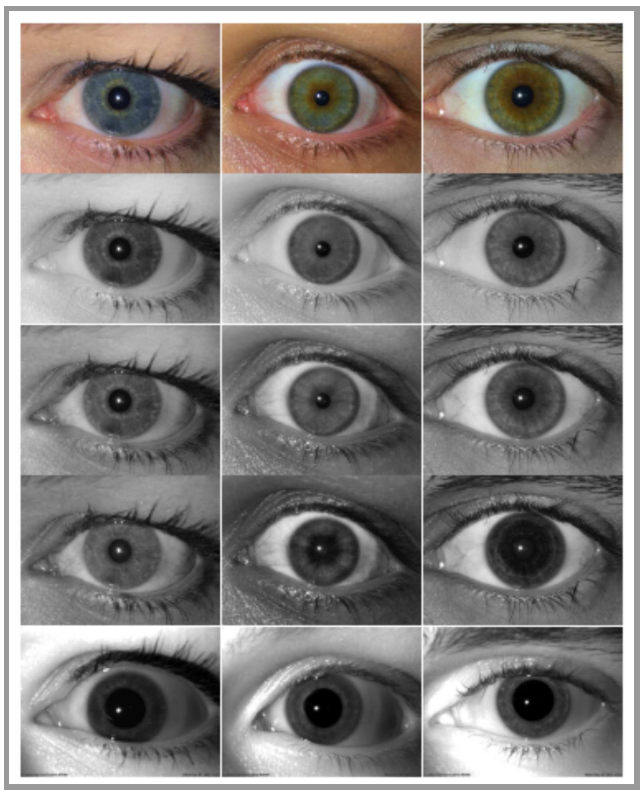


Fig. 1. Top row: cropped sample images obtained with the iPhone 5s: blue eye (left), green eye (middle), brown/hazel eye (right). Rows 2–4: grayscale versions of the images using red, green and blue channel of the RGB color space, respectively. Bottom row: NIR images obtained with the IrisGuard AD100. (See color pictures online at www.nit.eu/publications/journal-jtit)

5. Experimental Methodology

5.1. Iris Recognition Software

For the most comprehensive analysis, three commercial, state-of-the-art iris recognition methods and one algorithm of academic origin have been employed. This section briefly characterizes each of these solutions.

Monro Iris Recognition Library (**MIRLIN**) is a commercially available product, offered on the market by FotoNation (formerly SmartSensors) [31] as an SDK (Software Development Kit). Its methodology incorporates calculating binary iris code based on the output of a discrete cosine transform (DCT) applied to overlapping iris image patches [32]. The resulting binary iris templates are compared using XOR operation and comparison scores are generated in the form of fractional Hamming distance, i.e. the proportion of disagreeing bits in the two iris codes. With this metric in place, we should expect values close to zero for genuine (i.e. same-eye) comparisons, and values around 0.5 for impostor (i.e. different-eye) comparisons. The latter is due to the fact that comparing bits in iris codes of two different irises can be depicted as comparing two sequences of independent Bernoulli trials (such as symmetric coin tosses).

IriCore employs a proprietary and unpublished recognition methodology. Similarly to MIRLIN, it is offered on the market in the form of an SDK by IriTech [33]. With this matcher, values between 0 and 1.1 should be expected for same-eye comparisons, while different-eye comparisons should yield scores between 1.1 and 2.0.

The third method involved in this study, **VeriEye**, is available commercially from Neurotechnology [34] and, similarly to the IriCore method, the precise mechanisms of the recognition methodology are not disclosed in any scientific papers. The manufacturer, however, claims to employ active shape modeling for iris localization using non-circular approximations of pupillary and limbic iris boundaries. VeriEye, contrary to two previous methods, returns comparison scores in a form of similarity metric – the higher the score, the better the match. A perfect non-match should return a score equal to zero.

The last method employed for the purpose of this study is Open Source for IRIS (**OSIRIS**), developed within the BioSecure project [35] and offered by its authors as a free, open-source solution. OSIRIS follows the well-known concept originating in the works of Daugman, incorporating image segmentation and normalization by unwrapping the iris image from polar coordinates onto a Cartesian rectangle using Daugman's *rubber sheet* model. Encoding of the iris is carried out using phase quantization of multiple Gabor wavelet filtering outcomes, while matching is performed using XOR operation, with normalized Hamming distance as an output dissimilarity metric. As in the MIRLIN method, values close to zero are expected for genuine comparisons, while impostor comparisons should typically produce results around 0.5, however, due to shifting the iris code in search for the best match as a countermeasure against eye rotation, impostor score distributions will more likely be centered around 0.4 to 0.45 values.

5.2. Comparison Scores Generation

As this study aims at quantifying cross-spectral iris recognition accuracy in a scenario that would mimic potential real-world applications, where mobile-based verification would complement a typical enrollment using professional iris recognition hardware operating in NIR, the following experiments are performed. NIR images obtained using the IrisGuard AD100 camera are used as gallery (enrollment) samples. Visible light images obtained with the iPhone 5s are used as probe (verification) samples. All possible genuine and impostor comparisons are generated for all three subsets of eyes and all three RGB channels, for each of the four iris recognition methods employed. Thus, 36 Receiver Operating Characteristic (ROC) curves can be constructed (4 methods $\times$ 3 eye color subsets $\times$ 3 RGB channels), 9 for each method. These are presented and commented on in the following section.

6. Results

Figures 2–5 illustrate ROC curves obtained when generating genuine and impostor score distributions for each RGB channel and each eye color subset. EER-wise, the red channel offers the best performance in most of the method/channel/subset combinations. There are however, a few exceptions from this behavior. For the blue eyes subset, the green channel provides recognition accuracy that is very similar to this of the red channel (slightly better for the MIRLIN matcher, slightly worse for the VeriEye matcher, and the same for the remaining two methods). Interestingly, for the MIRLIN matcher, the blue channel gives the same EER as the green channel, and better than the red channel. For the green eyes subset, the red channel offers significantly better performance than the other channels for the OSIRIS and MIRLIN matchers. However, for the VeriEye matcher, using green channel instead decreased the EER from 5 to 2%, a significant improvement over the recognition accuracy offered by the red channel.
The brown/hazel eyes subset, unsurprisingly, achieves the optimal recognition performance for the red channel, as it offers significantly better iris pattern visibility than the other two channels. The IriCore method, however, seems to be less susceptible to the type of the input data, as decrease

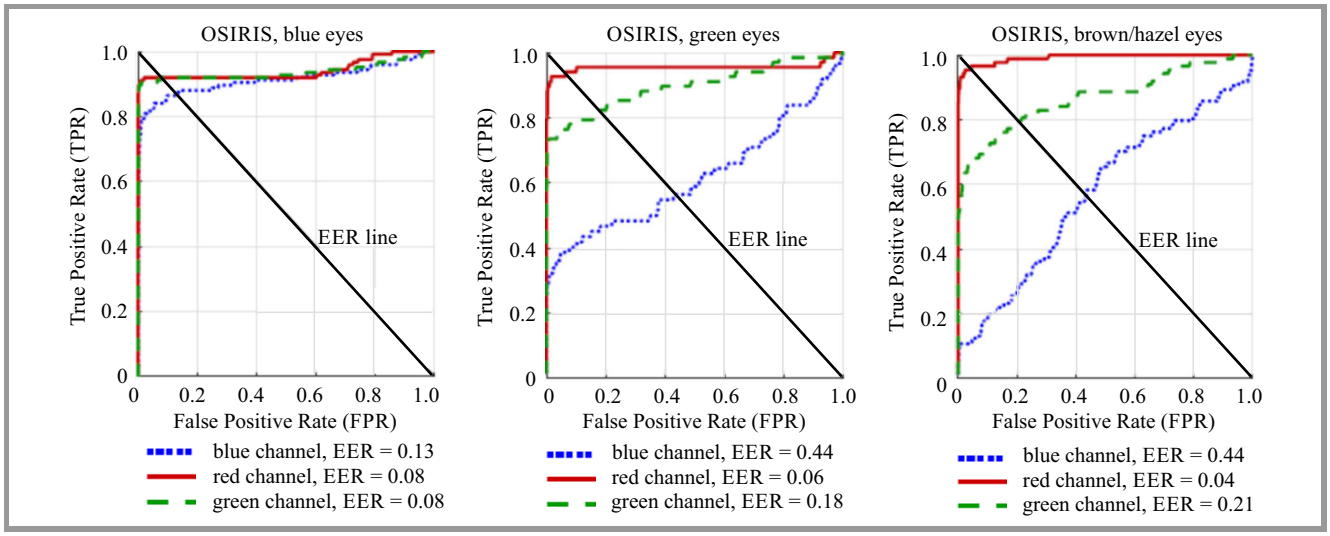


Fig. 2. ROC curves for **OSIRIS** matcher and scores obtained when matching different RGB channels of samples from the: (a) blue eyes, (b) green eyes, and (c) brown/hazel eyes subsets. Red channel scores are denoted with solid red line, blue channel scores: dotted blue line, green channel scores: dashed green line. Equal error rates (EER) are also shown.

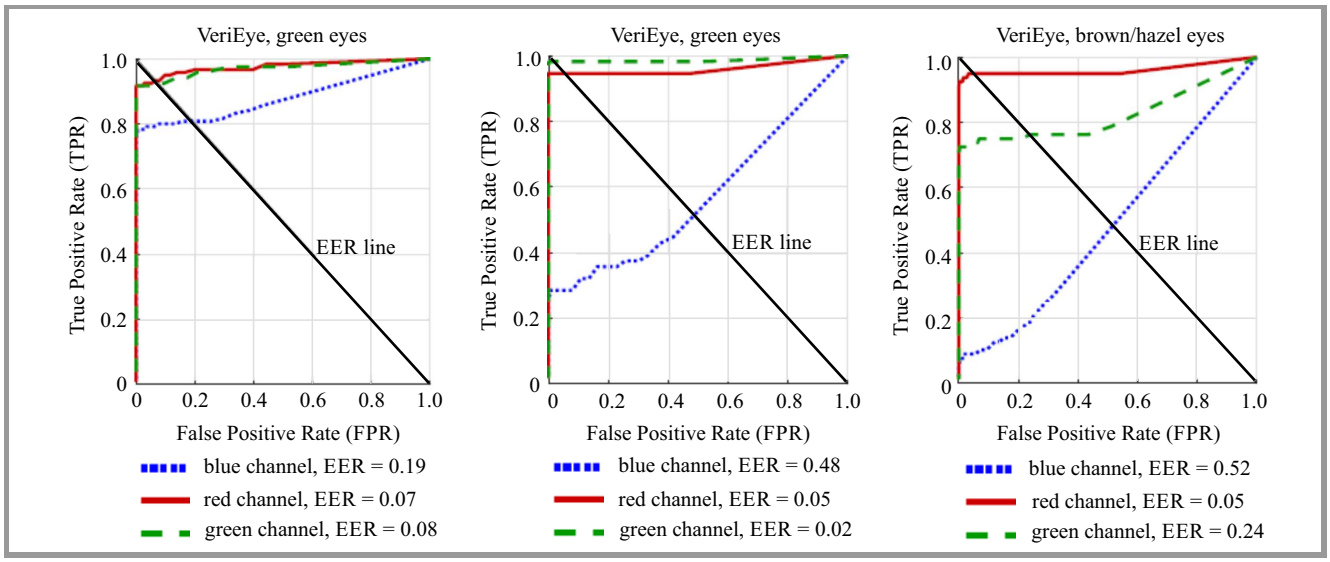


Fig. 3. Same as in Fig. 2, but for the VeriEye matcher: (a) blue eyes, (b) green eyes, and (c) brown/hazel eyes.

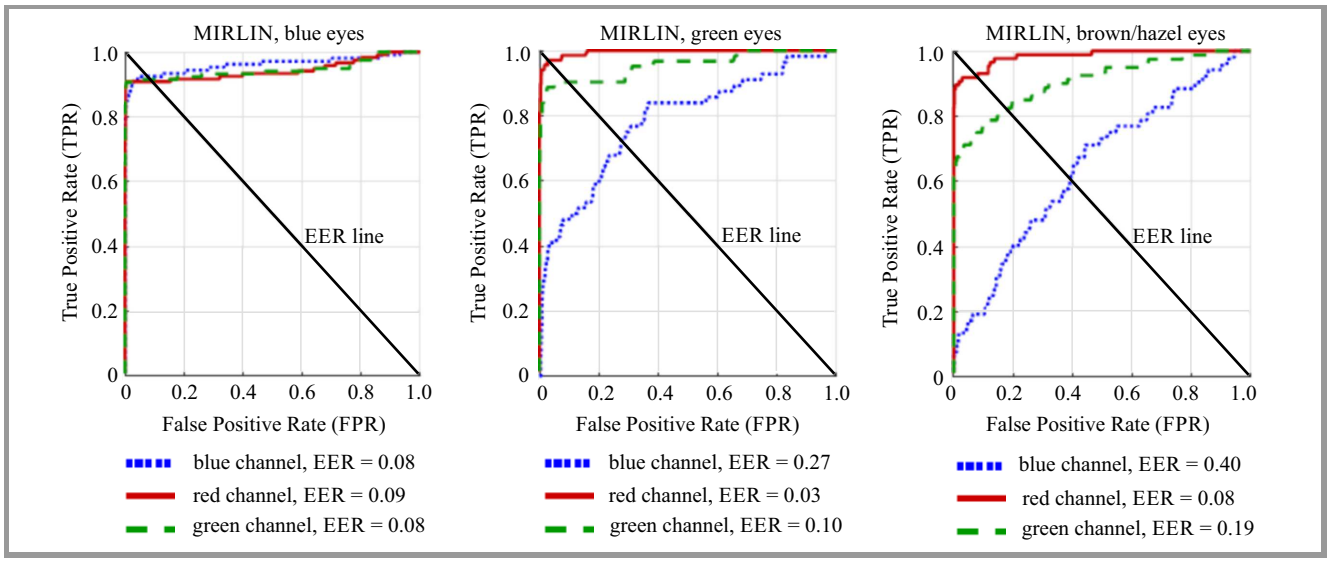


Fig. 4. Same as in Fig. 2, but for the MIRLIN matcher: (a) blue eyes, (b) green eyes, and (c) brown/hazel eyes.

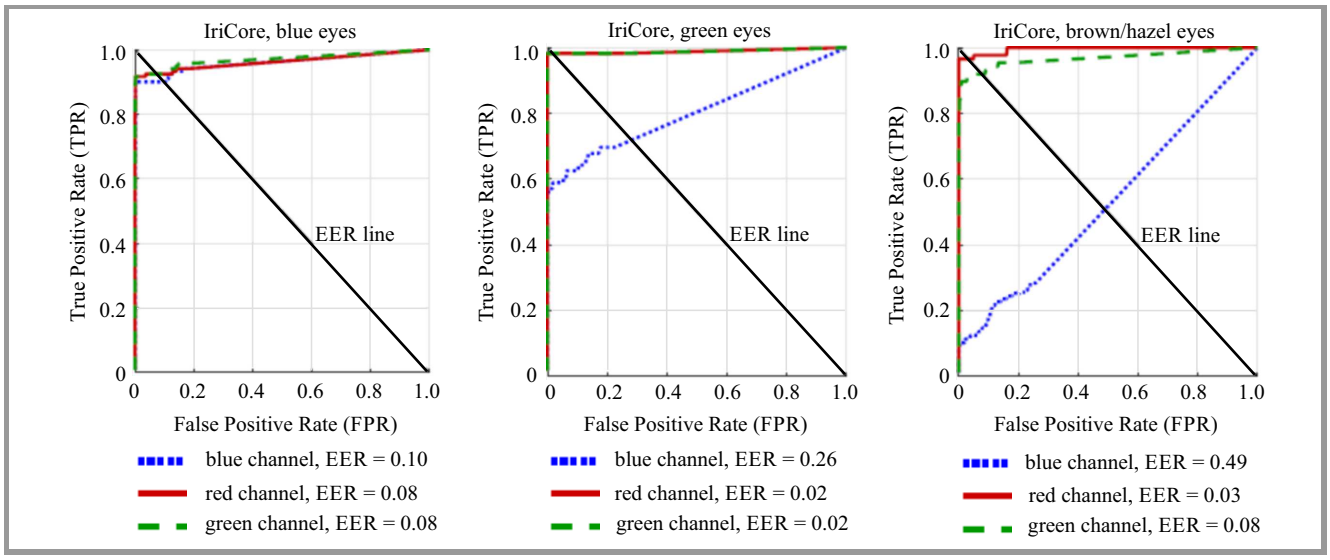


Fig. 5. Same as in Fig. 2, but for the IriCore matcher: (a) blue eyes, (b) green eyes, and (c) brown/hazel eyes.

in performance for the green channel is much lower than in the remaining three methods (compared to the red channel).

7. Conclusions

This study provides a valuable analysis of cross-spectral iris recognition, when high quality visible light images obtained with a mobile phone are used as verification counterparts for enrollment samples obtained in NIR. The red channel performs best in general, however, in selected cases, employing the green or the blue channel of the RGB color space when converting the color image to grayscale is shown to improve recognition accuracy. This is true for some combination of recognition methods and eye colors recognition accuracy can be improved this way in blue and green eyes, while dark brown and hazel eyes generally perform best when the red channel is used.

The experiments revealed that cross-spectral iris recognition in the discussed scenario is perfectly viable, with equal error rates not exceeding 7, 2 and 3% for the blue, green and brown/hazel eyes, respectively, when optimal combinations of the recognition method and grayscale transformation are selected. As this incorporated only a simple selection of the RGB channel best suited for a given eye color, future experiments employing more advanced image processing could bring the error rates even lower. This certainly lets us think of cross-spectral iris recognition using mobile phones with a great dose of optimism.

Acknowledgement

The authors would like to thank Dr. Adam Czajka for his valuable comments that contributed to the quality of this paper. We are also grateful for the help of the Biometrics Scientific Club members at the Warsaw University of Technology when building the database used in this study.

References

[1] L. Flom and A. Safir, "Iris recognition system", United States Patent, US 4641349, 1987.

[2] J. Daugman, "Biometric personal identification system based on iris analysis", United States Patent, US 5291560, 1994.

[3] J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence", *IEEE Trans. Pattern Anal. and Machine Intell.*, vol. 15, no. 11, pp. 1148–1161, 1993.

[4] Fujitsu Limited, Fujitsu Develops Prototype Smartphone with Iris Authentication [Online]. Available: http://www.fujitsu.com/global/about/resources/news/press-releases/2015/0302-03.html (accessed on Oct. 29, 2015).

[5] Planet Biometrics, Microsoft brings iris recognition to the masses with new Lumia [Online]. Available: http://www.planetbiometrics.com/article-details/i/3606/desc/microsoft-brings-iris-recognition-to-the-masses-with-new-lumia/ (accessed July 31, 2016).

[6] Samsung Electronics, Samsung Galaxy Note 7 [Online]. Available: www.samsung.com/global/galaxy/galaxy-note-7/security (accessed Aug. 10, 2016).

[7] C. Boyce, A. Ross, M. Monaco, L. Hornak, and X. Li, "Multispectral iris analysis: A preliminary study", in *Proc. Conf. Comp. Vision & Pattern Recogn. Worksh. CVPRW'06*, New York, NY, USA, 2006 (doi: 10.1109/CUPRW.2006.141).

[8] J. H. Park and M. G. Kang, "Multispectral iris authentication system against counterfeit attack using gradient-based image fusion", *Optical Engin.*, vol. 46, no. 11, 2007 (doi: 10.1117/1.2802367).

[9] A. Ross, R. Pasula, and L. Hornak, "Iris recognition: On the segmentation of degraded images acquired in the visible wavelength", in *Proc. IEEE 3rd Int. Conf. Biometrics: Theory, Appl. and Syst. BTAS 2009*, Washington, DC, USA, 2009.

[10] M. J. Burge and M. K. Monaco, "Multispectral iris fusion for enhancement, interoperability, and cross wavelength matching", in *Algorithms and Technologies for Multispectral, Hyperspectral, and Ultraspectral Imagery XV*, S. S. Shen and P. E. Lewis, Eds. *Proc. of SPIE*, vol. 7334, 73341D, 2009 (doi: 10.1117/12.819058).

[11] J. Zuo, F. Nicolo, and N. A. Schmid, "Cross spectral iris matching based on predictive image mapping", in *4th IEEE Int. Conf. Biometrics: Theory, Appl. and Syst. BTAS 2010*, Washington, DC, USA, 2010.

[12] M. Dobes, L. Machala, P. Tichavsky, and J. Pospisil, "Human eye iris recognition using the mutual information", *Optik*, vol. 115, no. 9, pp. 399–404, 2004.

[13] H. Proença and L. A. Alexandre, "UBIRIS: A noisy iris image database", Tech. Rep., ISBN: 972-99548-0-1, University of Beira Interior, Portugal, 2005.

[14] H. Proença, S. Filipe, R. Santos, J. Oliveira, and L. A. Alexandre, "The UBIRIS.v2: A database of visible wavelength iris images captured on-the-move and at-a-distance", *IEEE Trans. Pattern Anal. and Machine Intell.*, vol. 32, no. 8, pp. 1529–1535, 2010.

[15] M. Trokielewicz, "Iris recognition with a database of iris images obtained in visible light using smartphone camera", in *Proc. IEEE Int. Conf. on Ident., Secur. and Behavior Anal. ISBA 2016*, Sendai, Japan, 2016.

[16] Warsaw-BioBase-Smartphone-Iris-v1.0 [Online]. Available: http://zbum.ia.pw.edu.pl/en/node/46

[17] H. Proença, "On the feasibility of the visible wavelength, at-a-distance and on-the-move iris recognition", in *Proc. IEEE Symp. Series on Computat. Intell. in Biometr.: Theory, Algorithms, & Appl. SSCI 2009*, Nashville, TN, USA, 2009, vol. 1, pp. 9–15.

[18] H. Proença, "Iris recognition: On the segmentation of degraded images acquired in the visible wavelength", *IEEE Trans. on Pattern Anal. & Mach. Intellig.*, vol. 32, no. 8l pp. 1502–1516, 2010.

[19] H. Proença, "Quality assessment of degraded iris images acquired in the visible wavelength", *IEEE Trans. Inform. Forens. and Secur.*, vol. 6, no. 1, pp. 82–95, 2011.

[20] G. Santos, M. V. Bernardo, H. Proenca, and P. T. Fiadeiro, "Iris recognition: Preliminary assessment about the discriminating capacity of visible wavelength data", in *Proc. 6th IEEE Int. Worksh. Multim. Inform. Process. and Retrieval MIPR 2010*, Taichung, Taiwan China, 2010, pp. 324–329.

[21] P. Radu, K. Sirlantzis, G. Howells, S. Hoque, and F. Deravi, "A colour iris recognition system employing multiple classifier techniques", *Elec. Lett. Comp. Vision and Image Anal.*, vol. 12, no. 2, pp. 54–65, 2013.

[22] M. Frucci, C. Galdi, M. Nappi, D. Riccio, and G. Sanniti di Baja, "IDEM: Iris detection on mobile devices", in *Proc. 22nd Int. Conf. Pattern Recogn. ICPR 2014*, Stockholm, Sweden, 2014.

[23] K. Raja, R. Raghavendra, F. Cheikh, B. Yang, and C. Busch, "Robust iris recognition using light field camera", in *The 7th Colour and Visual Comput. Symp. CVCS 2013*, Gjøvik, Norway, 2013.

[24] K. Raja, R. Raghavendra, and C. Busch, "Iris imaging in visible spectrum using white LED", in *7th IEEE Int. Conf. on Biometr.: Theory, Appl. and Syst. BTAS 2015*, Arlington, VA, USA, 2015.

[25] K. Raja, R. Raghavendra, V. Vemuri, and C. Busch, "Smartphone based visible iris recognition using deep sparse filtering", *Pattern Recogn. Lett.*, vol. 57, pp. 33–42, 2014.

[26] K. B. Raja, R. Raghavendra, and C. Busch, "Smartphone based robust iris recognition in visible spectrum using clustered K-mean features", in *Proc. IEEE Worksh. Biometr. Measur. and Syst. for Secur. and Med. Appl. BioMS 2014*, Rome, Italy, 2014, pp. 15–21.

[27] M. De Marsico, C. Galdi, M. Nappi, and D. Riccio, "FIRME: Face and iris recognition engagement", *Image and Vis. Comput.*, vol. 32, no. 12, pp. 1161–1172, 2014.

[28] M. Trokielewicz, E. Bartuzi, K. Michowska, A. Andrzejewska, and M. Selegrat, "Exploring the feasibility of iris recognition for visible spectrum iris images obtained using smartphone camera", in *Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2015*, R. S. Romaniuk, Ed. *Proc. of SPIE*, vol. 9662, 2015 (doi: 10.1117/12.2205913).

[29] P. van Slembrouck, "Structural Eye Color is Amazing" [Online]. Available: http://medium.com/@ptvan/structural-eye-color-is-amazing-24f47723bf9a (accessed Aug. 8, 2016).

[30] ISO/IEC 19794-6:2011. Information technology – Biometric data interchange formats – Part 6: Iris image data, 2011.

[31] Smart Sensors Ltd., MIRLIN SDK, version 2.23, 2013.

[32] D. M. Monro, S. Rakshit, and D. Zhang, "DCT-based iris recognition", *IEEE Trans. Pattern Anal. and Machine Intell.*, vol. 29, no. 4, pp. 586–595, 2007.

[33] IriTech Inc., IriCore Software Develope's Manual, version 3.6, 2013 [Online]. Available: www.iritech.com/products/swoftware/iricore-eye-recognition-software

[34] Neurotechnology Company, VeriEye SDK, version 4.3 [Online]. Available: www.neurotechnology.com/verieye.html (accessed Aug. 11, 2015).

[35] G. Sutra, B. Dorizzi, S. Garcia-Salitcetti, and N. Othman, "A biometric reference system for iris. OSIRIS version 4.1 [Online]. Available: http://svnext.it-sudparis.eu/svnview2-eph/ref_syst/iris_osiris_v4.1 (accessed Oct. 1, 2014).

Mateusz Trokielewicz received his B.Sc. and M.Sc. in Biomedical Engineering from the Faculty of Mechatronics and the Faculty of Electronics and Information Technology at the Warsaw University of Technology, respectively. He is currently with the Biometrics Laboratory at the Research and Academic Computer Network and with the Institute of Control and Computation Engineering at the Warsaw University of Technology, where he is pursuing his Ph.D. in Biometrics. His current professional interests include iris biometrics and its reliability against biological processes, such as aging and diseases, and iris recognition on mobile devices.
E-mail: mateusz.trokielewicz@nask.pl
Biometrics Laboratory
Research and Academic Computer Network (NASK)
Kolska st 12
01-045 Warsaw, Poland

Institute of Control and Computation Engineering
Warsaw University of Technology
Nowowiejska st 15/19
00-665 Warsaw, Poland

Ewelina Bartuzi received her B.Sc. degree in Biomedical Engineering from the Faculty of Mechatronics at the Warsaw University of Technology in 2016. She is presently working as a Technical Specialist at the Biometrics Laboratory, Research and Academic Computer Network. Her current research interests include biometrics based on thermal hand images and iris recognition for mobile.
E-mail: ewelina.bartuzi@nask.pl
Biometrics Laboratory
Research and Academic Computer Network (NASK)
Kolska st 12
01-045 Warsaw, Poland

Paper

Faster Point Scalar Multiplication on Short Weierstrass Elliptic Curves over F_p using Twisted Hessian Curves over F_{p^2}

Michał Wroński

Military University of Technology, Warsaw, Poland

Abstract—This article shows how to use fast F_{p^2} arithmetic and twisted Hessian curves to obtain faster point scalar multiplication on elliptic curve E_{SW} in short Weierstrass form over F_p. It is assumed that p and $\#E_{SW}(F_p)$ are different large primes, $\#E(F_q)$ denotes number of points on curve E over field F_q and $\#E^t_{SW}(F_p)$, where E^t is twist of E, is divisible by 3. For example this method is suitable for two NIST curves over F_p: NIST P-224 and NIST P-256. The presented solution may be much faster than classic approach. Presented solution should also be resistant for side channel attacks and information about Y coordinate should not be lost (using for example Brier-Joye ladder such information may be lost). If coefficient A in equation of curve $E_{SW}: y^2 = x^3 + Ax + B$ in short Weierstrass curve is not of special form, presented solution is up to 30% faster than classic approach. If $A = -3$, proposed method may be up to 24% faster.

Keywords—elliptic curve cryptography, hardware implementations, twisted Hessian curves.

1. Introduction

The point scalar multiplication is used in many cryptographic applications, which are based on elliptic curve discrete logarithm problem (ECDLP). In this article a faster arithmetic on elliptic curves in short Weierstrass form E_{SW} over F_p is considered, where p is large prime and $\#E_{SW}$ is also prime. If twist of such a curve E^t_{SW} has its order $\#E^t_{SW}$ divisible by 3, then twisted Hessian curves arithmetic over F_{p^2} may be used to speed up point scalar multiplication on $E_{SW}(F_p)$. It is possible because $\#E_{SW}(F_{p^2}) = \#E_{SW}(F_p) \cdot \#E^t_{SW}(F_p)$. If $3|\#E^t_{SW}$ then $3|\#E_{SW}(F_{p^2})$. Hence, it is possible to find twisted Hessian curve $E_{TH}(F_{p^2})$ isomorphic to $E_{SW}(F_{p^2})$. If it is needed to make point scalar multiplication by $k \in \{2, \ldots, \#E_{SW}(F_p) - 2\}$ of point $P \in E_{SW}(F_p)$, to get in result point $Q \in E_{SW}(F_p)$ where $Q = [k]P$, it is not necessary to use short Weierstrass curve arithmetic. If ϕ is isomorphism from $E_{SW}(F_{p^2})$ to $E_{TH}(F_{p^2})$, so: $\phi : E_{SW}(F_{p^2}) \rightarrow E_{TH}(F_{p^2})$ then for every point $P \in E_{SW}(F_p)$ (then of course also $P \in E_{SW}(F_{p^2})$) may be found $P' \in E_{TH}(F_{p^2})$ for which $P' = \phi(P)$. To compute Q may be used formula $Q = \phi^{-1}\left([k]\phi(P)\right)$. One can see that $[k]\phi(P) = [k]P' = Q'$ and finally $\phi^{-1}(Q') = Q$. In hardware implementation F_{p^2} arithmetic, if is properly implemented, may be almost as fast as F_p arithmetic. Because twisted Hessian curves arithmetic for F_{p^2} fields (where $p \neq 2, 3$) is complete (point addition, doubling, addition of neutral and addition of opposite point are computed using the same formulas), it is possible to gain faster solution, resistant for side channel attacks in hardware implementations (especially in FPGA chips). Due to the fact that any information about value of Y coordinate should not be lost, Brier-Joye ladder for point scalar multiplication [1] is not considered in this article.

2. Arithmetic in F_{p^2}

The field F_{p^2} is generated by irreducible polynomial of degree 2 with coefficients from F_p. The main goal of this article is to get fast arithmetic in F_{p^2}. Only an irreducible polynomials of form $f(t) = t^2 \pm c$ are considered, where c is small positive integer.

Every element $A \in F_{p^2}$ may be written as $A = a_1 t + a_0$, where $a_0, a_1 \in F_p$.

Let's assume $A, B \in F_{p^2}$, where $A = a_1 t + a_0$ and $B = b_1 t + b_0$. Then $A \pm B = (a_1 t + a_0) \pm (b_1 t + b_0) = (a_1 \pm b_1)t + (a_0 \pm b_0)$. Addition and subtraction are not complex operations and may be computed in only one processor machine cycle. Although fast F_{p^2} arithmetic is presented in [2] to speed-up pairing, in this article is showed its different application. It is also showed how to fast compute inversion of element in F_{p^2}, based on idea presented in [3].

2.1. Multiplication

Multiplication is crucial operation in elliptic curve arithmetic. However, it is not the most time-consuming operation (it is inversion), during point scalar multiplication many times it is needed to compute multiplication in field over which elliptic curve is defined. Inversion is computed only once, at the end of all computations.

Let $A, B \in F_{p^2}$, where $A = a_1 t + a_0$ and $B = b_1 t + b_0$. Let $f(t) = t^2 \pm c$. Then using Karatsuba algorithm, element C is computed as:

$$C = A \cdot B = (a_1 b_0 + a_0 b_1)t + a_0 b_0 \mp c a_1 b_1 = Rt \mp Mc + N,$$

where:
$L = (a_1 + a_0)(b_1 + b_0)$,
$M = a_1 b_1$,
$N = a_0 b_0$,
$R = L - M - N = a_1 b_0 + a_0 b_1$.

One can notice that:

$$c_1 = R \quad \text{and} \quad c_2 = \mp Mc + N.$$

Multiplication in F_{p^2} requires 3 multiplications in F_p, 5 additions/subtractions in F_p and 1 multiplication in F_p by small constant.
Although in software applications the multiplication in F_{p^2} is still more complex than multiplication in F_p, using parallelism in hardware it is possible to compute it in almost the same time.
The total number of processor cycles required to make multiplication in F_{p^2} is $MAX\{T_M + 2, T_M + \lceil \log_2 c \rceil + 1\}$. One can see that the smaller c is chosen, the less operations are required to compute the result.
In the case when $p \equiv 3 (mod\ 4)$, an irreducible polynomial of form $f(t) = t^2 + 1$ may be chosen and then the cost of multiplication equals $MAX\{T_M + 2, T_M + \lfloor \log_2 1 \rfloor + 1\} = T_M + 2$ processor cycles. In the case $p \equiv 5 (mod\ 8)$, the irreducible polynomial of form $f(t) = t^2 - 2$ may be chosen and then the complexity of multiplication reach $MAX\{T_M + 2, T_M + \lceil \log_2 2 \rceil + 1\} = T_M + 2$ processor cycles.

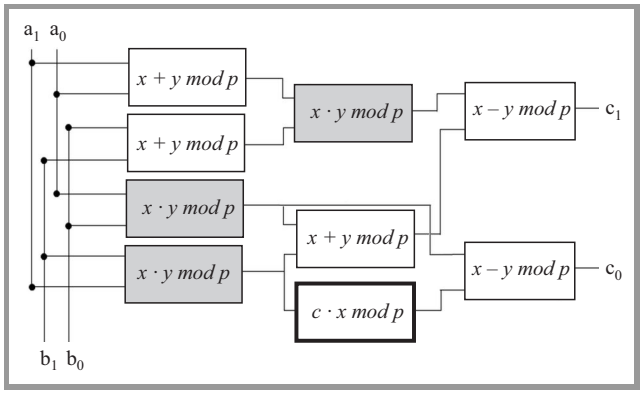


Fig. 1. Scheme of parallel multiplication in F_{p^2}.

2.2. Inversion

It is possible for every $A \in F_{p^2}$ to get its inversion A^{-1} by computing only one inversion of element from F_p. Hence, the method for irreducible polynomial of form $f(t) = t^2 \pm c$ is shown base on idea presented in [3]:

$$A = \begin{bmatrix} a_1 \\ a_0 \end{bmatrix} \quad \text{and} \quad A^{-1} = \begin{bmatrix} b_1 \\ b_0 \end{bmatrix}.$$

If

$$M = \begin{bmatrix} a_0 & a_1 \\ \mp a_1 c & a_0 \end{bmatrix},$$

then

$$M \cdot \begin{bmatrix} b_1 \\ b_0 \end{bmatrix} = \begin{bmatrix} a_0 & a_1 \\ \mp a_1 c & a_0 \end{bmatrix} \cdot \begin{bmatrix} b_1 \\ b_0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

The coefficients in matrix M may be taken from general form of element $C = A \cdot B$.
Then transformation should be made:

$$\begin{bmatrix} b_1 \\ b_0 \end{bmatrix} = \begin{bmatrix} a_0 & a_1 \\ \mp a_1 c & a_0 \end{bmatrix}^{-1} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = M^{-1} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Now the determinant of matrix M is equal to:

$$\det(M) = a_0^2 \pm a_1^2 c,$$

then

$$M^{-1} = \frac{1}{\det(M)} \begin{bmatrix} a_0 & -a_1 \\ \pm a_1 c & a_0 \end{bmatrix}$$

and

$$\begin{bmatrix} b_1 \\ b_0 \end{bmatrix} = \frac{1}{\det(M)} \begin{bmatrix} a_0 & -a_1 \\ \pm a_1 c & a_0 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\det(M)} \begin{bmatrix} -a_1 \\ a_0 \end{bmatrix}.$$

The computations may be done in the following 6 steps:

1. $D = a_0^2$,
2. $E = a_1^2 c$,
3. $H = E + D = \det(M)$,
4. $\overline{H} = H^{-1}$,
5. $b_1 = -a_1 \overline{H}$,
6. $b_0 = a_0 \overline{H}$.

The inversion in F_{p^2} requires 1 inversion in F_p, 4 multiplications in F_p, 1 multiplication by small constant c in F_p and 1 addition in F_p.

3. Elliptic Curves

An elliptic curve may be defined over every field K. Because in cryptographic applications only finite fields are used and in this article only fields with big characteristic $p \neq 2, 3$ are considered, then all definitions below are proper for such fields but may not be proper for fields with characteristic 2 or 3.

3.1. Short Weierstrass Elliptic Curve

Every elliptic curve E over F_q with $char(F_q) \neq 2, 3$ may be given in short Weierstrass form $E_{SW} : y^2 = x^3 + Ax + B$, where $-16\left(4A^3 - 27B^2\right) \neq 0$. The arithmetic on short Weierstrass curve is in general not complete (there is such a method described in [4] but it is not efficient) so different formulas for point addition, doubling, addition of neutral element and addition of opposite element are used. The short Weierstrass curve arithmetic is the fastest for

$A=-3$. In this case, points addition requires 14 multiplications and 7 additions in F_q. Mixed addition requires 11 multiplications and 7 additions in F_q. Point doubling requires 10 multiplications and 11 additions in F_q. If A is not of special form, then points addition requires 14 multiplications and 7 additions in F_q. Mixed addition requires 11 multiplications and 7 additions in F_q. Point doubling requires 12 multiplications and 12 additions in F_q. It is assumed that squaring, multiplication by vary elements and multiplication by big constant require the same time. All necessary formulas may be found in [5].

3.2. Twisted Hessian Curves

The twisted Hessian curve [6] over field F_q is given by:

$$E_{TH}: ax^3+y^3+1=dxy$$

with neutral point $(0,-1)$ in affine coordinates or by:

$$E_{TH}: aX^3+Y^3+Z^3=dXYZ$$

in projective coordinates with neutral point $(0,-1,1)$. Elements $a,d\in F_q$ and $a(27a-d^3)\neq 0$.
If $a=1$ then $E_{TH,a,d}: x^3+y^3+1=dxy$ is Hessian curve.
On twisted Hessian curves faster arithmetic than for short Weierstrass curves may be used. Moreover, on twisted Hessian curve over F_q, if $q\equiv 1(mod\ 3)$ and a is not cube in F_q, complete arithmetic may be used.
Arithmetic on twisted Hessian curves is described with all details in [6].
The best complete addition formula requires 12 multiplications, i.e. 11 multiplications of vary elements and 1 multiplication by constant and 16 additions/subtractions.

3.3. Isomorphism between Twisted Hessian Curves and Elliptic Curves in Short Weierstrass Form over Finite Fields

Let us consider computation of $Q=[k]P$ on elliptic curve $E_{SW}(F_q): y^2=x^3+Ax+B$, where $Ord(P)$ is prime. If $3|\#E_{SW}(F_q)$ (it means that curve E_{SW} has 3-torsion point) and $q\equiv 1(mod\ 3)$ then for curve E_{SW} may be found isomorphic twisted Hessian curve E_{TH} with complete arithmetic (when a is not cube in F_q). Note there is not any elliptic curve over F_p having isomorphic twisted Hessian curve over F_p if $\#E_{SW}(F_p)$ is prime.
One can see that for some elliptic curves over F_p for which $\#E_{SW}(F_p)$ is prime, there is some possibility that $\#E^t_{SW}$ is divisible by 3.
Let us see, that if $\#E_{SW}(F_p)=p+1-t$ over F_p then $\#E^t_{SW}=p+1+t$ and $\#E_{SW}(F_{p^2})=\#E_{SW}(F_p)\cdot\#E^t_{SW}(F_p)=(p+1)^2-t^2$ over F_{p^2}. So if $3|\#E^t_{SW}$ then $3|\#E_{SW}(F_{p^2})$. Because $p^2\equiv 1(mod\ 3)$ for all primes $p\neq 3$, therefore a twisted Hessian curve such as $E_{TH}(F_{p^2}): ax^3+y^3+1=dxy$ isomorphic to $E_{SW}(F_{p^2})$ exists and if a is not cube in F_{p^2}, then complete arithmetic on $E_{TH}(F_{p^2})$ may be used. Finally, point $Q\in E_{SW}$ may be computed using twisted Hessian curve over F_{p^2} instead of using short Weierstrass curve over F_p.

This rule was checked for NIST elliptic curves over F_p. For two curves, NIST P-224 and NIST P-256, may be used arithmetic on twisted Hessian curve over F_{p^2} isomorphic to $E_{SW}(F_{p^2})$.
The next important problem is how to find such twisted Hessian curve.
First, suppose that triangular elliptic curve is given by:

$$E_{TR}: \overline{y}^2=d\overline{xy}+a\overline{y}=\overline{x}^3 \quad \text{over} \quad F_{p^2},$$

where $a,d\in F_p$.
Then the transformations can be made:

$$\left(\overline{y}+\tfrac{dx+a}{2}\right)^2=\left(\overline{x}+\tfrac{d^2}{12}\right)^3+$$
$$+\left(\tfrac{da}{2}-\tfrac{d^4}{48}\right)\left(\overline{x}+\tfrac{d^2}{12}\right)-\tfrac{d^2}{12}\left(\tfrac{da}{2}-\tfrac{d^4}{48}\right)+a^2.$$

If

$$E_{SW}: y^2=x^3+Ax+B$$

then:

$$x=\overline{x}+\frac{d^2}{12},$$
$$y=\overline{y}+\frac{dx+a}{2},$$
$$A=\frac{da}{2}-\frac{d^4}{48},$$
$$B=-\frac{d^2}{12}A+a^2.$$

For elliptic curves over F_p it is possible to extend field from F_p to F_{p^2}. Then the coefficients of such a curve over field extension still belong to F_p. If coefficients $A,B\in F_p$ of such a curve are known, to find coefficients of twisted Hessian curve $a,d\in F_{p^2}$ it is necessary to compute d as one of the roots of polynomial $J(s)=\frac{-1}{6912}s^8-\frac{1}{24}As^4-Bs^2+A^2$. Note that if d is computed, then $a=(A+\frac{d^4}{48})\frac{2}{d}$, and in projective coordinates $E_{TR}: VW(V+dU+aW)=U^3$.
Then for triangular curve E_{TR} it is easy to find isomorphic twisted Hessian curve given by equation:

$$E_{TH,\left(d^3-27a\right),3d}: (d^3-27a)X^3+Y^3+Z^3=3dXYZ$$

and

$$X=U,$$
$$Y=\omega(V+dU+aW)-\omega^2V-aW,$$
$$Z=\omega^2\left(V+dU+aW\right)-\omega V-aW,$$

where ω is not trivial cubic root from 1 and $X,Y,Z,\omega\in F_{p^2}$.

Now the complete arithmetic (because presented solution must resistant for side channel attacks) may be used to compute $Q'\in E_{TH,(d^3-27a),3d}$ by $Q'=[k]P'$, where $P'=\phi(P)$. $\phi: E_{SW}\rightarrow E_{TH,(d^3-27a),3d}$ is isomorphism from E_{SW} to $E_{TH,(d^3-27a),3d}$. When Q' is known, it is necessary to find Q. It may be computed using $\phi^{-1}: E_{TH,(d^3-27a),3d}\rightarrow E_{SW}$, because $\phi^{-1}(Q')=Q$. However, $Q'\in E_{TH,(d^3-27a),3d}(F_{p^2})$

and $Q' \notin E_{TH,(d^3-27a),3d}(F_p)$, but $Q \in E_{SW}(F_{p^2})$ and $Q \in E_{SW}(F_p)$. Note that to find Q having $Q' = (X_Q, Y_Q, Z_Q)$, some more transformations are necessary.
Firstly, there a point on triangular curve

$$Q'' = (U_Q, V_Q, W_Q),$$

must be found, where:

$$U_Q = X_Q,$$

$$V_Q = -\frac{dX_Q + \omega Y_Q + \omega^2 Z_Q}{3},$$

$$W_Q = -\frac{dX_Q + Y_Q + Z_Q}{3a}.$$

Finally from the formulas

$$x_Q = \frac{U_Q}{W_Q} + \frac{d^2}{12},$$

$$y_Q = \frac{V_Q}{W_Q} + \frac{d\frac{U_Q}{W_Q} + a}{2}$$

the result $Q = (x_Q, y_Q) = [k]P$ can be found.

4. Speed-up for NIST Curves

Using presented ideas it is possible to speed-up point scalar multiplication on two NIST curves over F_p: NIST P-224 and NIST P-256. For both of these curves isomorphic twisted Hessian curves E_{TH} over F_{p^2} have coefficient a which is not cube in F_{p^2}, so it is impossible to use Hessian curves arithmetic [7], [8]. For others NIST curves over large prime fields the smallest field extensions, for which isomorphic twisted Hessian curves exist are:

- 8 for NIST P-192 and NIST P-384,
- 4 for NIST P-521.

One can see that the bigger the degree of field extension is, the more resources are required to implement F_{p^n} arithmetic in hardware. Hence, the most suitable are ellipitc curves for which F_{p^2} arithmetic may be used.
For NIST P-224 it is possible to find twisted Hessian curve over F_{p^2} which is isomorphic to NIST P-224 over F_{p^2}.
The irreducible polynomial of form $f(t) = t^2 + 11$ for arithmetic in F_{p^2} may be used in this case. Multiplication using such a polynomial requires then $T_M + \lceil \log_2 11 \rceil + 1 = T_M + 5$ processor cycles, where T_M is number of processor cycles required for multiplication in F_p.
For NIST P-224 it is possible to find twisted Hessian curve over F_{p^2} which is isomorphic to NIST P-256 over F_{p^2}.
The irreducible polynomial of form $f(t) = t^2 + 1$ for arithmetic in F_{p^2} may be used in this case. Multiplication using such a polynomial requires then $T_M + 2$ processor cycles, where T_M is number of processor cycles required for multiplication in F_p.

5. Comparison with Other Methods of Point Scalar Multiplication

Arithmetic on twisted Hessian curves may be very interesting, because:

- it is faster method than classic arithmetic on NIST curves in short Weierstrass form over F_p in hardware,
- it allows to use complete formula.

On the Figs. 2 and 3 the comparison between number of processor cycles required to compute point scalar multiplication is shown. It is assumed that on short Weierstrass curve over F_p in every step one doubling and one addition must be computed (then such solution is resistant for side channel attacks) and any information about value of Y is not lost. The Brier-Joye ladder may be used only for XZ coordinates, so information about Y may be lost.

T_M \ N_A	1	2	3	4	5	6	7	8
1	1.46	1.90	2.34	2.78	3.22	3.66	4.10	4.54
2	1.24	1.52	1.81	2.10	2.38	2.67	2.95	3.24
4	1.07	1.23	1.40	1.57	1.74	1.91	2.07	2.24
8	0.95	1.05	1.14	1.23	1.32	1.42	1.51	1.60
16	0.89	0.94	0.99	1.04	1.08	1.13	1.18	1.23
32	0.85	0.88	0.90	0.93	0.95	0.98	1.00	1.03
64	0.84	0.85	0.86	0.87	0.89	0.90	0.91	0.93
128	0.83	0.83	0.84	0.85	0.85	0.86	0.87	0.87
192	0.82	0.83	0.83	0.84	0.84	0.85	0.85	0.85
224	0.82	0.83	0.83	0.83	0.84	0.84	0.85	0.85
256	0.82	0.83	0.83	0.83	0.84	0.84	0.84	0.85
384	0.82	0.82	0.83	0.83	0.83	0.83	0.83	0.84
512	0.82	0.82	0.82	0.83	0.83	0.83	0.83	0.83
521	0.82	0.82	0.82	0.83	0.83	0.83	0.83	0.83

Fig. 2. Values of $\frac{T_{TH}}{T_{SW,-3}}$ for different number of processor cycles of T_M and different number of additions N_A required for multiplication in F_{p^n}.

T_M \ N_A	1	2	3	4	5	6	7	8
1	1.33	1.73	2.13	2.53	2.93	3.33	3.73	4.13
2	1.10	1.35	1.61	1.86	2.11	2.37	2.62	2.87
4	0.93	1.07	1.22	1.37	1.51	1.66	1.80	1.95
8	0.82	0.90	0.98	1.06	1.14	1.22	1.30	1.37
16	0.76	0.80	0.84	0.88	0.92	0.97	1.01	1.05
32	0.73	0.75	0.77	0.79	0.81	0.83	0.85	0.87
64	0.71	0.72	0.73	0.74	0.75	0.76	0.77	0.78
128	0.70	0.71	0.71	0.72	0.72	0.73	0.73	0.74
192	0.70	0.70	0.71	0.71	0.71	0.72	0.72	0.72
224	0.70	0.70	0.70	0.71	0.71	0.71	0.72	0.72
256	0.70	0.70	0.70	0.70	0.71	0.71	0.71	0.72
384	0.70	0.70	0.70	0.70	0.70	0.70	0.71	0.71
512	0.69	0.70	0.70	0.70	0.70	0.70	0.70	0.70
521	0.69	0.70	0.70	0.70	0.70	0.70	0.70	0.70

Fig. 3. Values of $\frac{T_{TH}}{T_{SW}}$ for different number of processor cycles of T_M and different number of additions N_A required for multiplication in F_{p^n}.

The results strongly depend on the number of processor cycles T_M required for multiplication in F_p and number of additions N_A required for making multiplication in F_{p^2}. N_A depends on form of irreducible polynomial $f(t)$, for example $N_A = 2$ for $f(t) = t^2 + 1$ and $N_A = 5$ for $f(t) = t^2 + 11$. Let's see that in average case k in binary form has the same number of 0 and 1. If l is length in bits of

$Ord(P)$ for which $[k]P$ is computed, then complete formula requires about l point doublings and $\frac{l}{2}$ points additions. So computing point scalar multiplication of point $P' = \phi(P)$ on twisted Hessian curve over F_{p^2} requires:

$$T_{TH} = l \cdot \big(12\,(T_M + N_A) + 16\big) + \tfrac{l}{2} \cdot \big(12\,(T_M + N_A) + 16\big) = \\ = \tfrac{3}{2} l \cdot \big(12\,(T_M + N_A) + 16\big)$$

processor cycles.

For short Weierstrass curve over F_p computing point scalar multiplication of point P requires about:

1. If $A = -3$:

$$T_{SW,-3} = l \cdot (10T_M + 11) + l \cdot (14T_M + 7) = \\ = l \cdot (24T_M + 18)\,.$$

   Hence,

$$\frac{T_{TH}}{T_{SW,-3}} = \frac{18\,(T_M + N_A) + 24}{24T_M + 18}.$$

2. If A is not of special form:

$$T_{SW} = l \cdot (12T_M + 12) + l \cdot (14T_M + 7) = \\ = l \cdot (26T_M + 19)$$

   and

$$\frac{T_{TH}}{T_{SW,-3}} = \frac{18\,(T_M + N_A) + 24}{26T_M + 19}.$$

The longer is T_M, the better results solution presented in this article gives. The more additions are required for multiplication in F_{p^2}, the worse results proposed solution gives. In real applications multiplication in F_p requires often as many processor cycles as binary length of field is. For example for NIST P-256 curve T_M may take even 256 processor cycles, without cycles required for initialization and then presented solution may give better results than standard methods.

6. Conclusion

Using F_{p^2} a reasonable speed-up in hardware implementation of point scalar multiplication on elliptic curves can be achieved. The article shows how to find for some elliptic curves with cofactor 1 isomorphic twisted Hessian curves in fields extension. For two NIST curves over large prime fields: NIST P-224 and NIST P-256 the degree of such extension is 2, so it is possible to use twisted Hessian curve arithmetic over F_{p^2}. Such a solution is faster than classic approach up to 30%, if solution resistant for side channel attacks is necessary and coefficient A of short Weierstrass curve is not of special form. For $A = -3$, the presented solution may be up to 24% faster than classic approach. Because implementation of parallel F_{p^2} arithmetic requires in hardware implementation much more resources than implementation of F_p arithmetic, the presented solution should be used only in some situations. For example, if necessary is to have arithmetic on two elliptic curves, which ensure different level of security. The first curve may use GLS method [9], because is very fast and on curve suitable for this method it is possible to use fast arithmetic in F_{p^2} and such a curve gives the security about p. Therefore, arithmetic on the second curve (which curve should give smaller security, for example about $\sqrt{p}$) may be implemented using the same F_{p^2} arithmetic, which is used for the first one. Then it is possible to use method presented in this article and such implementation is then faster than the classic one.

References

[1] E. Brier and M. Joye, "Weierstraß elliptic curves and side-channel attacks", in *Public Key Cryptography*, *LNCS*, vol. 2274, pp. 335–345. Springer, 2002 (doi: 10.007/3-540-45664-3_24).

[2] S. Ghosh, D. Mukhopadhyay, and D. Roychowdhury, "High speed flexible pairing cryptoprocessor on FPGA platform", in *Pairing-Based Cryptography – Pairing 2010*, S. Ghosh, D. Mukhopadhyay, and D. Roychowdhury, Eds. *LNCS*, vol. 6487, pp. 450–466. Springer, 2010 (doi: 10.1007/978/3/642-17455-1_28).

[3] H. Cohen and G. Frey, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. New York: Chapman & Hall/CRC, 2006.

[4] J. Renes, C. Costello, and L. Batina, "Complete addition formulas for prime order elliptic curves", Cryptology ePrint Archive, Report 2015/1060, 2015 [Online]. Available: https://eprint.iacr.org/2015/1060

[5] Explicit Formulas Database. [Online]. Available: http://hyperelliptic.org/EFD/g1p/index.html

[6] D. Bernstein, Ch. Chuengsatiansup, D. Kohel, and T. Lange, "Twisted Hessian curves", Cryptology ePrint Archive, Report 2015/781, 2015 [Online]. Available: https://eprint.iacr.org/2015/781

[7] N. P. Smart, "The Hessian form of an elliptic curve", in *Cryptographic Hardware and Embedded Systems – CHES 2001*, *LNCS*, vol. 2162, pp. 118–125. Springer, 2001 (doi: 10.1007/3-540-44709-1_11).

[8] "Recommended Elliptic Curves For Federal Government Use", National Institute of Standards and Technology, MA, USA, 1999 [Online]. Available: http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf, 1999

[9] S. Galbraith, X. Lin, and M. Scott, "Endomorphisms for faster elliptic curve cryptography on a large class of curves", *J. of Cryptol.*, vol. 24, no. 3, pp. 446–469, 2011.

Michał Wroński received in 2011 his M.Sc. degree in Computer Science from Military University of Technology in Warsaw, where he currently works. His research focuses on optimization of finite fields arithmetic and its hardware applications.

E-mail: michal.wronski@wat.edu.pl
Department of Mathematics and Cryptology
Military University of Technology
Kaliskiego st 2
00-908 Warsaw, Poland

Paper

Curved-Pentagonal Planar Monopole Antenna for UHF Television Broadcast Receiving Antenna

Rudy Yuwono, Endah Budi Purnomowati, and Mohamad Yasir Amri

Department of Electrical Engineering, Faculty of Engineering, University of Brawijaya East Java, Indonesia

Abstract—A planar monopole antenna is an aerial, which the radiating element is perpendicular to the ground plane. It has five equal curvy sides and works at Ultra High Frequency (UHF) band of terrestrial broadcast 478–806 MHz. The curvy sides are made of five equal trimmed ellipses and separated 72° each ellipse to another, form pentagonal shape. Optimizations are obviously necessary to gain the antenna performance at the desired frequency range. The dimensions to optimize this antenna performance are the length of the sides, the offset of curvature, the antenna height from the ground plane, and the ground plane size. Optimization process is done by simulating the proposed antenna with calculated designs using Computer Simulation Technology (CST) Studio Suite 2015 software. The optimized antenna design then fabricated with a 75 Ω coaxial line fed, measured, and results: Voltage Standing Wave Ratio (VSWR) range of 1.05–1.28, antenna gain at 600 MHz is 15.33 dBi, elliptical polarized, and omnidirectional. With these features, this antenna should satisfy the requirements of UHF television broadcasting.

Keywords—planar monopole antenna, television broadcasting, UHF band.

1. Introduction

A planar monopole antenna is a kind of aerial, which has planar element instead of wire. The planar element is located at the distance *h* above the ground plane [1]. This replacement with various shapes of planar element, increases the surface areas of the monopole and has direct impact on bandwidth [2]. Planar monopole antenna has wide range of frequency and yields various applications.

Terrestrial broadcast TV antenna operates in UHF at 478–806 MHz band. Today there are many Yagi-Uda and wire antennas used in such applications.

Planar monopole antennas have several common shapes such as circular, elliptical, square, rectangular, hexagonal, pentagonal, and provide wide impedance bandwidth. The circular monopole [1], [3] and the elliptical monopole [4] were reported maximum bandwidth [3], [5]. Hammound in [5] analyzed that square monopole provides smaller bandwidth but the radiation pattern suffers less degradation within the impedance bandwidth.

Since planar monopole antenna has a wide range of frequency and easy to manufacture by using aluminum as construction the material, it is realizable to build one as terrestrial television broadcast receiving antenna with better shape and design (Fig. 1).

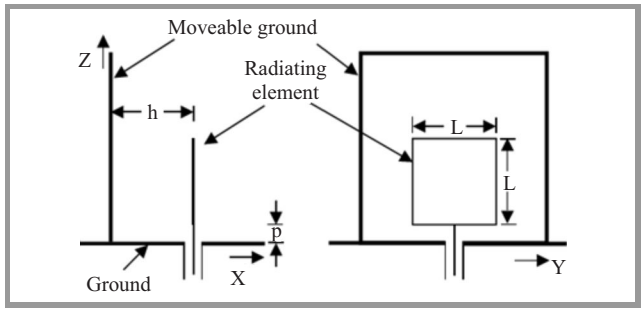


Fig. 1. Parts of planar monopole antenna [1].

Some of the planar monopole features are:

- planar monopole antennas provide wide impedance bandwidth,
- they have multiband operations capability and have omnidirectional radiation pattern [6], [7],
- theirs electrical heights are less than $\lambda/4$ [7]–[10].

2. Antenna Design

The main idea of this antenna type is based on additional curvy edges added to a pentagonal shape. The dimensions of the shapes are adjusted to gain the performance [11], [12]. As mentioned before, the shape of rectangular in planar monopole provides less degradation radiation pattern, while the elliptical shape provides the

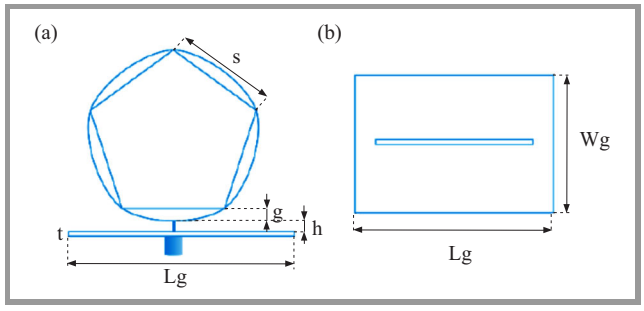


Fig. 2. Antenna design: (a) front view, (b) top view antenna design. (See color pictures online at www.nit.eu/publications/journal-jtit)

maximum bandwidth [13], [14]. Figure 2 shows the basic antenna geometry.

To maintain a standard shape of curvy sides, an ellipse is used as the component of the curvature. The offset is set by configure the ratio of ellipse (Fig. 3).

The side of pentagon is set by trim the ellipse in a distance of y from its center with equation below where s is the length of pentagon's sides, a is the major radius and b is the minor radius of ellipse, where $a = \frac{\lambda}{n-1}$, b is adjusted by the ratio to maintain the desired offset and n is the number of harmonic of lower operating channel frequency, i.e. 478 MHz.

$$y = \frac{b}{2} \cdot \sqrt{1 - \frac{\left(\frac{s}{2}\right)^2}{\left(\frac{a}{2}\right)^2}}. \tag{1}$$

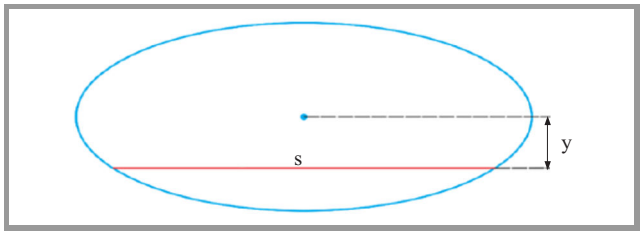


Fig. 3. Trimming position to get the curve and pentagon's side s.

Trimmed ellipse would be duplicated into five shapes and arranged at the distance 72° after each shapes as shown in Fig. 4.

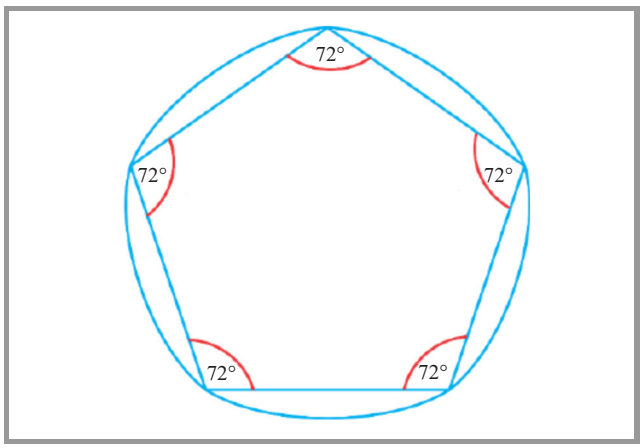


Fig. 4. Trimming position to get the curve and pentagon's side s.

Table 1
Comparison of different variable weight codes properties

Parameter	Description	Value [mm]
t	Base aluminum thickness	2
h	Radiating element distance from ground plane	10
g	Curve offset	0
Lg	Ground plane length	700
Wg	Ground plane width	700
s	Pentagonal side length	628

Initial antenna dimensions' before optimization are listed in Table 1 and are base to approximations for the first s, infinite for ground plane, and for h. After the initial dimensions are defined, then simulation is proceed with CST software.

3. Simulation and Measurement

The simulation process helps to define the best dimensions that yields the best performance antenna by the result of optimizations based on parameters, i.e. VSWR based bandwidth, radiation pattern, polarization, and gain.

Figure 5, shows the VSWR with the variation of s based on Table 1. One can see that $\lambda/5$ antenna is the best in 387 MHz bandwidth.

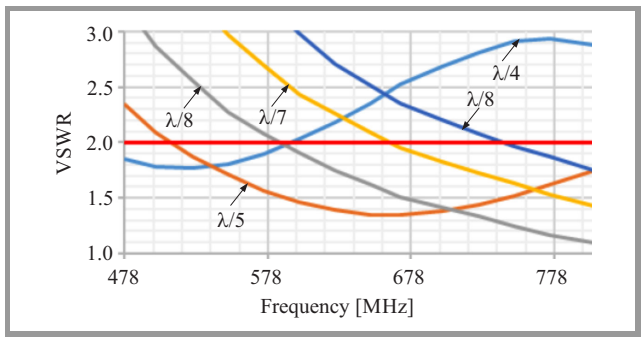


Fig. 5. VSWR vs. frequency on s dimension optimization.

Offset for the curvature from the pentagon's side to the edge of curvature optimizations result can be represent by the Fig. 6. The best performance has antenna with 15 mm offset.

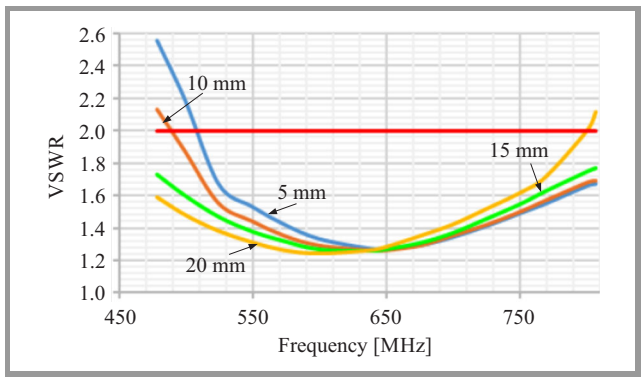


Fig. 6. VSWR vs. frequency on g dimension optimization.

The distance of the radiating element with ground plane does have influence to the performance. The performance slightly increasing when it reached 7 mm on antenna $h = 0.7$ (Fig. 7). The best performance is achieved by antenna $h = 0.8$ which has the lowest VSWR.

To maintain the best performance, the size of ground plane is optimized by adjusting the Lg and Wg (Fig. 2b). The change of ground plane does not influence VSWR perfor-

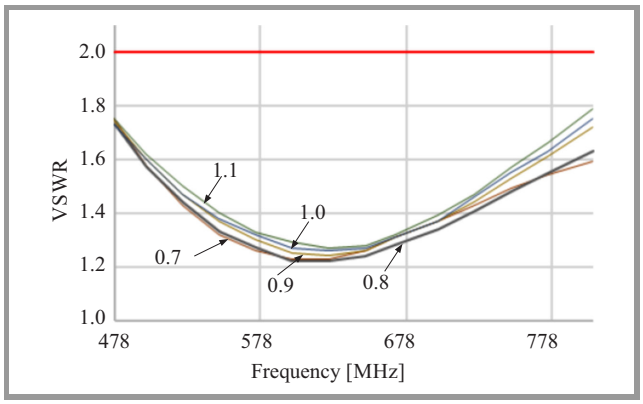


Fig. 7. VSWR vs. frequency on *h* dimension optimization.

mance a lot, yet influence the gain of the antenna. The optimized values are Wg = 8 cm and Lg = 26 cm, which resulted bandwidth of 328 MHz and gain at its middle frequency of 3.45 dBi.
The optimized for best performance dimensions are listed in Table 2.

Table 2
Optimized antenna parameters

Parameter	Description	Value [mm]
t	Base aluminum thickness	2
h	Radiating element distance from ground plane	8
g	Curve offset	15
Lg	Ground plane length	80
Wg	Ground plane width	260
s	Pentagonal side length	125.6

3.1. Measurement Results

The designed antenna was then fabricated and measured in antenna laboratory. The observed parameters were VSWR, radiation pattern, gain, and polarization.
Figure 8 shows the VSWR performance of the antenna. It can work in the entire band and the best performance is 1.02 at the 700 and 750 MHz.

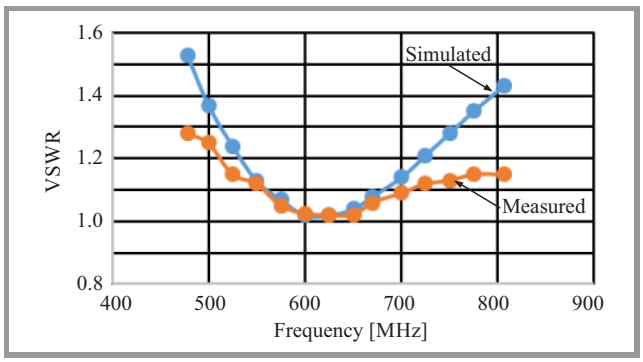


Fig. 8. VSWR within frequency band.

Polar diagram in Fig. 9 shows that the radiation pattern of this antenna is omnidirectional with stronger area at both front and back side.

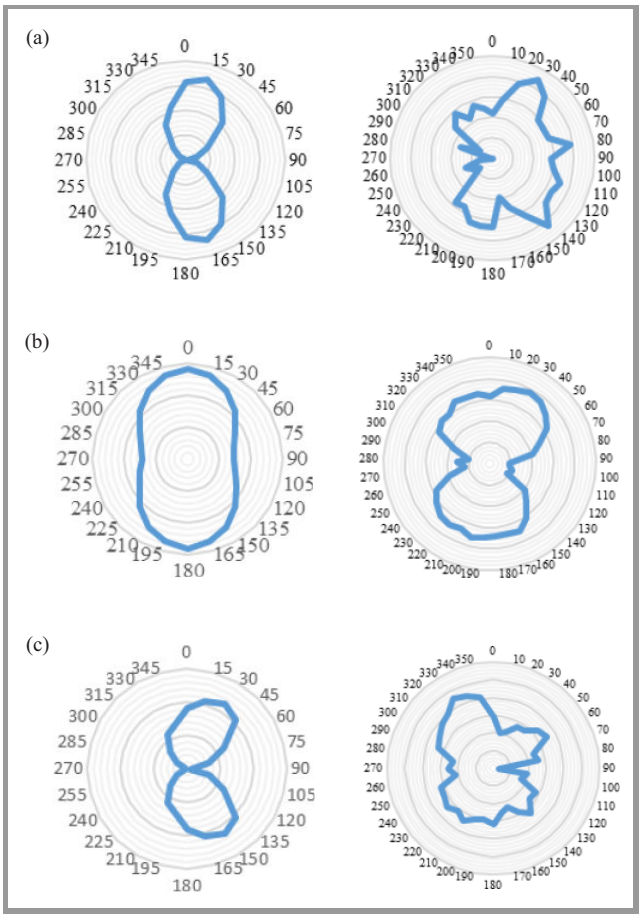


Fig. 9. Simulated (left) and measured (right) result of radiation pattern: (a) sweep φ at $\theta = 90°$, (b) sweep θ at $\varphi = 0°$, (c) sweep θ at $\varphi = 90°$.

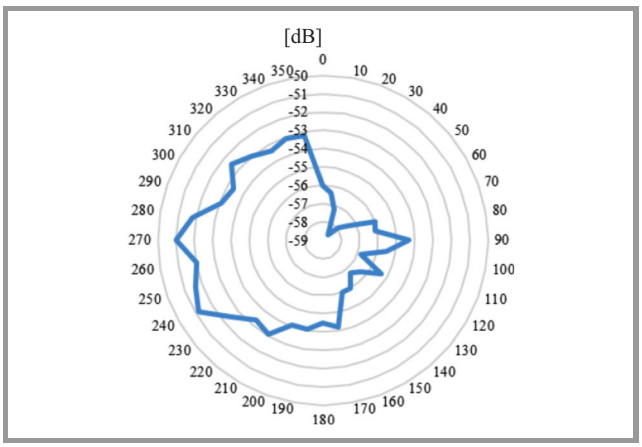


Fig. 10. Polar diagram of the receive level sweep φ at $\theta = 0°$.

The polar diagram of the receive level of the antenna sweep φ at $\theta = 0°$ shown in Fig. 10 that the polarization of the antenna is ellipse. Because it receives the signal poorly on 3–82° and receives better at 81–360°.

Gain measurement (Fig. 11) shows that the antenna has gain average of 3.90 dBi and tend to increase along the higher frequencies.

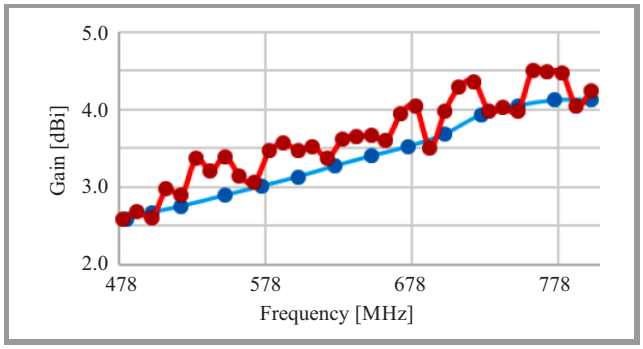


Fig. 11. Gain vs. frequency.

The change of antenna components size influence the performance:

- Wider curve offset *g* yields wider VSWR bandwidth with optimum at 15 mm.
- Shorter distance yields better VSWR bandwidth with optimum at 8 mm.
- Tighter length of sides *s* yields wider bandwidth and shifting to the higher frequency with optimum at 125.6 mm.
- Tighter ground plane Lg yields higher gain with optimum at 80 mm.
- Narrow ground plane Wg yields higher (optimum at 260 mm).

4. Conclusion

The proposed antenna has omnidirectional radiation pattern with almost equally stronger area at front and back, elliptical polarized, VSWR bandwidth of 3:1 worked at 300–900 MHz with average gain of 3.90 dBi. The antenna can be operated as TV broadcast receiver at UHF band (478–806 MHz).

Acknowledgement

This research is supported by Ministry of Research and Technology and Higher Education, the Republic of Indonesia for supporting this research under BOPTN 2015 and BOPTN 2016 batch research scheme.

References

[1] E. Lee, P. S. Hall, and P. Gardner, "Compact wideband planar monopole antenna", *Electron. Lett.*, vol. 35, pp. 2157–2159, 1999.

[2] R. Singh and G. Kumar, "Broadband Planar Monopole Antennas", M.Tech. credit seminar report, Electronic systems group, EE Dept., IIT Bombay, Nov. 2003.

[3] Y. Rudy, A. Baskoro, and A. D. Erfan, "Design of circular patch microstrip antenna for 2.4 GHz RFID applications", in *Future Information Communication Technology and Applications*, H.-K. Jung, J. T. Kim, T. Sahama, C.-H. Yang, Eds. *LNEE*, vol. 235, pp. 21–28. Springer, 2013.

[4] S. Honda, M. Ito, H. Seki, and Y. Jingo, "A disc monopole antenna with 1:8 Impedance bandwidth and omnidirectional radiation pattern", in *Proc. of ISAP'92*, Sapporo, Japan, 1992, pp. 1145–1148.

[5] M. Hammound, P. Poey, and F. Colombel, "Matching the input impedance of a broadband disc monopole", *Electron. Lett.*, vol. 29, pp. 406–407, 1993.

[6] S. Y. Lin, "Multi-band Planar Monopole Antenna for Handset", IEEE, 0-7803-7846-6/03, 2003.

[7] R. Yuwono, R. Syakura, and D. F. Kurniawan, "Design of the Circularly Polarized Microstrip Antenna as RFID Tag for 2.4 GHz of Frequency", *J. Comput. & Theoret. Nanosci.*, vol. 21, no. 1, 2015 (doi: 10.1166/asl.2015.5753).

[8] J. Y. Jan and L. C. Tseng, "Planar Monopole Antennas for 2.45/5.2 GHz Dual-Band Application", IEEE, 0-7803-7846-6/03, 2003.

[9] C. A. Balanis, *Antenna Theory*, 2nd ed. New York: Wiley, 1997.

[10] R. Yuwono and R. Syakura, "2.4 GHz circularly polarized microstrip antenna for RFID application", in *Advanced Computer and Communication Engineering Technology*, H. A. Sulaiman *et al.*, Eds. *LNEE*, vol. 315, pp. 37–42. Springer, 2015 (doi: 10.1007/978-3-319-07674-4_4).

[11] A. Ruengwaree, R. Yuwano, and G. Kompa, "A noble rugby-ball antenna for pulse radiation", in *Proc. Eur. Conf. Wirel. Technol.*, Paris, France, 2005, pp. 455–458 (doi: 10.1109/ECWT.2005.1617755).

[12] K. L. Wong, C. H. Wu, and S. W. Su , "Ultra wide-band square planar metal-plate monopole antenna with trident-shape feeding strip", *IEEE Trans. Antenna & Propag.*, vol. 53, no. 4, pp. 1262–1269, 2005.

[13] R. Yuwono, I. Mujahidin, and A. Mustofa, "Rectifier using UFO microstrip antenna as electromagnetic energy harvester", *Adv. Sci. Lett.*, vol. 21, no. 11, pp. 3439–3443, 2015 (doi: 10.1166/asl.2015.6574).

[14] R. Yuwono and R. Syakura, "Star-L-shaped circularly polarized ultra-wideband microstrip antenna for wireless applications", *Appl. Mechan. & Materials*, vol. 548–549, pp. 776–779, 2014 (doi: 10.4028/www.scientific.net/AMM.548-549.776).

Rudy Yuwono received his B.Sc. from University of Brawijaya, Malang, Indonesia, in 1997 and M.Sc. from University of Kassel, Germany, in 2005. Currently, he is working at Electrical Engineering, University of Brawijaya Malang as Lecturer and Researcher. His research interest are antenna and propagation, microwave and wireless communication.
E-mail: rudy_yuwono@ub.ac.id
Faculty of Engineering
Department of Electrical Engineering
Brawijaya University
MT. Haryono st 167 Malang
East Java, Indonesia

Endah Budi Purnomowati received B.Sc. from ITS, Surabaya Indonesia in 1982 and 1996, respectively. She is with at Electrical Engineering, University of Brawijaya Malang. Her areas of interest is mobile communication. She is a researcher at Telecommunication Laboratory, Electrical Engineering, University of Brawijaya Malang.
E-mail: endah_budi@ub.ac.id
Faculty of Engineering
Department of Electrical Engineering
Brawijaya University
MT. Haryono st 167 Malang
East Java, Indonesia

Mohamad Yasir Amri received his B.Sc. in Electrical Engineering from Brawijaya University, Indonesia, in 2016. From 2012 to 2014 he has been working as a laboratory assistant of Transmission and Microwave Laboratory Brawijaya University. His research and development interests are mostly about antenna design, included analysis, simulation, measurement, and optimizations of antenna design.
E-mail: amrimyw@gmail.com
Faculty of Engineering
Department of Electrical Engineering
Brawijaya University
MT. Haryono st 167 Malang
East Java, Indonesia

Reprint

On Radio-Frequency Spectrum Management

Ryszard Strużak[1], Terje Tjelta[2], and José P. Borrego[3]

[1] *National Institute of Telecommunications (NIT), Wroclaw, Poland*
[2] *Telenor, Fornebu, Norway*
[3] *Spectrum Management Department, ANACOM, Barcarena, Portugal*

Abstract—This article review lessons learned from the uses of radio-frequency (RF) spectrum at national and international scales. Its main purpose is to stimulate debate on how to allow new wireless systems to operate, and to reduce the chronic apparent shortage of RF spectrum. The article aims at a better understanding of the mechanisms behind spectrum management and their pertinence to the public interest. The main contributions if the article are:

- **Considering RF spectrum management as a construct that structures radio services and, at the same time, distributes wealth and power;**
- **Highlighting major doctrines of RF spectrum management;**
- **Promoting spectrum management directly by its users;**
- **Promoting cooperation and transparency.**

The several parts of the paper include the evolution of spectrum exploitation, and a foreseeable future by taking a closer look at major dilemmas and challenges. The paper ends with general comments and conclusions.

1. Introduction

"There is no more spectrum available".

This was stated by Herbert Hoover, the US Secretary of Commerce, in 1925. Since then, the statement has been heard each time a new wireless service has been proposed. That shortage of spectrum has been felt as a factor delaying the social and economic development of society. Various proposals have been put forward to solve the problem, but no satisfactory solution has yet been found. The laws of physics impose absolute limits. Progress in science and engineering bring us closer to these limits, while administrative means impose additional restrictions. The latter result from our choices, more or less deliberate. Better policy and organization could augment the outcome drawn from what is physically possible. For example, for all communications between fixed points, cables could be used instead of unguided radio waves, which would leave radio waves for mobile applications. Satellite networks could similarly take over from terrestrial networks. Better propagation and system models could lead to more efficient spectrum use. Alternatively, we could replace inefficient signal-coding and data-compression technologies with better technologies. The Regional Radio Conference (RRC) on terrestrial broadcasting, held in Geneva in 2004/2006, is a good example. The participating countries decided there to move from analog to digital television by June 2015, which freed a significant part of the electromagnetic spectrum for other uses. According to Martin Cooper, a pioneer of mobile radio, large segments of the radio-frequency spectrum are underutilized due to outdated ideas and practices that are still followed [1]. Other professionals have shared his opinion.

Science and engineering make the spectrum potentially usable, but its real use depends on local legal, regulatory, financial, and also perhaps other factors. Diplomats, lawyers, economists, and engineers gather every few years to review and improve the intergovernmental treaties that regulate the uses of radio waves. Traditionally, when doing that they strictly observe the consensus principle. The consensus requirement assures that the majority cannot impose regulations that would harm any vital interests of a single country. As a consequence, with unbalanced representation the conference results might be biased. That could put some spectrum user groups not represented at the conference in an inconvenient situation, which could last for decades. The nearest such event, the World Radio Conference, will be held in Geneva, Switzerland, from November 2 to 27, 2015 [2]. As at such previous conferences, URSI will certainly participate as an observer, i.e., with no voting rights. However, individual URSI scientists can participate and vote if they are members of national delegations.

The target readers of this review are all of those interested in radio and spectrum management mechanisms who do not actively participate in such activities. Because of this, this paper draws heavily from the authors' earlier publications, lectures, and discussions at spectrum management working groups they chaired in URSI and in other bodies, such as the International Telecommunication Union (ITU). However, the opinions expressed here are the authors' personal opinions.

2. Spectrum Exploitation

This section deals with key ideas and practices inherited from the past. It starts with the genesis of state intervention, national spectrum management, and intergovernmental collaboration. The USA is taken as an example for national management. The mechanism of international regulations

in the framework of the International Telecommunication Union is then briefly reviewed. The role of scientific research is outlined, as is the cooperation with URSI and other organizations.

2.1. Unregulated Commons

Radio is associated with the names of James Clerk Maxwell, Heinrich Hertz, and Alexander Popov. None of these marketed his discovery: they were motivated only by scientific curiosity. The first radio company in the world was the Wireless Telegraph & Signal Company, founded by Guglielmo Marconi in Great Britain, in 1897. It started with wireless telegraphs for navies. Since then, military needs have continued to be the major force behind the technological progress of the wireless sector, the extraordinary success of which continues until today. Marconi marked the birth of a new industry that began transforming the Industrial Society into the future Knowledge Society. We all take part in that process, whether we want to or not, having only minuscule influence on it and a very vague idea of where it will ultimately bring us. The way we use the spectrum can accelerate that process, or can slow it down.

Marconi's company offered equipment and services. The spectrum efficiency of his spark-gap transmitters was very low. Their emissions occupied almost the then entire usable radio spectrum over large geographic areas (e.g., some 250 million square kilometers), yet carried only of the order of single bits every few seconds. The Earth's surface could accommodate only a few such transmissions at a time. To avoid interference, the operators invented the rule of "*listen before transmit*", which has been adapted many years later in some local-area wireless computer networking systems, such as Aloha and Wi-Fi. This latter network, which is presently very popular, is based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards. The radio-frequency spectrum was dealt with as a natural "commons" for free use by everybody, just as the air is used for breathing. *Commons* refers to resources that are not privately owned, and are accessible to all members of society. They can include everything from natural resources and common land to computer software. When commonly held property is transformed into private property, this process is known as "*enclosure*" or "*privatization*".

Marconi patented his wireless telegraph to assure him a monopoly, and to block other companies from developing similar devices and services. However, his monopoly did not last long, and new companies appeared in the market. They all chose to compete instead of cooperating, and the competition was fierce. To strengthen his position, Marconi tried various means. He had a good relationship with the ruling class in Italy, as did his spouse in Great Britain. His opponents accused him of bribery of the highest governmental officials to obtain lucrative governmental contracts. The accusations led to political scandal in Great Britain, known widely as the "Marconi scandal", but Marconi did not lose much. It was the first known corruption case in the radio business.

To force people to use his services and devices, Marconi did order his radio operators to ignore messages sent using the competitors' devices, in spite of the fact that in maritime emergencies, the consequences could be tragic. With no regulations, this was quite normal, and in accordance with the concepts of free competition and the Darwinian doctrine of survival of the fittest. One of Marconi's competitors was Karl Ferdinand Braun (who shared the 1909 Nobel Prize in Physics with Marconi). Braun was associated with the German Telefunken Company.

Defending the company's interests, the German government intervened to break down Marconi's monopoly once and forever. The personal experience of a family member of the German Emperor had an effect: his courtesy radio telegram to the US President was rejected by a Marconi operator simply because it was sent from a German-made device. Certainly, there were numerous similar cases, but none directly touched such high personalities. They initiated the international radio regulatory activities that have continued until now. As a consequence of the incident, a preparatory radio conference was called in Berlin in 1903, just six years after Marconi opened his company. The focus was on the maritime services, interconnections, and financial settlements. Interconnectivity does not happen by itself, since it is not in the incumbent's interest to share the income with competitors.

2.2. First Intergovernmental Agreements

The proposed regulations included two important obligations. The first was to receive and process emergency radio messages, no matter what their origin. The second was to continuously watch for distress signals. These proposals turned out to be impossible to adopt at the conference, and the delegations decided to come back to them at the next conference, at the same place, three years later. The Berlin 1906 conference (1) allocated two frequency bands (around 0.5 MHz and 1 MHz) for public correspondence, (2) founded the International Radiotelegraph Union (IRU), and (3) signed the International Radiotelegraph Convention. By setting the rules on how the electromagnetic spectrum was to be used, the signatories de facto declared its collective ownership. However, other independent nations could join, acquiring the same rights. Specific spectrum uses were to be registered, and the IRU Bern Office recorded the ship stations in operation (known as the "Bern List").

However, an inherent conflict appeared at the conference between private interests and public interests. Marconi succeeded in ensuring that the governments of Great Britain and Italy opposed the convention, in order to defend his company's interests. The regulations had to wait six more years, until the following conference in London. The losses due to the delay have never been evaluated. It was the only case of direct governmental protection of a specific company at radio conferences [3] that the authors have found in official documents. If similar cases happened, they were made outside of the conference rooms.

International treaties are part of a worldwide game that governments agree to play. Consensus is an inevitable ingredient, as there are few things able to force a state. Conference negotiations aim at balancing conflicting interests, and large companies have a strong say there. The Berlin controversies had to wait until the 1912 London conference. The famous Titanic disaster was not without effect on the approval, which happened just three months before the conference, and could have been avoided if an agreement had been in place. This luxury ship sank with some 1500 passengers, after colliding with an iceberg during her maiden voyage. Distress signals were immediately sent by radio, but none of the ships that responded were near enough to reach her before she sank. However, a nearby ship that could assist, the Californian, failed because her radio operator switched his radio off after the daylong watch, and the message did not get through [4]. The Titanic disaster did directly or indirectly touch many very wealthy and influential people of the time. They were shocked by the story, and so was the general public. Numerous books and films have kept the memory of that tragedy alive until today. Certainly, the disaster contributed to the approval of the regulations proposed six years earlier.

To improve the coordination of the uses made of radio spectrum, the IRU was transformed into the present International Telecommunication Union (ITU), without major changes in the basic philosophy and regulations earlier agreed to. The ITU is the UN Agency for Information and Communication Technologies (ICT), with a total membership of over 190 Member States, and some 700 private companies from around the world. It consists of three Sectors: Radiocommunication, Standardization, and Development. The Radiocommunication Sector (ITU-R) coordinates radio-communication services, and the international management of the radio-frequency spectrum and satellite orbits. It also develops common technical standards and recommendations, and maintains Radio Regulations and the Master International Frequency Register (MIFR). The Radio Regulations are a binding international treaty, setting out the allocation of frequency bands for different radio services. They also set technical parameters to be observed by radio stations, and procedures for the notification and international coordination of specific frequencies assigned to the stations by Administrations, as well as other procedures and operational provisions. Radio Regulations are set and modified by consensus of all the Member countries at radio conferences; more details are given below.

2.3. National Spectrum Management

National spectrum management and international treaties regulating spectrum exploitation were born at about the same time. Since the very beginning, they have been closely interrelated: modifications of one of them in turn induce a series of consequential changes in the other. However, while the international use of spectrum requires collective consensus of all Member States, every State is fully sovereign for regulating its national uses, as long as it does not touch other country's interests. Consequently, if a station wants its use of radio frequency to be internationally recognized, it must be recorded in the ITU Master International Frequency Register. The notification process includes verification of whether or not the station's parameters agree with the radio regulations and plans in force. ITU only charges for the nominal cost of work. In 1963, the governments extended the concept of spectrum commons to include artificial satellites. Since then, the orbital parameters and frequencies of satellites have been recorded in the Master International Frequency Register.

In practice, the governments translate the Radio Regulations into their national regulations, and assign portions of the spectrum resources among their subjects. Most have introduced the obligatory national spectrum licensing associated with a spectrum-fee system, in spite of the fact that no country pays for the spectrum. Indeed, the fees can be seen as an extra tax imposed on the spectrum users to feed the governmental budget and development plans in sectors that may be far away from telecommunications. Details may differ from country to country. The license offers rights to exploit a specified band of frequencies under specified conditions and for a specified time, which can be – and most often is – extended over the following years. This makes the license quasi-permanent. In some countries, the license is transferable, which makes it not much different from an ownership certificate. The ways in which the licenses have been issued also differ from country to country, and may change with time. By issuing a license, a government can (and often does) control by whom, how, where, and when the spectrum is used, and for what purpose. This is often criticized: we will come back to that in a later section.

Traditionally, the license is awarded on the basis of seniority (the "first come – first served" rule), in comparative hearings, also called "beauty contests" (this could also be done by lottery). The first approach is the simplest to manage, automate, and control. The second approach is based on merit: a jury representing diverse entities considers all the proposals, compares their relative merits, and grants the license to the most-valued proposal. If the process is open to the public with an elected independent jury, the process is known as a "beauty contest". Otherwise, it is often named the "command and control" approach. This is more complex and more time-consuming than the previous procedure, and the "merits" and "values" are often vaguely defined. However, this is the only way to take into account the social consequences of the licensing decision. Distributing the licenses via lottery has not found supporters. Another approach is privatization or auctioning, discussed in a following section.

2.3.1. The FCC Example

This section deals with the US Federal Communications Commission (FCC), for two reasons. First, the FCC is one of the oldest and most-experienced radio regulatory agencies in the world. Second, a number of countries have drawn heavily from its experience, as did international

spectrum management. World War I accelerated the development of radio technology, and the global center of the radio industry moved to the USA after the war. New services appeared: the service that developed most dynamically was broadcasting. It has proven its usefulness in commerce (advertising) and in politics. It has become a strong force in modern society, often abused to manipulate public opinion. A growing number of transmitters soon resulted in mutual interference, which lowered both the quality of transmissions and profits. In their rivalry for listeners, the operators increased the signal power radiated, which led to a power race, more interference, and more litigation. The era of spectrum plenty ended. A new era of spectrum scarcity began: it was just at that time that Herbert Hoover declared the lack of spectrum, as quoted in the introduction. All those interested agreed that the free market could not solve the problem, and governmental intervention was necessary. In 1926, a special governmental agency, the Federal Radio Commission (FRC), was created to regulate spectrum uses. The FRC was later transformed into the present Federal Communications Commission (FCC), which exists now. It deals with commercial radio, television, wire, satellite, and cable "as the public interest, convenience, or necessity" require.

There are five independent Commissioners of equal power who direct the FCC, which is a rather unique structure: in other agencies, there is typically only one director. Every candidate is proposed by the US President and confirmed by the Congress; the president also nominates the Chair. None of the Commissioners can have a financial interest in any Commission-related business, but each is required to be thoroughly familiar with the radio sector. Only three of them may be members of the same political party. They have to act in a fully transparent manner. Supposedly, the US legislature set all these precautions to assure that FCC decisions are impartial, fair, and free of political or commercial influences. In spite of this, some FCC decisions have been criticized as being biased. Critical voices were also heard when it was disclosed that the FCC Chair nominated in 2013 had earlier worked as a lobbyist for the cable and wireless industry. The FCC alone employs about 1900 persons, and spends some US$350 million per year. These resources are needed to manage commercial applications of the spectrum. They do not cover the governmental spectrum uses that are managed by the National Telecommunication and Information Agency (NTIA). The FCC homepage also lists the Interdepartmental Radio Advisory Committee, which helps to coordinate all activities related to spectrum use in the country [5].

2.4. Spectrum Management Evolution

2.4.1. Global and Regional Spectrum Management

The two Berlin conferences marked the end of the era of unregulated spectrum commons, and the beginning of spectrum regulation. Garrett Hardin, a prominent American ecologist, showed many years later that any *unregulated* commons is unsustainable by its very nature [6]. His famous phrase, the "tragedy of commons", has often been misused in spectrum-related discussions. The spectrum has become the natural public goods (commons) belonging to the whole of humanity, represented by the sovereign governments: parties to the Convention. This was in accordance with the ideas of Henry George, an influential American economist, writer, and politician. George held that people could own and trade what they create, but things found in nature should belong to all. The States have agreed that they are the sole sovereign entities deciding (together) on how the spectrum is to be used. Each state shall have free access to the spectrum. The spectrum shall not be traded, but its uses shall be regulated.

World War I did freeze international cooperation and accelerated the development of radio technology at the same time. The first radio conference after the war was held in Washington, DC, in 1927, just after the FCC was created in the USA. Many famous scientists participated, including Edward V. Appleton, the future laureate of the 1947 Nobel Prize in Physics. The Washington Conference updated the international spectrum-management system. It reviewed the Radio Regulations, defined a number of new radio services, allocated a specific frequency band to each, and extended the regulated frequency range up to 60 MHz. Similarly, World War II again froze the collaboration, and accelerated the development of radio technology. Just after the war, the Allied countries imposed a new international deal, aimed at "lasting international peace, justice, collaboration, and mutual trust". The United Nations organization was created, and the ITU became straightaway its specialized agency. The 1947 conference held in Atlantic City again extended the amount of regulated spectrum, and introduced new allocations.

Among others milestones, the non-telecommunication use of radio-frequency energy was recognized there. Specific radio bands were reserved for industrial, scientific, medical [ISM], and domestic uses. Since then, the power industry developed enormously. Collecting solar power in outer space and transporting it to the Earth's surface using microwaves was proposed decades ago. Wireless powering reappeared in relation to the powering of drones, electric cars, and the Internet of Things. The present tiny ISM frequency bands may be insufficient for such new applications, and additional bands may be necessary. In addition, ISM bands have now successfully been used for new telecommunication systems, such as Wi-Fi and similar systems. New powering systems operating in these bands create a serious potential threat to them.

Technology development continued: the subsequent conferences adapted the regulations to the changing reality. The 1959 radio conference accepted the idea of "passive services". Until then, a service had to transmit radio waves to be qualified as such: those services that only received signals had been outside the purview of the Radio Regulations. For instance, radio astronomy, remote sensing of the Earth, etc., were excluded. The regulations began to differentiate between the *physical use of spectrum*, when a frequency

band and part of space was "filled in" with RF energy, and the *administrative use of spectrum*, when it was reserved for signal reception, or for a future use. The first Conference for Space Communications was held in 1963, just six years after the Soviet Union launched the first artificial satellite around the Earth. This conference extended the ITU-regulated commons over outer space and geostationary satellite orbits. New space services were defined, new spectrum allocations were made, satellite positions were assigned, and Radio Regulations were updated. The Outer Space Treaty entered into force in 1967. It explicitly stated that outer space was "not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means", like the earlier spectrum. In 1992, spectrum allocations for Global Mobile Personal Communications by Satellite (GMPCS) were made. This opened new possibilities, earlier unimagined and not yet explored in full. This also significantly removed the pressure on the terrestrial spectrum, but increased further disproportions existing among the ITU Member States, at the same time. As previously, the electromagnetic spectrum and satellite orbits were collectively managed by all the ITU Member States on behalf of and for the benefit of all the people of the world. Further information can be found in [7] and on the ITU Internet home page.

The radio conferences are practical means for managing the spectrum. They may be worldwide or regional, general or specialized. The general conferences are authorized to deal with virtually all aspects of spectrum use. The specialized conferences deal with particular services and/or particular portions of the spectrum. The regional conferences are held to solve specific spectrum use problems within particular geographic regions. Some Radiocommunication Conferences are convened to negotiate and agree upon international frequency plans for specific applications, geographical regions, and frequency bands, which are subject to a priori planning. They are organized regularly and when needed. The participants in the conferences are official governmental delegations of the ITU Member Countries, each having one voice. The conferences are also open to intergovernmental organizations and the specialized agencies of the United Nations. Nongovernmental entities authorized by their countries are admitted, too (since 1993).

2.4.2. Worldwide and Regional Radio Conferences

Radio Conferences, worldwide and regional, serve as the foundation of global spectrum management in the framework of the ITU. As they all are similar, we here present only one: the Regional Radio Conference (RRC) Geneva 2004/2006, which opened a new era in global management of spectrum for digital broadcasting. It was called to coordinate the deployment of some 70500 transmitting stations in 118 countries. Two conditions were imposed: (1) no more than 448 MHz of spectrum should be used, and (2) the plan should assure the conflict-free operation of the stations, without causing or suffering unacceptable interference as much as practical. The conference was split into two sessions, the first held in 2004 and the second in 2006. The preparations took six years. At the first session, the participating countries agreed upon the principles, technical characteristics, and working methods. Each country defined then its requirements during the intersession period. The requirements were submitted to the second session for iterative adjustments, if necessary. Over 1000 delegates worked hard for five weeks at formal sessions, working groups, and private meetings. The success was possible thanks to the good will and high competence of the participants, as well as the exemplary cooperation between the ITU Secretariat, the European Broadcasting Union (EBU), and the European Organization for Nuclear Research (CERN). The iterative planning was largely automated, based on the software developed by the European Broadcasting Union. Two computer networks were used. One was the ITU's distributed system of some 100 personal computers. The other was the CERN Grid infrastructure, with a few hundred dedicated computers. The outcome was a new treaty replacing the earlier agreements concerning analogue broadcasting plans that existed since 1961 for Europe, and since 1989 for Africa [8]. Figure 1 is a photo of the plan for digital television in the printed version (over 2000 A4 pages), and in the electronically readable version on CD. With this plan, a significant part of the electromagnetic spectrum was made open for other uses, the well-known "Digital Dividend" [9]. Not all countries participated in the conference. Some questioned the spectrum-planning idea in general: see the discussion below for the reasons.

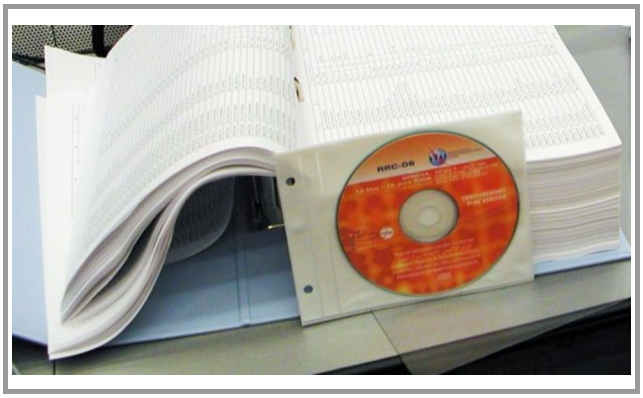


Fig. 1. A photo of the Plan TV GE 06, CD and printed versions (courtesy of the National Institute of Telecommunications, Poland).[1]

2.4.3. Radio Regulations Board

Consecutive ITU radio conferences are usually separated by a period of a few years. If an urgent international problem arises in the time between them, it is the Radio Regulations Board (RRB) that decides what to do until the nearest conference. It is the only ITU body authorized to decide which party is right and which party is wrong, in an objective and fully transparent procedure. During the conferences,

[1]See color pictures online at www.nit.eu/publications/journal-jtit

the board members participate in their advisory capacity. This section describes how the Radio Regulations Board has evolved.

Each Radio Conference makes Radio Regulations more detailed, and more difficult to interpret and to implement. From a few pages in 1906, their volume increased to more than 1000 pages, not counting numerous frequency plans and agreements separately published. Probably the largest changes introduced by a single conference took place at the 1947 Atlantic City conference. To assist the Members in practical implementation of these changes, the conference created the International Frequency Registration Board (IFRB), which years later became the present Radio Regulations Board (RRB). It was modeled after the FCC, discussed in a previous section. The board members are elected by all the Member States at the Plenipotentiary Conference. They have to act independently, and serve as "custodians of an international public trust". They must be "thoroughly qualified by technical training in the field of radio and possessing practical experience in the assignment and utilization of frequencies". Interestingly, such qualifications are only required in regard to the Board members: the other elected ITU officials can be lawyers, managers, etc., with no technical training at all. The board's decisions have been ultimate: only the Member States can change them. In spite of several revisions of the ITU's basic documents, the substance of these provisions has not been changed until now. Traditionally, the board works in full transparency, with the documentation of each case open to all interested ITU Members. However, recently a party requested that its case be considered behind closed doors, referring to its trade secrets, but the board rejected that request.

The board was envisioned "as something of a cross between the Federal Communication Commission and the International Court of Justice" to solve urgent intergovernmental conflicts that appear during the periods between the conferences [10]. In reality, it never achieved any status comparable to the Court of Justice. The major reason was the failure of Member States to allow the board to perform all of its functions as an intergovernmental arbitrator on the frequency uses: it seemingly was not in the best interest of the largest corporations. The 1965 Montreux Plenipotentiary Conference might even have abolished the board completely, had it not been strongly supported by the developing countries, as Codding noted. These countries considered the board as a neutral body, capable of assisting in protecting their interests in conflicts with foreign companies. The board has survived, but its size and importance was reduced, and the pressure of some countries to get rid of it continued. In 1994, the full-time board was replaced by a part-time board and its Secretariat was merged with the CCIR Secretariat into one Radiocommunication Bureau.

2.4.4. CCIR Supporting Studies

The success of the Geneva 2004/2006 conference was possible thanks to earlier careful studies in the European Broadcasting Union and elsewhere. Indeed, it was realized early that negotiations at the Radio Conferences required a lot of background scientific and engineering knowledge. With this in mind, the 1927 Washington conference created a special organ within the ITU, the International Radio Consultative Committee (CCIR) and its Study Groups. The aim was to facilitate the conferences by separating discussions on the well-defined engineering issues from political and economic negotiations. The Member Countries defined questions to be studied (voluntarily), and the results of these studies were submitted to the conference. They were also independently published in the form of the famous CCIR Green Books, Recommendations, Reports, and Handbooks. The CCIR studies significantly contributed to the diffusion of the progress in radio science and engineering.

The spectrum-scarcity problem had to wait until the CCIR General Assembly New Delhi 1970 created the Study Group on Spectrum Management and Monitoring. The assembly elected the first author (R. S.) as its Vice Chair; he served in that function until he became a CCIR official in 1985. CCIR contributed to the development of spectrum engineering, frequency planning, electromagnetic compatibility, and related disciplines. In 1994, CCIR became a part of the ITU-R Sector and ceased to exist as a separate organ, but the Study Groups and working methods have continued until now. Their publications have enjoyed great popularity, as have computer programs [11], [12]. More recently, in parallel with the Study Groups, the ITU has organized a series of open seminars and conferences devoted to specific problems of current interest, e.g., the Kaleidoscope Events. That collaboration proved to be extremely useful, in spite of some limitations discussed below.

2.4.5. URSI Contributions

The CCIR/ITU Study Groups have drawn heavily from the knowledge voluntarily brought by other organizations and individuals. Richard Kirby, the then CCIR Director, noted [13]:

> Even in the earliest days of radio, some of the best scientific minds were challenged by the problem of sharing the radio frequency spectrum among different users.

The International Union of Radio Science (URSI) was one of the first such organizations. The first URSI General Assembly was held in Brussels in July 1922 [14]. URSI was born under the patronage of the Belgian King Leopold II. As the possessor of the Belgian Congo, he was materially interested in having inexpensive communication means with (and within) his colony. At that time, with no satellites, only terrestrial radio could offer such communications, and URSI greatly contributed to progressing radio science and in removing obstacles in the way to global radio services. The second General Assembly of URSI and the ITU radio conference in Washington in 1927 were jointly organized, and URSI took an active part in the creation of the CCIR. Many URSI scientists were involved, contribut-

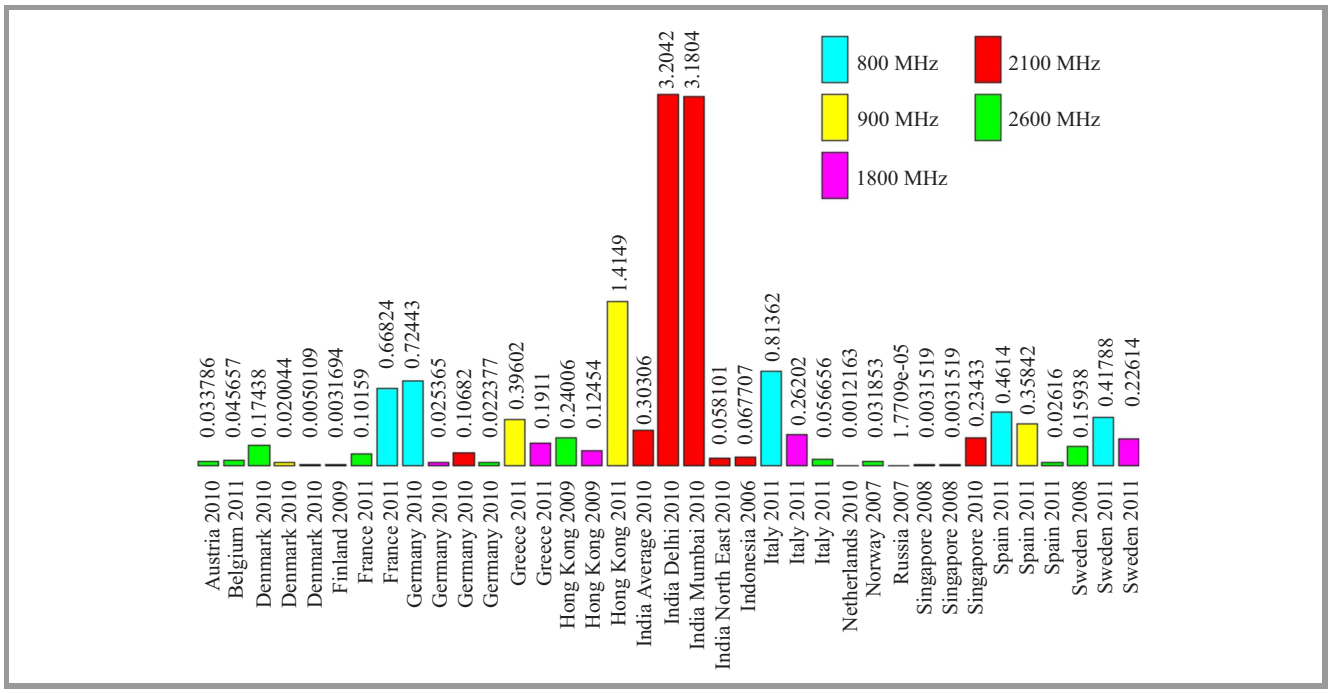


Fig. 2. Auction prices given in Euro/MHz/Population, from [22]. (Note: This is for paired spectrum. The Euro/MHz/Population values were based on historical exchange rates when the different auctions were worked out. When calculating Euro/MHz/Population, the sum of the uplink and downlink bandwidth was taken into account. In auctions where paired/unpaired spectrum was sold in bundles, the amount of paired spectrum was used.).

ing to the development of radio science and its applications, and to strengthening the role of science in intergovernmental agreements. Since then, a number of URSI reports have been approved by CCIR and used by ITU Members without modifications.

The collaboration was most effective when Balthazar Van der Pol, URSI Vice President (1934–1950) and Honorary President (1952–1959), also served as the CCIR Director (1949–1956). The URSI General Assembly in Tel Aviv in 1987, after the CCIR presentation [15], created the Working Group on Spectrum Management in Commission E, with the first author (R. S.) as its first Chair. However, he soon had to withdraw because it "could create potential conflicts" between CCIR and URSI according to ITU legal advisors, as URSI is a non-governmental entity, while CCIR/ITU was an intergovernmental organization. With time, some URSI scientists also lost their initial enthusiasm (except for radio astronomers and remote-sensing specialists), and the group was temporarily inactive. Some wonder if it could be related to changes in the funding mechanism of research projects and in an increased role of big companies, which are more interested in competition and exclusive spectrum use rather than in sharing the spectrum with others. The working group on spectrum was reestablished at the URSI General Assembly in 2005.

2.4.6. Other Contributions

URSI was not alone: numerous scientific and R&D laboratories (governmental and private) from around the world have supported the CCIR/ITU-R Study Groups. Their contributions to spectrum management cannot be overvalued. They are too many to be all listed here. The Institute of Radio Engineers (IRE), established in 1912, is one of the oldest. In 1963, it transformed into the Institute of Electrical and Electronic Engineers (IEEE), the world's largest professional association for the advancement of technology, according to their declaration. Among scientists, it is known not only through its numerous publications and conferences, but also through its Fellow program of professional recognition. The first IEEE Fellow was Jonathan Zenneck, a German physicist famous for his work on radiowave propagation over the Earth's surface in the 1900s. The IRE Professional Group on Communications Systems (PGCS) was organized in 1952. Five years later, the group on Radio Frequency Interference (PGRFI) was created. Later, they became the present IEEE Communication Society (ComSoc) and the IEEE Electromagnetic Compatibility Society (EMC-S), respectively. These are some of the first organizations that called attention to the spectrum-scarcity problems, and have played a major role in shaping spectrum management. Their reports are the definitive works representing the collective wisdom of some of the most distinguished leaders in science and engineering [16]–[18]. Recent IEEE activities in that area are coordinated by the IEEE Dynamic Spectrum Access Networks (DySpAN) Committee, among others. The spectrum-utilization issues were also debated at IEEE sponsored symposia around the globe, e.g., the International Wroclaw Symposia and EMC Zurich Symposia, organized since 1972, currently, the EMC Europe Symposia.

Lots of improvements in spectrum management came as a result of DARPA, MITRE, and NATO projects [19], [20]. In Europe, studies of the European Broadcasting Union (EBU) have been highly valued and often served as the basis for Radio Conferences: this was the case of the Regional Radio Conference Geneva 2004/2006, mentioned earlier. Many saw the UK's Radiocommunication Agency (now OFCOM), with its cooperating R&D university teams, as one of the world leaders in spectrum management and engineering [21]. More recently, the European Commission (EC), with the European Conference of Postal and Telecommunications Administrations (CEPT) and its European Communications Office (ECO), have been successfully working towards improved spectrum use. They have created various groups and committees (e.g., the Radio Spectrum Policy Group, RSPG, and the Radio Spectrum Committee, RSC), and supported specialized symposia and conferences. These studies are in close association with the ITU studies, and most of their results are freely available via the Internet.

2.4.7. National Spectrum Management

Since the nineties, in addition to traditional administrative spectrum licensing, auctions have become a popular national methodology also believed to create incentives for effective utilization of spectrum, as well as revenue for governments. Figure 2 shows the spectrum price (in Euros per MHz per capita) observed at auctions in various countries in the years 2006 to 2011. The amount paid in the auctions was covered in consumer bills, as no company would operate to lose money. It was the highest in India, some three thousand times higher than in the Netherlands: if related to the average income per capita, the difference would be even greater.

2.5. Regulated RF Spectrum

This section is a short summary of the major practical results of common studies and collaborative negotiations within the ITU framework. Historically, the ITU has divided the world into three regions, as shown in Fig. 3, for the purposes of managing the global radio spectrum and in order to avoid harmful interference between systems. Each region has specific allocation plans, by considering regionally harmonized bands, which take into account regional standards and peculiar aspects of the respective markets.

Region 1 comprises Europe, Africa, the Middle East, the former Soviet Union, and Mongolia. Region 2 covers the Americas, Greenland, and some Pacific Islands. Region 3 contains most of non-former-Soviet-Union, Asia, and most of Oceania. The ITU Members have been dealing with the regulated frequency bands as often as they found it useful, according to the above three regions.

Radio Conferences change Radio Regulations, often extending the spectrum limits as shown in Fig. 4. The 2015

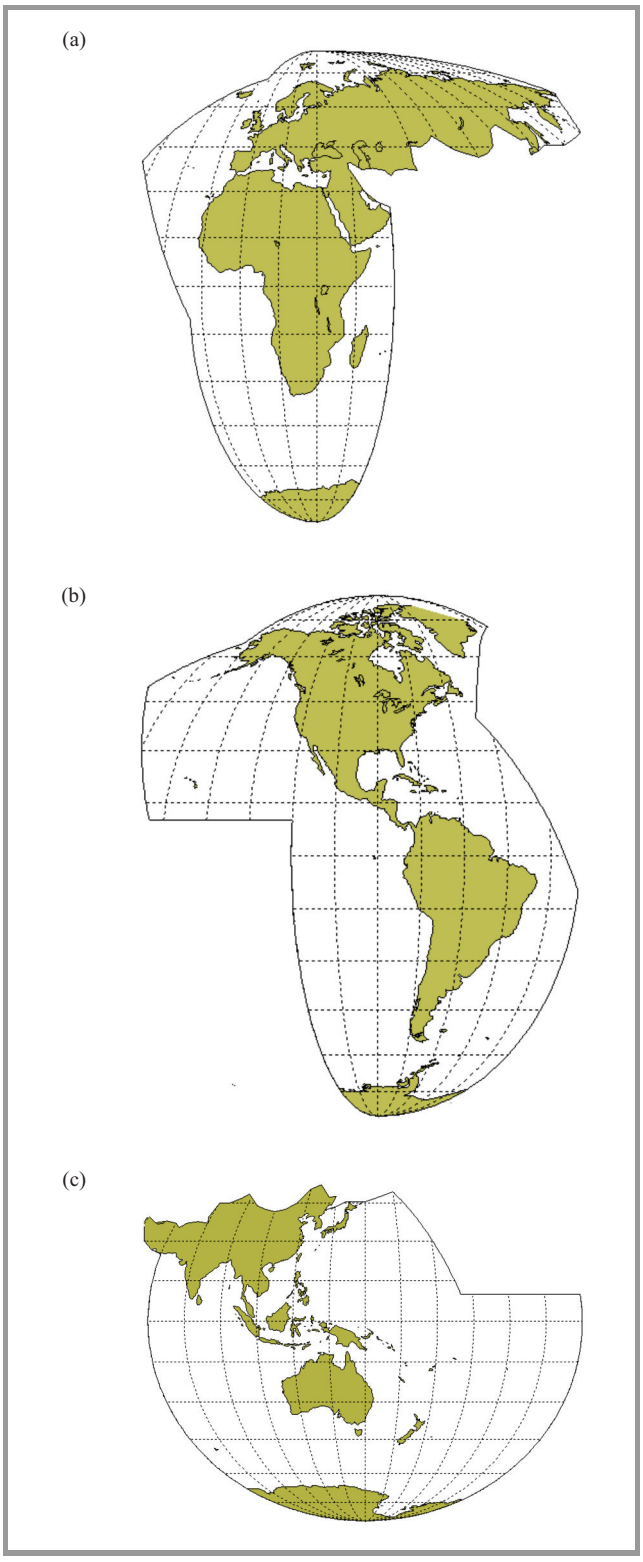


Fig. 3. A map of ITU: (a) Region 1, (b) Region 2, (c) Region 3.

World Radio Conference will discuss possible further extensions.

The total volume of regulated spectrum has been approximately doubling every 30 months or so, as Cooper, quoted earlier, calculated. He added [1]:

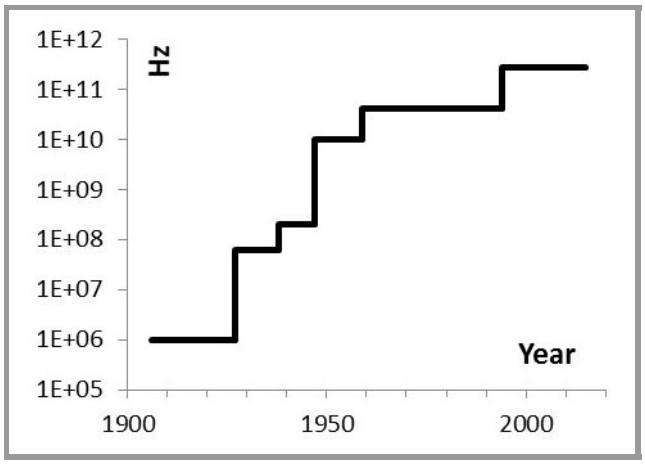


Fig. 4. The maximum frequency allocated in the Radio Regulations by Radio Conferences in the years from 1906 to 2015. (Note: The complete lists of the ITU conferences can be found in [23]).

> Since 1901,... spectral efficiency in telephone communications has improved by a factor of about one trillion. Since 1948, it has improved a million times over. And when introduced in 1983, cellular communications immediately offered a ten-fold increase in spectrum capacity – by transmitting in 30 MHz of spectrum what would have taken 300 MHz to transmit with the previous generation of technology. Today's cellular systems are better than 100 times more efficient than the mobile telephones of the 1980s.

It should be noted here that radiowave propagation effects make some frequency bands unsuitable for specific applications. The total regulated spectrum is divided into small pieces, each allocated to a specific service or use, such as terrestrial, or space services; fixed, or mobile services; industrial, medical, domestic, and scientific applications, generally the same in all Regions. Some details may, however, differ from country to country and from region to region, which obstructs the free movement of devices (e.g., mobile phones) and international exchange. For example, Fig. 5 shows the current national allocations for Portugal.

3. Spectrum-Management Trends

This part focuses on foreseeable perspectives of spectrum management. Radio services [24] have increased in popularity. This has been a steady trend since the radio was first invented. This has also been true of the demand for access to radio frequencies. One traditional way of meeting the demand is to use increasingly higher and not-yet-explored radio frequencies, and to develop more-efficient methods for spectrum utilization. The management of the spectrum of these must also be developed, as described in previous sections. Spectrum management in the future will be a mixture of the current practice of today, with an emphasis on improving efficient spectrum utilization. There are several multidisciplinary factors that play important roles. These comprise the physics of electromagnetic waves and their propagation, technology for spectrum utilization and handling interference, market mechanisms for access to spectrum, and regulatory regimes.

Future spectrum management must take all of these into consideration through a good understanding of physics, technology, and economics in developing the rules for the actors involved. Furthermore, spectrum efficiency must be taken into account, addressing the desired benefit from our collective utilization of the radio spectrum. There is no single metric that can be used in this respect [25]. Technical, economic, and societal judgments therefore apply. In the following, the article is organized in subsections on spectrum management through administrative, trade, and free access to the resources.

3.1. Administrative Assignment

In a way, there must be some administrative rules irrespective of the spectrum-management method used. By assigning exclusive rights to use spectrum at a frequency and in an area, the national spectrum authority gives a user great freedom within the set of constraints that come with the right. No one else can deploy the same spectrum in this area. The rights are often given for many years, to allow sustainable business to be established or continued. Although this describes current spectrum management in many situations, it will most likely continue this way in the foreseeable future for a large part of the spectrum.

Within some services, there is an increasing concern about spectrum scarcity. In particular, mobile data is growing so fast that many operators will be looking for new spectrum resources. Of course, the scarcity also leads to innovation, such that the same amount of spectrum can be used for more traffic and more terminals. Furthermore, many applicants often wish to establish business, and this itself becomes an incentive to make good use of often highly costly access rights. The authorities must look for improved methods of assigning frequency rights. One example is to use graphtheoretic methods in assigning frequency for radio links in popular bands [26], contrasting the usually simplistic methods used today for making assignments. The study indeed indicated a potential for getting noticeably more out of the spectrum, and suggested a closer interdisciplinary collaboration between experts of radiowave propagation and frequency assignments.

Although often all spectrum of interest is already allocated for some service types and even assigned to users, measurements show that only a limited part is utilized at given location and time (see, for example, [27], indicating an overall utilization of 11.2% in Hull, UK, of bands ranging from 180 MHz to 2700 MHz). These types of observa-

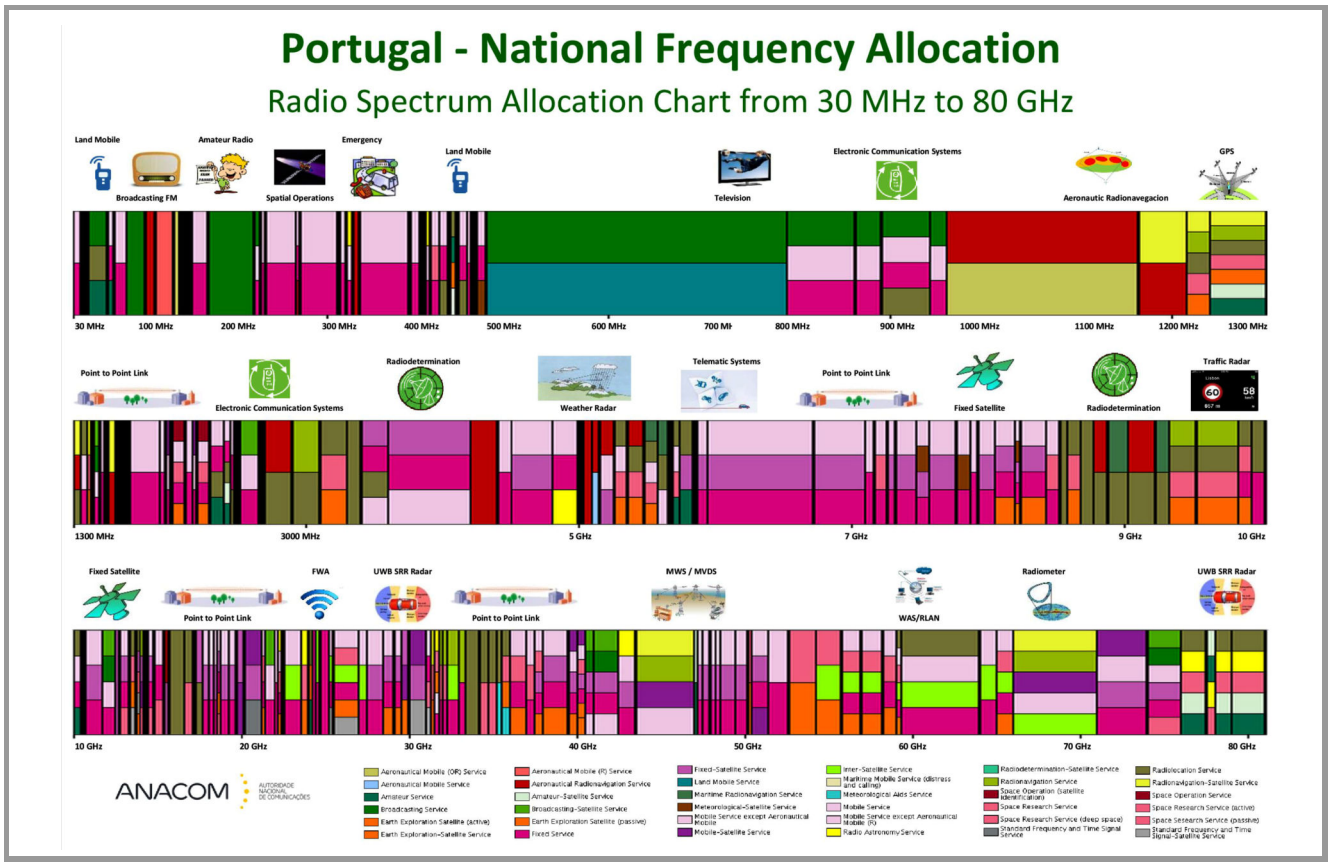


Fig. 5. The national spectrum allocation in Portugal (courtesy of ANACOM).

tions, among other aspects, have motivated the development of cognitive radio equipment that can take advantage of the frequency blocks and time slots when no one else is using them. From the spectrum-management side, this needs development of rules that on the one side motivates equipment vendors to develop suitable technology, and on the other side motivates operators to invest in the technology.

A broad area is dynamic spectrum sharing, as different from traditional long-term spectrum sharing for different services, such a fixed terrestrial and fixed satellite links. There are several methods of shorter-term more-dynamic sharing that have been put forward. At a political level, sharing seems to be pushed believing that this will lead to far better spectrum utilization [28]. It has been suggested that beneficial sharing opportunities be identified in licensed and license-exempt-bands, making sufficient license-exempt band spectrum available for wireless innovation, and defining common paths to sharing based on contractual arrangements.

New spectrum-sharing techniques can be sorted into two groups [29], [30]. One is dynamic spectrum sharing, utilizing parts or "holes" of spectrum with limited spectrum rights. The other is a more-protected form, called authorized shared access, licensed shared access, or priority access. These methods span a gradually decreasing degree of control, from exclusive rights to opportunistic dynamic shared access.

3.2. Spectrum Trading

The economics of spectrum management cover many parts. Some are tightly linked, and are of command and control regimes under an administrative spectrum management regime. At the other end, spectrum access is a free-market item [31]. However, for services such as mobile communications, spectrum is largely treated as property, following on from suggestions by Coase [32]. Spectrum authorities organize auctions for allocation of frequency blocks, rather than other methods such as a contest or lottery.

Spectrum auctions have evolved since they were first used 20 years ago. The goal should be a high degree of spectrum efficiency, and not maximum revenue from the auction, since the first will create greater revenues, in the long run. Cramton suggested a combinatorial clock auction as being much better than a simultaneous ascending auction, and that this will as well enable a technology-neutral approach, if wanted [33].

In free-market-controlled spectrum management, a spectrum-property system must be defined [34], such as the time for utilization, the area where it is valid, and the spectrum identified. These rights must be exchangeable. An example deploying cognitive radio was given for micro-trading of spectrum rights for mobile-service operations in bands on a secondary basis [35], e.g., in broadcast bands utilizing "holes", called "white spaces", opportunistically non-used in the primary-user spectrum.

Game-theoretical approaches have been suggested to effectively take advantage of the shared-spectrum regimes [36]. Intelligence in next-generation networks, with the concept of equilibrium, will enable fair optimum spectrum utilization. These ideas are still in the early phases, and more research is needed.

An idea of a fully free spectrum utilization for any type of network was suggested for the future mobile and wireless system [37]. The marketplace took over and services were delivered by virtual operators. The value chain consisted of the various elements, such as the spectrum, radio access network, value-added services, and so on, with the different actors and not with a single mobile-network operator.

3.3. Free Access

Wireless local area networks (WLANs) in the form of Wi-Fi have become a great success. A significant part of the broadband traffic from a large number of terminals will go over Wi-Fi for at least part of the route. This happens in spite of the fact that radio systems have no guaranties for satisfactory access to the spectrum at 2.4 GHz or 5 GHz. It is therefore not strange that the so-called "commons" spectrum is thought of as a future solution, and more should be allocated for commons. In commons, specific rules apply, and no management is needed. A rule can simply be just to limit the radiated power to a maximum value. However, as such, it is not really free use, as someone has to set the rules and control the regime [38].

A radical suggestion has been proposed to allow anyone to transit anywhere and anytime, as long as the transmission does not cause interference that cannot be dealt with by the other user [39]. The proposal is to create something called "supercommons", where technology manages both wanted and unwanted signals, without other management.

4. Challenges and Dilemmas

The ITU's spectrum management, based on intergovernmental negotiations at radio conferences, has matured since the first meetings in Berlin. Previous sections outlined the way it has evolved and may further evolve. During the century, this has assured the phenomenal progress in all the fields that depend on applications of information and communication technologies, and specifically wireless. The history of radio has proven the ITU radio conferences to be practical: no other field of human activity has noted a comparable rate of progress. The ITU has made it possible to seamlessly communicate around the globe, and to assure the benefits of scale. The mechanism is not ideal, but it has been the only one possible: the only mechanism all the ITU Member Countries could accept. Nevertheless, this mechanism has been criticized by the private sector and by civil society activists, by developed countries and those developing: they all doubt if that mechanism fairly serves all members of society. To complete this review, this part offers a closer look at some of these critical comments, raised by various parties at various occasions.

For instance, a fundamental issue is the difference in the national and international spectrum treatments. Internationally, spectrum is offered for use for free, with no quotas or licenses, and with only basic operational restrictions imposed on its use globally and regionally. However, nationally it offered as a sellable, rentable, or licensable commodity (except for tiny ISM bands that are license-exempted). The idea of spectrum sharing contradicts the concept of exclusive spectrum use. License exempting negates the licensing. Free competition rules out regulations. Dynamic spectrum management goes against spectrum plans, which in turn excludes ad-hoc spectrum allocations. The idea of transparency negates the trade-secret principle.

All of these ideas seem to follow the Cartesian approach, in which a complex problem is broken down into smaller and simpler bits, each for a specific partial problem separately analyzed. Spectrum scarcity is a complex issue. It cannot be fully understood in terms of its individual component parts, disregarding complex interactions among them and with the rest of the surrounding world. Spectrum scarcity involves a combination of engineering, economic, political, and social issues that cannot be separately solved [40]. A holistic approach is needed, treating the problem as a whole within its full context. There is a striking similarity between the radio-frequency spectrum and environmental problems. The concept of a *supernetwork* may be helpful here. Anna Nagurney [41] defined it as a network that is above and beyond classic networks (informational, financial, social, etc.), including complex interactions among them, both visible and hidden. She classified supernetworks as "*system-optimized*" or "*user-optimized*". Equally well, they could be termed "*investor-profit-optimized*" and "*customer-benefit-optimized*".

4.1. Representation

Some private sector representatives note that problems considered at the ITU radio conferences are in reality those of competing companies. Direct negotiations between those interested, without involvement of third parties, would be cheaper, easier, and quicker, and the results would be better for all, they say: governmental interventions distort the competition. On the other hand, some civil society activists accuse governments of representing only the interests of the largest companies. They say such companies have quite different interests from small companies and individuals, which are the weaker parts of society in each country. Similarly, some delegates from developing countries believe their negotiation positions are weaker, and their interests are not taken into account as they should be. At intergovernmental forums, large enterprises lobby national delegations to adopt their views as the country's position. Small companies and citizens usually lack resources to do so. Often, they are unable to even properly formulate, justify, and convey their views, or to predict all the consequences of the proposals just negotiated. This section sums these up.

4.1.1. Developing Regions

The ITU Member States differ in population, wealth, knowledge, and in many other aspects. Similar disparities among regions and social groups exist in each country. They have different potentials, needs, and lobbying powers [42]. Radio-spectrum negotiations imply a lot of difficult work to be done before and during the negotiations. Documents for consideration may include hundreds and thousands of statements, proposals, and counter-proposals, each being a complex mixture of technical and legal issues. Some of them may require an immediate reaction during the meeting, as even a small oversight may have consequences difficult to correct later. Multiple committees and ad-hoc groups at the conference, often working in parallel, create serious problems for small delegations unable to participate in more than one group at a time. The following excerpt from the Bogota Declaration describes problems seen by some delegates [43]:

> The Treaty . . . cannot be considered as a final answer to the problem of the exploration and use of outer space, even less when the international community is questioning all the terms of international law which were elaborated when the developing countries could not count on adequate scientific advice and were thus not able to observe and evaluate the omissions, contradictions and consequences of the proposals which were prepared with great ability by the industrialized powers for their own benefit.

The declaration, published by a group of a few equatorial states that felt they were being misled, voiced the opinion of a larger group of countries that were only partially familiar with the newest achievements of science and technology, and felt to be outside of the closed "club of rich". The consensus idea is great under the assumption of a common interest, common understanding, and good will of all the negotiators. Study Groups, mentioned earlier, aim at reaching that, but unfortunately, not all Members can participate in their studies, for various reasons. With this in mind, conference preparatory meetings were long ago proposed [44], [45], where the future delegates could be familiarized well in advance with problems to be negotiated. That makes the preparations for Radio Conferences almost a continuing occupation, which not all companies or even countries can easily bear. Proposals to facilitate this by wider automation of the ITU [46], which would close it to medium access control (MAC) known from computer technology, are not very popular; automates are still too simplistic now. They cannot completely substitute for humans at the negotiations; moreover, they could make some informal deals and secret agreements difficult, if not impossible.

Wireless technologies eliminate the need for expensive cable networks, and their wide use would reduce the disparity among countries and improve connection with social groups in poor, underdeveloped, or remote regions. Unfortunately, the scarcity of free spectrum is a serious obstacle. The world is now in the midst of a major debate about the public-policy goals. The issue has been discussed at the United Nations, the World Summit on Information Society, the UNESCO-ITU Broadband Commission for Digital Development, and at other forums. They have all set up universal broadband connectivity as an essential element of sustainable development. A series of steps have already been made in order to make these more popular. However, in spite of the progress made, the *digital divide* has not disappeared. Figure 6 shows that it increased from about some 20 percentage points in 2007 up to 70 percentage points in 2014, and that the trend continues.

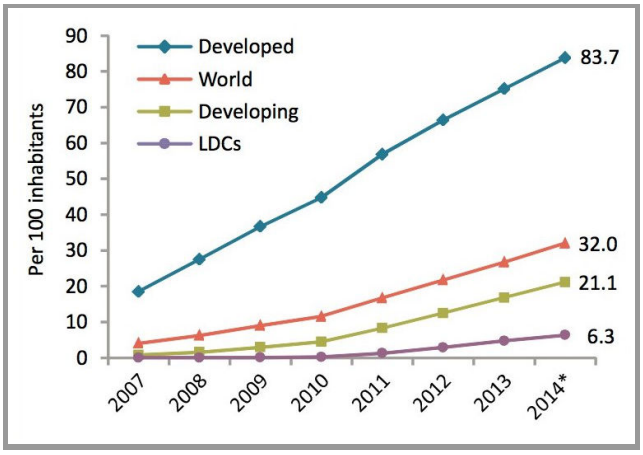


Fig. 6. The active mobile broadband subscriptions by level of development, 2007 to 2014 (* denotes estimate [47]).

Generally, the growth of telecommunication services can be described by logistic functions, which indicate that in some cases the divide cannot be reduced, or could be chaotic [48], [49]. The diverging lines of Figure 6 send a strong message: the goal to eliminate the digital divide is physically unrealizable, or our approach to it is inefficient, and needs a substantial review.

4.1.2. Civil Society

Ideally, a government operates diligently, and represents the interests of all citizens in a just way. Unfortunately, this is not always the case: not every government is seen by all the citizens as trustworthy. To force honesty, civil-society activists demand more transparency. They demand the right to see the documents and negotiations to be sure that there is no difference between what the government publicly declares and what it does behind closed doors, hoping this will limit corruption. In some countries, this has appeared to be impossible, and they do not consent to allowing civil society observers at ITU negotiations. However, recently, under public pressure, the ITU has decided to provide free online access to ITU-R recommendations, and some other documents, to the general public. Providing such access to all input and output documents of all ITU conferences

(postulated since long ago, among others by the first author when he served at the ITU headquarters) was questioned. The argument is that it would cause potential harm to private or public interests, which could outweigh the benefits of accessibility.

Civil society activists also want to bring to the process a variety of views and expertise that relate to ITU activities, such as expansion, development, and adoption of information and communication technologies, sustainable development, access to knowledge, consumer rights, social justice, and human rights. More and more often, one hears from critics that profit-oriented needs dominate those non-profit needs such as health care, education, science, etc., not mentioning the communication costs for ordinary citizens.

4.1.3. Science Interests

Observational radio astronomy explores extremely weak electromagnetic radiations coming from the universe. Space research, remote Earth exploration, and some other sciences do similar exploration. Manmade radiations, no matter whether intentional or spurious, can falsify these observations, or make them useless. Unfortunately, the intensity of manmade radiations increases from year to year. The 1992 UNESCO conference [50] appealed to all intergovernmental organizations to amplify efforts toward protecting the future of such research. One of the ways to do so is to improve the transparency of governmental decisions at all levels, including voting at radio conferences. We mentioned earlier the votes of two delegations at the first Berlin conference, which delayed the solution of communications at high seas until the Titanic disaster. This was the only case the authors found noted in conference documents since the time of Marconi. If there were other such cases, they were outside of the conferences. Unfortunately, bribery has been in the limelight from time to time, and according to Brian Robinson, Chair of the Scientific Committee on Frequency Allocations for Radio Astronomy and Space Science, known by its short designation as IUCAF, the following note was included in his report [51]:

> IUCAF members had to evolve from being starry-eyed astronomers as they encountered a world of politics, lobbying, entertainment, threats, espionage, and bribery. On one occasion, an offer (in Geneva) of two million dollars in cash "to shut up" proved no match for dedication to the joys and excitement of twentieth century astrophysics.

The note mirrors relations existing within some countries, rather than characterizing the ITU radio conferences.

4.2. Spectrum Planning

Plans introduce predictability valued by many: the participants in the TV planning conference in Geneva 2004/2006 considered their plan a great success. Planning is also the only way to reserve a portion of the resource when it cannot be shared after a faster competitor takes it. A position in the geostationary satellite orbit is a good example here, as the total number of such positions is physically limited. However, spectrum planning has been criticized, and this section explains why.

A frequency plan is understood as a table, or generally, a function that assigns appropriate static characteristics to each of the radio stations at hand. Examples are the operating frequency; power radiated; antenna location, height, and radiation pattern; polarization; service area; etc. In frequency plans, specific frequency bands are reserved a priori for particular applications, well in advance of their real use. Individual regions may have various allotment plans for specific services (e.g., broadcasting), within their respective areas.

The plans make a one-time distribution of the spectrum resource on the basis of the expected or declared needs of all interested parties. Critics of the planning approach indicate that it is inflexible and freezes technological progress. Indeed, the progress is very fast, and implementation of the plan may last several years. Technology known at the time of creation of the plan may be obsolete at the time of its implementation. Another difficulty is the impossibility of predicting future requirements with a needed degree of accuracy, and plans based on unrealistic data have no value. Next, radio spectrum is available at no cost at international planning conferences, and there is no mechanism to limit the requirements, except for a general appeal for minimizing its use. There are no accepted or objective criteria for evaluating each country's stated needs, and there are no quotas on the amount of spectrum assigned to each country. In fact, the individual country itself may have no idea of its needs over the time period for which the plan is to be constructed. It is thus not surprising that each country has an incentive to overstate its requirements, rather than underestimate. Under these circumstances, it is easy to make a case that the plans are not only difficult to construct, but when constructed, will lead to a waste of spectrum and orbit, as noted by Glen O. Robinson of the Virginia School of Law, a former FCC Commissioner [18].

4.2.1. Emergency Communications

The 1912 London Conference resolved the problem of emergency communication at high seas, but left open other problems for more than eighty years. In 1995, Hans Zimmermann of the UN Office for the Coordination of Humanitarian Affairs (OCHA) described the issue as follows [52]:

> If anywhere on the ocean a vessel with a crew of one is in distress, all related communications have absolute priority and are free of charge…The necessity for absolute priority of distress signals has been recognized worldwide since the 14 of April 1912, when the "Titanic" hit an iceberg. However when, after earthquake, some 10000 persons are trapped un-

> der the debris of buildings and houses, any customs official can prevent the arriving rescue teams from outside the affected country from entering this country with walkie-talkies. And another official might easily prevent the teams from using their communications equipment, unless they first obtain a license from a national telecommunication authority whose building may just have collapsed in the earthquake. Also, if a team is, by chance, nevertheless able to use its satellite terminal, they are three months later presented with telephone bills for tens of thousands of dollars. Such is the sad experience of those who provide international humanitarian assistance in the age of information super highways.

The problem was known for long and its solution was known too. What was missing has been the willingness to make practical steps, or there were insurmountable differences in the hierarchies of values, or in conflicting interests of large corporations. Many tragic disasters had to happen until, under the pressure of the general public, the governments agreed to remove interstate obstacles to quick deployment of communication means during emergencies. The 1986 Chernobyl Nuclear Power Plant disaster was an example. A long time passed until the Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations was signed in Tampere, in 1998 [53]. Although the convention has removed major legal obstacles, physical and organizational barriers have remained. Emergency communications are still far away from what are needed and what are technically possible, as indicated in the 2000 OCHA evaluation report [54]. To discharge the OCHA duties, the report proposed a global emergency communication infrastructure accessible to all, from any place at any time. The proposed infrastructure would be based on a constellation of low-orbiting satellites, continuously accessible, like the GPS. In spite of the fifteen years that have passed since its publication, no public discussion about its possible implementation even started.

4.3. Monopoly

Monopoly means a lack of economic competition to produce the good or service, a lack of viable substitute goods, and a high profit. In most countries, monopoly is against the law, except for the state monopoly. However, in many countries, a *legal monopoly* is approved by the state if it is justified by the need to provide an incentive to invest in a risky venture, or for other reasons, e.g., to enrich an interest group. Intellectual property rights (IPR), such as copyrights, trademarks, patents, industrial design rights, and trade secrets, are examples of such government-granted monopolies. This section sums up some comments on the topic.

4.3.1. AT&T Example

While the breaking of Marconi's monopoly took a decade or so, AT&T's monopoly (and that of its subsidiaries, the Bell System) operated in the USA for more than a century: from 1875 until 1984. There were six thousand independent (wired) telephone companies in the US serving three million subscribers. However, subscribers to different companies could not call each other because the competing companies refused connections. The AT&T monopoly solved the problem. AT&T was granted the status of a "regulated natural monopoly", obliged to provide *universal, end-to-end integrated, efficient, and inexpensive telecommunication services*. The doctrine of natural monopoly says that regulation is the most appropriate substitute for the competitive marketplace *provided it is independent, intelligent, considerate, thorough, and just*. Due to economies of scale, grouping of like activities in a single company in many cases could assure better and more efficient service to the public than a number of separate mutually competing companies could offer.

AT&T used its unique position and wealth to create the Bell Laboratories in 1925, which became one of the best and largest telecommunication research laboratories in the world. They developed radio astronomy, the transistor, the laser, the charge-coupled device (CCD), the *UNIX* operating system, the *C*, *S*, and *C++* programming languages, information theory, and many other things. Seven Nobel Prizes were awarded for work completed at Bell Laboratories. Being a regulated monopoly, Bell Labs were largely insulated from market pressures. That allowed them to develop a culture that venerated quality and excellence within a noncompetitive framework of innovation and practicability. In 1984, AT&T ended operation as a monopolist, and most of the former Bell Labs have been scaled down, or shut down entirely. The divestiture was not welcomed by everybody, as one can read in the history of AT&T [55]:

> ...the global telecommunications industry entered an era of unprecedented chaos and instability – marked by oversupply, fraud, a complicated regulatory environment and nonstop pricing pressures. Combined, these forces led to an industry meltdown in which numerous bankruptcies, defaults and business failures occurred; investors lost billions and countless workers in the communications sector lost their jobs.

Other critics pointed out fragmentation and repetition of efforts, and a lot of energy and resources lost in mutual fights. Another comment underlined that after the divestiture, no company could create and maintain a research laboratory of comparable scale and quality. The reason was high costs and risk of research confronted with smaller income (due to a divided market) and an uncertain future (due to competition). Some one hundred years after breaking Marconi's monopoly, the OECD stated [56]:

> Limited spectrum and increasing demand for data services mean that mobile networks will strive to offload traffic to fixed networks... The challenge for regulator is that, regardless of the technology used, many parts of the OECD look likely to face monopolies or duopolies for fixed networks. Wireless can provide competition, but spectrum availability will always limit that are not a constraint for fibre.

4.3.2. Intellectual Property Rights

Intellectual property rights (IPR) have two sides. One side is the interest of the owner of the rights. On the other side are the interests of the rest. This helps in protecting a monopoly from competition, with society often paying for it. Consider smartphones, for example. The last few years noted over 140 patent disputes on these alone, with the litigation costs running up to US$3 million per suit. Just two companies, Apple and Samsung, have disputed over US$2 billion in patent-related damage compensations [57]–[59]. Armstrong and his colleagues estimated patent royalties on a hypothetical US$400 smartphone to be in excess of US$120, which almost equals the cost of the device's components. The costs of the disputes may reduce the profitability and incentives to invest and compete. Most patent disputes are sterile, and not in the best interest of society. They absorb time and money that could instead be better used improving the products or lowering their price. Intellectual property rights play an important societal role that largely exceeds the commercial interests of a single company. With the present practices, "only lawyers win in patent wars", as Popelka briefly put it [60].

4.3.3. Spectrum Privatization

Guaranteed exclusivity in the use of a band of spectrum is a form of monopoly. It can be granted through privatization or licensing. The former offers the owner maximum freedom in the use of spectrum. From the access viewpoint, the licensed exclusivity does not differ much from spectrum ownership. The influence of large corporations has been growing, and so has been the pressure to privatize the spectrum and free it from any regulations as much as possible. The ultimate goal is to replace the spectrum commons by private spectrum [61], and licensing by free competition, also known as the *survival-of-the-fittest doctrine*. This doctrine says that the strong should see their wealth and power increase, while the weak should see their wealth and power decrease, disappearing at the end. It implies taking out some form of collective ownership and handing over resources to private owners, if possible. David Bollier, a popular promoter of public interests, compared the private appropriation of collectively owned resources to the movement to enclose common lands in England. The process started there in the XVIth century, and now most of the previously common land belongs to individuals that in total account for less than 0.1% of the population [62]–[64]. Its more recent variant is known as *free-market environmentalism*.

More and more countries grant exclusive licenses to the highest bidders, and open the secondary spectrum markets. Seeking the maximum possible return on the investment dollar is a strong motivating force, but it threatens other important values. Not everybody accepts that a rush for profit should be the only, or the most important, driving force in life. Many prophets and philosophers have long since indicated the negative effects of this. Recently, even major economists noticed this problem [65]. If not restricted by rules of tradition, religion, law, ethics, rational moderation, or by other factors, excessive greed may easily destroy the social order, and lead to crime and wars.

4.3.4. Spectrum Ownership Doctrine

Except for radio waves of natural origin, radio frequencies are inherent characteristics of radio devices: the latter cannot exist or operate without the former. The ownership of a device logically extends over the RF waves radiated or received by it. The spectrum-ownership concept interrupts that connection. Named *flexible spectrum use* by Robert Matheson [66], the concept also ignores electromagnetic interactions and the inherent dynamics of the radio-signal environment. The doctrine is based on two simple rules. One assures the owner's rights: "Transmit within signal power restrictions inside your licensed electro-space region", while the other protects the neighbor's rights: "Keep your signals below 'X' outside that region". This exploits an apparent analogy between land ownership and spectrum ownership over the specific service region. When you own a walled garden, you can arrange the garden at will as long as you remain within the walls. However, with spectrum it is not as simple as it might look at first glance, because it is impossible to determine the "walls" of spectrum property with any precision.

One has to realize that the unguided wave-propagation laws do not allow for any abrupt change of signal power. Simple *borderlines* between the inside and outside at the edge of the service region are physically unrealizable in free space: a finite-sized *buffer region* separates neighboring service regions. That buffer region must be sterile. None of the neighbors can extend his/her radio services there, unless special precautions are applied; careful coordination of geographic distance, signal-power density, frequency, time, or coding might be necessary. Second, the flexible-spectrum-use doctrine is static, and neglects the impact of a changing environment, which can change [67], [68] without the owner's consent or even knowledge.

Without firmly freezing the future signal environment, e.g., through strict spectrum planning, such uncertainties reduce the secondary spectrum marked to nil. That fact calls into question the very concept of private spectrum and its flexible use for active services, not mentioning the more difficult case of the property of frequencies used for passive services. Laws of physics firmly say that in a dense signal environment, no freedom exists in the use of spectrum.

While the idea of privately owned spectrum makes sense in the case of isolated radio systems, it is physically unrealizable where the spectrum is congested. With proper spectrum management, the probability of such interactions is analyzed before issuing the license, and is kept at an acceptable level.

4.4. Spectrum Market

The spectrum market is not a new idea. The thought of selling spectrum rights was put forward for the first time at the 1906 Berlin conference. The Russian delegation suggested a kind of transit fees for radio waves propagating over the country's territory. Some fifty years later, in 1959 Ronald Coase of the FCC suggested property rights and spectrum market as a more efficient method of allocating the spectrum to users. (He was the laureate of the 1991 Nobel Prize in Economic Sciences, for his work on transaction costs and property rights). Then Equatorial countries, in their *Bogota Declaration*, mentioned earlier, claimed that the satellites located above their territories should pay a kind of *parking fee*. In 1995, Richard Butler, then the ITU Secretary General, put forward that positions of orbiting satellites be traded, and the income be used to finance the activities of the ITU. He did that when some ITU Member States failed to pay their contributions: with no cash, he would have been forced to close operations and fire the staff. The Member States rather preferred to pay the contributions than to rent orbital positions or shut down the ITU. None of the privatization ideas have been accepted until now at the international forum. The majority of ITU Member States firmly supported the commons character of the radio spectrum and satellite orbits.

Spectrum auctioning has been practiced in a number of countries. For governments, it has become attractive because it solves the access rights to spectrum in cases where too many are interested, and also provides money inflow to the budget. However, the FCC Commissioners, like many other experts, long opposed the idea of a spectrum market, so it had to wait some thirty years for its first implementation. Interestingly, it did happen in New Zealand and not in the USA, as one could expect. New Zealand introduced spectrum auctions for tradable leases up to 20 years in 1989. However, many are against spectrum auctions. Earl Holliman, the US Army Spectrum Manager, wrote:

> We hear a lot about auctions. The auction approach does not stimulate technology towards more efficient frequency uses. It lets a successful bidder only get richer and pushes the smaller operator back.

For companies, auctions involve large uncertainties and high risks: the expected and needed profits for planned operations might never come true. For customers, they may mean an increase in the price of services. Huge amounts have been paid for frequency bands that were never used [69], [70]. Some auctions are seemingly used to block competitors rather than to put the spectrum into use. Auctions have been claimed to be corruption-immune, but several scandals have shown the opposite. The 2010 spectrum scam in India, quoted earlier, was an example.

Some economists do not believe in the efficiency of the free market. For instance, Joseph Stiglitz, the laureate of the 2001 Nobel Prize in Economic Sciences, says it is only under exceptional circumstances the markets can be efficient. He wrote [71]:

> For more than 20 years, economists were enthralled by so-called 'rational expectations' models which assumed that all participants have the same (if not perfect) information and act perfectly rationally, that markets are perfectly efficient, that unemployment never exists… and where there is never any credit rationing. That such models prevailed, especially in America's graduate schools, despite evidence to the contrary, bears testimony to a triumph of ideology over science. Unfortunately, students of these graduate programmes now act as policymakers in many countries, and are trying to implement programmes based on the ideas that have come to be called market fundamentalism.

Numerous other authors are of similar opinions, such as, e.g., Eli M. Noam, Samuel A. Simon, Joseph H. Weber, and Yohai Benkler. Most surprisingly, George Soros, a famous billionaire, joined other critics, writing [72]:

> Although I have made a fortune in the financial markets, I now fear that the untrammeled intensification of laissez-faire capitalism and the spread of market values into all areas of life is endangering our open and democratic society.

The UN has called a special summit to consider, among other problems, the "Fundamental Defects of the Free Market System" [73]. The 2011 Washington Declaration on intellectual property and the public interest clearly stated [74]:

> Markets alone cannot be relied upon to achieve a just allocation of information goods – that is, one that promotes the full range of human values at stake in intellectual property systems. This is clear, for example, from recent experiences in the areas of public health and education, where intellectual property has complicated progress toward meeting these basic public needs.

This would indicate that practices protecting intellectual property rights should be seen from a wider socio-economic viewpoint, taking into account society as a whole: not only those who benefit now, but also those who pay or loose in a longer perspective.

Many worry that privatization, if widely introduced, would be incapable of assuring balanced sustainable socio-economic development; that government and corporate

surveillance would increase without limits; that the free flow of content we are now proud of would stop; and that intellectual property rights would extend into the interminable past. The uncertainty results from our dilemmas on the hierarchy of values. Erich Fromm, a German philosopher, put it briefly: "to have, or to be?" – a basic question to which everybody has their own answer. Spectrum trading also offers opportunities to the benefit of both operators and the society served, when spectrum can be more effectively utilized in an area or a market.

4.4.1. Competition

In the opinion of many experts, the progress in mobile and broadband communications, and generally in the radio applications we enjoy today, would not have developed at the pace we have seen if there were no competition. It may not be so easy to prove generally, but for many, the cost of communication services has not increased in the latest decades. Rather, the opposite has occurred relative to daily spending for living, and such services have become much more affordable [75]. Furthermore, information and communication technology services have become much more important, highly beneficial, and even absolute necessary for a well-functioning society.

However, other cases show that competition may not serve society well, as illustrated by the following example. When serving in the ITU headquarters, the first author organized the CCIR library of spectrum-management software freely offered by ITU Members. The software could be copied and used at no cost by all those interested. This was functioning well, but a problem appeared when the program for practical planning of low-power (local) TV stations was offered [76]. It was then one of few programs using digital terrain models and inexpensive personal computers. It generated great interest among small and medium enterprises, in both developed and developing countries. Its user interface was in Polish, and it was proposed to translate it into English and other ITU official languages, which would make it more useful in many countries. However, a few delegates representing private business were against this, arguing that "it would kill our business". As no required consensus was reached, the proposal was not approved. In addition, as a consequence, there is no such free software provided by ITU today.

With the consensus rule, a single company can easily block other enterprises, but opposite cases also happened. For instance, one can learn from the FCC home page that Edwin Armstrong, an American inventor, proposed his frequency-modulation system in 1935. However, companies in the United States, afraid that it would reduce their profits, blocked it for some twenty-five years, until the 1960s. Similarly, for more than a decade, civilian applications of spread-spectrum technology were blocked. More recently, the promising low-Earth orbit (LEO) [77] and high-altitude platform (HAP) [78] technologies were blocked. The majority blamed the general crisis for that, but some suspected the competing companies of significantly contributing to that. More recently, the FCC stated that it had to protect consumers from mobile-broadband providers' commercial practices masquerading as "reasonable network management". Working hand in hand with citizens, the FCC is setting "strong rules that protect consumers from past and future tactics that threaten the Open Internet" and promote "more broadband, better broadband, and open broadband networks". The providers hold all the tools necessary to deceive consumers, degrade content, or disfavor the content that they don't like. Some companies make practical use of these tools, keeping third-party applications within a carrier-controlled "walled garden", as in the early days of electrical communications. That practice ended when the Internet protocol (IP) created the opportunity to leap the wall, but the FCC has continued to hear concerns about other broadband-provider practices involving blocking or degrading third-party applications.

4.5. Spectrum Sharing

Privatization pressure provoked countermovement and the revival of interest in spectrum commons and cooperatives. One of the most respected researchers in that area was Elinor Ostrom, a US economist and the only woman who won the Nobel Prize in Economic Sciences (in 2009), for "her analysis of economic governance, especially the commons". Her studies have indicated that the commons are sustainable if they are well managed, best done by their owners, themselves. Interestingly, that principle has intuitively been practiced on the global scale by ITU Members since 1906, well before Ostrom's studies. More recently, the principle was extended over the users of Wi-Fi and similar technologies, which became the most popular use of spectrum commons. For instance, in 2013, more Internet traffic was carried over Wi-Fi than via any other path, resulting in some US$222 billion in value added to the US economy alone [79]. That evidences the practicality of spectrum sharing and the numerous benefits in comparison with the exclusive (private or licensed) spectrum, including lower access cost. Note that there has always been a part of the wealth kept in common, examples being public roads and parks. Since the very beginning, spectrum access has been free for each and any government: what many civil society activists expect is an extension of that practice over individual spectrum users, without any governmental brokerage.

The US President's Council of Advisors on Science and Technology (PCAST) suggested a three-tier "dynamic sharing" Spectrum Access System (SAS), making spectrum sharing the norm. Under the Spectrum Access System, Federal primary systems would receive the highest priority and protection from harmful interference. Secondary licensees would register deployments and receive some quality-of-service protections, possibly in exchange for fees. General Authorized-Access users would be allowed opportunistic access to unoccupied spectrum (when no Primary or Secondary Access users were using a given frequency band in a specific geographical area or time period) [80]. The

National Telecommunication and Information Agency has already identified a total of 960 MHz of federal spectrum as candidates for sharing using that approach. The European Commission is considering similar sharing possibilities, based on contracts between the users. This is seen as a natural extension of the previous spectrum policies: licensed access allowing operators to offer a predicted quality of service, and license-exempt access fostering widespread contributions to innovation and fast-paced investment in emerging technologies [81]. However, incumbent commercial or government users may be reluctant to give up their exclusive rights to individual spectrum bands, concerned about already made or planned long-term investments in communication networks, including access to spectrum. And yet, technology is being developed and deployed to allow for such sharing by new entrants without risking interference to the incumbents' systems. A number of countries have pursued regulations or trials that enable license-exempt, Wi-Fi-like devices to access vacant spectrum in the television broadcast bands ("white spaces"). These are expected to improve Internet access, facilitate the delivery of government services, establish communication channels in the wake of earthquakes, typhoons, etc.

4.6. Other Issues

Since the very beginning, scientists have worked on issues that have extended our knowledge about the universe, and made our lives easier, safer, and richer. There is a wealth of literature on the benefits radio waves have brought to humanity. However, that progress has also brought negative effects. The perception of electromagnetic waves has been changing. From an abstract concept, it morphed to a tradable commodity, and from a scientific curiosity, to an apparatus of indoctrination, a weapon in physical conflicts, and a tool for criminals. In addition to the unknown long-term biological side effects of man-generated electromagnetic waves, there are also other sources of worry. Like health, they only indirectly relate to spectrum use. Discussing them in detail clearly exceeds the scope of this article, so we only mention some here, which we believe are needed to better understand the role and complexity of spectrum management.

4.6.1. Orbital Debris

Since 1957, after the launch of the first Earth-orbiting artificial satellite, the near-Earth environment has served as a gigantic rubbish collector. Orbital debris (also called space debris) is a collection of man-made objects launched into space and left there with no purpose after their mission ended. They are dead satellites and their fragments, upper stages of rockets and their fragments, and other abandoned objects. The total number of these objects is counted in the millions of pieces. It increases with every new launch of a space object and with each new satellite explosion, and with accidental fragmentation or due to anti-satellite tests in outer space. These objects are all orbiting with hyper velocities of a few to dozens of kilometers per second, and can damage operating satellites and space vehicles. For comparison, the velocity of a bullet fired from the famous AK 101 Kalashnikov rifle is less that one kilometer per second. The threat of impact damage is a growing concern. Medium-size objects (0.1 cm to 10 cm in diameter) are the greatest challenge, because they are not easily tracked, and have a kinetic energy high enough to cause catastrophic damage. For instance, a particle with a mass of 10 g moving 10 km/s has a kinetic energy comparable to a one-ton car running on a highway at a speed of 100 km/h. Penetration of even a small particle through a critical component, such as a flight computer or propellant tank, can result in loss of a spacecraft. If a 10 cm object of 1 kg mass collided with a typical spacecraft bus, over one million fragments of 1 mm in size and larger could be created, according to NASA. Such a collision would result in the formation of a debris cloud, which poses a magnified impact risk to any other spacecraft in the orbital vicinity. Mutual collisions can further multiply the numbers. Encounters with clouds of smaller particles can also be devastating for future missions. For instance, the solar panels of the Hubble Space Telescope (launched in 1990 and remaining in operation) have been replaced several times because of damage caused by tiny objects. Such objects may also efficiently block scientific observations of some regions in the sky.

A few countries do radar, optical, and infrared surveillance of space for security reasons. The smallest traceable objects are about 10 cm in diameter at low altitudes, and about 1 m in diameter at geostationary orbit. Some space debris could escape towards other celestial bodies, burn in the atmosphere, or fall on the Earth. However, to do so their velocity must change. What slows them and forces them to fall down is air drag, but this decreases with altitude. At high altitudes, it is negligible, which implies a long time for orbiting in space. Table 1 lists the expected orbital lifetimes for selected circular orbits.

Table 1
The lifetimes of circular orbits [82]

Orbital Altitude [km]	Lifetime
200	1–4 days
600	25–30 years
1000	2000 years
2000	20 000 years
36 000 (GSO)	Indefinite

At geostationary (GSO) altitude, no effective natural removal mechanism exists, except for solar-radiation pressure. From a practical standpoint, objects located in geostationary orbit would indefinitely remain in that vicinity, if not moved at the end of a mission. Orbital debris is a good illustration of the CC-PP (communize costs – privatize profits) behavior of satellite companies first described by Hardin, mentioned earlier. Some of the ob-

jects launched are sent back to the Earth, especially after the invention of re-useable space vehicles, but the creation rate of debris has outpaced the removal rate. Maintaining the current design and operational practices could ultimately render some regions in space useless, and even dangerous.

4.6.2. Issues to Watch

The future of radio applications may not be as wonderful as it could be, and as most people would like it to be. Technological progress is often driven by military programs that aim at improving ways enemies are destroyed, or allies are protected. However, many byproducts of these programs find later civilian applications, making our life easier, healthier, and pleasanter. Unfortunately, a military invention might also become accessible to criminals, or a government might use it against their own citizens: the latter practice ends often in a government overthrow or revolution.

4.6.2.1. Propaganda

Radio as a wartime propaganda tool become popular during World War II (it later was supplemented by television). Wireless can bring all the persuasive power to millions of people at relatively low cost, ignoring national borders and front lines. However, its power was demonstrated earlier, in 1938, in the USA, after the airing of *The War of the Worlds*, an innocent episode of a radio drama series. Orson Wells presented it so realistically that the radio transmission was taken as real news, and caused mass panic, difficult to manage. Since then, radio and television have become major advertising means. However, they also serve as efficient *propaganda* and *brainwashing* tools in political/ideological campaigns. More recently, mobile phones, SMS (short messaging service) and online social-networking services such as *Twitter* and *Facebook* have similarly affected the social lives and activities of people, starting from the election campaigns in the USA to social protests such as Occupy Wall Street or the Arab Spring of 2010. The unprecedented ease and scale of wirelessly manipulating public opinion worries many. The Arab Spring protests transformed into revolutions that overthrew a few governments. It explains why so many other governments want to control the access to radio waves and to the information they carry.

4.6.2.2. Espionage, Cyber Attacks, and Jamming

The fear of war, criminal acts, or losing power pushes governments not only to license access to spectrum, but to also develop intelligence, eavesdropping, and surveillance, which is relatively easy in the case of wireless communications. However, these may also be used against the citizens' right to privacy. Some years ago, the European Parliament initiated an investigation into the ECHELON system [83], created to monitor the military and diplomatic communications of the Soviet Union and its allies during the Cold War. With time, it had evolved, allegedly becoming a global system for the interception of any communications over the globe, including private and commercial communications. Another worrying issue is massive surveying of people. According to the press, there is one surveillance camera for every eleven people in Great Britain. An even more worrying issue is the use of radio waves for criminal attacks and secret wars in cyberspace [84]. Real data from that area are rarely published, but the scale of the issue can be judged from the expenses incurred. According to the press, the defense cyberspace budget for 2015 includes US$5 billion in the USA alone; other countries may spend proportionally.

Jamming was widely used during World War II and the Cold War. Later, unintended interference was often noted. For instance, deliberate jamming of telecommunications satellites was observed and increased between 2009 and 2012. In several circumstances, France raised this issue to the Radio Regulations Board. Several European countries also submitted a proposal to WRC-12 on this issue, which led to an evolution of the Radio Regulations that gave more weight to the issue of deliberate interference.

4.6.3. Power from Space

New, cheap, and environmentally friendly energy sources are now sought in several countries. The world's population is expected to reach 10 billion people by the year 2050, and the present energy sources will be insufficient to satisfy their needs, according to current projections. Among various ideas, the space solar power (SSP) concept has been studied. In 2007, URSI published a comprehensive report on the topic [85]. Among additional possible solar-power satellite (SPS) applications, the report listed sending energy from spacecraft to spacecraft, bringing energy to remote areas on the globe that are difficult to otherwise access, or providing energy to the dark side of the moon. The report stressed that URSI did not unanimously advocate solar-power satellites. Within URSI, there are both advocates of solar-power satellites, and voices of concern and severe reservation.

The solar-power satellite studies started in the USA, during the oil crisis of the seventies, aimed at limiting the dependence of the national economy on foreign oil. In 1974, a patent was granted for a solar power satellite to collect power from the sun in space, and then transmit it down using a microwave beam to the Earth for use. One of the more recent solar-power satellite systems considered huge ($\sim$10 km^2) arrays of photovoltaic cells placed in an Earth orbit, or on the moon to convert the sunlight into electricity. Such arrays would be unaffected by cloud cover, atmospheric dust, or by the Earth's twelve-hour day-night cycle. To reduce the necessary area of costly solar arrays, sunlight could be additionally concentrated using giant mirrors. The incident solar radiation would be converted into electricity using the photovoltaic process. Another part that would manifest itself as heat could also be converted into elec-

tricity using thermoelectric devices. These would serve as thermal pumps, removing heat from the photovoltaic panels and lowering their temperature.

The electricity would then be converted to microwaves, and beamed by a composite space antenna ($\sim$6 km^2) towards a huge Earth antenna ($\sim$12 km^2). The space antenna would assure a pointing accuracy of about 0.0005°, which would mean about a $\sim$300 m pointing error on the Earth's surface. The terrestrial antenna would contain a large number of receiving antennas combined with rectifiers and filters (called a rectenna), which would convert the microwave power into electrical current, injected into the power network. To limit the health danger, the receiving antenna would be located in the desert, or in mountains far away from densely populated areas. The size of the microwave beam could be large enough to keep the power density within safe limits.

A space solar-power system using today's technology could generate energy at a higher cost than the current market price. One estimate was that it would take 15 to 25 years of further research to overcome that difference. In 2001, Japan announced that they plan to launch a giant solar-power station by 2040. Preparatory studies are also being undertaken in the European Union and in the United States. There are many questions to be solved. For instance, the URSI report quoted earlier lists the following:

> What is the impact of SPS electromagnetic emissions – both intended and unwanted (harmonics of the microwave frequency, unexpected and harmful radiation resulting from malfunctions) at microwave frequencies and other related frequencies – on telecommunications, remote sensing, navigation satellite systems, and radio-astronomical observations? What actions can be taken to suppress this unwanted emission? Constraints imposed by the Radio Regulations of the International Telecommunication Union must be taken into account.

However, more important questions remain to be solved before solar-power satellites could operate, e.g., health and environmental problems not yet solved. Others have indicated that it is potentially a double application technology: a solar-power satellite station could easily be converted into a dangerous weapon. Space weapons using solar energy are not a new idea. In World War II, some German scientists were speculating on the use of gigantic mirrors that could concentrate solar energy to set fire to an enemy's cities, manufacturing, crop fields, etc., during wartime. High-power microwave beams could cause similar damage. Between the wars, the solar-power satellite mirrors could be used to control local weather conditions over a selected region. The size, complexity, environmental hazards, and cost of a space solar power undertaking are daunting challenges.

5. Concluding Remarks

This paper has reviewed basic issues of radiofrequency spectrum use. It has shown how deeply our current concepts are rooted in the past, and how often they are dictated by the short-term benefits of the few. It has summarized arguments and lessons learned since the invention of radio, which could be usable in current debates on how to reduce the chronic apparent shortage of RF spectrum. It has highlighted major doctrines focusing on a better understanding of how the spectrum-management mechanisms are associated with the public interest and distribution of information, knowledge, wealth, and power. It pointed up similarities between spectrum conservation and environmental protection. The paper is intended to promote cooperation, transparency, and direct involvement of spectrum users into its management process. It focused on issues that could be improved through good will, negotiations, and consensus without in principle requiring extra resources.

The fundamental question of whether it is better to privatize the spectrum or to keep it as a regulated commons, to sell it, or to distribute it freely, will probably be open for decades. Many have hoped for a long time that science and engineering will solve the spectrum-scarcity problem. Science and engineering are universal – independent of nationality, ideological convictions, or political orientation – which makes joint efforts much easier than in any other field. However, history shows the opposite: spectrum scarcity increases with the progress made in science and engineering. Many have anticipated such an approach to spectrum management could be as useful as it has been found to be in the military. However, negotiations and lobbying will probably continue as the basis for spectrum management for a long time. Human motivations and ways of thinking have not changed much since the invention of radio, and most probably will not change in the foreseeable future, shaping spectrum use. The reason is that society is not uniform. It is composed of groups, each having different world views, interests, needs, and powers. What is best for one group is not necessarily good for the others. The dominant group usually tries to use all possible means and ways to keep the benefits it acquired as long as possible.

The ITU negotiation system has evolved during 150 years and each radio conference makes it better, but it is still not ideal: some of its weaknesses were indicated in the above sections. Notwithstanding this, the history of radio has evidenced that in spite of the threat of supporting some particular interests [22], it has been serving humanity well, not to mention that it has been the only acceptable mechanism. That is an optimistic view. An even more optimistic remark is that the ITU system is not static: it is a dynamic and self-healing system (even if it now recommends static spectrum allocations). The more people understand better spectrum-management mechanisms, the more chances the system will be improved at a future conference. Various forums exist within and outside of the ITU to discuss and understand better problems accompanying the uses of

the radio spectrum, not only the positive uses but also the negative uses; not only seen from a narrow engineering or economic viewpoint, but also from a wider perspective. These forums try to call attention to the need for limiting the negative effects before they develop in full. Should the voice of radio scientists be heard there? ITU has not yet definitely solved the spectrum-scarcity problem, just as the whole of humanity has not solved problems of hunger, health, and many others. According to Hardin, quoted earlier, the scarcity problem cannot be ultimately solved only by technical means, without involving the system of human values and ideas. Mahatma Gandhi, the famous Indian leader, put it briefly as follows:

> There is enough on the Earth to meet everybody's need but not sufficient to meet anybody's greed.

Acknowledgments

The authors would like to thank their directors and colleagues in the National Institute of Telecommunications, Telenor, and ANACOM, respectively, for their support of the present work.

References

[1] M. Cooper, "The Myth of Spectrum Scarcity", http://dynallc.com/2010/03/the-myth-of-spectrum-scarcity-position-paperby-martin-cooper-march-2010/, March 2010 (accessed September 2015).

[2] ITU-R, "World Radiocommunication Conference 2015 (WRC15)", http://www.itu.int/en/ITU-R/conferences/wrc/2015/Pages/default.aspx, (accessed September 2015).

[3] F. Donaldson, "The Marconi Scandal", Bloomsburry Reader, 2013, ISBN: 9781448205851.

[4] G. Havoc, "The Titanic's Role in Radio Reform", IEEE Spectrum, April 15, 2012, pp. 4–6.

[5] National Telecommunications & Information Administration (NTIA), United Stated Department of Commerce, Spectrum Management, http://www.ntia.doc.gov/category/spectrummanagement (accessed April 2015).

[6] Garrett Hardin, "The Tragedy of the Commons", Science, 162, December 1968, pp. 1243–1248.

[7] S. Radicella, "Introduction to International Radio Regulations", ICTP 2003, ISBN 92-95003-23-3, http://publications.ictp.it/lns/vol16.html

[8] T. O'Leary, E. Puigrefagut and W. Sami, "GE 06 – Overview of the Second Session (RRC-06)", EBU Technical Review, https://tech.ebu.ch/docs/techreview/trev_308-rrc-06.pdf, October 2006, pp. 1–20 (accessed November 2014).

[9] E. Pietrosemoli and M. Zennaro, "TV White Spaces – A Pragmatic Approach", ICTP 2013, ISBN 978-9295003-50-7, http://wireless.ictp.it/tvws/book/ (accessed September 21, 2014).

[10] G. A. Codding Jr., "International Constraints on the Use of Telecommunications", in L. Lewin (ed.), Telecommunications – An Interdisciplinary Text, Norwood, MA, Artech House, ISBN 0-89006-140-8, 1984.

[11] R. Struzak, "Software for Radio Frequency Spectrum Engineering", Radio Science Bulletin, No. 262, September 1992, pp. 41–48.

[12] R. Struzak and K. Olms, "Frequency Management and Software for Spectrum Engineering for Personal Computers", Telecommunication Journal, April 1993, pp. 168–174.

[13] W. Rotkiewicz, Electromagnetic Compatibility in Radio Engineering, New York, Elsevier, 1982, ISBN 0-444-99722-9.

[14] URSI, "History of URSI", http://www.ursi.org/en/ursi_history.asp, (accessed September 2015).

[15] R. Struzak and R. C. Kirby, "On Radio Spectrum, Competition and Collaboration", Proceedings of the 17th General Assembly of URSI, (ITU/CCIR presentation), Tel-Aviv, September 24 October 2, 1987.

[16] JTAC IRE - RTMA, Radio Spectrum Conservation, Report of the JTAC IRE - RTMA, New York, McGraw-Hill Book Co., 1952, Library of Congress Nr. 52-9444.

[17] JTAC IEEE and EIA, Spectrum Engineering – The Key to Progress, Report of the JTAC IEEE and EIA, New York, IEEE, 1968, Library of Congress Nr. 68-8567.

[18] F. Matos, Spectrum Management and Engineering, New York, IEEE Press, 1985, ISBN 0-87942-189-4.

[19] W. G. Duff, "Electromagnetic Compatibility in Telecommunications", Interference Control Technologies, 1988, ISBN 0-944916-07-4.

[20] J. A. Stine and D. L. Portigal, "Spectrum 101 – An Introduction to Spectrum Management", MITRE Technical Report, March 2004.

[21] R. Leese and S. Hurley, Methods and Algorithms for Radio Channel Assignment, Oxford, Oxford University Press, 2002, ISBN 0 19 850314 8.

[22] T. Tjelta and R. Struzak, "Spectrum Management Overview", URSI Radio Science Bulletin, No. 340, September 2012, pp. 25–28.

[23] ITU, History of ITU Portal, "Complete List of Radio Conferences", http://www.itu.int/en/history/Pages/ CompleteListOfRadioConferences.aspx (accessed May 2015).

[24] ITU, "Radio Regulations", Edition of 2012, http://www.itu.int/dms_pub/itu-s/oth/02/02/S02020000244501PDFE.PDF (accessed September 2015).

[25] P. Rysavy, "Challenges and Considerations in Defining Spectrum Efficiency", Proceedings of the IEEE, 102, 3, March 2014, pp. 386–392.

[26] I. Flood and M. Allen, "Equipment Selection Heuristic for Microwave Fixed Links", Radio Science, 49, August 2014, pp. 630–64.

[27] M. Mehdawi, N. Riley, K. Paulson, A. Fanan, and M. Ammar, "Spectrum Occupancy Survey in Hull-UK for Cognitive Radio Applications: Measurement & Analysis", International Journal of Scientific & Technology Research, 2, 4, April 2013, pp. 231–236.

[28] European Commission, "Promoting the Shared Use of Radio Spectrum Resources in the Internal Market", Communication from the Commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the regions, COM(2012) 478 final, Brussels, September 3, 2012.

[29] J. M. Chapin and W. H. Lehr, "The Path to Market Success for Dynamic Spectrum Access Technology", IEEE Communications Magazine, May 2007, pp. 96–103.

[30] W. Lehr (chair), "Towards More Efficient Spectrum Management", MIT Communications Futures Program White Paper, March 2014.

[31] M. Falch and R. Tadayoni, "Economic Versus Technical Approaches to Frequency Management", Telecommunications Policy, 28, 2004, pp. 197–211.

[32] R. H. Coase, "The Federal Communication Commission", Law & Economics, II, October 1959, pp. 1–40.

[33] P. Cramton, "Spectrum Auction Design", Review of Industrial Organization, 42, 2, March 2013, pp. 161–190.

[34] A. S. De Vany, R. E. Eckert, C. J. Meyers, D. J. O'Hara and R. C. Scott, "A Property System for Market Allocation of the Electromagnetic Spectrum: A Legal-Economic-Engineering Study", Stanford Law Review, 21, 6, June 1969, pp. 1499–1561.

[35] R. MacKenzie, K. Briggs, P. Grønsund, P. H. Lehne, "Spectrum Micro-Trading for Mobile Operators", IEEE Wireless Communications, December 2013, pp. 6–13.

[36] Z. Ji and K. J. R. Liu, "Dynamic Spectrum Sharing: A Game Theoretical Overview", IEEE Communications Magazine, May 2014, pp. 88–94.

[37] L. Doyle, J. Kibiłda, T. K. Forde and L. Da Silva, "Spectrum Without Bounds, Networks Without Borders", Proceedings of the IEEE, 102, 3, March 2014, pp. 351–365.

[38] J. Brito, "The Spectrum Commons in Theory and Practice", Stan. Tech. L. Rev., 1, 2007.

[39] K. Werbach, "Supercommons: Toward a Unified Theory of Wireless Communication", Texas Law Review, 82, 2004, pp. 863–963.

[40] R. Struzak, "Spectrum Management: Key Issues", Pacific Telecommunications Review, September 1996, No. 1 pp. 2–11.

[41] A. Nagurney, "Supernetworks", in M.G.C. Resende and P. M. Pardalos (eds.), Handbook of Optimization in Telecommunications, Berlin, Springer, 2006, ISBN-10: 0-387-30662-5, pp. 1073–1119.

[42] T. Harbert, "Internet Giants Adopt New Lobbying Tactics", IEEE Spectrum, October 2012, http://spectrum.ieee.org/telecom/internet/internet-giants-adopt-new-lobbying-tactics (accessed March 2013).

[43] "Bogota Declaration of 1976: Declaration of the First Meeting of Equatorial Countries", http://www.jaxa.jp/library/space_law/chapter_2/2-2-1-2_e.html

[44] R. Struzak, "CCIR Preparations for WARC'92", URSI Radio Science Bulletin, No. 259, December 1991, pp. 50–57.

[45] R. Struzak, M. Hunt and A. Nalbandian, "CCIR Preparations for World Administrative Radio Conference WARC '92", Telecommunication Journal, February 1992, pp. 56–59.

[46] R. Struzak, "On Future Information System for Management of Radio Frequency Spectrum Resource", Telecommunication Journal, November 1993, pp. 429–437.

[47] ITU, "Executive Summary", Measuring the Information Society Report 2014, 2014.

[48] R. Struzak, "Broadband Internet in EU Countries: Limits to Growth", IEEE Communications Magazine, 48, 4, April 2010, pp. 52–55.

[49] R. Struzak, "Diffusion of Broadband Services: An Empirical Study", IEEE Communications Magazine, 50, 8, 2012, pp. 128–134.

[50] D. McNally, "The Vanishing Universe", Cambridge, Cambridge University Press, 1994, ISBN 0 521 450209.

[51] B. Robinson, "Frequency Allocations - The First Forty Years", Annual Review of Astronomy and Astrophysics, 37, 1999, pp. 65–96.

[52] H. Zimmermann, "The Vital Role of Telecommunications in Disaster Relief and Mitigation", Emergency Telecommunications DHA Issues, Focus Series No. 2, United Nations, 1995, pp. 3–5.

[53] A. Rahrig, "Love Thy Neighbor: The Tampere Convention as Global Legislation", Indiana Journal of Global Legal Studies, 17, 2, January 2010.

[54] R. Struzak, "Evaluation of the OCHA (DRB) Project on Emergency Telecommunications with and in the Field, Rev. 1", New York and Geneva, United Nations, July 2000, September 2000.

[55] AT&T, "A Brief History: The Bell System", http://www.corp.att.com/history/history3.html (accessed February 2013).

[56] OECD, "Report OECD Communications Outlook 2013", DOI: 10.1787/comms_outlook-2013-en, http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/oecd-communications-outlook-2013_comms_outlook-2013en

[57] C. Guglielmo, "The Apple vs. Samsung Patent Dispute: 20-Talking Points", http://www.forbes.com/sites/connieguglielmo/2012/08/21/the-apple-vs-samsung-patentdispute-20-talking-points/

[58] J. P. Kesan and G. G. Ball, "How Are Patent Cases Resolved? An Empirical Examination of the Adjudication and Settlement of Patent Disputes", Washington University Law Review 2006, 84, 2, pp. 237–312.

[59] A. Armstrong, J. J. Mueller and T. D. Syrett, "The Smartphone Royalty Stack", http://www.wilmerhale.com/uploadedFiles/Shared_Content/Editorial/Publications/Documents/TheSmartphone-Royalty-Stack-Armstrong-Mueller-Syrett.pdf (accessed July 2014).

[60] L. Popelka, "Only Lawyers Win in Patent Wars", http://www.businessweek.com/articles/2012-04-24/patent-wars-lawyersare-the-only-winners (accessed December 2014).

[61] B. Marcus, "The Spectrum Should be Private Property: The Economics, History and Future of Wireless Technology", Mises Daily, Ludvig von Mises Institute, 2004.

[62] D. Bollier, "Reclaiming the Commons. Why We Need to Protect Our Public Resources from Private Encroachment", http:// bostonreview.net/BR27.3/ bollier.html#* (accessed May 2013).

[63] D. Bollier, "Silent Theft: The Private Plunder of Our Common Wealth", New York Routledge, 2002.

[64] S. Fairlie, "A Short History of Enclosure in Britain", The Land, Issue 7, summer 2009, http://www.thelandmagazine.org.uk/articles/short-history-enclosure-britain (accessed June 2014).

[65] J. Helliwell, R. Layard and J. Sachs, "World Happiness Report 2013."

[66] R. J. Matheson, "Flexible Spectrum Use Rights. Tutorial", International Symposium on Advance Radio Technologies (ISART) 2005.

[67] R. Struzak, "Flexible Spectrum Use and Laws of Physics", ITU-FUB Workshop: Market Mechanisms for Spectrum Management, Geneva, January 22-23, 2007.

[68] R. Struzak, "On Spectrum Congestion and Capacity of Radio Links", Annals of Operation Research 2001, 107, 2001, pp. 339–347.

[69] BBC News, December 19, 2002, http://news.bbc.co.uk/2/hi/business/2591993.stm, (accessed May 2015).

[70] D. Daniel Sokol, "The European Mobile 3G UMTS Process: Lessons from the Spectrum Auctions and Beauty Contests", Virginia Journal of Law and Technology, University of Virginia, Fall 2001, VA. J.L. & TECH. 17, http://www.vjolt.net/vol6/ issue3/v6i3-a17-Sokol.html (accessed May 2015).

[71] J. Stiglitz, The Price of Inequality: How Today's Divided Society Endangers Our Future, New York, W. W. Norton & Co., 2013, ISBN-10: 0393345068.

[72] G. Soros, "The Capitalist Threat", The Atlantic Monthly, February 1997, pp. 45–58.

[73] United Nations Conference on the World Financial and Economic Crisis and Its Impact on Development, Abu Dhabi, United Arab Emirates, July 8-11, 2013.

[74] The Washington Declaration on Intellectual Property and the Public Interest Adopted at American University Washington College of Law, Washington DC, August 27, 2011.

[75] ITU, "ICT Services Getting More Affordable Worldwide", ITU Newsroom, Press Release, https://www.itu.int/net/ pressoffice/press_releases/2011/15.aspx#.VVBS5O901aQ (accessed May 2015).

[76] R. Struzak, "Microcomputer Modeling, Analysis and Planning in Terrestrial Television Broadcasting", Telecommunication Journal, 59-X, 1992, pp. 453, 459-492 (see also: http://www. piast.edu.pl/).

[77] R. Struzak, "Internet in the Sky: T1 Tests have Started...", ITU News, Nr. 6/98, pp. 22-26.

[78] R. Struzak, "Mobile Telecommunications via Stratosphere", Intercomms – International Communications Project, 2003, http://www.intercomms.net/AUG03/docs/features.php (accessed November 2014).

[79] S. Forge, C. Blackman and R. Horwitz, "Perspectives on the Value of Shared Spectrum Access", Final Report for the European Commission, SCF Associates, DTI, GNKS-Consult, ICEGEC and RAND Europe, 2012.

[80] M. Gorenberg, "A Modern Approach to Maximizing Spectrum Utility and Economic Value", in N. Kroes (ed.), Digital Minds for a New Europe, http://ec.europa.eu/commission_2010-2014/kroes/en/content/digital-minds-new-europe, (accessed November 2014).

[81] Radio Spectrum Policy Group, "Report on Collective Use of Spectrum (CUS) and Other Spectrum Sharing Approaches", RSPG11-392 Final, November 2011.

[82] W. Flury, "The Space Debris Environment of the Earth", in D. McNally, The Vanishing Universe, Cambridge, Cambridge University Press, 1994.

[83] G. Schmid, "On the Existence of a Global System for the Interception of Private and Commercial Communications - ECHELON Interception System", European Parliament: Temporary Committee on the ECHELON Interception System, 2001/2098(INI).

[84] S. Rehman, "Estonia's Lessons in Cyberwarfare", US News, January 14, 2013.

[85] URSI, "White Paper on Solar Power Satellite (SPS) Systems", Report of the URSI Inter-Commission Working Group on SPS, http://www.rish.kyoto-u.ac.jp/SPS/WPReportStd.pdf, (accessed May 2015).

Source: Radio Science Bulletin 2015, no. 354, pp. 11–34, http://www.ursi.org/en/publications_rsb.asp

Reprinted with permission from Mr W. Ross Stone, PhD, Editor, URSI Radio Science Bulletin, URSI Assistant Secretary General (Publications and GASS).

Information for Authors

Journal of Telecommunications and Information Technology **(JTIT)** is published quarterly. It comprises original contributions, dealing with a wide range of topics related to telecommunications and information technology. **All papers are subject to peer review**. Topics presented in the JTIT report primary and/or experimental research results, which advance the base of scientific and technological knowledge about telecommunications and information technology.

JTIT is dedicated to publishing research results which advance the level of current research or add to the understanding of problems related to modulation and signal design, wireless communications, optical communications and photonic systems, voice communications devices, image and signal processing, transmission systems, network architecture, coding and communication theory, as well as information technology.

Suitable research-related papers should hold the potential to advance the technological base of telecommunications and information technology. Tutorial and review papers are published only by invitation.

Manuscript. TEX and LATEX are preferable, standard Microsoft Word format (.doc) is acceptable. The author's JTIT LATEX style file is available:
http://www.nit.eu/for-authors

Papers published should contain up to 10 printed pages in LATEX author's style (Word processor one printed page corresponds approximately to 6000 characters).

The manuscript should include an abstract about 150–200 words long and the relevant keywords. The abstract should contain statement of the problem, assumptions and methodology, results and conclusion or discussion on the importance of the results. Abstracts must not include mathematical expressions or bibliographic references.

Keywords should not repeat the title of the manuscript. About four keywords or phrases in alphabetical order should be used, separated by commas.

The original files accompanied with pdf file should be submitted by e-mail: redakcja@itl.waw.pl

Figures, tables and photographs. Original figures should be submitted. Drawings in Corel Draw and PostScript formats are preferred. Figure captions should be placed below the figures and can not be included as a part of the figure. Each figure should be submitted as a separated graphic file, in .cdr, .eps, .ps, .png or .tif format. Tables and figures should be numbered consecutively with Arabic numerals.

Each photograph with minimum 300 dpi resolution should be delivered in electronic formats (TIFF, JPG or PNG) as a separated file.

References. All references should be marked in the text by Arabic numerals in square brackets and listed at the end of the paper in order of their appearance in the text, including exclusively publications cited inside. Samples of correct formats for various types of references are presented below:

[1] Y. Namihira, "Relationship between nonlinear effective area and mode field diameter for dispersion shifted fibres", *Electron. Lett*., vol. 30, no. 3, pp. 262–264, 1994.

[2] C. Kittel, *Introduction to Solid State Physics*. New York: Wiley, 1986.

[3] S. Demri and E. Orłowska, "Informational representability: Abstract models versus concrete models", in *Fuzzy Sets, Logics and Knowledge-Based Reasoning*, D. Dubois and H. Prade, Eds. Dordrecht: Kluwer, 1999, pp. 301–314.

Biographies and photographs of authors. A brief professional author's biography of up to 200 words and a photo of each author should be included with the manuscript.

Galley proofs. Authors should return proofs as a list of corrections as soon as possible. In other cases, the article will be proof-read against manuscript by the editor and printed without the author's corrections. Remarks to the errata should be provided within one week after receiving the offprint.

Copyright. Manuscript submitted to JTIT should not be published or simultaneously submitted for publication elsewhere. By submitting a manuscript, the author(s) agree to automatically transfer the copyright for their article to the publisher, if and when the article is accepted for publication. The copyright comprises the exclusive rights to reproduce and distribute the article, including reprints and all translation rights. No part of the present JTIT should not be reproduced in any form nor transmitted or translated into a machine language without prior written consent of the publisher.
For copyright form see: http://www.nit.eu/for-authors

A copy of the JTIT is provided to each author of paper published.

Journal of Telecommunications and Information Technology has entered into an electronic licencing relationship with EBSCO Publishing, the world's most prolific aggregator of full text journals, magazines and other sources. The text of *Journal of Telecommunications and Information Technology* can be found on EBSCO Publishing's databases. For more information on EBSCO Publishing, please visit www.epnet.com.

(*Contents Continued from Front Cover*)

INSTYTUT ŁĄCZNOŚCI
PAŃSTWOWY INSTYTUT BADAWCZY

Editorial Office
National Institute
of Telecommunications
Szachowa st 1
04-894 Warsaw, Poland

tel. +48 22 512 81 83
fax: +48 22 512 84 00
e-mail: redakcja@itl.waw.pl

JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY 3/2016