JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY

2/2019

(Contents Continued on Back Cover)

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

Circulation: 300 copies Sowa – Druk na życzenie, www.sowadruk.pl, tel. 22 431-81-40

Ministry of Science and Higher Education
Republic of Poland

Improvement of the linguistic quality of the journal; Assignment of DOI numbers; Access to the anti-plagiarism system; Editing and printing of the journal – tasks financed under 706/P-DUN/2019 agreement from budget of the Ministry of Science and Higher Education under the science dissemination fund.

JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY

Preface

This issue of the *Journal of Telecommunications and Information Technology* contains eleven papers that deal with a wide range of problems related to the security of computer and industrial networks, focusing primarily on assessing risks that affect critical infrastructures, as well as on protecting mobile service robots, the Internet of things and blockchain systems against cyber-attacks. The articles deal also with wire and wireless communications, various aspects of energy conservation in data centers and computer networks, and with the application of modern multimedia techniques in didactics.

The first four papers published in this issue of the Journal are devoted to the protection of critical national infrastructure. Research conducted in this field was inspired by the authors' participation in the National Cybersecurity Platform – a project funded by the National Centre for Research and Development, under the CyberSecIdent Program. The goal of this project is to develop a comprehensive, integrated system enabling to monitor, detect and warn about threats identified, virtually in real time, in the State's cyberspace. Two subsequent articles deal with the assessment of cyber risk existing at national level. Selected approaches to cyber risk management are discussed in the paper titled *A Novel Approach to National-level Cyber Risk Assessment Based on Vulnerability Management and Threat Intelligence*. Marek Janiszewski, Anna Felkner and Piotr Lewandowski claim that there are no comprehensive platforms for national level risk assessment. In the majority of cases, the risk is estimated for specific institutions only. The authors propose a method for real-time risk analysis, performed by clients at various levels, and suggest a technique used for aggregating the results on the nationwide level. This technique allows to foresee cyber threats and to build situational awareness by monitoring the current situation in any computer network. Another approach to risk management is proposed by Andrzej Karbowski *et al*. in the paper titled *Critical Infrastructure Risk Assessment Using Markov Chain Model*. Application of the Markov chain model for the purpose of assessing the risk affecting critical infrastructure is described in the article. In this model, specific states represent the potential security levels of different services, assessed based on their availability. Results of preliminary experiments

performed in relation to a scenario involving two services, i.e. healthcare and power supply, are presented and discussed. The authors argue that application of Markov chains is one of the most promising approaches to modeling the propagation of risky events in the area of cybersecurity. The problem of security in operational technology networks (OT) is outlined in the paper titled *On Preventing and Detecting Cyber Attacks in Industrial Control System Networks*. Adam Padée *et al*. provide a review of techniques for protecting and detecting cyber-attacks affecting industrial systems. Their attention is focused on the nuclear industry. Common components of OT security systems are described and compared with those used in the IT domain. In the paper titled *Cyber-security for Mobile Service Robots – Challenges for Cyber-physical System Safety*, Wojciech Dudek and Wojciech Szynkiewicz consider the problem of cybersecurity of robot systems. They provide a brief overview of threats affecting cyber-physical robotic systems, caused by cybernetic attacks, and propose methods that may be relied upon to detect and mitigate the consequences of such attacks. The authors claim that there is a great need to develop new solutions for securing service robots against cyber-attacks, and present those issues regarding the cybersecurity of robot systems that still need to be resolved.

Next two papers focus on the security of IoT and blockchain networks. In the paper titled *Battery Drain Denial-of-Service Attacks and Defenses in the Internet of Things*, Philokypros P. Ioulianou, Vassilios G. Vassilakis and Michael D. Logothetis investigate the possibility of battery drain Denial-of-Service (DoS) attacks affecting the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) of the Contiki operating system. The authors present the results of simulation experiments that demonstrate the impact of DoS attacks on the power consumption of IoT devices. They discuss the potential defense techniques relying on distributed intrusion detection systems. In the paper *Blockchain Networks – Security Aspects and Consensus Models*, Andrzej Wilczyński and Adrian Widłak propose a generic architecture model of a blockchain system, and offer the concept of consensus models used in blockchain transactions. To illustrate the performance of the proposed solutions, the results of practical use cases are presented and discussed as well. The authors' attention focuses primarily on security-related aspects.

The paper titled *CL-mWSNs: Cross Layer Model-Based QoS Centric Routing Protocol for Mission-Critical Cooperative Communication in Mobile WSNs* deals with efficient wireless communication techniques and with practical application scenarios involving wireless sensor networks (WSN). A robust Quality of Service (QoS)-centric routing protocol that exploits dynamic network states from the various layers of the IEEE 802.15.4 standard is presented. The protocol is dedicated to mission-critical communication in mobile WSNs. Kummathi C. Reddy, Geetha D. Devanagavi and Thippeswamy M. N. argue that their protocol ensures high throughput, as well as minimum loss and low latency rates. The results of simulation experiments presented in the paper confirm the efficiency of the presented technique.

Communication protocols for Unmanned Aerial Vehicle (UAV) systems are investigated by Kiyoshi Ueda and Takumi Miyoshi in their paper titled *Autonomous Navigation Control of UAV Using Wireless Smart Meter Devices*. The authors introduce and describe a new routing protocol enabling to establish a safe route based on a network of smart meters. They propose a control method in which the UAV communicates with the nodes, acquires information necessary for sensing its position and navigates by following the route, as if the UAV were a data packet within a network. The current distance between the UAV and a given node within the network of smart meters is measured by means of radio transmission loss value. The solution may be used for performing home deliveries that rely on UAVs.

Two subsequent papers address the vital problem of infrastructure and energy conservation in computer networks and data centers. In the paper titled *Infrastructure and Energy Conservation in Big Data Computing: A Survey*, Ewa Niewiadomska-Szynkiewicz and Michał P. Karpowicz provide a review of recent Big Data processing technologies. The emphasis is placed on the most popular middleware and software platforms and energy saving approaches that may be relied upon by data centers. A heuristic algorithm for energy efficient allocation of network resources, based on the current workload, is presented in the paper titled *Optimized Energy Aware Resource Allocation Algorithm Using Software Defined Network Technology*. The solution presented is based on the architecture of a Software Defined Network (SDN). Ranya Al-Musawi and Obada Al Khatib present simulation results confirming

good performance of their method which allows to reduce energy consumption compared to solutions described in literature.

The last paper, titled *Multimedia Mathematical Communication in a Diverse Group of Students*, tackles the problem of learning mathematics by visually impaired persons. The emphasis is placed on efficiency of communication in the learning process. Jolanta Brzostek-Pawłowska presents interactive multimedia solutions fostering mathematical communication within a group of students with a range of diverse visual impairments, under the teacher's guidance. The results of qualitative surveys of the proposed approach confirm its usefulness and positive impact on the efficiency of the work of a group learning mathematic.

We do hope that our Readers will find this issue of the Journal both interesting and enjoyable.

Ewa Niewiadomska-Szynkiewicz
Guest Editor

https://doi.org/10.26636/jtit.2019.preface2

Paper

A Novel Approach to National-level Cyber Risk Assessment Based on Vulnerability Management and Threat Intelligence

Marek Janiszewski, Anna Felkner, and Piotr Lewandowski

Information Security Methods Team, Research and Academic Computer Network (NASK), Warsaw, Poland

https://doi.org/10.26636/jtit.2019.130919

Abstract—Real-time assessment of IT-related risks, performed at the national level, is very important due to the evolving nature of threats that may originate from individual hackers, organized cyber-criminal groups, as well as state activities. Evaluation of risk that is based on technical information, as well as on mutual relationships between various institutions and services, may result in very valuable situational awareness. The paper describes (in general) cyber risk analysis method which will be implemented in Polish National Cybersecurity Platform.

Keywords—digital services, essential services, incident management, risk assessment, risk management, situational awareness, threat intelligence, vulnerability management.

1. Introduction

The main goal of the National Cybersecurity Platform is to provide a comprehensive, state-wide view of cyber threats in order to evaluate risks in real-time, as well as to monitor the current status of various essential, digital services. In cybersecurity, the broader the perspective, the more threats may be noticed. Therefore, various relationships may be identified to prevent many ramifications, helping protect the essential services, their operators and, as a consequence, various entities and citizens. The National Cybersecurity Platform consists of two types of entities, namely the platform's customers and its operational center. Any institution may become a customer of the platform, but essential service operators and digital service providers may be obliged to become its members. The operational center is a central unit that provides customers with various types of information and acts as an intermediary in sharing information between individual users. The operational center monitors also various events, calculates risks based on the information provided by customers, submits information on current threat levels and provides recommendations based on the risk analyses performed.

Risk estimation relying on objective and quantified measures is very rare, due to the fact that it is a non trivial task. Most solutions use qualified measures to assess the risk affecting information systems that use different programs. Risk estimation is based on a methodology that tries to ensure objective nature of the risk assessment process. However, such an approach requires that the task be always performed by an analyst or auditor (with the support of a specific methodology and a system that may facilitate this process). Due to the fact that the human factor is involved, the results of such a risk assessment process are, to some extent, always subjective. In addition, this process is time-consuming and is repeated not more frequently than once every few months (in most cases risk assessment is performed annually or every other year). The fact that such analysis often fails to focus on technical vulnerabilities of software and on and other technical information (such as Indicators of Compromise – IoC) also needs to be taken into account. In fact, such technical information plays a key role in assessing the level of security of a given system or service. In addition, new vulnerabilities are still being discovered (with new incidents and IoCs being reported as well). Therefore, risk estimation should be carried out in real-time [1]. The statements given above are true even for individual institutions, but at a higher level (for example – within a given economic sector) the task of risk assessment is significantly more complicated. On the national level, due to the heterogeneity of institutions (and sectors), the task is much more difficult, but this paper presents a general approach which may be relied upon to satisfy the need of quantitative risk assessment performed on the national level.

The article is organized as follows. Section 2 discusses works related to the risk analysis domain. Section 3 describes, in more detail, the main characteristics of the approach used to model relationships between services and also the general approach to risk calculation. Section 4 lists and describes the sources of information which are used to calculate risk and monitor situational awareness. Section 5 presents the model of the proposed risk calcula-

tion algorithm. Conclusions and proposals of future work are provided in Section 6.

2. State of the Art

Risk management is very important, but no comprehensive frameworks exist facilitating the performance of this task on the national level. In most cases the problem is considered with regard to an individual institution, and cannot be easily transposed to the national level. Still, approaches exist which may be relied upon in a more comprehensive manner. Therefore, this section briefly describes the most important problems and approaches associated to risk assessment.

2.1. Standards and Norms

The best-known risk management methods and methodologies include the following:

- ISO 16085:2006 – Systems and software engineering – Life cycle processes – Risk management,
- ISO 31000 Risk management – Principles and guidelines,
- ISO/IEC 27005:2014,
- AS/NZS 4360:2004 – Risk Management,
- COSO Enterprise Risk Management,
- FERMA Risk Management Standard,
- CRAMM – CCTA Risk Analysis and Management Method,
- COBRA – Control Objectives for Risk Analysis,
- OCTAVE – Operationally Critical Threat, Asset and Vulnerability Evaluation,
- MARION – Methodology of Analysis of Computer Risks Directed by Levels,
- MEHARI – MEthod for Harmonized Analysis of RIsk.

All standards and methods referred to above are very useful in the context of risk management at the level of individual organizations. Guidelines contained in the above standards may be applied within an institution, whereas in order to estimate the risk on the level of the entire cyberspace, where no access to information about the infrastructure of individual institutions is available, such guidelines prove to be insufficient. They may be taken into account, but unfortunately, they cannot be applied directly.

2.2. Types of Tools Relevant for Risk Assessment

Risk assessment, risk analysis and risk management processes of an organization may be supported with different types of software, covering various domains. The most comprehensive tool for this work is a GRC system (Governance, Risk management, and Compliance). Applications such as IBM OpenPages (for more details, see IBM website [2]) may help to define risks, connect them with the organization's missions, assets and responsible people, as well as rate and manage these risks. This approach is very much focused on the business dimension, so it lacks some detailed technical information required by those who are more interested in analyzing risks affecting IT assets and resources.

To overcome those shortcomings of GRC software, some ITAM (IT Asset Management) and Configuration Management Database (CMDB) applications have been designed, incorporating IT inventory risk analysis modules. ITAM software (e.g. Device42 [3]) helps manage the IT asset life-cycle in an organization (i.e. cost, warranty, ownership, depreciation), while CMDB (e.g. BMC Discovery [4] or Qualys Asset Inventory [5]) applications store the configuration of IT assets (both hardware and software) and their current operational status. In spite of differences in core functionality of ITAM and CMDB applications, both store some information about the configuration of IT assets. Combining this data with information about well-known vulnerabilities may help performing in risk analysis and management processes.

Complex platforms composed of modules (such as ITAM, CMDB, GRC etc.) which cooperate to cover every aspect of risk assessment, analysis and management are also available. These include, for instance: RSA Archer and ServiceNow Now Platform. Even if the manufacturer is not offering its own module for a certain task, the platform can import data from a third party application via API. A detailed description of these platforms may be found on their respective websites: [6], [7].

2.3. International Projects

While conducting research, we analyzed several international, EU-funded projects concerning IT security and risk analysis. The most important of these include the following: PANOPTESEC, WISER, PROTECTIVE and NECOMA. Some of them (NECOMA or PANOPTESEC) focus, to a more considerable degree, on IT security, while others (WISER, PROTECTIVE) attach a greater emphasis to risk analysis. In the following subsections, the authors' conclusions about these projects, which are important in the context of the objectives of the article, may be found.

The NECOMA project [8] was driven by European and Japanese organizations: Institut Mines-Télécom (France), Atos Spain (Spain), 6cure (France), NASK – Research and Academic Computer Network (Poland), Foundation for Research and Technology – Hellas (Greece), Nara Institute of Science and Technology (Japan), Internet Initiative Japan Inc. (Japan), National Institute of Informatics (Japan), Keio University (Japan) and University of Tokyo (Japan). The

main goal of the NECOMA project was to create a tool for collecting network traffic, analyzing it, identifying cyber-attack attempts and mitigating them. The idea was to collect data from network devices, such as switches, routers, IDS, etc., and to analyze such data in a dedicated system with the use of original algorithms. This system also uses external databases, such as n6 [9] or PhishTank [10], to improve the ability to detect attacks [11]. In order to mitigate attacks, the system tries to automatically reconfigure the network devices with the use of their Application Programming Interface (API) [12]. Although risk analysis involving threats, attacks or supervised networks was out of the scope of the NECOMA project, we find this project to be very interesting because the idea of an advanced network traffic analysis may be relied upon to evaluate various risks.

The PANOPTESEC [13] project was pursued by a consortium comprising Institut Mines-Télécom (France), RHEA System (Belgium), Technische Universität Hamburg-Harburg (Germany), Universität zu Lübeck (Germany), Nokia Bell Labs France (France), L'École Supérieure d'Électricité (France), ACEA (Italy), Universita degli Studi di Roma La Sapienza (Italy), Epistematica (Italy), L'Institut national de recherche en informatique et en automatique (Inria) (France), RHEA System (Netherlands) and RHEATECH (Great Britain). The outcome of the PANOPTESEC project was a system that can predict paths of cyber-attacks on the supervised IT infrastructure. To achieve this, the system must be filled with all information about the network infrastructure, including: devices, network connections between them, firewall rule sets, operating system version, application version, and so on. Having this knowledge and information about vulnerabilities in hardware and software, the system can simulate paths of attacks or malware infections. To make this simulation more actionable, it is supplemented with information about mission impact in the case of a failure of some devices [14]. Mission impact and risk analysis must be performed by the system user (e.g. organization or company) in advance [15]. These simulations and the potential mission impact are visualized alongside with examples of mitigation, to help the user take the proper action [16]. All these features make PANOPTESEC a very promising solution in terms of analyzing the risk of IT-related threats. Unfortunately, processing this amount of data requires lots of computing power. Benchmarks performed by PANOPTESEC authors show that the analysis of connections between 10,000 network nodes may take up to 1 hour [17].

WISER [18] was a project led by Atos Spain, with other participating entities including the following: Trust-It Services Limited (Great Britain), Stiftelsen Sintef (Norway), XLAB Razvoj Programske Opreme In Svetovanje (Slovenia), Aon UK Limited (Great Britain), Rexel Dévéloppement (France), Domotecnica (Italy), Enervalis (Belgium) and Aon Insurance & Reinsurance Brokers (Italy). The product of this project is now available commercially and is known as the CYBERWISER service [19]. The WISER system requires two types of input to operate. The first type of input comes from sensors (software- and hardware-based) which analyze network traffic and system logs to detect cyber-attacks. The other type of input originates from a risk analysis performed for various cyber-attack scenarios (such as denial of service attack, bypass login by brute force or DNS login attack, compromise security via trojan-malware, SQL injection, buffer overflow, relative path traversal, and so on) [20]. The risk analysis is carried out using CORAS diagrams to identify attack scenarios with the affected assets, and DEXi or R language to define Bayesian networks to model specific risks. With risk-related information obtained from sensors, the system may dynamically present the current level of threat [21]. WISER presents an interesting approach to connecting, in real time, risk analysis to specific vulnerabilities and threats.

PROTECTIVE [22] is an ongoing project of Athlone Institute of Technology (Ireland), Synyo (Austria), Poznań Supercomputing and Networking Center (Poland), The Email Laundry (Ireland), Technische Universität Darmstadt (Germany), Agency Arniec – RoEduNet (Romania), GMV Soluciones Globales Internet (Spain), Cesnet (Czech Republic), ITTI (Poland) and University of Oxford (Great Britain). As the project will conclude by September 2019, its final implementation date is subject to change. This project is focused on sharing threat intelligence between the platform's participants. At the time when this paper is being compiled, architecture of the PROTECTIVE system assumes that each participant is collecting information about network traffic within their organization, using a set of probes (software and hardware) [23]. The collected data is standardized and analyzed to identify malicious or undesired activities, or potentially unwanted applications. Based on these findings, the system creates IoCs. IoCs may then be shared with other participants to help them protect their networks or identify and mitigate attacks [24]. The description of the PROTECTIVE project contains references to risk analysis performed with regard to the participants' assets, but it lacks any details.

Summary

Over the past five years, at least four big international projects focused on cyber threats and/or risk analysis have been pursued. All projects presented above propose certain interesting ideas in the field of risk analysis, information aggregation, sharing of intelligence data, as well as monitoring and mitigating threat. Nevertheless, none of them are capable of monitoring the threat level nationwide. This shows how complex the task of analyzing risk and monitoring threats affecting the networks of organizations and enterprises of various sizes, organizational structures, IT infrastructures, etc. is. The National Cybersecurity Platform is designed to solve this problem and help enhance the level of cybersecurity.

3. Approach to the Model of Relationships between Services and Risk Assessment

One of the main motivations of the National Cybersecurity Platform is the implementation of the Directive on security of network and information systems (NIS Directive, [25]) which was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. The NCP platform creates a map of key services that depend on ICT infrastructure. It is the task of the platform to achieve several objectives, such as monitoring the security of cyberspace, early detection of threats and taking proactive measures to mitigate the risks.

The risk level will be estimated for individual services, sectors and the entire cyberspace of a given country based on the vulnerabilities identified, sightings, incidents, assessment of the criticality of services and based on the criticality of relationships between individual services. Both static and dynamic risks will be analyzed. Based on the risk analysis performed in the context of services, sectors and cyberspace of the Republic of Poland, recommendations for platform participants will be issued using the expert module.

Relationships between services are presented by means of a graph depicting their mutual interdependencies, in particular as far as the aspect of security (confidentiality, integrity and availability) us concerned. The said graph presents also the affiliation of specific services to institutions (operators) and sectors. The graph depicting the relationships between key services is based on data from questionnaires completed by the platform's clients.

4. Information Used to Build Situational Awareness

The following types of information may be relied upon to analyze and calculate risk:

- vulnerabilities,
- Indicators of Compromise (IoC),
- sightings,
- incidents,
- network monitoring results (e.g. results of open port scanning),
- inventory (software and hardware used, relationships with services and criticality of relationships),
- catalog of services and relationships between services.

The most important types of information are described in the following subsections.

4.1. Vulnerabilities

One may undoubtedly argue that each software and hardware component suffers from certain vulnerabilities, even if many of them have failed to be discovered so far. However, the claim that each software element is equally sensitive is not true and unjustified. The normal process of revealing a newly discovered vulnerability assumes that the vendor of the product in which the vulnerability has been discovered is informed first. The vendor, after conducting an investigation and relevant research, prepares an appropriate software patch (also known as a fix or an update) which should eliminate the vulnerability concerned. After preparing the patch, the vendor informs (for example via bulletins published on the vendor's website) all potential users and the community about the new fix and about the vulnerability itself. This process is known as the process of responsible disclosure. Vulnerabilities are discovered not only by white hats (cyber security analysts whose goal is to boost the level of the software security), but also by black hats (crackers whose purpose is to compromise information systems to obtain certain information or to prevent their fair use). When the cracker finds a new vulnerability (so called "0-day"), they try to exploit it to generate benefits, instead of informing the vendor. Therefore, unknown vulnerabilities are associated with an enormous potential to compromise system security [1].

The vulnerability management system should support the system administrator in two areas. First of all, its main task should be to support the administrator in the process of managing updates. The system administrator should be able to indicate all software components making up the system. Vulnerabilities and patches published after the last update should be detected using an automated system that collects information about patches and vulnerabilities obtained from several different sources. Secondly, the vulnerability management system should assess the technical risks associated with the software used. This risk stems from the existing security vulnerabilities [1].

Technical vulnerability databases are very important, but they contain information about well-known vulnerabilities only (mainly those for which patches have been released). To calculate risk, the administrator has to identify the presence of a vulnerable asset, and, consequently, the presence of the vulnerability itself. Because of that, in theory, the chances that the administrator takes corrective actions are greater than the chances that the administrator conducts (even in an automated manner) a risk analysis taking into account the vulnerability concerned. After successful correction, no additional risk associated with this vulnerability is present (due to its elimination). In practice, however, sometimes it is not possible to apply the patch or other proposed recommendations or such measures cannot be introduced immediately. In such scenario, it makes sense to update the risk calculations performed.

To calculate the level of risk affecting a system or a service based on its vulnerabilities, the Common Vulnera-

bility Scoring System (CVSS) may be used. CVSS is a methodology that characterizes the impact of security vulnerabilities. The CVSS score may be perceived as an indicator of the severity of a specific vulnerability. The CVSS score may vary from 0.0 to 10.0, where values from 0.0 to 3.9 indicate a "low" level of severity, and values from 7.0 to 10.0 mean "high" or "critical" severity. The CVSS result is widely used as an indicator of the severity of vulnerabilities, but not all sources of information list it [1].

Risk calculation will be performed by each client based on the vulnerability database shared by the operational center. Each client should perform inventory identification, and based thereon, they should automatically match vulnerabilities that may affect their systems and services.

Many approaches rely on NVD only, as the best-known database of security vulnerabilities. However, NVD is not the only database and it does not provide the most information. Several limitations of the NVD database were also indicated by the author of [26]. While conducting our research, we analyzed the generally available databases of vulnerabilities and patches. One may conclude that in order to build a comprehensive database of vulnerabilities, many sources of information about vulnerabilities should be relied upon.

4.2. Inventory

The inventory, which can be perceived as a database of IT assets, is crucial from the point of view of the vulnerability management process. The inventory needs to be taken by each client individually. However, details of the inventory are not shared with the operations center or any other client. Lists of software or hardware elements and applications are used to calculate the risks which stem from the existing vulnerabilities.

4.3. Indicators of Compromise and Sightings

Indicators of compromise are characteristics observed within a network or a system indicating an intrusion. Aggregation and provision of such information to clients may be beneficial for security monitoring. The presence of an artifact described by IoC (sighting) may also impact current risk calculations.

4.4. Incidents

Incidents reported by all participants of the platform may be aggregated by the operations center and may be used for risk assessment purposes. Based on historical information, the incident prediction mechanisms may be implemented. Information about incidents reported by various institutions may be used to identify similar features of incidents and targeted institutions. Based thereon, the risk of the threat propagating between services and institutions may be estimated as well.

5. Risk Calculation

One of the main goals of the National Cybersecurity Platform is to provide a comprehensive analysis of risks arising from the potential exploitation of known vulnerabilities affecting the company's IT assets, as well as from potential security incidents, such as: hacker attacks, malware infections or data breaches. The risk analysis process is divided between clients and the NCP operations center, because the results of this analysis concern risks at the institution- and nationwide level. The flow of data (related to risk analysis) between the client and the NCP operations center is depicted in Fig. 1. More details on risk analysis may be found in the subsequent sections.

5.1. Institution Level

Risk analysis performed at the institution level concerns cyberthreats to the company's IT infrastructure that supports the services. The risk analysis is carried out for each service offered by the client. The National Cybersecurity Platform is responsible for services which are essential for the country's economy or security. The criteria for such services are set out in the National Cybersecurity System Act. The services may produce goods or may be completely intangible. For the purpose of a more detailed risk analysis, it is important to define whether the risk analysis cover intangible services rendered in an electronic form (the so called e-service) or not.

Each client joining NCP has to fill out a questionnaire about the services they would like the National Cybersecurity Platform to cover (denoted as S_E). The questions are related to the following information: type of service (electronic or not), scale of service expressed in applicable units of measure (e.g. tons of coal for mines or number of passengers in the case of transport services) – (global criticality of the service – $C_g^{S_E}$), relevance of service for the client's business (internal criticality of $C_i^{S_E}$ service), standards, procedures and means of security incorporated to protect the service against cyberthreats and the time needed to recover the service after a failure (the shortest and the longest period of time experienced before the questionnaire is filled out).

There are also questions about relationships between services enrolled in NCP and supporting services provided by a third party. The questionnaire examines the strength of the relationship between such services. The client has to declare the portion of their enrolled services that depends on each supporting service (denoted as S_S), as far as their confidentiality, integrity and availability are concerned. The strength of the relationship $K^{(S_S \rightarrow S_E)}$ is defined as a 3×3 matrix with a numerical value for each pair of one of the three aspects. For example, in the context of the relationship between integrity and availability, this value indicates the impact of the integrity of the supporting service being compromised on the availability of the enrolled service. Such a relationship may be observed, for example, if one service aggregates data from other services

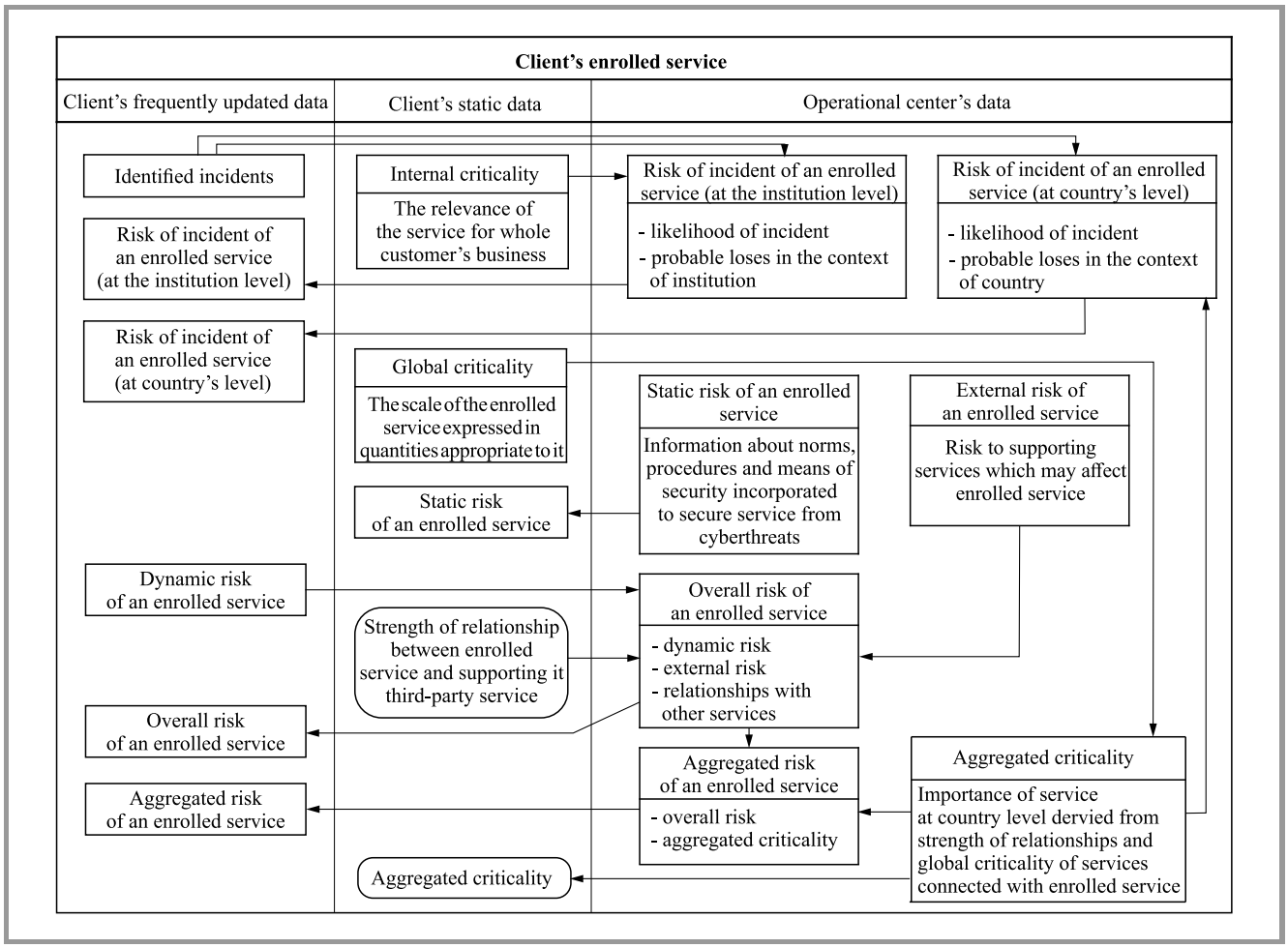


Fig. 1. Data flow between client and National Cybersecurity Platform's operations center.

to return some complex datasets. If one of the data pools loses its integrity, no access to the output dataset should be provided, as it may be based on invalid or missing data. If no such a relationship for a certain pair of aspects exists, the value in the matrix equals zero. The pairs of attributes whose consideration is mandatory are presented in Table 1.

Table 1

Strength of relationship matrices $K^{(S_S \to S_E)}$. Depending on the character of the connected services – enrolled and supporting service – different sets of pairs of aspects are mandatory to be considered by the client (marked with ✓)

		Supporting e-service			Supporting service		
		C	I	A	C	I	A
Enrolled e-service	C	✓	✓	✓	X	X	✓
	I	✓	✓	✓	X	X	✓
	A	✓	✓	✓	X	X	✓
Enrolled service	C	X	X	X	X	X	X
	I	X	X	X	X	X	X
	A	✓	✓	✓	X	X	✓

Moreover, the client has to declare how long his service is capable of running after a failure of one of the supporting services.

All information referred to above may be updated on a regular basis, for instance every six months or once a year, as well as when the client makes any changes to their organization that affect the previously stated answers. Such data are referred to as static. Information about the standards, procedures and means of security incorporated to protect the service against cyberthreats is used to calculate the static risk affecting the enrolled service – $R_{is}^{S_E}$. These calculations are performed by the NCP operations center.

Some information needs to be updated frequently. Clients will be receiving a definition of new vulnerabilities discovered in the software and hardware as soon as the NCP's operations center becomes aware of them. It is the client's responsibility to check if their IT infrastructure is prone to these vulnerabilities, and if so, the client has to update the dynamic risk indicator relevant for the enrolled service – $R_{id}^{S_E}$ as quick as possible and return the result to the NCP operations center. To calculate the dynamic risk value pertaining to a given service, the client has to follow instructions provided by National Cybersecurity Platform or use their own risk calculation method, provided it takes into

account the IT infrastructure and the presence of vulnerabilities. Dynamic risks may be valuable to the NCP client as they may identify IT assets that require extra attention in terms of cybersecurity and potential losses that may be suffered in the event of a compromise, with the context of the services supported by these assets taken into consideration. The client's reports on incidents detected in their infrastructure also constitute information that is important from the point of view of risk analysis. These incidents may be related to malware, cyberattacks, data security breaches or any other cyber threats that may interrupt or completely stop a given service. To help clients detect incidents, the NCP operations center will provide them with indicators of compromise (IoC) for known cyber threats. Knowledge about the number and severity of incidents detected by clients is used to calculate the risk of an incident affecting the service, in the context of the institution – $R_{iI}^{S_E}$ and the risk of an incident affecting the service in the context of the entire country – $R_{cI}^{S_E}$. These calculations are carried by the operations center.

5.2. Operations Center Level

The National Cybersecurity Platform's operations center collects dynamic risk values for all enrolled services. The knowledge of such values, as well as of details concerning relationships between services (reported by clients in questionnaires), the software used by the operations center is capable of calculating how the risk of one service affects the risk of associated services (the ones depending on the former service). This type of risk is referred to as external risk of the enrolled service – $R_e^{S_E}$. In conjunction with dynamic risk, external risk determines the overall risk affecting the enrolled service – $R_o^{S_E}$. These risks may help clients perceive their business in the context of a network of services.

Knowing the overall risk affecting the services and the importance of those services for the country's economy and for the continuity of other businesses, the NCP operations center may calculate the aggregated of all enrolled services – $R_a^{S_E}$. As this risk takes into account the importance of services at the national level ($C_a^{S_E}$), it helps analysts at the NCP operations center monitor the current level of risk of the vulnerabilities known to be existing in supervised services of being exploited. The aggregated risk of services is utilized to calculate the risk for economic sectors, groups of services or for the entire cyberspace. This will be elaborated on in the following section.

Analysts at the operations center will have access to statistics and data from sources other than the clients only. Such additional information will be presented on a per service basis, with the ability to aggregate it for a specific set of services (e.g. the entire cyberspace, an economic sector, etc.) in order to provide a quick security overview. Statistical data may be presented as trends, total and averages for a period of time defined by an analyst. Such statistics includes the following: number of incidents along with their severity, number of detected vulnerabilities and number of mitigated vulnerabilities. The system will also show an indicator related to ongoing cyber-attacks affecting specific services. Additional data from auxiliary sources includes events from the n6 database [9] and the results of automatic scans of hosts visible in the Internet. This information will be presented on a per-service or per-client basis, depending on how detailed the information about IP address space the client provides to NCP is.

5.3. Risk Propagation

As mentioned above, the NCP operations center will be able to calculate how the risk affecting one service may impact the risks pertaining to another service. Risk propagation may be monitored thanks to detailed information about the relationships between services. The idea of risk propagation is presented in Fig. 2. Each client has to describe the strength of the connection between their services and the support provided by third party services. Such an approach offers the most reliable data, as business owners have the best knowledge on the degree to which their services rely on others. Information about the connection may be very detailed, as it may describe how the fact of any aspect (confidentiality, integrity and availability) of the support service being compromised may impact any aspect of the enrolled service – up to 9 separate values of influence are distinguished (see Table 1).

The level of reliability of information about the relationships between services is a major but not the only problem experienced when monitoring risk propagation. The other problem consists in finding a solution to cyclic relationships between services. It is possible that one service relies on another which, in turn, depends on the first one – this creates a loop in the graph of relationships between services. In such a loop, the increase in the dynamic risk affecting one of the services will boost the overall risk as well. A higher overall risk will cause a higher external risk affecting the dependent service. This will lead to a growth in the overall risk of the dependent service (as overall risk is a combination of dynamic risk and external risk). This increase in the risk of one of the services would propagate infinitely over all services in the loop.

Software relied upon by the National Cybersecurity Platform uses a proprietary algorithm to propagate changes to risk values between services connected within loops, preventing such an infinite growth or reduction of risk due to propagation. This makes the results of risk analysis more realistic, as they take into account the fact the compromising of one of the services may propagate even to services which are not directly related.

5.4. High-level Situational Cybersecurity Awareness

One of the advantages of the National Cybersecurity Platform is the ability to aggregate the risks of a set of services. It helps analysts at the operations center to assess the security in cyberspace. An analyst may quickly check the risk

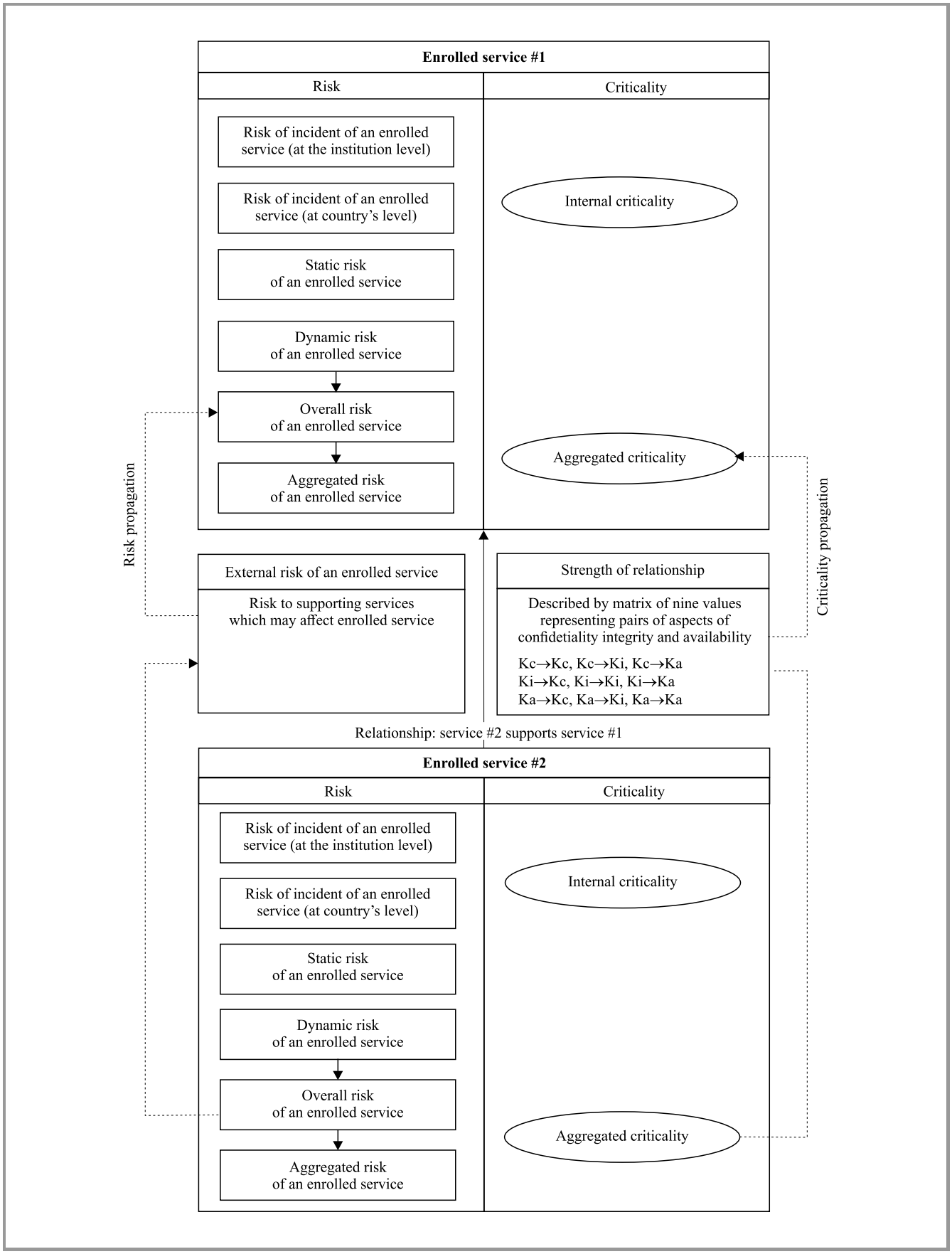


Fig. 2. Risk propagation diagram.

values for the entire cyberspace, for each economic sector or for any set of services.
Aggregation may also show some emerging threats affecting services in cyberspace. For example, analysts can easily spot if the overall risk is rising in a given economic sector. Such a situation may indicate that there is a new vulnerability of some element of the IT infrastructure (software or hardware) which is popular among services in the sector concerned.
In addition to risk aggregation, NCP will enable aggregating other information, such as reported incidents or data from external sources, as described above. For example, it may be helpful in identifying if cyber-attacks are aimed at a particular type of services or a specific industry, as it will identify the service for which the incident has been reported over the past few weeks.
Such a detailed insight into the level of risks experienced so far, as well as into incident reports, sightings and other security-related data, helps both analysts at the operations center and NCP clients manage their risk and keep the essential services safe from cyberthreats.

6. Summary and Future Work

To the best of the authors' knowledge, the approach proposed is the first which may be applied at the national level. The novelty of the approach is based on real-time risk analysis performed by clients at various levels. Because of a unified and quantitative methodology is used, the results may be aggregated on the national level. Based on the risk calculation approach proposed, one may foresee threats and build situational awareness by monitoring the current situation. The proposed approach requires further research and verification in the operational environment, but it seems to be rather promising.

Acknowledgements

Work done as part of the CYBERSECIDENT/369195/I/NCBR/2017 project supported by the National Centre of Research and Development in the frame of CyberSecIdent Programme.

References

[1] M. Janiszewski, A. Felkner, and J. Olszak, "Trust and risk assessment model of popular software based on known vulnerabilities", *Int. J. of Electron. and Telecommun.*, vol. 63, pp. 329–336, 2017 (doi: 10.1515/eletel-2017-0044).

[2] IBM OpenPages with Watson [Online]. Available: https://www.ibm.com/us-en/marketplace/governance-risk-and-compliance (accessed 23.11.2018).

[3] Data Center Management and Network Management Software from Device42 Software [Online]. Available: https://www.device42.com/ (accessed 23.11.2018).

[4] Helix Discovery – BMC Software [Online]. Available: https://www.bmc.com/it-solutions/discovery-dependency-mapping.html (accessed 23.11.2018).

[5] Asset Inventory [Online]. Available: https://www.qualys.com/apps/asset-inventory/ (accessed 23.11.2018).

[6] Integrated Risk Management [Online]. Available: https://www.rsa.com/en-us/products/integrated-risk-management (accessed 23.11.2018).

[7] Products by Category – ServiceNow [Online]. Available: https://www.servicenow.com/products-by-category.html (accessed 23.11.2018).

[8] NECOMA [Online]. Available: http://www.necoma-project.eu/ (accessed 26.11.2018).

[9] n6 – network security incident exchange [Online]. Available: https://n6.cert.pl/ (accessed 26.11.2018).

[10] PhishTank [Online]. Available: https://www.phishtank.com (accessed 26.11.2018).

[11] NECOMA Nippon-European Cyberdefense-Oriented Multilayer threat Analysis "Deliverable D1.4: Threat Data Final Report" April 20th, 2016 [Online]. Available: http://www.necoma-project.eu/m/filer_public/55/ec/55ec2e53-14fa-40f4-a67f-c7a092cfe463/necoma-d14.pdf (accessed 26.11.2018).

[12] NECOMA Nippon-European Cyberdefense-Oriented Multilayer threat Analysis "Deliverable D3.1: Policy Enforcement Point Survey" November 30th, 2013 [Online]. Available: http://www.necoma-project.eu/m/filer_public/0e/75/0e75c773-a857-416b-99a0-090ec0b38388/necoma-d31r207.pdf (accessed 26.11.2018).

[13] PANOPTESEC [Online]. Available: http://www.panoptesec.eu (accessed 26.11.2018).

[14] PANOPTESEC Dynamic Risk Approaches for Automated Cyber Defence "D3.1.2: System High Level Design" March 27th, 2015 [Online]. Available: http://www.panoptesec.eu/dissemination/FP7-ICT-610416-PANOPTESEC_D312_v2.0-QA-Approved.pdf (accessed 26.11.2018).

[15] PANOPTESEC Dynamic Risk Approaches for Automated Cyber Defence "D5.1.1 – Response System for Dynamic Risk Management Requirements" March 27th, 2015 [Online]. Available: http://www.panoptesec.eu/dissemination/FP7-ICT-610416-PANOPTESEC_D511_v2.1-QA-Approved.pdf (accessed 26.11.2018).

[16] PANOPTESEC Dynamic Risk Approaches for Automated Cyber Defence "D6.3.2: Visualization Integration Prototype Report" June 30th, 2016 [Online]. Available: http://www.panoptesec.eu/dissemination/FP7-ICT-610416-PANOPTESEC_D632_v1.0-QA-Approved.pdf (accessed 26.11.2018).

[17] PANOPTESEC Dynamic Risk Approaches for Automated Cyber Defence "D7.4.2 Demonstration System Prototype Report" November 5th, 2016 [Online]. Available: http://www.panoptesec.eu/dissemination/FP7-ICT-610416-PANOPTESEC_D742_v1.1.pdf (accessed 26.11.2018).

[18] Deliverables [Online]. Available: https://cyberwiser.eu/deliverables (accessed 26.11.2018).

[19] CYBERWISER.eu – Cyber Range & Capacity Building in Cybersecurity [Online]. Available: https://www.cyberwiser.eu (accessed 26.11.2018).

[20] Wide – Impact cyber Security Risk framework "D3.1 – Cyber Risk Patterns" May 31st, 2016 [Online]. Available: https://cyberwiser.eu/system/files/WISER_D3_1_v10_0.pdf (accessed 26.11.2018).

[21] Wide – Impact cyber Security Risk framework "D3.4 Cyber Risk Modelling Language and Guidelines, Final Version" March 29th, 2017 [Online]. Available: https://cyberwiser.eu/system/files/WISER_D3_4_v10_0.pdf (accessed 26.11.2018).

[22] Protective – Proactive Risk Management through Improved Cyber Situational Awareness [Online]. Available: https://protective-h2020.eu (accessed 26.11.2018).

[23] PROTECTIVE Proactive Risk Management through Improved Cyber Situational Awareness "D6.1 Framework Specification" June 28th, 2017 [Online]. Available: https://protective-h2020.eu/wp-content/uploads/2017/07/PROTECTIVE-D6.1-E-0417-Framework-Specification.pdf

[24] PROTECTIVE Proactive Risk Management through Improved Cyber Situational Awareness "D2.1 Requirements Capture, Specification, Architectural Design and Model" June 15th, 2017 [Online]. Available: https://protective-h2020.eu/wp-content/uploads/2017/07/PROTECTIVE-D2.1-E-0615-Requirements_Architecture.pdf (accessed 26.11.2018).

[25] "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union" [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&rid=1

[26] A. Felkner, "Przegląd i analiza źródeł informacji o podatnościach (Review and analysis of sources of information about vulnerabilities)", *Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne*, vol. 8-9/2016, 2016, pp. 929–933 (doi: 10.15199/59.2016.8-9.37) [in Polish].

Marek Janiszewski is a Research Associate on the Information Security Methods Team in the R&D division at Research and Academic Computer Network NASK. His research interests include intrusion detection systems, penetration testing, personal data and identity management and trust and reputation management systems. He is preparing his Ph.D. thesis at the Telecommunication Institute, Warsaw University of Technology.

https://orcid.org/0000-0001-8965-6302
E-mail: marek.janiszewski@nask.pl
Information Security Methods Team
Research and Academic Computer Network (NASK)
Kolska 12
01-045 Warsaw, Poland

Anna Felkner holds a Ph.D. degree in Information Technology from the Warsaw University of Technology and an M.Sc. degree from Bialystok University of Technology. She is an Assistant Professor and head of the Information Security Methods Team. Her interests include access control, trust modeling, risk analysis and vulnerability management. She is the author of over forty publications, has spoken at many conferences.

https://orcid.org/0000-0003-3813-4840
E-mail: anna.felkner@nask.pl
Information Security Methods Team
Research and Academic Computer Network (NASK)
Kolska 12
01-045 Warsaw, Poland

Piotr Lewandowski is a specialist on the Information Security Methods Team in the R&D division at Research and Academic Computer Network NASK. His research interests include practical aspects of personal and enterprise networks' security. He received an M.Sc. in Physics from the Warsaw University of Technology.

https://orcid.org/0000-0003-0964-6812
E-mail: piotr.lewandowski@nask.pl
Information Security Methods Team
Research and Academic Computer Network (NASK)
Kolska 12
01-045 Warsaw, Poland

Paper

Critical Infrastructure Risk Assessment Using Markov Chain Model

Andrzej Karbowski, Krzysztof Malinowski, Sebastian Szwaczyk, and Przemysław Jaskóła

Research and Academic Computer Network (NASK), Warsaw, Poland

https://doi.org/10.26636/jtit.2019.130819

Abstract—The paper presents application of the Markov chain model to assess the risk affecting critical national infrastructure. A method for relating different service states to transition probabilities is shown. Then, a real-life example is thoroughly analyzed. Finally, results of a numerical test concerning this problem are provided.

Keywords—cybersecurity, Markov chains, networks, NIS Directive, simulation.

1. Introduction

As stated in Directive (EU) 2016/1148 of the European Parliament and of the Council of the European Union [1], magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of networks and information systems. Those systems may also become a target of deliberate harmful actions intended to damage or interrupt their operation. Such incidents may impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy. The security of network and information systems is explained in [1] as the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data, as well as of the related services offered by or accessible via such network and information systems. Any reasonably identifiable circumstances or events exerting a potential adverse effect on the security of network and information systems are defined as risk.

The European IEC/ISO 31010 Standard [2], being the main document concerning risk assessment and risk management (i.e., the measures to identify the risk of specific incidents, as well as to prevent, detect and handle such incidents and to mitigate their impact), lists as many as 31 risk assessment techniques including, inter alia: Delphi method, hazard analysis and critical control points, scenario analysis, fault tree analysis, event tree analysis, reliability centered maintenance, Markov analysis, Bayes nets. A review of various risk analysis methods used in network applications may be found in [3].

Markov analysis seems to be one of the most promising approaches adopted in the domain of network and information systems – it is used when the probability distribution of a future state of a system depends upon the distribution of its present state [4]. In this work we take into account the most important criterion – availability – understood as the ability of an ICT service to perform its agreed function when it is required. Availability is defined by reliability, reparability, ability to provide the service, efficiency and security.

2. Application of the Markov Chain Model in the Cybersecurity

The basic idea behind the concept of a detection and prevention system is to attempt to provide information about potential events that have not yet taken place, depending on the current and historical knowledge about the same or similar events that occurred in the past. The more actual data are available, the more accurate predictions should be generated, and the evaluation of the consequences of future incidents will be more realistic.

In the case of multistage processes with a finite number of possible states, the Markov chain model is an attractive option. In particular, this model is more general than the Bayesian network model which refers to directed (rather small) and acyclic graphs (DAG), because it allows feedback.

When building a dynamic discrete Markov process model, we introduce a finite set of states $S_i, i \in I$ in which the system may be at a given stage (time interval) [4]. Next, we estimate the probabilities of transitions between states in the successive stages, corresponding to successive time intervals. The probabilities $p_{ij}(k) = P(S_j(k+1)|S_i(k), m(k))$ of transition from state S_i in stage (time instant) k to the state S_j in stage $k+1$ may depend on the external values $m(k)$ concerning, for example, emerging threats, such as possible failures of supporting services or actions enhancing security of the system. If at instant k one can determine the current state of the system, then for a given number of consecutive moments, one may perform a simulation analysis of the future behavior of the system.

Being able to modify the values of transition probabilities, we can influence the evolution of events. In the case of fixed p_{ij} values, we can determine the probability of the system reaching certain states in the long term, by solving a system of $\bar{\bar{I}}$ linear equations.

An interesting method of assessing the risk affecting a system model, having the form of a Markov chain, was proposed by Afful-Dada and Allen [5]. They introduced a cost function for various decisions related to defense against threats. Using transition matrices, they count not only the expected value of the cost (in their case it is a formulation with an infinite time horizon and a discount), but also its variance, and then they illustrate both on a box-and-whisker plot.

In article [6], an innovative probabilistic approach is proposed, called advanced probabilistic approach for network-based intrusion detection systems (APAN). It does not only detect the presence of an attack. It also provides an assessment of the degree of its risk, using a probability scale.

The paper by Ye *et al.* [7] presents a technique to detect cyberattacks by detecting anomalies, and discusses robustness of the modeling technique applied. In this technique, the Markov chain model represents the profile of network event transitions under the system's normal operating conditions (the so-called normal profile). The lower the probability that the observed effects are consistent with the Markov chain model for the normal profile, the more likely it is that the observed effects are anomalies resulting from cyberattacks and vice versa.

Here, we use the Markov chain model for states defined in a way that is similar to those used in the works mentioned above, and assess the risk of unfavorable events through calculation of an indicator concerning availability, which is a function of the current state of the system. The situation is assessed, as in [8], from the point of view of a nationwide Operations Center (OC).

3. Threat Imaging Model

Let us introduce a description of a dynamic model in the form of a Markov chain operating a set of discrete states characterizing the behavior of a given service. The transition from one state to another may take place under the influence of events observed in the local digital space, as well as in connection with events regarding the information systems of other services.

The basic state of the service r model is the state S_0^r in which we deal with the normal situation. We assume that $r = 1,\ldots,R$. In this state, of course, there are threats, including those related to IT space (both to the local part of this space and to IT systems of other platform participants).

As a result of the materialization (in different scales) of these threats, the state of service r may change. Then, transition to a state S_i^r occurs, which indicates an appropriately increased state of emergency. Let us assume that level i may take values from 0 (normal situation) to n^r (state of the highest threat in the field of cybersecurity). The subsequent states may be, in particular, related to the breach of availability of the relevant elements of IT systems. The number of states may be different for the models of individual services, allowing to increase the flexibility of the proposed description.

Let us also assume that state $S_{n^r+1}^r$ corresponds to the extreme (critical) situation in which the provision of a given service is no longer possible, at least at the lowest satisfactory level. This state, from the point of view of the cybersecurity analysis, may be considered as terminal. After it has been achieved, further activities related to a given service must take place on a different plane.

The transition from state $S^r(k) = S_i^r$ at a given moment (stage) k, to $S^r(k+1) = S_j^r$ at moment $k+1$, where $j > i$ or $j < i$, takes place with a given probability $p_{ij}^r(k)$, which may be dependent on the state of other services at time k, i.e., on:

$$S^{-r}(k) = (S^1(k),\ldots,S^{r-1}(k),\, S^{r+1}(k),\ldots,S^R(k))\,, \quad (1)$$

as well as on some external variables concerning, for instance, potential failures of supporting services or actions enhancing system security at OC level that we may mark as $m(k)$. Thus

$$p_{ij}^r(k) = p_{ij}^r(S^{-r}(k), m(k)). \quad (2)$$

In fact, in the case of service r, only a subset of the entire set of states of other services $S^{-r}(k)$ should be considered, limited to those services on which service r depends.

We will further consider vector $S^{-r}(k)$ in this sense. In turn, service r may exert an impact on other services. The period of time between consecutive transition moments k and $k+1$ is assumed to be fixed.

In the simplest case, it may be assumed that the sets of all possible states for all services have the same number of elements, that is:

$$n^1 = n^2 = \ldots = n^R = n \quad (3)$$

and

$$\bar{\bar{I}}^1 = \bar{\bar{I}}^2 = \ldots, = \bar{\bar{I}}^R = n+2\,, \quad (4)$$

where I^r is the set of all possible states of the service $r = 1,\ldots,R$. Then, the Markov chain equation for stage probability distributions may be written in the matrix form:

$$\pi(k+1)^T = \pi(k)^T P(k)\,, \quad (5)$$

where $\pi(k)$ is the vector of probabilities of all possible state level combinations of dimension $(n+2)^R$ and $P(k)$ are $(n+2)^R \times (n+2)^R$ matrices build of $p_{ij}^r(k)$ given by Eq. (2).

Such a description allows us to illustrate well the general situation, assuming that at a given stage the OC knows the states of models of particular system services. It is

possible to assign to these services various criticalities corresponding to the assessment of the relative importance of a given service from the point of view of the functioning of the entire state organism.

The basic difficulty associated with the presented approach lies, of course, in determining the subsequent time stages k, including the intervals between the successive moments, and in estimating the probability values $p_{ij}^r(S^{-r}(k),m(k))$. One may consider obtaining such estimates as unrealistic and, therefore, reject the proposed approach. However, the question arises what it should be replaced with, while maintaining the ability to perform a dynamic assessment of the situation and to generate sensible recommendations. In particular, there is no other way to enable the OC to conduct simulation analyses related to the future behavior of the entire IT infrastructure.

It must be admitted that the estimation of the required probabilities will be, to some extent, of subjective and coarse nature, especially during the initial period of the operation. The introduction of different variants of these estimates, corresponding to more or less cautious assessments, is also possible. Of course, the information needed for this purpose must be provided by the operators of individual services. In particular, knowing actions $m(k+l)$ for subsequent stages, e.g., $l = 1,\ldots,L$, proposed by the OC, the operator of a given service r should be able to present the operator's estimate of value $p_{ij}^r(S^{-r}(k+l),m(k+l))$ at time $k+l$, taking into account the impact of the current state of other services, or rather the IT systems of these services, on possible changes in the status of its part of the model used at the OC level. In particular, the terminal state of a relevant auxiliary service will have a very significant impact on the probabilities of adverse changes in the service status.

At this point, it is worth noting that current state $S^r(k)$ of service r, transferred to the OC level, will in fact be an appropriate aggregate of a much more detailed depiction of the status of a given service considered at the level of its operator. This means that the operator must play a leading role in determining the structure and parameters of the service model used by the OC. In this approach, descriptions of individual services may be modified as and when a need arises.

4. A Real Life Example

Let us suppose that we are considering a system in which a service corresponding to $r = 1$ means the provision of health care services by, say, a specific hospital. Service $r = 2$ is related to the supply of electricity to the network to which the hospital is connected. Of course, the hospital may use, in the case of a failure resulting in the lack of energy supply, its own electricity generator. However, let us assume that the generator's capabilities are limited and, at least in the long term, it may happen that the hospital will suspend the provision of all or at least a significant portion of medical services in the absence of energy supplied from the external network.

Thus, we consider a system composed of two entities, i.e., $r = 1,2$. Let us distinguish, in the case of each service, outside of the normal state (labeled with "0"), only one state of heightened IT risk (labeled with "1"), related to, say, an identified violation of susceptibility from a particular set, i.e., $n^1 = n^2 = 1$, and, of course, the state of inability to provide this service (labeled with "2"). Let us assume that the threat (including of IT-related nature) of service 1 depends on the current state of service 2, while service 2 does not depend on the condition of service 1.

Let us suppose that one may estimate, based on the analysis carried out at the level of operators, in the system's normal state, described by pair (S_0^1,S_0^2), the probabilities of an increased risk of relevant IT infrastructures, i.e., respectively, $p_{01}^1(S_0^2) = 0.01$ and $p_{01}^2(S_0^1) = p_{01}^2(S_1^1) = p_{01}^2(S_2^1) = p_{01}^2 = 0.005$ (we assume that S^1 has no influence on S^2). Let at the same time $p_{02}^1(S_0^2) = 0.001$ and $p_{02}^2(S_0^1) = p_{02}^2(S_1^1) = p_{02}^2(S_2^1) = p_{02}^2 = 0.001$ – we assume that in the normal state, the probability of withholding the services in question is very small. The values of probabilities refer to, say, the time interval between moments k and $k+1$ equaling one day. In the case of changing the time scale considered in our model, these values have to be changed accordingly.

Then, in the situation when $S^1(k) = S_0^1$ but $S^2(k) = S_1^2$, i.e., an increased risk has taken place in the service model associated with the delivery of energy, we evaluate $p_{01}^1(S_1^2)$ equal to 0.1. In this case an increased risk of information services 2 associated with the observed digital attack and the violation of the corresponding susceptibility of the operator of the service increases the potential threat to service 1. At the same time we can estimate $p_{02}^1(S_1^2)$ as equal to 0.05 – we seriously expect that the observed increased risk of service 2 ($S^2(k) = S_1^2$) makes it possible to suspend the provision of service 1.

Further, when $S^1(k) = S_0^1$ but $S^2(k) = S_2^2$, i.e., service 2 is not provided, we assess $p_{01}^1(S_2^2)$ as also equal to 0.1, but, at the same time $p_{02}^1(S_2^2) = 0.4$ – the probability of interrupting the operation of the hospital is high. This means that the lack of service 2 does not influence, in itself, the state of IT security of service 1, but substantially decreases the ability to maintain service 1. If we are able to determine, in a similar manner, the value of the probability p_{12}^2, e.g., $p_{12}^2 = 0.2$, and of other necessary probabilities, including the return to normal states $p_{10}^1(S_0^2)$, $p_{10}^1(S_1^2)$, $p_{10}^1(S_2^2)$, $p_{20}^1(S_0^2)$, $p_{20}^1(S_1^2)$, $p_{20}^1(S_2^2)$ and finally p_{10}^2 and p_{20}^2, we can, starting from any state at time k, conduct further simulation analysis of the system behavior. We can also calculate stationary probabilities which allow to assess the long-term behavior of the entire system if external and internal conditions remain unchanged.

This example clearly shows how many values of relevant probabilities need to be estimated in order to be able to dynamically analyze the development and propagation of threats. It seems that little can be done about it. It is nec-

essary to count on the fact that the development of threats within a given service will actually depend on the condition of a few other services. This should, to a large extent, alleviate the difficulty of estimating a large number of probabilities. The example also shows that dynamic threat analysis limited to the analysis regarding the nearest time perspective in the currently observed condition of services only, requires knowledge of the values of probabilities related to this state. If, suppose, our exemplary system is currently in state $S^1(k) = S_0^1, S^2(k) = S_1^2$, then, for such an analysis, we need to know the values of p_{10}^2, p_{12}^2 and, as specified above, $p_{01}^1(S_1^2)$ and $p_{02}^1(S_1^2)$. In particular, knowing the approximate values of these probabilities, we can, being also aware of the short-term effects of individual states expressed in the appropriate scale, determine the expected value of these effects, i.e., the degree of a given risk.

5. Implementation and a Numerical Test

In order to test the behavior of the Markov model presented above, it was implemented using Java language and Java FX framework. It is concerned with the availability aspect of two services considered in Section 4, but, for simplicity, we assumed that they both have two states only: normal (labelled with "0") and failure (labelled with "1"). In other words, we assumed that there are no higher threat states ($n^1 = n^2 = 0$). The two services from Section 4 are Energy supply provided by Power plant in Energy sector and Health care provided by Hospital in Health sector. The relationship between them is depicted, in the form of a graph, in Fig. 1.

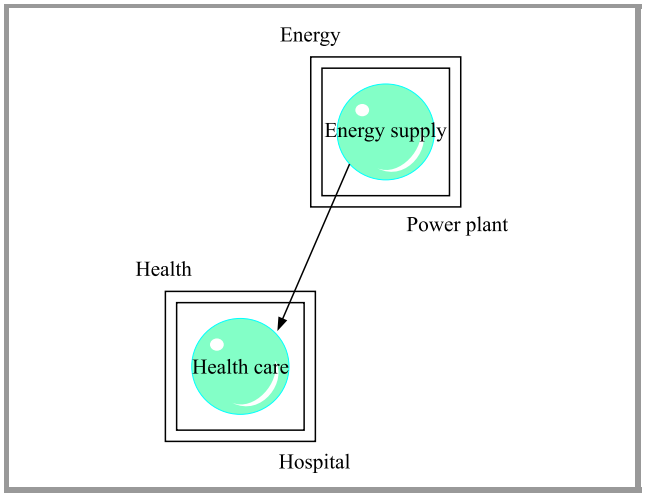


Fig. 1. Graph depicting the services.

When configuring the model, the user enters the number of iterations (stages), the transition matrix P and the vector of initial input probabilities $\pi(0)$. If we assume that each service can have two states, this matrix will be of size 4×4 (Fig. 2). Accordingly, the vector of input probabilities has 4 elements (Fig. 3).

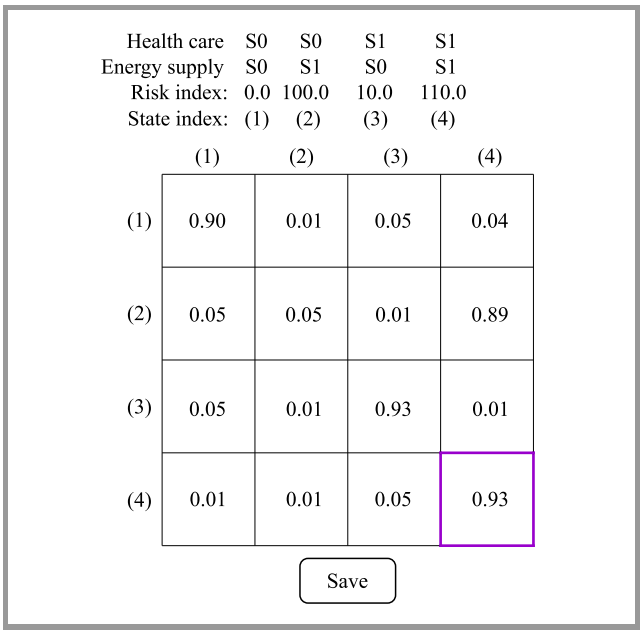


Fig. 2. Transition matrix.

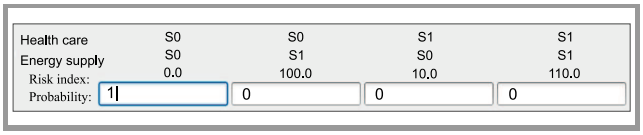


Fig. 3. Probabilities and risk index vector.

There is also a certain cost, here named "risk index", of being in state S. It will be denoted hereafter by $g(S)$. The total level of risk R at time k can be interpreted as the expected value of this cost:

$$R(k, S(0)) = R\left(k, [S^1(0), S^2(0)]\right) = \mathop{\mathbf{E}}_{S(k)} g(S(k)) \ . \qquad (6)$$

The vector of probabilities π and the value of R were calculated for subsequent iterations $k = 1, 2, \ldots$. They are presented in Fig. 4 and Fig. 5, respectively. For example, for $k = 10$, $\pi^T = [\mathbf{0.4252} \quad \mathbf{0.0104} \quad \mathbf{0.2983} \quad \mathbf{0.2661}]$ and $R = \mathbf{33.29}$.

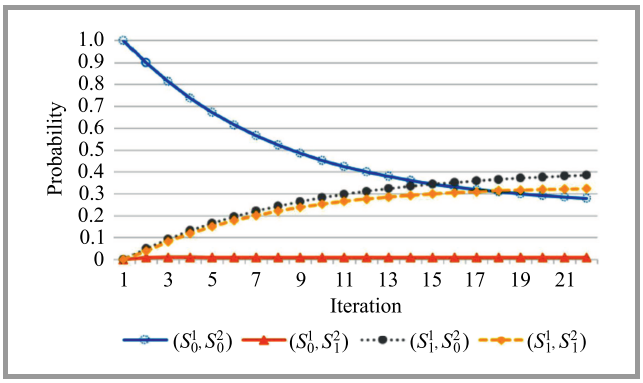


Fig. 4. Time series of probabilities of different states of the Markov chain.

It is clearly visible, that the probability of the system staying in the initial "sane" state decreases with time. Also, the probability of the service S^1 being available despite the service S^2 being shut down remains very low, regardless of time (line labeled (S_0^1, S_1^2) in Fig. 4).

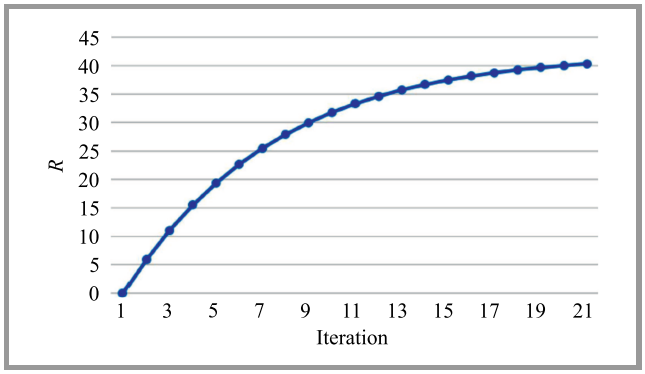


Fig. 5. Time series of the total risk level R.

The written shell is general and has a convenient graphic interface. It is easily configurable and can be used to model much more complicated systems.

6. Perspectives

The model was created as part of the National Cybersecurity Platform (NCP) project. In addition to offering other functionalities, the platform is responsible for simulation and modeling of interactions between critical services, especially through ITC infrastructure, in a way similar to the SACIN framework described in [8].

The data necessary for creating the model of interconnections are collected through a survey. The provision of a full probability matrix is unlikely with this method. A mechanism mapping the strength of connections between the services declared in the questionnaires and the Markov model must be created. Moreover, the influence of one service on the other is expressed with three dimensions taken into consideration: confidentiality, integrity and availability, following the general pattern described, for instance, in [9], while the model presented above deals with availability only.

7. Conclusions

Application of Markov chains is one of the most promising approaches to modeling the propagation of risky events in the area of cybersecurity. In this model, states represent the possible levels of security of different services assessed from the point of view of their availability.

This model has been implemented and preliminarily tested on an example concerning two services: healthcare and power supply. It must be significantly expanded to address the full range of NCP-related needs.

Acknowledgements

Work on the paper has been performed as part of the CYBERSECIDENT/369195/I/NCBR/2017 project supported by the National Center for Research and Development in the frame of CyberSecIdent Programme.

The yFiles for JavaFX diagramming library yWorks GmbH was used to create the diagrams Figs. 1–3 presented in the paper (https://www.yworks.com/products/yfiles-for-javafx). The authors wish to thank yWorks GmbH for offering this opportunity.

References

[1] "Directive (EU) 2016/1148 of The European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union", The European Parliament and the Council of the European Union, *Official Journal of the European Union*, vol. 59, pp. L194/1–L194/30, 2016 [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[2] IEC/ISO 31010 "Risk management – Risk assessment techniques", International Organization for Standardization, International Electrotechnical Commission, Geneva, 2009 [Online]. Available: https://www.iso.org/obp/ui#iso:std:iec:31010:ed-1:v1:en

[3] S. Szwaczyk, K. Wrona, and M. Amanowicz, "Applicability of risk analysis methods to risk-aware routing in software-defined networks", in *Proc. Int. Conf. on Milit. Commun. and Inform. Syst. ICMCIS 2018*, Warsaw, Poland, 2018 (doi: 10.1109/ICMCIS.2018.8398688).

[4] M. L. Puterman, *Markov Decision Processes: Discrete Stochastic Dynamic Programming*. Wiley, 2014 (ISBN: 9780471619772).

[5] A. Afful-Dada and T. T. Allen, "Data-driven cyber-vulnerability maintenance policies", *J. of Qual. Technol.*, vol. 46, pp. 234–250, 2014 (doi: 10.1080/00224065.2014.11917967).

[6] S. Shin, S. Lee, H. Kim, and S. Kim, "Advanced probabilistic approach for network intrusion forecasting and detection", *Expert Syst. With Appl.*, vol. 40, pp. 315–322, 2013 (doi: 10.1016/j.eswa.2012.07.057).

[7] N. Ye, Y. Zhang, and C. M. Borror, "Robustness of the Markov-chain model for cyber-attack detection", *IEEE Trans. on Reliabil.*, vol. 53, pp. 116–123, 2004 (doi: 10.1109/TR.2004.823851).

[8] S. Puuska *et al.*, "Nationwide critical infrastructure monitoring using a common operating picture framework", *Int. J. of Critical Infrastruc. Protect.*, vol. 20, pp. 28–47, 2018 (doi: 10.1016/j.ijcip.2017.11.005).

[9] K. Wrona, S. Oudkerk, S. Szwaczyk, and M. Amanowicz, "Content-based security and protected core networking with software-defined networks", *IEEE Commun. Mag.*, vol. 54, pp. 138–144, 2016 (doi: 10.1109/MCOM.2016.7588283).

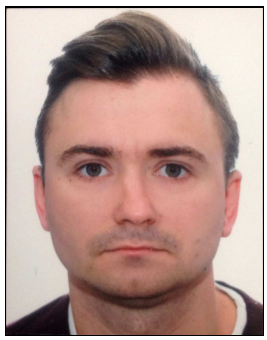
Andrzej Karbowski received his Ph.D. (1990) and D.Sc. (2012) in Automatic Control and Robotics from the Warsaw University of Technology, Faculty of Electronics and Information Technology. Currently he is an Associate Professor at the Institute of Control and Computation Engineering of Warsaw University of Technology and at

the Research and Academic Computer Network (NASK). He is the editor and the co-author of two books (on parallel and distributed computing), the author and the co-author of two e-books (on grid computing and optimal control synthesis) and of over 130 journal and conference papers. His research interests concentrate on optimal control, data networks management, cybersecurity, decomposition and parallel implementation of optimization algorithms.

https://orcid.org/0000-0002-8162-1575
E-mail: Andrzej.Karbowski@nask.pl
Research and Academic Computer Network (NASK)
Kolska 12
01-045 Warsaw, Poland

Krzysztof Malinowski Prof. of Techn. Sciences, D.Sc., Ph.D., M.Eng., Professor emeritus of control and information engineering at the Warsaw University of Technology. Malinowski was the former Research Director at NASK, and then the CEO of NASK. He is the author or co-author of four books and over 160 journal and conference papers. For many years he was involved in research on hierarchical control and management methods. He was a visiting professor at the University of Minnesota. He also served as a consultant to the Decision Technologies Group of UMIST in Manchester (UK). Prof. K. Malinowski is also a member of the Polish Academy of Sciences.

https://orcid.org/0000-0002-7655-2050
E-mail. Krzysztof.Malinowski@nask.pl
Research and Academic Computer Network (NASK)
Kolska 12
01-045 Warsaw, Poland



Sebastian Szwaczyk received his M.Sc. degree in Telecommunication Engineering from the Military University of Technology, Warsaw, Poland in 2015. Currently he is a Ph.D. student in the Military University of Technology, Warsaw. His research interests include software engineering, computer engineering, communications protocols, network management, and virtualization.

https://orcid.org/0000-0002-3657-4685
E-mail: sebastian.szwaczyk@nask.pl
Research and Academic Computer Network (NASK)
Kolska 12
01-045 Warsaw, Poland

Przemysław Jaskóła received his M.Sc. in Automatic Control and Robotics from the Warsaw University of Technology, Poland, in 1999. He works as a research associate at the Research and Academic Computer Network (NASK). His current research interests focus on cybersecurity, modeling and multicriteria optimization of computer networks.

https://orcid.org/0000-0002-0562-1602
E-mail: pjaskola@nask.pl
Research and Academic Computer Network (NASK)
Kolska 12
01-045 Warsaw, Poland

Paper

On Preventing and Detecting Cyber Attacks in Industrial Control System Networks

Adam Padée, Michał Wójcik, Arkadiusz Ćwiek, Konrad Klimaszewski, Przemysław Kopka, Sylwester Kozioł, Krzysztof Kuźmicki, Rafał Możdżonek, Wojciech Wiślicki, and Tomasz Włodarski

National Centre for Nuclear Research, Otwock, Poland

https://doi.org/10.26636/jtit.2019.131219

Abstract—This paper outlines the problem of cybersecurity in OT (operations/operational technology) networks. It provides descriptions of the most common components of these systems, summarizes the threats and compares them with those present in the IT domain. A considerable section of the paper summarizes research conducted over the past decade, focusing on how common the problem is and in which countries it prevails. The article presents techniques most commonly used in the protection of these systems, with many examples from the nuclear industry given.

Keywords—attack preventing, cybersecurity, industrial control systems.

1. Security of Industrial Control Systems

It is common belief that cybersecurity threats affect primarily typical IT systems, such as databases, web servers or corporate LANs, and that the main focus of cybercriminals is on confidential information stored in these systems. This image somewhat overshadows an equally important question of the security of Industrial Control Systems (ICS). The approach to the issue has begun to change recently, with the discovery of Stuxnet worm and with the subsequent publication of Blackout – a novel by Marc Elsberg. Cybersecurity of ICS has been gaining more and more public attention since that time. Despite such a recent growth in popularity, security issues related to ICS have a much longer history. It dates back to the year 1982, when CIA agents, in response to the large-scale efforts of the soviet National Security Committee (KGB) to bypass the embargo and steal Western technology, designed special software, installed it on programmable logic controllers through a chain of fictitious companies, and sold them to Russians. This has eventually led to a huge explosion of the Trans-Siberian gas pipeline, severely affecting the Soviet economy [1]. This historical example is interesting, because it shows that neither the Internet (which did not exist at that time in its current form), nor direct access to the facility being targeted are necessary to perform a successful attack.

Another interesting example is a local Polish case that is much more recent than the previous one, as it occurred in 2008 in Łódź. A fourteen-year-old boy modified an old TV remote and used it to arbitrarily change the settings of the city tram system switch points. Using this device, he caused several road accidents and tram collisions. As he testified later, he did it "just for fun", and he got the knowledge necessary to build the remote talking to old engineers at tram depots.

This example shows that no extensive resources are necessary to exploit an ICS, and that there are more ways to attack an ICS than just via a typical IT system or network [2]. This problem has been gaining in importance, as with advances in automation, more processes vital to the economy can be targeted by cybercriminals. It is also harder to protect them by physical isolation, because many of these systems require constant external control and updates from the outside.

Technically, there are two types of advanced, distributed ICSs: Supervisory Control And Data Acquisition (SCADA) and Distributed Control Systems (DCS). They share many common features, and the boundary between them is not sharp, but it is usually assumed that SCADA systems focus on data gathering, while their DCS counterparts – on

Table 1
ICS systems components

Low level (field devices)	High level (central systems)
PLC – Programmable Logic Controller	HMI – Human-Machine Interface
RTU – Remote Terminal Unit	FEP – SCADA servers
IED – Intelligent Electronic Device	Front End Processors
	Historians (for storing logs, etc.)

processes. This implies that DCSs are process state driven, and SCADAs are event driven. This makes DCSs harder to protect, because disturbing process continuity or integrity may lead to severe consequences. There are several components of these systems that have standard names which are abbreviated in the same way. The most popular of them are shown in Table 1.

SCADA and DCS systems may ultimately serve the same purpose, but while SCADA vendors concentrate on providing higher-level functions and human operator interaction, and assume that lower-level components can be provided by different vendors as long as they implement standard protocols, DCS solutions are generally sold as a whole, with low-level control elements included. DCS systems may use proprietary protocols for internal communication. They may be supplemented with some high-level application servers and SCADA components from other vendors, but the core of the system remains homogenous.

The ISO/IEC 27005 (Information Technology – Security Techniques – Information Security Risk Management) standard defines vulnerability as "a weakness of an asset or group of assets that can be exploited by one or more threats", where "assets" are defined as anything that has a non-zero value to the organization. This definition, contrary to more specific ones, e.g. those used by the Internet Engineering Task Force, is so general that it can be applied to ICS and IT systems alike. The main difference appears to be in the relative value of the assets (listed in Table 1). In IT systems, the threat hierarchy is described with the CIA acronym: confidentiality, integrity, availability. The order of the threats reflects their importance. Usually, the most severe consequences are associated with information leaks (which are, in most cases, irrecoverable), then with breaching the system's integrity (which can be restored using backups or through system reinstallation), and ultimately with rendering the system inaccessible, e.g. by means of a Distributed Denial of Service (DDoS) attack which often requires considerable resources and is effective only as long as the attack takes place. In ICS the threats are similar, but their hierarchy is reversed (AIC instead of CIA), because availability of the system has usually the biggest influence on safety, especially for DCS. The biggest risks are associated with rendering the system inoperable, because it means losing control over industrial processes and may lead to catastrophic consequences.

Unauthorized alteration of the system's state is the second item in the list. It may lead to severe implications as well, but if the system is still operational, more or less successful countermeasures may be immediately applied by the facility staff, thus minimizing the negative consequences. ICSs are also equipped with many independent safety devices and procedures, so it is hard for the attacker to turn them all off. This minimizes the impact of unauthorized alterations as long as the system remains operational as a whole. Information loss is by far the least important factor – information stored in ICSs comprises mainly monitoring data and logs. Someone may use this data to gather some knowledge about the system and launch a more successful attack in the future, but disclosure of this information does not pose any immediate risks to the process.

There is also a difference at the other end of the definition, concerning "weakness". In IT systems, especially in lower layers of the OSI model, we have just a few standardized and well described protocols, such as Ethernet, IP, TCP/UDP etc. In ICS, in turn, the situation is a bit more complicated, because many vendors of the components listed in Table 1 utilize their own, proprietary protocols which are not disclosed to the general public. This makes the security analysis of the system harder and means that many more unknown factors need to be dealt with. Another problem consists in inherent lack of security of some of the protocols used in ICSs, even those that are open standards with publicly available specifications. The very popular Modbus protocol may serve as a perfect example here. It originates from simple point-to-point serial connections, so it lacks any encryption and security mechanisms, but now is commonly used over Ethernet networks[1]. In this case, it is sufficient for the attacker to obtain physical access to any of the network components (cables, switches) to be able to control the entire system. There are also examples of ICS equipment where, although encryption is implemented, weak algorithms and/or self-signed certificates are used.

2. Statistics and Geographical Distribution of Potentially Insecure ICS

The reasons outlined in Section 1 create a strong belief that the best solution to ensure the security of ICS networks is to isolate them completely from the Internet and to maximally restrict access to them. This recipe is true and confirmed by a vast majority of ICS security specialists (cf. [4] as an example), but it is equally true that it often impairs the functionality and accessibility of specific solutions. ICSs seldom serve company clients directly via the Internet, so remote access to them may be very limited, but is often hard to eliminate completely due to such reasons as software upgrades, configuration changes and supervision over the system performed by engineering team members. For these reasons, the engineering side usually stands in opposition to security people. For the former of these two groups, restricting remote access to the system actually lowers the safety level of the industrial process, because it drastically increases their response time to any problems, especially outside normal working hours, and increases the amount of work needed to fix them. This is the reason why too strict a policy enforced by the security team may

[1] Since 2018, some security extensions to Modbus have been introduced, but most of the equipment present on the market does not support them yet [3].

Table 2
Number of indexed systems for each query, data taken from [8]

Shodan query	Connections	Category	Note
Niagara+Web+Server	2794	HAN/BMS	Web server for EMS/BMS
TAC/Xenta	1880	BMS	Self certs for HTTPS
i.LON	1342	BMS	Primarily for energy
EnergyICT	585	RTU	Primarily energy
Powerlink	257	BMS/HAN	
/BroadWeb/	148	HMI	Known vulnerabilities
EIG+Embedded+Web+Server	104	Embedded web server	
CIMPLICITY	90	HMI	Zero config web view
SoftPLC	80	PAC	Eastern Europe
HMS+AnyBus-S+WebServer	40	Embedded web server	
ioLogik	36	PLC	Small vendor
Allen-Bradley	23	PAC	
RTS+Scada	15	SCADA	Runs on FreeBSD
SIMATIC+NET	13	HMI	Affected by Stuxnet
Simatic+S7	13	PLC	Affected by Stuxnet
Modbus+Bridge	12	Protocol bridge	IP to Modbus
ModbusGW	11	Protocol bridge	
Reliance+4+Control+Server	10	SCADA	
Simatic+HMI	9	HMI	Affected by Stuxnet
Cimetrics+Eplus+Web+Server	6	Embedded web server	
A850+Telemetry+Gateway	3	Telemetry	
ABB+Webmodule	3	Embedded web server	
CitectSCADA	3	PCS	
Modicon+M340+CPU	3	Protocol Bridge	
webSCADA-Modbus	3	HAN	
RTU560	2	RTU	Web interface
WAGO	2	Telemetry	
eiPortal	1	Historian	
NovaTech+HTTPD	1	Embedded web server	Substation automation
Total	**7489**		

be in fact counterproductive, because then the engineering people may set up their own backdoors to the system, remaining outside any control or supervision of the security people.

These may take the form of unauthorized VPN tunnels, sometimes disguised in some other protocols to avoid detection and closure by the security team, or even worse, GSM modems connected directly to the industrial systems, completely bypassing all levels of security within the corporate network. This is not a purely theoretical threat, as poorly secured VPN tunnels were used as an attack vector in the recent successful attack on the Ukrainian power grid that took place on December 23, 2015 [5]. As far as GSM modems or other communication devices that completely expose the industrial system components via the Internet are concerned, they are, quite incredibly, much more common than one could expect.

Cryptographic tools, mainly encryption of web traffic, are nowadays rarely used in ICS (both DCS and SCADA), but are seriously considered as a future standard [6]. Management of cryptographic keys and optimization of resources are subjects of extensive discussions. In 2009, John Matherly created Shodan – search engine indexing services exposed to the Internet [7]. Two years later, E. P. Leverett, a student at Cambridge University, wrote a set of queries for Shodan that are based on signatures of the most popular ICS components. Although the list includes some popular BMS vendors as well, it is partly justified, because BMS often control factory premises and have access to deeper parts of ICS networks. A detailed description of the tests may be found in [8].

A look at the geographical distribution of these systems is interesting as well, because it is common belief that the problem of ICS security exists only in developed countries.

Table 2 shows that the problem exists all over the world, on all continents. Indeed, most of the indexed systems are located in developed countries with large numbers of industrial users, such as the United States of America, Sweden, the Netherlands or Canada. However, there are interesting exceptions, e.g. a relatively low number of connections in China, despite their big industry, rapid economic growth and large number of users. But this may be attributed rather to a relatively low number of IP numbers assigned to China, so the scale of the problem is probably the same as in other industrially developed countries, just hidden in private subnets used by Internet operators or in the IPv6 address space. Nevertheless, exposing ICS components even in a private network of a large Internet operator is only a little less dangerous than doing it openly on the Internet. It is of particular interest for the authors of this paper that a relatively high number of exposed systems exist in Poland, despite the fact that most operators have not been assigning, for a few years now, public IP addresses to their users by default. It is a feature that has to be paid for extra. This increases the probability that these exposures are intentional rather than accidental.

Table 3
Number of indexed systems per country, data taken from [6]

Country	Count	Country	Count
United States	3920	Greece	10
Sweden	442	Israel	10
Netherlands	370	Luxembourg	9
Canada	365	South Africa	9
Finland	301	Philippines	8
Norway	271	Thailand	7
Denmark	194	Turkey	7
Poland	191	Mexico	7
United Kingdom	122	Malaysia	6
Portugal	93	Singapore	5
Germany	92	Panama	4
Czech Republic	90	Puerto Rico	4
Spain	86	Hong Kong	3
Australia	81	Serbia	3
Ireland	76	New Zealand	3
Taiwan	66	Argentina	2
Japan	59	Chile	2
Italy	57	Croatia	2
France	53	Iceland	2
Slovenia	50	Indonesia	2
Korea, Republic of	41	Dutch Antilles	2
Belgium	39	Albania	1
Russian Federation	37	Armenia	1
Switzerland	34	Bermuda	1
No country information available	31	Faroe Islands	1
China	29	Guernsey	1
Brazil	27	Iran, Islamic Republic of	1
Cyprus	23	Jersey	1
Estonia	20	Kazakhstan	1
Austria	17	Vietnam	1
Slovakia	16	Macedonia	1
Hungary	14	Namibia	1
India	14	Trinidad and Tobago	1
Romania	13	Latvia	1
Ukraine	12	Kuwait	1
Lithuania	12	Malta	1
Bulgaria	10	**Total**	7489

The results published by Leverett stirred up a vivid discussion about cybersecurity in modern industry and inspired many other researchers to follow with similar tests. Especially interesting is work [9] by Roland C. Bodenheim, because he repeated exactly the same queries as Leverett two years later, in 2013. Although one may expect that the number will drop because of increasing awareness of the problem, the actual result is reverse. The total number of connections raised from 7489 in 2011 to 57409 in 2013. It is more than 7500% increase in just two years. Following huge media interest in the results of the searches, authors of Shodan limited the access to the search engine, so it is harder to find data from the next years, but extrapolating the growth from 2011–2013, there is no reason to believe that the trend is no longer present.

3. Protection of ICS Against the Attacks

Absolute safety against cybercrime is a goal that is impossible to attain. Even if we imagine we have perfectly designed system running bug-free code, there is always some space for human error. There are several ways to lower the probability of successful break-in and minimize the impact if such event occurs. They are in principle similar to those used in IT systems, but not all techniques used for IT can be applied also to ICS. For example, penetration or red team tests are generally avoided, as they may impair the industrial process and lead to irrecoverable damage. They may be tried in simulated environments mimicking parts of the real system, but this severely limits usefulness of these methods. Also whitebox tests are often hard to conduct, because, as stated in Section 1, many components utilize proprietary hardware architectures with closed-source software. Security of the system begins with proper design. It is especially important with ICS, where large parts of the system (e.g. aforementioned Modbus network) lack any security mechanisms at all.

There are many publications covering different aspects of ICS security, but it is hard to find a general and up-to-date guidebook thoroughly covering all the aspects, from technical designs, through staff employment to operational procedures. There is one special branch of the industry though, where such guidebooks exist and are constantly updated and improved. It is the nuclear energy industry. They are necessary because of potentially catastrophic con-

sequences of a security breach there. The standards are created and maintained by the International Atomic Energy Agency (IAEA). Their quality is proven in practice, because up to now there were only several publicly known, successful cyber break-ins to nuclear facilities [10]. And the only one that really inflicted some damage to the industrial process was with Stuxnet worm in 2010 on Iranian military factories for uranium enrichment. These factories were outside IAEA control then and were using illegally acquired ICS components (because of embargo). Other attempts, like the one in 2014 in South Korea, did not affect anything besides office computers of the company staff, not reaching any of the critical systems. The reason for this is that there are strict design requirements, described in [11], and compliance with them is later checked at the licensing stage.

One of the most important general design rules, formulated in [11], is defense-in-depth – there have to be as many independent levels of protection as possible, and a single point of failure which exposes vital parts of the system disqualifies the design. Such a point of failure does not have to have the form of a physical entity. For example, it may be the same model of firewall used to separate different network levels. If a remotely exploitable vulnerability is found in its software, access to all network levels may be obtained. The defense-in-depth rule is well known in the IT security world, but is rarely strictly obeyed. In the nuclear sector, it is been applied to the construction of reactors almost since the beginning of their commercial use, so naturally it is also strictly required in the field of cybersecurity. Security checks of industrial facilities must deal with the problem outlined at the beginning of this chapter. Therefore, a strong emphasis is placed on security assessments considered to be the most effective way of preventing break-ins. There are many good general guides on how to perform a cybersecurity assessment of an ICS, so the process will not be described in detail here. [12] may be a good starting point. But in this aspect, the nuclear industry also has its own procedures that are worth mentioning. In the book [13], there is a detailed guide on how to perform a security assessment of the entire facility, including such aspects as physical access and human resource policies. Apart from the questions devoted directly to the protection of radioactive materials, this publication may serve as a good basis for performing cybersecurity assessments in any advanced industrial facility.

4. Software

Because of very limited access of ICS systems to the Internet, no automatic software updates may be performed. Moreover, such an approach is discouraged in the case of production systems. Availability and security of industrial processes come first, so if the software patch fixing some less important security issues contains a bug or a change in the functionality, the entire process is jeopardized. Therefore, complicated procedures regarding the installation of new software versions are usually in place at industrial facilities, including thorough tests performed in simulated environments, and possibly even with some quarantine periods. On the other hand, updates are necessary, especially when a severe security flaw or a functionality problem is detected. Propagation of information about the vulnerabilities and updates constitutes another problem. Unlike in IT systems, where information about vulnerabilities found in most of the popular operating systems and applications is available at a single location, e.g. NVD (National Vulnerability Database), it is much harder to identify such a service for ICS. Most big vendors publish their own security bulletins in different formats and with different access rules. There are several national CERTs aggregating such information and republishing it, but the range of covered vendors may vary. The most complete and verbose are the services maintained by the American ICS-CERT [14]. There is a certain problem with them though – preparation of such data takes time, so alerts and advisories are often published by ICS CERT with a delay of several days compared to the original publication by the vendor of the affected system. System administrators interested in getting the information immediately are still forced to check security bulletins of the vendors of all the components used in the system. This does not guarantee anything, though. Many PLCs are now built using standardized x86 or ARM architectures, so they often share many operating system components with IT systems. When analyzing publications in NVD and security bulletins of the ICS component vendors, it may be noticed that bug reports (and software patches) in the latter case may appear even a year after their initial publication in NVD. This means that very dangerous periods are experienced when unpatched ICS components can be attacked by relying on general purpose IT exploits. This constitutes another reason for keeping ICS networks as isolated from the Internet as possible.

The last aspect requiring consideration is personnel training. All the people in the organization should know and understand the security policy, including engineering team and even office staff which has nothing to do with plant operations. Recent successful break-in examples, like the one in Ukraine [5], show that the first stage of the attack usually consists in spear phishing targeted at several people within the organization. Getting inside the internal network, even via office computers, gives the attacker numerous opportunities to spread the infection further. This is where the defense-in-depth paradigm shows its usefulness, because the aforementioned attack in Korea in 2014 ended within the office network – the attackers were not able to breach deeper levels of security. The results gathered by Leverett, Bondenheim and others, as cited in Section 2, show indirectly the danger of too tight security policies. Even if the policy is known by the engineering team, when it feels it hinders their work, they will look for a way to go around it. This may result in fully exposed systems using unauthorized modems, etc. That is why it is equally important to ensure that the technical people responsible for plant operations have real influence on security policies. This

cannot work one way, because an enforced policy written without taking into account any feedback will be generally contested.

5. Detection of Successful Attacks

Advanced persistent threat (APT) attacks are extremely hard to prevent and detect, as they use some sophisticated social engineering techniques often paired with 0-day vulnerabilities and structural weaknesses of the organization. Traditional means of detection, like antivirus software, are not sufficient to stop this kind of attackers. That is why specialized Security Operations Centers (SOCs) have been becoming ever more popular recently. The idea of SOC is to proactively analyze network traffic and logs in order to detect any suspicious behaviors.

A detailed setup falls outside of the scope of this article, but there are many commercial products helping in performing task, or even companies that may provide a complete SOC as an outsourced service. It is worth mentioning though that it is possible to set up a functional SOC using open source tools, such as Elasticsearch + Logstash + Kibana (ELK), Bro network monitor, topped off by the Malware Information Sharing Platform (MISP). Especially the last of these tools is very useful, because it is constantly fed with information by a very large community of users, so indicators of compromise (IOCs) are quickly recognized. Such a setup is being successfully used at the European Organization for Nuclear Research (CERN) and other institutes federated in the Worldwide LHC Computing Grid (WLCG), including the National Centre for Nuclear Research in Poland [15].

Detection of backdoors using modems and other means of independent, unauthorized communication outside of the facility is another topic that is not necessarily covered even by a well setup SOC. The risk of installation of such devices can be minimized with proper policies (e.g. forbidding bringing any USB devices or mobile phones into the critical areas of the facility). It cannot be eliminated entirely though, without very expensive and troublesome means of security. Monitoring of Shodan results in search for company's specific equipment by the security team is not an effective means of protection. Shodan indexes new systems in approx. 19 days [9], and, as stated earlier, does not cover private networks of Internet operators. It is also not easy to use Shodan for malicious purposes, because of strict limits on the number of results in the free, anonymous version. For this reason, cybercriminals use their own botnets to do the same work, and their indexing schemes may be different. The use of radio-frequency (RF) shielding or signal jammers may be an effective way of ensuring protection of critical assets, but effective shielding is very expensive and jammers are usually forbidden by law. It is possible, though, to monitor RF signals in the area and even identify active client stations, in a search for unauthorized ones. The required hardware is expensive and difficult to come by, but good results can be achieved even with software defined radio. Example of such an application may be found [16].

6. Conclusions

This article presents the scale of the problem of insecure ICS systems. The data summarized in the paper and available in cited publications shows an alarming trend in the security of ICS/OT networks. Strong evidence exists that the number of ICS installations without proper isolation of components from the Internet is growing, despite the increasing level of awareness of the problem among ICS vendors and despite constant presence of this topic in the media. This can be partially attributed to the threat hierarchy outlined in the introduction to this article. When availability of the process is treated as the most important asset, cybersecurity issues are often overlooked, because their direct impact on availability is delayed in time.

The paper outlines several good practices on how to improve cybersecurity of ICS/OT networks, with references to more detailed sources of information, e.g. the process of establishing a simple SOC using open source tools to facilitate the detection of attacks. It also mentions the problem of locating unauthorized RF devices and ways to detect them. The article shows how standards set for the nuclear industry may be used to protect critical assets in other domains where ICS are used, with references to detailed guidelines included. These simple countermeasures may increase the security of the systems at a relatively low implementation cost. More in-depth methods, such as introduction of cryptographic measures to ICS (e.g. with new versions of the Modbus protocol [3]) are deliberately skipped in this paper because they often require serious changes of the architecture of the system and its components.

Acknowledgments

Work done as part of the CYBERSECIDENT/369195/I/NCBR/2017 project supported by the National Centre of Research and Development in the frame of CyberSecIdent Programme.

References

[1] T. C. Reed, *At the Abyss: An Insider's History of the Cold War*. Presidio Press, 2004 (ISBN 0891418210).

[2] T. Jablonski and M. Jach, "Jak 14-latek spowodował katastrofę", 2008 [Online]. Available: http://lodz.naszemiasto.pl/archiwum/jak-14-latek-spowodowal-katastrofe,1602388,art,t,id,tm.html [in Polish]

[3] "MODBUS/TCP Security Protocol Specification" [Online]. Available: http://modbus.org/docs/MB-TCP-Security-v21_2018-07-24.pdf

[4] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to industrial control systems (ICS) security", NIST Special Publication 800-82 Revision 2, 2015 (doi: 10.6028/NIST.SP.800-82r2).

[5] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid", E-ISAC publication, March 18, 2016 [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[6] D. Fauri *et al*., "Encryption in ICS networks: A blessing or a curse?", in *Proc. IEEE Int. Conf. on Smart Grid Commun. SmartGridComm 2017*, Dresden, Germany, 2017 (doi: 10.1109/SmartGridComm.2017.8340732).

[7] Shodan search engine home page [Online]. Available: https://www.shodan.io/

[8] E. P. Leverett, "Quantitatively assessing and visualising industrial system attack surfaces", Master Thesis, University of Cambridge, 2011 [Online]. Available: https://www.cl.cam.ac.uk/∼fms27/papers/2011-Leverett-industrial.pdf

[9] R. C. Bodenheim, "Impact of the Shodan computer search engine on Internet-facing industrial control system devices", Master Thesis, Air Force Institute of Technology, Ohio, USA, 2014 [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a601219.pdf

[10] P. Hitchin, "Cyber attacks on the nuclear industry", Nuclear Engineering International, 15 September 2015 [Online]. Available: https://www.neimagazine.com/features/featurecyber-attacks-on-the-nuclear-industry-4671329/

[11] "Computer Security at Nuclear Facilities", IAEA Nuclear Security Series No. 17 [Online]. Available: https://www-pub.iaea.org/mtcd/publications/pdf/pub1527_web.pdf

[12] "Cyber security assessments of industrial control systems. A good practice guide", Centre for the Protection Of National Infrastructure, U.S. Department of Homeland Security, Apr. 2011 [Online]. Available: https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/CPNI-Guia-SCI.pdf

[13] *Conducting Computer Security Assessments at Nuclear Facilities*, IAEA, Vienna 2016 (ISBN: 978-92-0-104616-1).

[14] ICS-CERT Alerts home page [Online]. Available: https://ics-cert.us-cert.gov/alerts?page=1

[15] D. Crooks *et al*., "Operational security, threat intelligence & distributed computing: the WLCG Security Operations Center Working Group", in *Proc. of 23rd Int. Conf. on Comput. in High Energy and Nuclear Phys. CHEP 2018*, Sofia, Bulgaria, 2018.

[16] R. Feroze, "Passive GSM sniffing with Software Defined Radio", 02/06/2017 [Online]. Available: https://payatu.com/passive-gsm-sniffing-software-defined-radio/

Adam Padée received his M.Sc. in 2003 and his Ph.D. degree in 2013, both from the Faculty of Electronics and Information Technology of the Warsaw University of Technology, Poland. He participated in many European and national projects focused on supercomputing and distributed computing. Since 2009 he has been working for the National Centre for Nuclear Research (NCNR). He was one of the founders of Świerk Computing Centre. Currently he is the Head of Division of Computing Technologies and Deputy Director of Department of Complex Systems at NCNR. His scientific interests are focused mainly on high performance computing and infrastructure, evolutionary computation, IT and OT security.

E-mail: adam.padee@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland

Michał Wójcik received his B.Sc. and M.Sc. degrees in Computer Science from Warsaw School of Information Technology, Poland in 2013 and 2018, respectively. His main areas of interest are computer networks and, in particular, network security, as well as information security management systems according to ISO 27001.

E-mail: michal.wojcik@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland

Arkadiusz Ćwiek graduated from the University of Warsaw, M.Sc. in Physics, in 2011, in Biophysics and Didactics in mathematics and physics. From 2012 to 2018 leader of IT in the "Pi of the Sky" robotic telescopes project in which he worked with the best Polish research institutions, i.e. the National Centre for Nuclear Research, the Faculty of Physics of the University of Warsaw and the Centre for Theoretical Physics of the PAS. Responsible for development and maintenance of the telescope data acquisition and control systems, several facility instruments, and a suite of tools used for the preparation, planning and execution of observations. He was also responsible for research, design, specification and implementation of solutions. He also managed computer systems of the project spanning located on 2 continents. He also supported Creotech Instruments in some projects correlated with outer space observation. Since 2018 he works at Świerk Computing Centre. Currently he developing solutions using neural networks applied to computer network security and computer vision.

E-mail: arkadiusz.cwiek@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland

Konrad Klimaszewski received his M.Sc. in Physics from the Warsaw University of Technology, Poland, and the Ph.D. degree in Physics from the Soltan Institute for Nuclear Studies, Poland, in 2004 and 2010, respectively. From 2015 he has been the Head of Information Technology Services

Laboratory at the National Centre for Nuclear Research, Poland. His scientific interests are focused mainly on high energy particle physics and nuclear medicine as well as high performance computing, could computing security and machine learning.

https://orcid.org/0000-0003-0741-5922
E-mail: konrad.klimaszewski@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland

Przemysław Kopka is a last-year student at the Warsaw University of Technology at the Faculty of Physics. He has been with the National Centre for Nuclear Research as Python developer since 2018. He holds an B.Sc. in Mathematics and Physics from Warsaw University. His research areas focus on data processing and image reconstruction.

E-mail: przemyslaw.kopka@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland

Sylwester Kozioł received his M.Sc. degree in Automation and Electrical Metrology, with distinction, from the Warsaw University of Technology, Poland, in 1979. Currently, he is a Major Technical Infrastructure Specialist at National Centre for Nuclear Research Świerk, Poland.

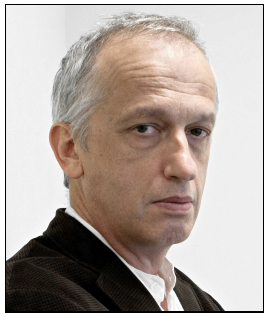
E-mail: sylwester.koziol@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland

Krzysztof Kuźmicki received engineer's education at Warsaw School of Computer Science with an excellent degree in the major Managing Information Resources. Currently, he is a Technical Infrastructure Specialist at National Centre for Nuclear Research Świerk, Poland.

E-mail: krzysztof.kuzmicki@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland

Rafał Możdżonek received his B.Sc. in Computational Physics and M.Sc. in Nuclear Physics from Warsaw University of Technology in 2011 and 2013, respectively. Currently he is a senior programmer at Laboratory for Information Technologies, Department of Complex Systems, National Centre for Nuclear Research. His main fields of interest include programming, numerical methods and data analysis.

E-mail: rafal.mozdzonek@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland



Wojciech Wiślicki graduated from Department of Physics of the University of Warsaw in 1982, received Ph.D. in Physics from A. Soltan Institute for Nuclear Studies in 1986, since 2007 and is a Professor Ordinarius at National Centre for Nuclear Research in Warsaw, Poland. Currently he is a Director of Department of Complex Systems and Computing Centre at this institute, also leads scientific groups participating in LHCb experiment at Large Hadron Collider at European Centre for Nuclear Research and KLOE at Frascati National Laboratory. His areas of scientific activity cover experimental high-energy physics and high-performance computing. He is an author of about 600 papers in various areas of physics and scientific computing, member of many committees, editorial boards and scientific bodies.

https://orcid.org/0000-0001-5765-6308
E-mail: wojciech.wislicki@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland

Tomasz Włodarski received his M.Sc. degree in Optoelectronics from Gdańsk University of Technology, Poland, in 2006. His main fields of interest include high performance computing clusters, network security and protocols, cloud computing and virtualization.

E-mail: tomasz.wlodarski@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland

Paper

Cyber-security for Mobile Service Robots – Challenges for Cyber-physical System Safety

Wojciech Dudek and Wojciech Szynkiewicz

Warsaw University of Technology, Institute of Control and Computation Engineering, Warsaw, Poland

https://doi.org/10.26636/jtit.2019.131019

Abstract—A review of the known and an indication of the new threats for cyber-physical robotic systems, caused by cybernetic attacks, serves, in this paper, as a basis for the analysis of the known methods relied upon to detect and mitigate consequences of such attacks. A particular emphasis is placed on threats specific for cyber-physical systems, as they are a feature distinguishing these systems from their traditional Information and Communication Technologies (ICT) counterparts. Based on the review of literature and own analyses, unresolved issues regarding the cyber-security of robot systems are presented and discussed.

Keywords—cyber-security, mobile robot safety, robot, robot threats.

1. Introduction

Robots are commonly considered as devices that sense their environment with receptors and act upon the environment with effectors to accomplish a given task. Their intelligence, imperative to act, and the tasks they execute are managed by a control system. The control system, using sensory data and models, plans high-level activities and commands the effectors to execute elementary actions or movements. Service robots are well-equipped with a variety of sensors in order to perform complex robotic tasks (e.g. door approaching and opening [1]) and to store classified data (e.g. medical information [2], door lock types [3]).

Development of robot control systems, with utilization of complex control and planning algorithms included, has a strong impact on the robot's requirements regarding computing power and memory size. Instead of increasing onboard robot computational resources, developers of robot software commonly distribute processing operations between the built-in computer and a cloud. A machine backed with cloud computing technology is not only able to accomplish more complex tasks, but is also capable of sharing its knowledge and experience with other devices [4].

Furthermore, there are platforms that remotely provide robotic applications to perform diverse tasks [5]. The concept behind such platforms is to not only to deliver services which are typical of connected robots, but also to provide independent applications. After an application has been downloaded from the cloud, it takes control of the robot's sensors and effectors. The hazard detection application [6] is an example of a solution that takes advantage of distributed robot software. In addition, work has been performed to develop cloud services suited for robots [7], [8].

Connection of robots to clouds brings about many other benefits, e.g. the ability to integrate the robot with a network of devices, such as the Internet of Things (IoT) or wireless sensor networks [9], [10] where the machine is able to sense the environment with distributed sensors and act upon the enivronment with external effectors, being a part of a distributed network.

Distribution of the control system between the on-board computer and a cloud, and its integration with IoT opens new research paths. One of them focuses on the design of a distributed robot software architecture [11] and on the development of a software framework by means of which this concept may be implemented. The key issue that needs to be considered in the design process is the requirement for a short response time. A significant share of robot control systems requires real time constraints to be satisfied [12]. Additionally, end users expect responsivity, i.e. a short lead time between task request and the beginning of its execution. Robot software architectures should also be developer-friendly. Fast prototyping and quick implementation of robot tasks should be considered a standard requirement.

Another research area that is crucial for the integration of robots and IoT is cyber-security of such distributed systems. A robot, being a software-controlled machine, should be well tested against various cyber-attacks and developers of robot systems should be aware of vulnerabilities of robot programming frameworks and components. However, most of the projects implement its own connections with the cloud (sometimes even as plain text, as it's not the main scope of these works), and robot control system designers do not pay enough attention to protect the systems against cyber-attacks.

As robots are connected to the Internet and rely upon sensors and effectors, they are considered to be cyber-physical systems (CPS) [13]. While no commonly accepted defini-

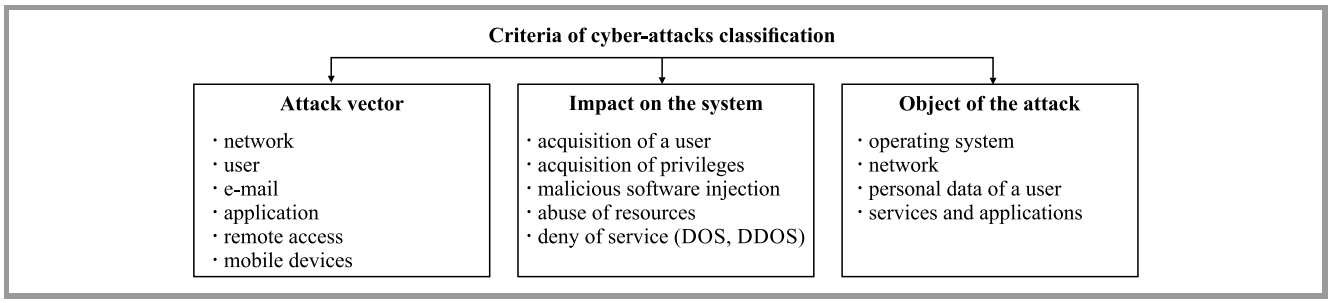


Fig. 1. Example of criteria for classification of cyber-attacks.

tion of CPS exists, we may state that it is a specifically designed network of collaborating components used to monitor and control the physical world. There are two types of components: "cyber" (computation, communication) and physical (e.g. sensors, effectors). Such components are integrated, their operation is monitored and managed [14]. It is expected that CPS, when connected to the Internet, may revolutionize many areas, e.g. transport, healthcare, manufacturing, agriculture, military, civil and space engineering. Many attacks on CPS area have been identified and categorized to date [14], [15]. Some examples of criteria used for the classification of cyber-attacks are: attack vector (route or means by which the attacker acquires access to a system or network), impact on the system, object of the attack.
Specific cases for each of those types are presented in Fig. 1. The examples of consequences of a CPS cyber-attack include the following:

- physical damage to a CPS device and/or objects within its environment,
- financial and image-related losses of the user/developer,
- injuries or death of people.

More threats and potential consequences of cyber-attacks on CPS are discussed in [16].
Many types of devices are classified as CPS and they differ in terms of the potential threats and consequences of cyber-attacks. Robots are usually well-equipped with sensors (e.g. RGB, RGB-D, IR and time-of-flight cameras, microphones, inertial measurement units, laser scanners, IR emitters) and they are able to move around. Therefore, this type of CPS should be considered as particularly vulnerable to a wide range of risk categories arising from cyber-threats.
In this paper we present cyber-attacks that are specific for CPS, methods for identification of such cyber-attacks and tools to protect against them. Section 2 contains an analysis of the different types of cyber-attacks, methods of their detection and CPS security-related issues. In Section 3, a survey of issues related to cyber-security of robots, based on the analysis performed, is presented. Section 4 discusses future work and research areas in the field of robot cyber-security.

2. Cyber-security in Cyber-Physical Systems

Stuxnet was one of the first worms used against CPS [17]. It was discovered in June 2010 and was used to attack industrial installations. Its impact was huge – the authors of the report [17] estimate that approximately 100,000 hosts from over 155 countries were infected. The successor of this worm – Industroyer malware – was used in a cyber-attack on Ukraine's power grid that deprived a part of its capital, Kiev, of power for an hour [18]. The next recent attack relied on ransomware with which the Office of Urban Transport in San Francisco (SMFTA) was infected. In October 2016, a hacker hashed 900 computers that belonged to the SMFTA. The attack disabled the ticket distribution system and the value of the ransom required was 73,000 USD.
It is quite obvious that the problem of cyber-security in cyber-physical systems is essential not only for the industry, state offices and city authorities, but also for almost every single person. The cost of the ransom, repairs of damaged systems, reconstruction of important data is huge and may impact the reliability of a company, a government or any other attacked institution. Some countries have established organizations to coordinate various aspects of cyber-security and cyber-attack mitigation efforts. In the US, such an entity is known as The National Cyber-security and Communications Integration Center (NCCIC). In its 2016 report [19], the organization published statistical data pertaining to incidents that have been identified and technologies used during the attacks. Figure 2 is based on data from this report and presents the prevalence of known threat vectors in CPS. Based on its annual reports, NCCIC released a cyber-security review tool – the Cyber Security Evaluation Tool (CSET). It contains a set of questionnaires, analyzes the answers given and generates a set of graphs and plots that visualize the strong and the weak points of the system concerned. The program gives also recommendations to enhance the level of protection. Many projects and papers are available that refer to methods used for anomaly, breach and cyber-attack detection and defense in CPSs [15], [20], [21].
It should be noted that the above analysis is focused on industrial installations based on the CPS concept. Technological evolution makes it possible to create CPS devices that are used in private homes, e.g. small service robots,

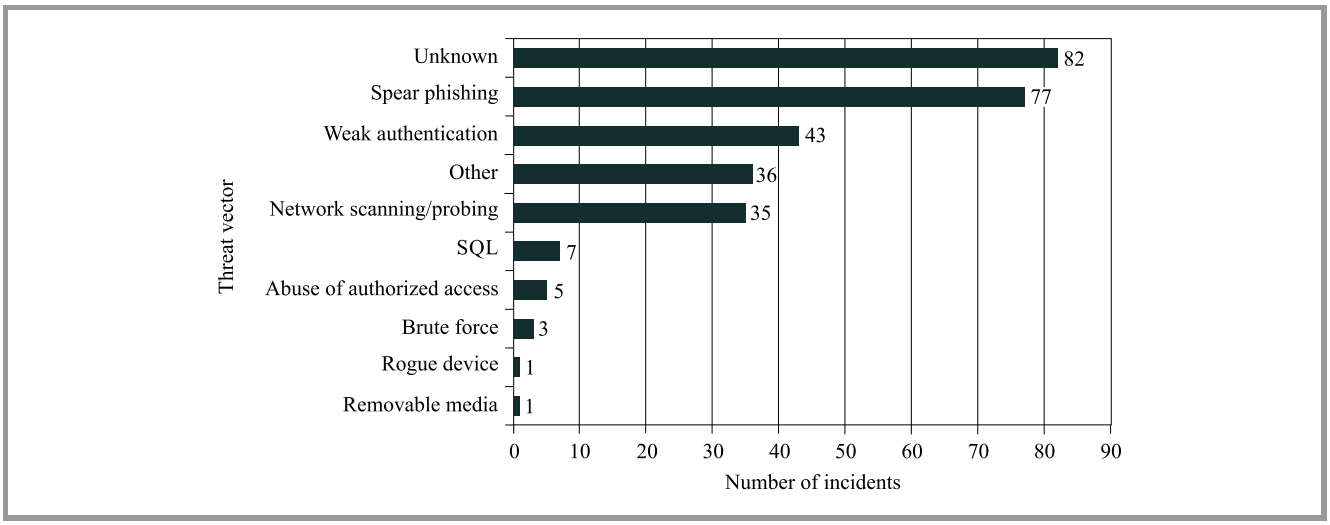


Fig. 2. Prevalence of known threat vectors in the case of CPS [22].

toys and appliances connected to the Internet. A robot that has been conquered poses an obvious physical threat residents (especially the young ones). Such a device may also exert a strong impact on human privacy and compromise sensitive data (bank accounts, passwords, etc.), or may be used to blackmail the device user. By collecting information, a corrupted robot may be also used as an element of a more sophisticated attack. In contrast to industry workers, people at home are neither aware of cyber-security, nor trained on how to diagnose a cyber-attack.

The security of CPS is mainly based on seven security functions that have been proposed for IT systems in the ISO/IEC 10746-3 [23] standard:

- **access control** – prevents unauthorized interactions with an object,
- **security audit** – ensures that security-related information is collected and monitored. Such information is analyzed to review security policies and procedures,
- **authentication** – guarantees that a given object is identified properly,
- **integrity** – detection and/or prevention of an unauthorized creation, alteration or deletion of data,
- **confidentiality** – prevents unauthorized disclosure of information,
- **non-repudiation** – provides assurance that a given object is/was involved in all or part of the interaction,
- **key management** – provides mechanisms for the management of cryptographic keys and includes all of the following key-related operations: generation, registration, certification, deregistration, distribution, storage, archiving and deletion.

The above functions are used to achieve three main security-related objectives:

- **integrity** – maintaining the reliability of data sources,
- **availability** – providing access to the system and its services,
- **confidentiality** – hiding data from unauthorized objects.

The authors of [24] reveal that although CPS are based on information systems, there is a need to widen the definition of integrity, availability and confidentiality due to physical elements of CPS. For example, providing integrity in CPS means also an ability to remain operational in the case of an attack on sensors or effectors. Furthermore, availability of CPS should take into consideration a scenario in which an attack is performed on the network of sensors, control-related transmissions and on actions performed by effectors. One of the tasks of CPS is to register information about its environment. Because of that, in many applications there is a high risk of corruption of the user's privacy. Moreover, reasoning about the state of CPS based on its inter-component communication is yet another important threat.

In order to perform the aforementioned security functions, system developers rely on a variety of tools to secure CPS. The classification of tools that were presented in [24] (Table 1) is used as well. Prevention tools are used to limit the range of threats to the system. Every object of the system and any object that cooperates with the system should be identified, should operate with a limited access, and messages that the objects exchange should be protected. Reactive tools comprise a collection of mechanisms that are activated during an attack. Intrusion Detection System (IDS), for example, observes the communication patterns and behaviors of objects within the entire system [25], [26]. Its role is to identify any exceptional situations, behaviors or any undesired actions within the system that may be the trace of an attack. The attacker's model is a profile of threats and potential attack scenarios affecting the system.

Table 1
Tools and functions used for securing cyber-physical systems

Prevention	Reaction	Adversary model
Authentication	Intrusion Detection System	Assumptions of probable attacks
Access control	Key revocation	Threat profile
Redundancy of communication channels, diversity of technology and secure methods		Identifiers of trusted system elements
Message signatures and freshness		
Managing access privileges of system components		
Tools for security verification		

It offers a whole picture of the system's security, and as the development of the adversary model progresses, security updates are released.

3. Mobile Robot Cyber-security Survey

Robots are complex CPS systems, thus their cyber-security still poses a big challenge. Frequently, security systems developed for conventional information systems are insufficient and cannot be implemented in a scenario with mobile robots. Some of the security systems demand too much computational and storage resources, while others are incorrect due to insufficient experimental data or inaccurate adversary models. Most of works described in the literature consider the detection of an attack on a robot system only. There are many works regarding IDS, and some studies on securing specific components of the robot system. Table 2 shows the selected, recent works that consider the implementation of cyber-security functions in the robotics domain. The survey presents a comparison taking into account the following aspects:

- considered security functions and attack vectors,
- methods used to establish the security function,
- data needed by the method to realize the function,
- purpose of the solution (prevention against an attack, detection of an attack and reaction in the case of an attack).

The first two papers [21], [27] are concerned with the principles of research on robot cyber-security and with a general analysis of the issue. In [21], authors present a study and some clues for conducting experiments related to robot cyber-security, in the event of a sensor spoofing attack[1]. Furthermore, the work presents an analysis of machine vulnerabilities and attack detection methods. The purpose of the work is to maintain proper behavior of the system. However, the authors do not address the problems of ensuring the privacy of users (e.g. confidentiality of user data). Paper [27] describes the process of research platform design, as well as presents metrics and key performance indicators for robot security analysis.

Recent works concentrate on the threat detection aspect. Authors of [28], [29] propose an algorithm to detect an attack based on the network traffic analysis, data gathered and the physical system parameters. The algorithm relies on machine learning and rule tracking methods. Papers [30], [31] present algorithms which are also based on machine learning. This work, however, uses them to secure the Real-Time Locating System (RTLS). Based on data gathered by the localization system, the algorithm identifies a potential attack.

Detection of the attack on the robot system has also been considered by the authors of [32]. Their solution is based on confronting sensor data with the robot motion dynamic model, and on identification of potential anomalies. In work [33], a security audit of a popular robot programming framework – ROS – is described. The authors identify a potential threats, propose lightweight security mechanisms for the application level and a key management component for the ROS framework. Most of the above works focus on the prevention and detection aspects of the security system. In paper [34], authors describe the recursive state estimator that compares the calculated state with measurements obtained from redundant sources. The algorithm returns a high variance of measurement noise for the compromised sensor driver. The solution requires a well-defined noise profile for every sensor used. An inaccurate profile for a given sensor may result in the rejection of most of its measurements, or in the acceptance of data crafted by the attacker.

The most recent work [35] targets securing the successor of ROS – ROS2. A new release of the framework is expected to be more suitable for real world applications and for implementing robots to the IoT environment. The work

[1] Set of attacks that are based on imitations of the system's elements and that rely on injecting crafted data packets into the communication network of the system.

Table 2
A survey of recent studies on implementation of cyber-security functions in the robot systems

Work	Cyber-security function	Attack vector	Method used	Data required	Purpose
[21]	Security audit, integrity	Injection, sensor spoofing, hidden attacks	Penetration testing	Tests results and conclusions	Detection
[27]	Security audit	DoS	Construction of the research platform, determination of key performance indicators	Analysis of the platform tests	Prevention
[28], [29]	Access control, integrity	DoS, data injection, malware	Tracking of the defined rules, machine learning	Network traffic, obtained data, robot speed, physical vibration, power consumption	Detection
[30], [31]	Integrity	DoS, sensor spoofing	Machine learning	Data from the RTLS localization system	Detection
[32]	Integrity	Sensor spoofing, logic bomb, signal interruption, physical damage	Comparison of real-time data with dynamics model of the physical system, anomaly spotting	Dynamics equations of the physical system	Detection
[33]	Security audit, key management, non-repudiation, confidentiality	Injection, unauthorized access, DoS	Threats analysis, penetration tests	Conclusions and results of the tests	Prevention
[34]	Integrity	Sensor spoofing	Sensor data fusion	Redundancy of data sources	Reaction

describes the implementation of a secure data distribution service (DDS) into the ROS2 framework. The method provides valuable tools for securing robot systems that utilize the ROS2 framework and offers procedural provisioned access control policies for the software layer. Moreover, the authors of the article show a method for the verification of compliance between generated transport artifacts and decision point implementation.

4. Research Paths in Cyber-security for Robots

Our analysis of the literature regarding cyber-security of robots has identified numerous open research issues. The most obvious one is the fragmentary character of secure systems. Juxtaposition of potential threat vectors that are typical of CPS (Fig. 2), and of the security solutions proposed in the literature shows some crucial gaps in the robot security systems.

For example, there is a shortage of methods protecting against spear phishing[2]. Gaps in the robot cyber-security system may provide access to a considerable amount of crucial, personal information about the victim and his or her family. Such information may be used, for instance, to submit blackmail or ransom demands. Moreover, an attacker using an unsecured robot may gain access to confidential information or the victim's passwords.

[2] Directed form of a phishing attack. Fake messages are being sent to a specific organization or person in order of gain access to confidential information.

In order to develop a secure robot system, a need exists to design a security policy for such a system. This issue is another research area that required more attention. The abovementioned CSET tool that verifies the security of CPS is a good clue for the task of designing a similar tool suitable for robot systems. It should take into account the vulnerabilities, threats and attack vectors that are specific for robot systems.

One of the greatest challenges in the field of robot security is the design of a range of methods that will cover every aspect of service robot cyber-security. Service robots usually utilize a control system that is extremely complex and often distributed across the network. Furthermore, it is well equipped with a great variety of sensors that are used to investigate the environment. The first step in the design of a security system for such a robot is to define threats and vulnerabilities of a typical service robot control system. This step should be followed by the design of secure methods and tools. Figure 3 presents the result of a preliminary analysis of such system threats. The analysis has rendered the following conclusions.

A robot application that uses a low-level robot controller gains access to critical information about the environment and the robot itself. Furthermore, it has the ability to command robot effectors. Therefore, every application that may interact with the low-level controller should require authentication. Such a security mechanism is especially crucial in a situation in which robot applications are downloaded from a remote repository.

Developers of low level controllers should take into account a possibility of the attacker hindering communication

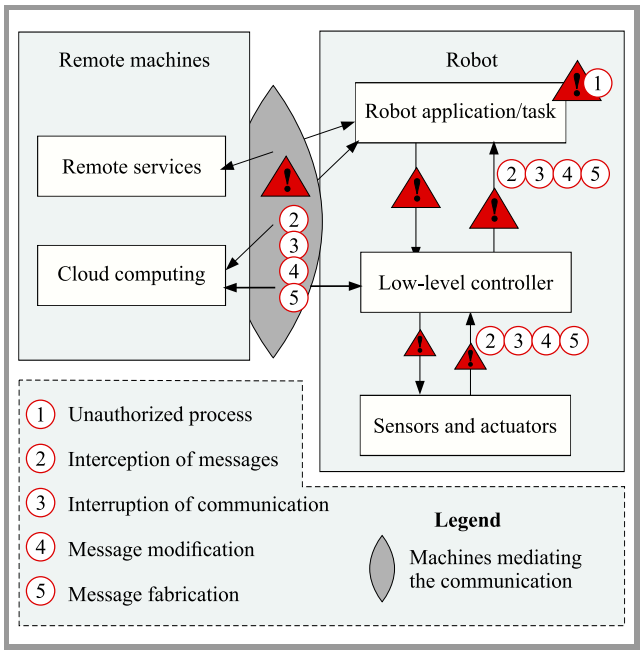


Fig. 3. Examples of threats to a complex, distributed control system of a service robot.

with hardware. One of the possible solutions is to develop a built-in IPS[3] into the robot system, or at least provide interfaces to integrate one. This kind of security mechanism depends on the robot structure and the equipment (especially the sensors) used. Therefore, it is difficult to devise both a complete and a universal model of a security system for robots.

Nowadays, when robots frequently utilize cloud computing, developers should address the issue of secure communication between these entities. As information exchange is performed by two computers through the network, this aspect of the robot cyber-security domain is similar to the well-known security aspect of information systems. The main differences are in the data that is transferred and in the Quality of Service (QoS) required, as some parts of the robot system are controlled in real time.

Developers of robot systems and providers of remote services for robots should define and disseminate standards of secure communication applicable to robot systems, so that various types of robots could take advantage of services rendered by different providers.

Another remark based on the cyber-security analysis of the service robot system performed is that the current classification of cyber-attacks (Fig. 1) is insufficient and needs to be supplemented with new subgroups.

Taking into account that both robot structures and their software are frequently application-specific, the design of a robot security system model is necessary. It would empower developers of a dedicated robot system to deliver more secure machines. Moreover, there is another crucial area in the field of robots cyber-security that has not been addressed so far, namely design and implementation of reaction methods relied upon in the event of a cyber-attack. The easiest one would be to restart the robot software from a backup. However, in some configurations and during execution of some tasks, the machine should not be shut down. Such a reaction may result in damage to the robot or the environment, or may even may threaten the health or life of people present nearby.

[3] IPS (Intrusion Prevention Systems) is designed to protect the secured system from attacks by detection of an intrusion and prevention from carrying out of one. IPSs are either software or hardware based.

5. Summary

Service robots are equipped with many types of sensors. They acquire a lot of information about the surrounding environment. Access to such data has to be well protected, or an unauthorized person may collect confidential information about the user or even take over control of the robot to inflict damage on the environment or its owner. Leakage of confidential information may be related to: presence of people, passwords and logins, banking information and many other domains.

Moreover, media reports about attacks on the privacy of many people will undoubtedly have a negative impact on the sale of service robots. Hence, the interest of potential investors in financing research in this area. In addition to known types of attacks on IT systems, service robots may be affected by specific attack vectors, and after by-passing security, the attacker will have access to a well-equipped spying device. Therefore, security solutions used in traditional ICT systems are not sufficient for robotic system applications.

It is necessary to develop appropriate methods for securing service robots against cyber-attacks. Several such methods are already known, but they do not provide consistent and comprehensive protection against all known attack vectors. New and robot-specific solutions are still expected in response to the newly identified vulnerabilities and threats. Additionally to the development of new security features and identification of new threats related to the service robots operating in domestic environment, it is necessary to devise a comprehensive protection module that will be easily integrable with service robot controllers. Such a module should be configurable due to a variety of machine structures and applications, whereas it should not significantly affect the implementation of the task itself while working in the mode of identification of a potential attack. In addition, invention of cyber-attack detection and defense methods that depend on the task being currently performed is needed.

Acknowledgements

This work constitutes a part of the CYBERSECIDENT/ 369195/I/NCBR/2017 project supported by the National Centre of Research and Development, within the framework of the CyberSecIdent Programme.

References

[1] T. Winiarski, K. Banachowicz, and D. Seredyński, "Multi-sensory feedback control in door approaching and opening", in *Intelligent Systems '2014. Proceedings of the 7th IEEE International Conference Intelligent Systems ISñ2014, September 24-26, 2014, Warsaw, Poland, Volume 2: Tools, Architectures, Systems, Applications*, D. Filev, J. Jabłkowski, J. Kacprzyk, M. Krawczak, I. Popchev, L. Rutkowski, V. Sgurev, E. Sotirova, P. Szynkarczyk, S. Zadrozny, Eds. Springer, 2015, pp. 57–70 (doi: 10.1007/978-3-319-11310-4_6).

[2] A. M. Okamura, M. J. Mataric, and H. I. Christensen, "Medical and health-care robotics", *IEEE Robotics & Autom. Mag.*, vol. 17, no 3, pp. 26–37, 2010 (doi: 10.1109/MRA.2010.937861).

[3] T. Winiarski, W. Kasprzak, M. Stefańczyk, and M. Wałęcki, "Automated inspection of door parts based on fuzzy recognition system", in *Proc. 21th IEEE Int. Conf. on Methods and Models in Autom. and Robot. MMAR'2016*, Międzyzdroje, Poland, 2016, pp. 478–483 (doi: 10.1109/MMAR.2016.7575182).

[4] M. Tenorth and M. Beetz, "KnowRob – knowledge processing for autonomous personal robots", in *Proc. IEEE/RSJ Int. Conf. on Intell. Robots and Syst. IROS 2009*, St. Louis, NO, USA, 2009, pp. 4261–4266 (doi: 10.1109/IROS.2009.5354602).

[5] C. Zieliński *et al.*, "Variable structure robot control systems: The RAPP approach", *Robot. and Autonom. Syst.*, vol. 94, pp. 226–244, 2017 (doi: 10.1016/j.robot.2017.05.002).

[6] W. Dudek, K. Banachowicz, W. Szynkiewicz, and T. Winiarski, "Distributed NAO robot navigation system in the hazard detection application", in *Proc. 21st Int. Conf. on Methods and Models in Autom. and Robot. MMAR 2016*, Międzyzdroje, Poland, 2016, pp. 942–947 (doi: 10.1109/MMAR.2016.7575264).

[7] R. Doriya, P. Chakraborty, and G. Nandi, "Robot-cloud: A framework to assist heterogeneous low cost robots", in *Proc. Int. Conf. on Commun., Inform. & Comput. Technol. ICCICT 2012*, Mumbai, India, 2012 (doi: 10.1109/ICCICT.2012.6398208).

[8] W. Dudek, W. Szynkiewicz, and T. Winiarski, "Cloud computing support for the multi-agent robot navigation system", *J. of Autom., Mob. Robot. and Intell. Syst.*, vol. 11, no 2, pp. 67–74, 2017 (doi: 10.14313/JAMRIS_2-2017/18).

[9] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey", *J. of Netw. and Comp. Appl.*, vol. 88, pp. 10–28, 2017 (doi: 10.1016/j.jnca.2017.04.002).

[10] E. Niewiadomska-Szynkiewicz and A. Sikora, "A software tool for federated simulation of wireless sensor networks and mobile ad hoc networks", in *Applied Parallel and Scientific Computing, PARA 2010, Reykjavík, Iceland, June 6-9, 2010, Revised Selected Papers, Part I*, K. Jónasson, Ed. *LNCS*, vol. 7133, pp. 303–313, Berlin, Heidelberg: Springer, 2012 (doi: 10.1007/978-3-642-28151-8_30).

[11] A. Ahmad and M. A. Babar, "Software architectures for robotic systems: A systematic mapping study", *J. of Syst. and Software*, vol. 122, pp. 16–39, 2016 (doi: 10.1016/j.jss.2016.08.039).

[12] F. Dietrich *et al.*, "Dynamic distribution of robot control components under hard realtime constraints–modeling, experimental results and practical considerations", *J. of Syst. Architecture*, vol. 59, no. 10, pp. 1047–1066, 2013 (doi: 10.1016/j.sysarc.2012.12.001).

[13] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution", in *Proc. of the 47th Design Autom. Conf.*, Anaheim, CA, USA, 2010, pp. 731–736 (doi: 10.1145/1837274.1837461).

[14] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions", *Computers & Secur.*, vol. 68, pp. 81–97, 2017 (doi: 10.1016/j.cose.2017.04.005).

[15] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security – a survey" *IEEE Internet of Things J.*, vol. 4, no. 6, pp. 1802–1831, 2017 (doi: 10.1109/JIOT.2017.2703172).

[16] C. W. Axelrod, "Managing the risks of cyber-physical systems", in *Proc. IEEE Long Island Syst., Appl. and Technol. Conf. LISAT 2013*, Farmingdale, NY, USA, 2013 (doi: 10.1109/LISAT.2013.6578215).

[17] N. Falliere, L. O. Murchu, and E. Chien, "W32.stuxnet dossier", White paper, Symantec Corp., Security Response, vol. 5, no. 6, p. 29, 2011 [Online]. Available: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[18] A. Cherepanov and R. Lipovsky, "Industroyer: Biggest threat to industrial control systems since Stuxnet", 2017 [Online]. Available: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ (accessed 15 Nov., 2018).

[19] National Cybersecurity and Communications Integration Center, ICS-CERT Year in Review, 2016 [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf (accessed 15 Nov., 2018).

[20] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, "Security and privacy in cyber-physical systems: a survey of surveys", *IEEE Design Test*, vol. 34, no. 4, pp. 7–17, 2017 (doi: 10.1109/MDAT.2017.2709310).

[21] G. Sabaliauskaite, G. S. Ng, J. Ruths, and A. Mathur, "A comprehensive approach, and a case study, for conducting attack detection experiments in cyber–physical systems", *Robot. and Autonom. Sys.*, vol. 98, pp. 174–191, 2017 (doi: 10.1016/j.robot.2017.09.018).

[22] National Cybersecurity and Communications Integration Center, Incident response pie charts FY2016, 2016 [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_IR_Pie_Chart_S508C.pdf (accessed 15 Nov., 2018).

[23] "ISO/IEC JTC 1/SC 7 security functions iso/iec 10746-3" [Online]. Available: http://joaquin.net/ODP/Part3/15.html (accessed 15 Nov., 2018).

[24] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems", in *Proc. 28th Int. Conf. on Distrib. Comput. Syst. Worksh. ICDCS'08*, Beijing, China, 2008, pp. 495–500 (doi: 101109/ICDCS.Workshops.2008.40).

[25] A. A. Aburomman and M. B. Ibne Reaz, "A survey of intrusion detection systems based on ensemble and hybrid classifiers", *Computers & Secur.*, vol. 65, pp. 135–152, 2017 (doi: 10.1016/j.cose.2016.11.004).

[26] P. Szynkiewicz and A. Kozakiewicz, "Design and evaluation of a system for network threat signatures generation", *J. of Computat. Sci.*, vol. 22, pp. 187–197, 2017 (doi: 10.1016/j.jocs.2017.05.006).

[27] T. A. Zimmerman, "Metrics and Key Performance Indicators for Robotic Cybersecurity Performance Analysis", US Department of Commerce, National Institute of Standards and Technology, 2017 [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8177.pdf

[28] T. P. Vuong, G. Loukas, D. Gan, and A. Bezemskij, "Decision tree-based detection of denial of service and command injection attacks on robotic vehicles", in *Proc. IEEE Int. Worksh. on Inform. Forensics and Secur. WIFS2015*, Rome, Italy, 2015 (doi: 10.1109/WIFS.2015.7368559).

[29] T. P. Vuong, G. Loukas, and D. Gan, "Performance evaluation of cyber-physical intrusion detection on a robotic vehicle", in *Proc. IEEE Int. Conf. on Comp. and Inform. Technol.; Ubiquitous Comput. and Commun.; Dependable, Auton. and Secure Comput.; Pervasive Intell. & Comput. CIT/IUCC/DASC/PICOM 2015*, Liverpool, UK, 2015, pp. 2106–2113 (doi: 10.1109.CIT/IUCC/DASC/PICOM.2015.313).

[30] Á. M. Guerrero-Higueras, N. DeCastro-García, F. J. Rodríguez-Lera, and V. Matellán, "Empirical analysis of cyber-attacks to an indoor real time localization system for autonomous robots", *Computers & Secur.*, vol. 70, pp. 422–435, 2017 (doi: 10.1016/j.cose.2017.06.013).

[31] Á. M. Guerrero-Higueras, N. DeCastro-García, and V. Matellán, "Detection of cyber-attacks to indoor real time localization systems for autonomous robots", *Robot. and Auton. Syst.*, vol. 99, pp. 75–83, 2018 (doi: 10.1016/j.robot.2017.10.006).

[32] P. Guo, H. Kim, N. Virani, J. Xu, M. Zhu, and P. Liu, "Exploiting physical dynamics to detect actuator and sensor attacks in mobile robots", *arXiv preprint arXiv:1708.01834*, 2017.

[33] B. Dieber *et al.*, "Security for the robot operating system", *Robot. and Auton. Syst.*, vol. 98, pp. 192–203, 2017 (doi: 10.1016/j.robot.2017.09.017).

[34] N. Bezzo et *al.*, "Attack resilient state estimation for autonomous robotic systems", in *Proc. IEEE/RSJ Int. Conf. on Intell. Robots and Syst. IROS 2014*, Chicago, IL, USA, 2014, pp. 3692–3698 (doi: 10.1109/IROS.2014.6943080).

[35] R. White, G. Caiazza, H. Christensen, and A. Cortesi, "Procedurally provisioned access control for robotic systems", in *Proc. IEEE/RSJ Int. Conf. on Intell. Robots and Syst. IROS 2018*, Madrid, Spain, 2018, arXiv:1810.08125 [cs.RO].

Wojciech Dudek received his B.Sc. and M.Sc. degrees in Automation and Robotics from WUT and is currently a Research Assistant at Warsaw University of Technology (WUT), Institute of Control and Computation Engineering. His M.Sc. thesis has been recognized with the 1st place in the 2017 Young Innovators' Competition organized by the Industrial Research Institute for Automation and Measurements (PIAP). He is a contributor to international projects i.a. RAPP (European Commission – FP 7) and INCARE (European Commission AAL Joint Programme). His scientific interests focus on mobile robot control systems, their localization and navigation and harmonization of their tasks.

https://orcid.org/0000-0001-5326-1034
E-mail: wojciech.dudek@pw.edu.pl
Institute of Control and Computation Engineering
Warsaw University of Technology
Nowowiejska 15/19
00-665 Warsaw, Poland

Wojciech Szynkiewicz received his Ph.D. and D.Sc. (habilitation) degrees in Control and Robotics both from the Warsaw University of Technology (WUT). He works at WUT's Institute of Control and Computation Engineering. His research activities concentrate on multi-robot systems, sensor based motion planning, autonomous navigation of mobile robots, robot controller structures and robot cybersecurity. He is the author and co-author of over 90 papers published in conference proceedings, journals and books concerned with the above mentioned research subjects.

https://orcid.org/0000-0001-6348-1129
E-mail: W.Szynkiewicz@elka.pw.edu.pl
Institute of Control and Computation Engineering
Warsaw University of Technology
Nowowiejska 15/19
00-665 Warsaw, Poland

Paper

Battery Drain Denial-of-Service Attacks and Defenses in the Internet of Things

Philokypros P. Ioulianou[1], Vassilios G. Vassilakis[1], and Michael D. Logothetis[2]

[1] *Department of Computer Science, University of York, York, United Kingdom*
[2] *Department of Electrical and Computer Engineering, University of Patras, Patras, Greece*

https://doi.org/10.26636/jtit.2019.131919

Abstract—IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) is a popular routing protocol used in wireless sensor networks and in the Internet of Things (IoT). RPL was standardized by the IETF in 2012 and has been designed for devices with limited resources and capabilities. Open-source RPL implementations are supported by popular IoT operating systems (OS), such as ContikiOS and TinyOS. In this work, we investigate the possibility of battery drain Denial-of-Service (DoS) attacks in the RPL implementation of ContikiOS. In particular, we use the popular Cooja simulator and implement two types of DoS attacks, particularly version number modification and "Hello" flooding. We demonstrate the impact of these attacks on the power consumption of IoT devices. Finally, we discuss potential defenses relying on distributed intrusion detection modules.

Keywords—battery drain, ContikiOS, Cooja simulator, denial-of-service, intrusion detection, IoT, RPL.

1. Introduction

The Internet of Things (IoT) has found numerous applications in different domains, such as home automation, industrial control, health monitoring, intelligent transportation, and smart grid [1], [2]. IoT devices usually have limited resources, low computational power, small batteries, as well as limited memory and storage. Nevertheless, IoT devices are able to collect data, exchange small pieces of data through the Internet or directly with other devices, and perform lightweight computations.

Many IoT networks rely on the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) [3]. In 2012, the Internet Engineering Task Force (IETF) standardized RPL, which has been designed for resource-constrained devices. Open-source RPL implementations are supported by well-known IoT operating systems (OS), such as ContikiOS [4] and TinyOS [5].

Nowadays, many security approaches and cryptographic mechanisms exist for securing traditional networks. However, oftentimes these measures cannot be applied to IoT devices due to their limited capabilities mentioned above. As a result, many IoT devices are equipped with weak or no security measures [6] and become targets of cyberattacks. Such attacks have multiplied over the past years [7]. Recent examples of cyberattacks include the Mirai botnet [8] and its evolution, Chalubo botnet [9], which exploited the default/weak passwords or OS vulnerabilities in more than 100,000 IoT devices (such as IP cameras and home routers) and launched Distributed Denial of Service (DDoS) attacks affecting multiple targets. Such incidents suggest that IoT devices offer weak security and that proper defenses should be implemented to secure consumers, businesses and critical infrastructure.

Many attacks on IoT devices that have been launched recently exploit the properties of RPL and typically include DoS [10], [11] and routing attacks [12], [13]. Detection of and effective defense against such attacks is currently an open research problem [14], [15].

In this paper, we consider the RPL implementation of ContikiOS, namely ContikiRPL [16]. We focus on two popular types of DoS attacks: "Hello" flooding [11] and version number modification [17], [18], which can drain the batteries of IoT devices. We have implemented these attacks using the Cooja simulator [19], which is used to simulate the behavior of ContikiOS. We demonstrate how these attacks may impact the power consumption of IoT devices and render some devices unreachable. Following the presentation of our simulation results, we discuss potential defenses and detection approaches. In particular, we propose a modular Intrusion Detection System (IDS) that comprises a set of distributed detection modules and a border router acting as a centralized detection module.

The rest of the paper is structured as follows: In Section 2, we describe the Cisco 7-layer IoT model we have adopted. In Section 3, we briefly review the possible attacks in IoT networks. In Section 4, we demonstrate the most significant IDS solutions currently existing for IoT. In Section 5, we describe our "Hello" flooding and version number modification attack launched with the use of the Cooja simulator and present the simulation results obtained. In Section 6, we present our proposed IDS design. In Section 7, we conclude and discuss potential future research directions.

2. Cisco's 7-Layer IoT Model

In this work, we adopt Cisco's 7-layer model [20], as it is one of the most detailed IoT references. Figure 1 shows its layers. In this paper, we mostly focus on layers 1–3.

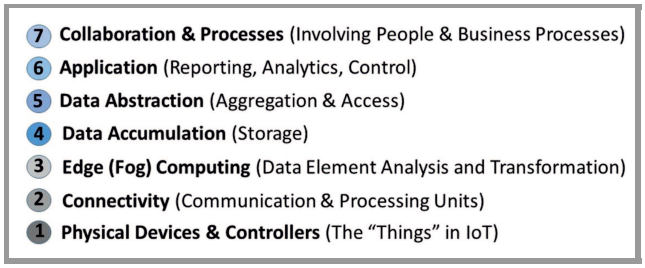


Fig. 1. Cisco's 7-layer IoT model.

Beginning from layer 1, smart or physical devices transmit or receive data. Layer 2 refers to the connectivity among the devices, located within the same network or across multiple networks. In many implementations, data may be transferred reliably between IoT devices using the existing network infrastructure. Layer 3 includes functionalities related to data analysis and transformation. Specifically, the processing of network packets occurs in that layer, so that packets are understandable to the higher layers. Layer 4 is where data is accumulated and is available for use by specific applications. Data is abstracted in layer 5. In other words, data from various sources is collected and processed to be easily accessible by applications. IoT applications read the information in layer 6. The top layer, layer 7, is where the end user's business processes live. The IoT system will become useful only when people cooperate and make use of IoT applications and their data.

3. Attacks in IoT

The majority of IoT devices have weak or no security at all, making it easy for an attacker to exploit them. As a result, critical information may be stolen from devices or they may be used to cause harm in other networks. Below, we briefly review the most significant attack types against IoT devices. The 7-layer model by Cisco is assumed to describe attacks.

At the layer of physical devices, replacing firmware of a smart device with its malicious counterpart could permit the attacker to read data in transit or data stored in the device. Another method of hardware exploitation is the non-network side-channel attack. In that attack, electromagnetic signals of the device are monitored by the attacker to expose the status of the device. DoS attack constitutes another threat for smart devices. Resource exhaustion and battery draining are some examples of DoS attacks [21]. In these attacks the attacker may prevent a device from sleeping by periodically transmitting "Hello" messages or may drain the limited power resources by submitting heavy computational tasks. Apart from DoS attacks, the adversary could attack the network by cloning a node. In this way, packets received by the node could be redirected or modified.

At the connectivity level, eavesdropping is a popular attack method in which the goal of the attacker is to export confidential information including usernames and passwords. Therefore, the attacker may learn about the network infrastructure, enter and modify device data or steal important information. Also, at this level, devices are vulnerable to Man-in-the-Middle (MitM), routing and replay attacks [22] in which attackers try to spoof and drop packets or even modify routing information. In addition, connectivity level DoS attacks may exert a negative impact on the performance of the IoT network. Some examples of DoS attacks include packet flooding and signal jamming, whose goal is to corrupt the device's communication signal. Last but not least, IoT devices may be exploited and transformed into bots to carry out DoS attacks against selected targets. Chalubo and Mirai botnets are the most recent examples of this threat [8], [9].

At the edge computing level, servers could be exploited by injecting malicious input and stealing important data. Similarly, attackers may try to leak information from a device or server to learn which services are used in the vulnerable IoT network. Database warnings or errors, for example, provide valuable information to attackers.

4. Intrusion Detection Systems for IoT

Over time, IDSs have been considered by researchers as security measures for keeping IoT networks secured. However, traditional network detection algorithms have different requirements than those based on IoT. Thus, adapting traditional methods in IoT environments is a challenging task. Certain IoT characteristics, such as the limited processing power of intelligent devices, different network structures and a variety of IoT device protocols, introduce new challenges which an IoT-based IDS must take into account [23]. Below, we present the latest IDS solutions for IoT.

The first developed IDS that aims at protecting smart devices irrespective of specific IoT protocols or applications is Kalis [24]. Kalis is a network-based, hybrid signature/anomaly-based, hybrid centralized/distributed, online IDS. The detection strategy selected depends on the specific features of the protected network. Furthermore, Kalis obtains knowledge from network-installed modules and tries to prevent intrusion by taking into account the current topology of the network and by conducting traffic analysis. Moreover, it can be extended to support new protocol standards and may improve detection performance by allowing knowledge sharing between the nodes. It is implemented on routers using the OpenWRT firmware [25]. Evaluation is performed using 6 TelosB devices programmed in TinyOS [5]. Experimental results show that Kalis achieves 100% accuracy in detecting most of the attacks. Thus, it offers better detection performance than Snort [26] and other traditional IDS solutions.

Svelte IDS is another interesting work in the field [27]. This is an anomaly- and signature-based IDS, developed to prevent RPL-based routing attacks affecting IoT devices [3]. Some of the attacks considered include selective forwarding, sink-hole attack and spoofed or altered information. As far as the approach to node placement is concerned, Svelte has a centralized module, called 6LoWPAN border router (6BR), which carries out heavy calculations, and a number of resource-restricted modules monitoring network devices. The 6BR consists of three components. The first one is the 6LoWPAN mapper which gathers information from sensors to regenerate the network. The second component is the detection system which uses the obtained information to detect potential intrusions. The third component is a mini firewall that prevents the entry of malicious traffic into the network. In IoT devices, the first and third components are integrated.

Although quite a few IoT-based IDSs have been developed recently, current solutions have certain constraints. Kalis, for example, requires deployment of detection modules specific for the attack type. This could create a complex network resulting in poor detection performance. Additionally, it utilizes Wi-Fi for communication. This means that interference between smart sensors and Kalis nodes could occur if nodes are in close proximity. Svelte has also some limitations as it is a host-based IDS, meaning that the sensor's software must be modified. This, however, would be very challenging for larger networks, which is a typical case in many IoT application domains. Another major issue is that Svelte has a high false detection rate. This was proved by Matsunaga *et al*. [28], who proposed a scheme to reduce false detection rate. However, further experiments are needed to ensure that the solution is robust and scalable.

In conclusion, a technologically enhanced solution is needed to protect IoT networks against several possible attacks. We considered the aforementioned limitations during the design of our proposed IDS.

5. Implementing Battery Drain DoS Attacks in Cooja

Before designing an effective IDS, the initial step is to implement and study the impact of several attacks on each device and on the entire network. After that, by launching attacks using various configuration parameters and intensities, different detection methods can be implemented, tested, and enhanced.

We use the Cooja simulator [19] for testing and experimentation, which is becoming increasingly popular among IoT researchers. It is also particularly suitable for experiments in the real world, since the developed applications can be directly uploaded to real hardware. Cooja can be used to simulate the behavior of ContikiOS – a popular open source IoT operating system [29].

In this work, two IoT-specific DoS attacks have been implemented in Cooja, namely version number modification and "Hello" flooding. These attacks exploit the RPL protocol's features and affect the power consumption of IoT devices. Cooja provides an implementation of the RPL protocol, called ContikiRPL [16].

5.1. RPL Overview

RPL organizes nodes along a destination-oriented, directed, acyclic graph (DODAG) [30]. The root node initiates the creation of graphs by regularly generating DODAG information object (DIO) messages, which are advertised via link-local multicasts. DIO messages include such information as identity of the root, the metrics used for routing and the depth of the originating router (called "rank").

The "Hello" flooding attack in RPL occurs when a large number of DODAG information solicitation (DIS) messages are transmitted by the malicious node to other nodes. This causes the recipient nodes to reply by sending DIO messages. Consequently, network floods with packets and the node's batteries are drained. Similarly, in the version number modification attack [18], the malicious node changes the DODAG version number before forwarding the received DIO messages to the next hop. Nodes receiving a malicious DIO message with the modified version number reset their trickle timer, store the new version number in their memory and advertise it to their neighbors via DIO messages. Note that the root uses the version number to control the so-called "global repairs" of the RPL network and to ensure that the latest routes are available to nodes in DODAG. Global repair is the repair mechanism that is initiated by the root to rebuild the network. During this process, it increases the version number of RPL DODAG and the whole DODAG is reconstructed. This method ensures a loop free and optimized tree based on the objective function used. Still, this makes IoT nodes perform useless computations and waste their energy. Thus, modifying the version number will cause unnecessary global rebuilds of the DODAG, create loops in the topology, as well as exhaust the nodes.

5.2. Simulation Scenarios and Results

Below are two scenarios, simulated in Cooja, which show the effects of the DoS attacks mentioned above. Applications of the UDP client-server model are used on top of each node. Seven Tmote Sky nodes [31] were simulated running ContikiOS. The network, depicted in Fig. 2, consists of one server (root node with ID 1) and six client nodes with IDs from 2 to 7.

In the first scenario, no compromised nodes exist. Each node is configured to send messages to the server at specific intervals. These messages contain various information about the sending node, such as its battery indicator and temperature. In the second scenario, node 7 is malicious/compromised and performs DoS attacks. Specifically, node 7 has been configured to transmit a big number of DIS messages to its neighbors. In addition, it changes the DODAG version number, so that global repairs are initiated.

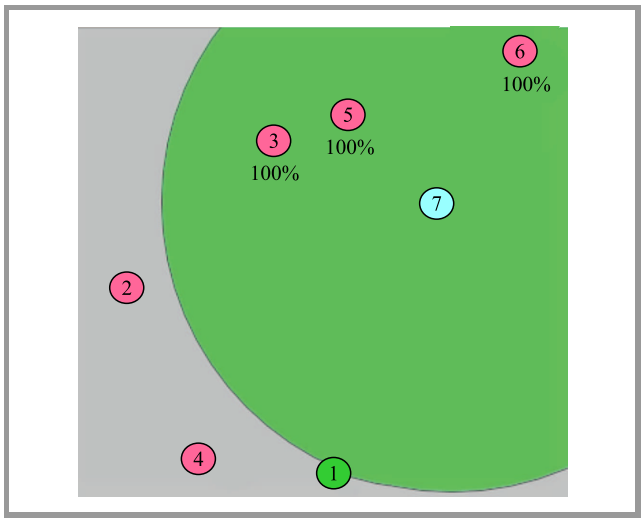


Fig. 2. Network topology for Cooja simulations.

The simulation time in our experiments in each scenario is 10 min. The configuration used for each node is shown in Table 1. The server is the receiver of all messages exchanged in the network. As a result, it is always powered on. The Radio Duty Cycle (RDC) driver is responsible for saving as much as possible power for the device. ContikiOS implements several RDC drivers, but the server uses NullRDC, which does not save power. The Medium Access Control (MAC) driver is responsible for reliably transferring packets via the radio medium. If any collisions occur, it re-transmits the packets until they are delivered. All nodes in our scenarios use the Carrier Sense Multiple Access (CSMA) driver at the MAC layer to guarantee packet delivery. In contrast with benign and malicious nodes, the server does not transmit DIS messages.

Benign nodes send data to the server. They are configured to send a DIS message every 60 s until they successfully join the network. The malicious node broadcasts 80 DIS message every second, thus launching the "Hello" flooding attack. Benign and malicious nodes in this scenario are configured to use NullRDC as RDC driver and CSMA as MAC driver. This setup will keep the devices always on.

In the first scenario, the network topology is formed as shown in Fig. 3. The numbers displayed on each link indicate the expected number of transmission (ETX) that a node

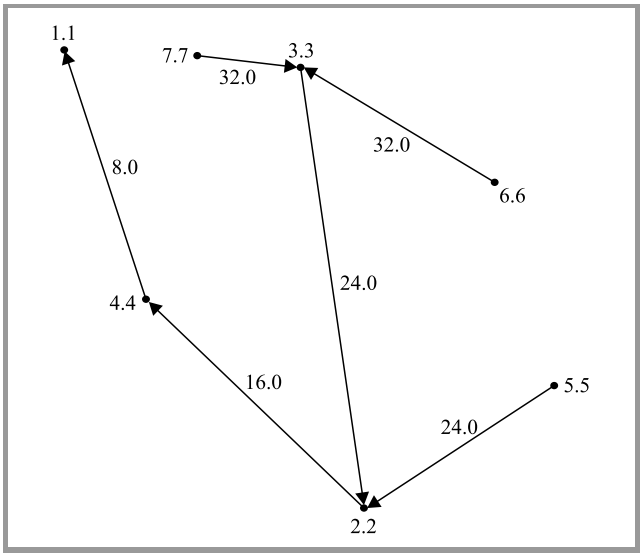


Fig. 3. Scenario 1 (normal operation): network topology.

needs to make to the destination in order to successfully deliver a message. For instance, the ETX value of node 4 next to the server (node 1) is 8. In Fig. 3 we also note that messages of node 7 must be transmitted via nodes 3, 2 and 4 to get to the server. Note that node 7 is not malicious and runs the same code as all other nodes in this scenario. In Fig. 4 the power consumption of each node is shown. Measurements were collected using the PowerTracker tool in Cooja. As expected, all nodes are almost always on (99.87% of the time, on average) and have very low values of radio TX and radio RX. This is normal for small-sized networks.

In the second scenario, nodes use the same RDC and MAC driver configuration as before. Node 7 has, however, been modified to transmit 80 DIS messages and to increase the DODAG version number before transmitting the received

Table 1
Types and configuration of nodes

Node type	Description	Radio Duty Cycle (RDC)	Medium Access Control (MAC)	RPL conf. (DIS interval)
Server	Receives messages without doing any processing or sending acknowledgments	NullRDC	CSMA	—
Benign node	Creates a mesh network by using RPL protocol and sends data to server	ContikiMAC or NullRDC	CSMA	60 s
Malicious node	Uses RPL protocol to broadcast DIS control messages to neighbors (flooding attack) and modify version number	ContikiMAC or NullRDC	CSMA	Every second

Mote	Radio on (%)	Radio TX (%)	Radio RX (%)
Sky 1	99.91%	0.01%	0.06%
Sky 2	99.79%	0.05%	0.11%
Sky 3	99.92%	0.03%	0.10%
Sky 4	99.86%	0.06%	0.06%
Sky 5	99.91%	0.02%	0.11%
Sky 6	99.79%	0.02%	0.07%
Sky 7	99.88%	0.02%	0.07%
AVERAGE	99.87%	0.03%	0.08%

Fig. 4. Scenario 1 (normal operation): power consumption measurements.

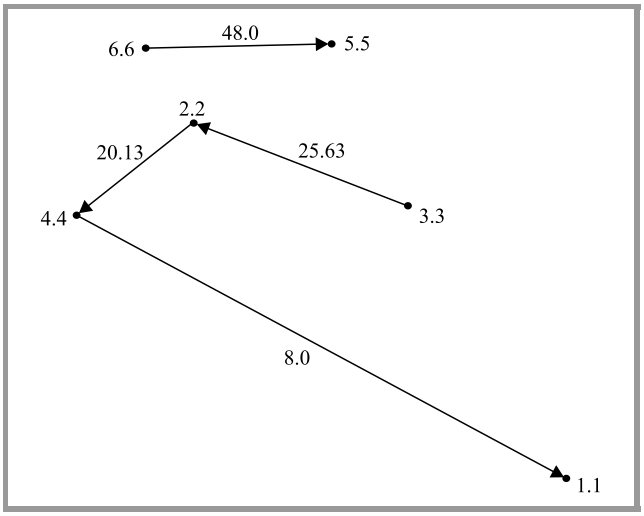


Fig. 5. Scenario 2 (attack): network topology.

DIO messages to the server. Changing the version number leads to global repair and to the formation of two different DODAGs. Every few minutes, global repair is triggered. As a result, the routes change quickly. The topology of the network is therefore not stable and some nodes may be disconnected from the server or from other nodes. There is one such situation Fig. 5, where at that particular moment nodes 5 and 6 do not have a route to the server. The impact of the attack is demonstrated in Fig. 6, which shows the measurements of power consumption. In adjacent nodes 3, 5, and 6, the attack caused high radio RX, and high radio TX in node 7. As a result, both malicious/compromised and neighboring nodes are depleted of energy.

Mote	Radio on (%)	Radio TX (%)	Radio RX (%)
Sky 1	99.88%	0.04%	0.12%
Sky 2	99.89%	0.11%	0.36%
Sky 3	99.80%	0.12%	2.12%
Sky 4	99.92%	0.14%	0.14%
Sky 5	99.80%	0.15%	2.09%
Sky 6	99.83%	0.09%	2.04%
Sky 7	99.91%	1.82%	0.32%
AVERAGE	99.86%	0.35%	1.03%

Fig. 6. Scenario 2 (attack): power consumption measurements.

In the previous scenarios, nodes used the same RDC and MAC drivers. However, using a different RDC driver may produce different results. In ContikiOS, ContikiMAC is another option for RDC driver. For this reason, the two scenarios were repeated using the ContikiMAC RDC driver in benign and malicious nodes, while keeping the same MAC driver. Starting with the normal scenario, the nodes' power consumption is shown in Fig. 7. As expected, ContikiMAC enables sleep mode and this is clearly shown by the very low percentage of radio on for all nodes except for the server.

Mote	Radio on (%)	Radio TX (%)	Radio RX (%)
Sky 1	99.82%	0.11%	0.18%
Sky 2	1.93%	0.87%	0.05%
Sky 3	1.94%	0.87%	0.06%
Sky 4	1.16%	0.24%	0.06%
Sky 5	1.25%	0.35%	0.07%
Sky 6	1.20%	0.30%	0.04%
Sky 7	1.29%	0.39%	0.06%
AVERAGE	15.34%	0.45%	0.07%

Fig. 7. Scenario 1 using ContikiMAC: power consumption measurements.

In addition, radio TX is 0.45%, on average, which means that nodes sleep most of the time and send very few packets within the network. Average radio RX is even lower than radio TX, because it is the server that is the destination of the majority of packets. The corresponding network topology is shown in Fig. 8. It may be noticed that all nodes communicate with the server by using their next hop.

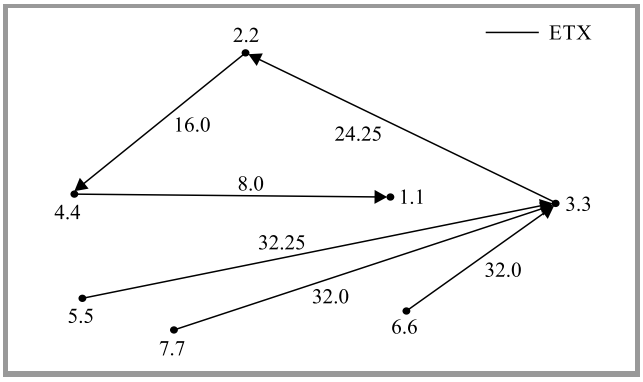


Fig. 8. Scenario 1 using ContikiMAC: network topology.

Mote	Radio on (%)	Radio TX (%)	Radio RX (%)
Sky 1	100.00%	0.07%	0.24%
Sky 2	3.78%	2.08%	0.19%
Sky 3	59.37%	2.20%	35.70%
Sky 4	4.28%	2.67%	0.03%
Sky 5	59.60%	1.99%	36.06%
Sky 6	60.17%	2.42%	36.08%
Sky 7	63.98%	47.33%	0.94%
AVERAGE	50.17%	8.39%	15.61%

Fig. 9. Scenario 2 using ContikiMAC: power consumption measurements.

Using the same node configuration, the second scenario with a malicious node was repeated. In this case, the power consumption of nodes is affected by the malicious node, as shown in Fig. 9. Although nodes should be sleeping most of the time, they are ON for 50% of the time. This is true for the server as well. The difference compared with the nor-

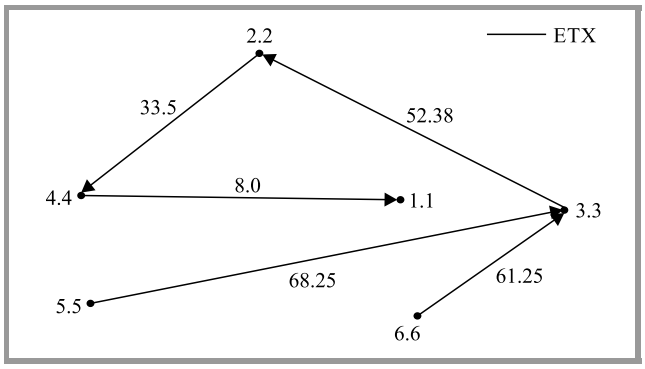


Fig. 10. Scenario 2 using ContikiMAC: network topology.

mal scenario is about 35%, which is significant. The reason for this behavior is caused by the fact that the malicious node 7 broadcasts DIS messages requiring a DIO reply from its neighbors. This is also the reason why nodes 3, 5 and 6 have the highest radio RX percentage in comparison with other nodes. These nodes are closer to node 7 and are more affected than other nodes. Furthermore, node 7 transmits all the time and has, therefore, the highest percentage of radio TX. Looking at the network topology in Fig. 10, one may see that some links have unusually high ETX values. The reason for that are the global repairs initiated, which assign different ETX values to links. Nodes located near the malicious node have a worse ETX value in their links in comparison with other nodes. Moreover, the malicious node is not shown in the presented network topology because it never joins the DODAG and, therefore, no information is sent to the server.

6. Proposed IDS

6.1. Architecture and Components

In addition to the typical sensor nodes, two new types of devices are considered: i) IDS routers for the handling of both the detection module and the firewall, and ii) sensor-like devices, called IDS detectors, for the monitoring and transmission of suspicious traffic to the router. In a typical scenario of a small IoT network, one IDS router acts as the border router (BR) of the network, while several IDS detectors are deployed near the nodes. This scenario is demonstrated in Fig. 11. This means that devices that need to communicate with an external server send all requests via the IDS router. The router analyses all passing traffic, and determines whether or not the sending node is malicious.

IDS detectors monitor packets to help detect malicious nodes. Malicious devices may try to interrupt normal network operation internally without having to communicate with the router or external networks. In such cases, detectors log packets and if the behavior of a node corresponds to a known attack, relevant information is sent to the IDS router.

In the scenario shown in Fig. 11, we have 5 Tmote Sky sensors and an IDS consisting of one router and 2 detectors.

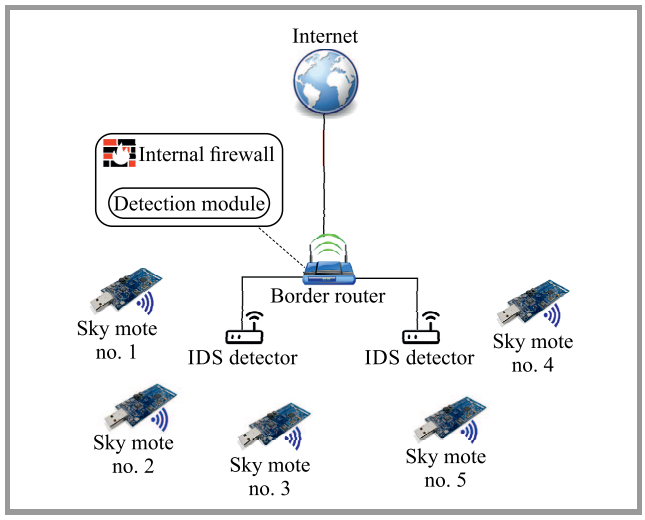


Fig. 11. High-level IDS architecture

The router is Internet connected and has two components: a detection module and a firewall. These components contribute to the internal and external protection of the network. The detection module executes specific algorithms to determine if malicious nodes exist or not in the network, while the firewall generates and enforces rules for stopping malicious traffic. The detectors are wired to the router in order to prevent interference or eavesdropping via a wireless channel. If the communication of the router and the detectors needs to be wireless, a proper secure wireless communication scheme will be used (e.g. [32]). IDS detectors capture any traffic exchanged among nearby sensors. Afterwards, a decision whether traffic should be forwarded to the router or not is taken based on a lightweight algorithm. We assume that detectors are resource-constrained. Algorithms that need heavy calculations or large memory are therefore not appropriate.

Collaboration between the router and the detectors helps monitor traffic from both internal and external interfaces. Some malicious devices, for example, may attempt to communicate with a remote & control server to download malicious files or instructions [33]. Other devices that are compromised may exchange traffic locally. The presented design takes all types of communications into account in order to block malicious nodes. The router captures Wi-Fi and IEEE 802.15.4 traffic. It is also capable of detecting attacks from ZigBee and IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) devices [3].

The proposed IDS stores malicious patterns in the router's detection module in the same way as other signature-based solutions. The router connects the internal network to the Internet and is assumed to have sufficient computing power to execute algorithms required to detect various attack types.

6.2. Mitigating Attacks

As mentioned earlier, the goal of the proposed IDS is to detect and prevent a large number of different types of

attacks, for instance DoS attacks that may occur in IoT networks to exhaust sensor node batteries. Moreover, routing attacks usually exploit RPL which is a routing protocol that many smart IoT network sensors currently use. Selective forwarding, sinkhole attack and clone ID are some of other well-known routing attacks [23], [34], [35].

The previous attacks can be detected using various techniques. Measuring the packet dropping rate, packet sending rate, the received signal strength (RSS), packet interval, and monitoring the number of node IDs in the network are some of the mitigation methods [36]. Specifically, the packet sending rate could be a good metric for detecting malicious nodes, as smart devices do not exchange many packets. A device that behaves abnormally and sends too many packets could be considered a malicious one.

Another useful metric is the packet interval. Each device is configured to communicate with other in specific time intervals. Malicious devices could exploit this feature and send more requests in small intervals. Our IDS can detect this behavior by taking into account the time intervals of all nodes in the network and by calculating the average time interval which will be considered normal behavior. Thus, any node exceeding the normal packet interval threshold will be considered as malicious. A threshold-based detection is a lightweight mechanism that allows IDS detectors to perform fast calculations and detect compromised nodes. According to [6], these well-known attacks may have a significant impact on the availability, as well as on the integrity of IoT systems.

Regarding the scalability of the proposed IDS, it is expected to have good efficiency even in large networks. To ensure that, only the suspicious traffic will be forwarded from detectors to the router. This means that detectors will perform some specific computations (e.g. packet sending rate and packet interval) and will forward the node's traffic to the router for further investigation (e.g. signature matching) only if the metric of interest is above the threshold value. Apart from that, the router will have an overall picture of the network and will block suspicious nodes.

6.3. Detection Module and Firewall

As mentioned before, the detection module at the router plays an important role in the proposed IDS. This component determines if a node is malicious or not. Decision will be taken based on the information collected for each individual device. For example, a device sending a large number of packets with a high rate or a node with RSS value above the threshold value may be regarded as malicious. As a consequence, that device may be removed from the network, its IP address will be blacklisted, a proper firewall rule will be generated and the network administrator will be notified. However, complex attacks, such as selective forwarding, are not easy to detect and may need more time to identify. For this reason, the detection module will store signatures of known IoT malware. Packets matching a stored malicious signature will be blocked and the source and destination nodes will be blacklisted.

The firewall at the router is added as an extra layer of protection. The IP addresses of malicious nodes will be blocked if they match any stored firewall rules. The detection module will proceed to banning a node from the network only if it has information of its malicious behavior. In this case, a new firewall rule will be created including the IP of the node, and traffic between the node and the Internet will be stopped.

As regards the strategy of placing IDS modules, two methods are usually distinguished: network-based and host-based [36]. In the network-based method, the agent is placed near the base station, so that it can monitor the traffic sent by the devices, creating an additional communication overhead. In the host-based method, the agent is embedded in all nodes, consuming a significant portion of the node's resources and energy. In this work, a hybrid approach that combines both methods, has been followed. A centralized node (i.e. the router) keeps signatures, analyzes traffic and detects sensor or Internet attacks. Some decentralized nodes (i.e. detectors) execute lightweight tasks, such as monitoring and sending suspicious packets to the router. The advantage of this placement strategy is that traffic can be captured and attacks can be detected from all network segments. Furthermore, deploying detectors near sensors helps detect attack attempts faster and more efficiently, instead of waiting for the malicious packets to pass via the router.

7. Conclusion and Future Work

In this paper, we studied the impact of battery drain DoS attacks on IoT devices. Cooja simulator is the platform chosen for implementing IoT-based attacks. It supports application development for ContikiOS. The demonstrated scenarios include attack scenarios where a compromised sensor performs DoS attacks based on "Hello" flooding and version number modifications. As demonstrated, the attack may negatively affect the energy consumption of IoT devices.

We also proposed a new IDS for securing IoT networks and devices. The proposed IDS follows the hybrid placement approach for effective detection of intrusions originating both from external and internal networks. Some of the advantages of the proposed IDS are: i) no firmware modification of IoT devices is needed, ii) the detectors are wired to avoid jamming and other wireless attacks, iii) support for generic IDS modules, and iv) support for heterogeneous devices (e.g. ZigBee and 6LoWPAN).

As a future work, we plan to simulate attacks on larger networks of different topologies. In addition, the "Hello" flooding attack will be further studied using different temporal and spatial distributions of RPL messages. Apart from that, we aim to develop and test the proposed IDS in Cooja. IDS performance will be evaluated by simulating attack scenarios and obtaining useful metrics, such as detection rate and false positives rate. The IDS will be tested for DoS, routing and other types of attacks. Finally,

to test their performance in a real world IoT environment, IDS modules will be imported into ContikiOS.

References

[1] V. G. Vassilakis, I. D. Moscholios, J. S. Vardakas, and M. D. Logothetis, "On the digital certificate management in advanced metering infrastructure networks", in *Proc. IEICE Inform. and Commun. Technol. Forum ICTF*, Poznań, Poland, 2017.

[2] B. A. Alohali and V. G. Vassilakis, "Secure and energy-efficient multicast routing in smart grids", in *Proc. 10th IEEE Int. Conf. on Intell. Sensors, Sensor Netw. and Inform. Process. ISSNIP*, Singapore, 2015 (doi: 10.1109/ISSNIP.2015.7106929).

[3] T. Winter *et al.*, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, IETF, March 2012.

[4] Contiki: The Open Source OS for the Internet of Things [Online]. Available: http://www.contiki-os.org/ (accessed: 2019.01.14).

[5] TinyOS: An OS for Embedded, Wireless Devices [Online]. Available: https://github.com/tinyos/tinyos-main (accessed: 2019.01.14).

[6] Gemalto. The State of Internet of Things Security [Online]. Available: http://www2.gemalto.com/iot/index.html (accessed: 2019.01.14).

[7] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks", in *Proc. 3rd Int. Conf. on Elec. Design ICED*, Phuket, Thailand, 2016, pp. 321–326 (doi: 10.1109/ICED.2016.7804660).

[8] Symantec Security Response, Mirai: What you need to know about the botnet behind recent major DDoS attacks, Oct. 2016 [Online]. Available: https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks

[9] T. Easton, "Chalubo botnet wants to DDoS from your server or IoT device", Oct. 2018 [Online]. Available: https://news.sophos.com/en-us/2018/10/22/chalubo-botnet-wants-to-ddos-from-your-server-or-iot-device

[10] C. Pu and T. Song, "Hatchetman attack: A denial of service attack against routing in low power and lossy networks", in *5th IEEE Int. Conf. on Cyber Secur. and Cloud Comput. CSCloud and 4th IEEE Int. Conf. on Edge Comput. and Scalable Cloud EdgeCom*, Shanghai, China, 2018, pp. 12–17 (doi: 10.1109/CSCloud/EdgeCom.2018.00012).

[11] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-service detection in 6LoWPAN based Internet of Things", in *Proc. 9th IEEE Int. Conf. on Wirel. and Mobile Comput., Netw. and Commun. WiMob*, Lyon, France, 2013, pp. 600–607 (doi: 10.1109/WiMOB.2013.6673419).

[12] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the RPL-based Internet of Things", *Int. J. of Distrib. Sensor Netw.*, vol. 9, no. 8, pp. 1–11, 2013 (doi: 10.1155/2013/794326).

[13] A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in RPL-based Internet of Things", *Int. J. of Netw. Secur.*, vol. 18, no. 3, pp. 459–473, 2016 (doi: 10.6633/IJNS.201605.18(3).07).

[14] H.-S. Kim, J. Ko, D. E. Culler, and J. Paek, "Challenging the IPv6 routing protocol for low-power and lossy networks (RPL): A survey", *IEEE Commun. Surveys & Tutor.*, vol. 19, no. 4, pp. 2502–2525, 2017 (doi: 10.1109/COMST.2017.2751617).

[15] P. P. Ioulianou, V. G. Vassilakis, I. D. Moscholios, and M. D. Logothetis, "A signature-based intrusion detection system for the Internet of Things", in *Proc. IEICE Inform. and Commun. Technol. Forum ICTF*, Graz, Austria, 2018.

[16] N. Tsiftes, J. Eriksson, and A. Dunkels, "Low-power wireless IPv6 routing with ContikiRPL", in *Proc. 9th ACM/IEEE Int. Conf. on Inform. Process. in Sensor Netw.*, Stockholm, Sweden, 2010, pp. 406–407 (doi: 10.1145/1791212.1791277).

[17] A. Dvir, T. Holczer, and L. Buttyan, "VeRA-version number and rank authentication in RPL", in *Proc. IEEE 8th Int. Conf. on Mob. Ad-hoc and Sensor Syst. MASS 2011*, Valencia, Spain, 2011, pp. 709–714 (doi: 10.1109/MASS.2011.76).

[18] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "A study of RPL DODAG version attacks", in *Proc. IFIP Int. Conf. on Autonomous Infrastruc., Manag. and Secur.*, Brno, Czech Republic, 2014, pp. 92–104 (doi: 10.1007/978-3-662-43862-6_12).

[19] F. Osterlind *et al.*, "Cross-level sensor network simulation with Cooja", in *Proc. 31st IEEE Int. Conf. on Local Comp. Netw.*, Tampa, FL, USA, 2006, pp. 641–648 (doi: 10.1109/LCN.2006.322172).

[20] "The Internet of Things Reference Model", Cisco, 2014 [Online]. Available: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf

[21] Y. Yang *et al.*, "A survey on security and privacy issues in Internet-of-Things", *IEEE Internet of Things J.*, vol. 4. no. 5, pp. 1250–1258, 2017 (doi: 10.1109/JIOT.2017.2694844).

[22] F. Ayotunde Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey", *J. of Network and Comp. Appl.*, vol. 88, pp. 10–28, 2017 (doi: 10.1016/j.jnca.2017.04.002).

[23] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things", *J. of Network and Comp. Appl.*, vol. 84, pp. 25–37, 2017 (doi: 10.1016/j.jnca.2017.02.009).

[24] D. Midi, A. Rullo, A. Mudgerikar, and E. Bertino. "Kalis – a system for knowledge-driven adaptable intrusion detection for the Internet of Things", in *Proc. IEEE 37th Int. Conf. on Distrib. Comput. Syst. ICDCS 2017*, Atlanta, GA, USA, 2017, pp. 656–666 (doi: 10.1109/ICDCS.2017.104).

[25] OpenWRT: a Linux OS for Embedded Devices [Online]. Available: https://openwrt.org (accessed: 2019.01.14).

[26] M. Roesch *et al.*, "Snort: Lightweight intrusion detection for networks", in *Proc. of the 13th USENIX Conf. on System Admin. LISA'99*, Seattle, WA, USA, 1999, vol. 99, pp. 229–238.

[27] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: real-time intrusion detection in the Internet of Things", *Ad Hoc Netw.*, vol. 11. no. 8, pp. 2661–2674, 2013 (doi: 10.1016/j.adhoc.2013.04.014).

[28] T. Matsunaga, K. Toyoda, and I. Sasase, "Low false alarm rate RPL network monitoring system by considering timing inconstancy between the rank measurements", in *Proc. 11th Int. Symp. on Wirel. Commun. Syst. ISWCS 2014*, Barcelona, Spain, 2014, pp. 427–431 (doi: 10.1109/ISWCS.2014.6933391).

[29] A. Dunkels, B. Gronvall, and T. Voigt, "Contiki – a lightweight and flexible operating system for tiny networked sensors", in *Proc. 29th IEEE Int. Conf. on Local Comp. Netw.*, Tampa, FL, USA, 2004, pp. 455–462 (doi: 10.1109/LCN.2004.38).

[30] E. Baccelli, M. Philipp, and M. Goyal, "The P2P-RPL routing protocol for IPv6 sensor networks: Testbed experiments", in *Proc. 19th Int. Conf. on Software, Telecommun. and Comp. Netw. SoftCOM 2011*, Split, Croatia, 2011, pp. 656–666 [Online]. Available: https://hal.archives-ouvertes.fr/hal-00651603/document

[31] J. Polastre, R. Szewczyk, and D. Culler, "Telos: enabling ultra-low power wireless research", in *Proc. 4th Int. Symp. on Inform. Process. in Sensor Netw.*, Boise, ID, USA, 2005, pp. 364–369 (doi: 10.1109/IPSN.2005.1440950).

[32] B. A. Alohali, V. G. Vassilakis, I. D. Moscholios, and M. D. Logothetis, "A secure scheme for group communication of wireless IoT devices", in *Proc. 11th IEEE/IET Int. Symp. on Commun. Syst., Netw., and Digit. Sig. Process. CSNDSP 2018*, Budapest, Hungary, 2018 (doi: 10.1109/CSNDSP.2018.8471871).

[33] S. Khattak, N. R. Ramay, K. R. Khan, A. A Syed, and S. Ali Khayam, "A taxonomy of botnet behavior, detection, and defense", *IEEE Commun. Surveys & Tutor.*, vol. 16, no. 2, pp. 898–924, 2014 (doi: 10.1109/SURV.2013.091213.00134).

[34] P. Pongle and G. Chavan, "A survey: attacks on RPL and 6LoWPAN in IoT", in *Proc. Int. Conf. on Pervasive Comput. ICPC 2015*, Pune, India, 2015 (doi: 10.1109/PERVASIVE.2015.7087034).

[35] P. Perazzo, C. Vallati, G. Anastasi, and G. Dini, "DIO suppression attack against routing in the Internet of Things", *IEEE Commun. Lett.*, vol. 21, no. 11, pp. 2524–2527, 2017 (doi: 10.1109/LCOMM.2017.2738629).

[36] A. Rghioui, A. Khannous, and M. Bouhorma, "Denial-of-service attacks on 6LoWPAN-RPL networks: threats and an intrusion detection system proposition", *J. of Adv. Comp. Sci. & Technol.*, vol. 3, no. 2, pp. 143–153, 2014 (doi: 10.14419/jacst.v3i2.3321).

Philokypros P. Ioulianou received his B.Sc. degree in Computer Science from the University of Cyprus in 2016, and M.Sc. in Advanced Computer Science with specialization in Computer Security from the University of Manchester in 2017. He is currently a Ph.D. student at the University of York, UK. His research interests are in the area of computer and network security, IoT (Internet of Things) and wireless sensor security.

https://orcid.org/0000-0001-7436-4470
E-mail: pi533@york.ac.uk
Department of Computer Science
University of York
York, United Kingdom

Vassilios G. Vassilakis received his Ph.D. degree in Electrical and Computer Engineering from the University of Patras, Greece in 2011. He is currently a lecturer in Cyber Security at the University of York, UK. He's been involved in EU, UK, and industry funded R&D projects related to the design and analysis of future mobile networks and Internet technologies. His main research interests are in the areas of network security, Internet of Things, next-generation wireless and mobile networks, and software-defined networks. He is published over 90 journal/conference papers. He is served as an Associate Editor in IEICE Transactions on Communications, IET Networks, and Elsevier Optical Switching & Networking.

https://orcid.org/0000-0003-4902-8226
E-mail: vv573@york.ac.uk
Department of Computer Science
University of York
York, United Kingdom

Michael D. Logothetis received his Dipl. Eng. degree and Doctorate in Electrical Engineering, both from the University of Patras, Patras, Greece, in 1981 and 1990 respectively. From 1991 to 1992 he was Research Associate in NTT's Telecommunication Networks Laboratories, Tokyo, Japan. In 2009 elected (Full) Professor in the ECE Department of the University of Patras. His research interests include teletraffic theory, simulation and performance optimization of telecommunications networks. He has published over 200 conference/journal papers. He has become a Guest Editor in: Mediterranean Journal of Electronics and Communications, Mediterranean Journal of Computers and Networks, IET Circuits, Devices & Systems, IET Networks and Ubiquitous Computing and Communication Journal. He is a member of the IARIA (Fellow), IEEE (Senior), IEICE (Senior), FITCE and the Technical Chamber of Greece (TEE).

https://orcid.org/0000-0001-6315-5382
E-mail: mlogo@upatras.gr
Department of Electrical & Computer Engineering
University of Patras
Patras, Greece

Paper

Blockchain Networks – Security Aspects and Consensus Models

Andrzej Wilczyński[1,2] and Adrian Widłak[2]

[1] *AGH University of Science and Technology, Cracow, Poland*
[2] *Tadeusz Kosciuszko Cracow University of Technology, Cracow, Poland*

https://doi.org/10.26636/jtit.2019.132019

Abstract—Data integration and fast effective data processing are the primary challenges in today's high-performance computing systems used for Big Data processing and analysis in practical scenarios. Blockchain (BC) is a hot, modern technology that ensures high security of data processes stored in highly distributed networks and ICT infrastructures. BC enables secure data transfers in distributed systems without the need for all operations and processes in the network to be initiated and monitored by any central authority (system manager). This paper presents the background of a generic architectural model of a BC system and explains the concept behind the consensus models used in BC transactions. Security is the main aspect of all defined operations and BC nodes. The paper presents also specific BC use cases to illustrate the performance of the system in practical scenarios.

Keywords—blocks, cryptography, ledger, proof of work.

1. Introduction

Over the few past years, the Blockchain (BC) became the topic of interest for many engineers and companies, especially from financial and ICT sectors. This makes BC one of the most popular technologies used in ICT infrastructures developed for the needs of public institutions, financial markets, cloud storage systems and many other domains [1]. BC may be defined as a decentralized computer network without a central management unit. Data stored in BC blocks within such a system may be efficiently protected against external attacks. Data in a given block cannot be modified without an additional, significant power supply for the ICT infrastructure, which is usually not provided (it would rapidly increase the cost of energy used in BC nodes). In BC networks, the extra supervised transactions are not necessary (no central authority), each node is autonomous and may take decisions about transactions based on consensus procedures. This prevents any data manipulation and intrusions aimed at impersonating entities and performing unauthorized operations. Such consensus models define crucial procedures of the process of creating the chain of BC blocks and data transactions.

In this paper, the backgrounds of the BC architectural model and the consensus procedures are presented, and security-related issues affecting the entire BC system and the users' actions are illustrated. Unlike in existing papers and other publications concerned with BC essentials [2], [3], the BC system is shown from the ICT and engineering perspective, where the BC network may be applied as a potential supportive technology used for data and task processing in HPC computing environments (such as clouds, grids, fogs, etc.) Based on the authors' experience with BC technology, the practical scenario BC use cases are demonstrated.

The rest of the paper is organized as follows. In Section 2, the background of BC architecture is defined, and some most important security issues are presented. Section 3 presents the proof of work, proof of stake and round robin consensus models. In Section 4 the main use cases of BC are specified. The paper ends with a short summary given in Section 5.

2. Blockchain Backgrounds and Security Aspects

Pursuant to the most popular definition of a BC system, Blockchain is a distributed ledger of records in which data transactions and other system information may be specified. From the technological point of view, BC may be defined as a technological protocol that allows the exchange of data between different users in a network (usually external- or end-users) without the need for intermediaries [4]. The following characteristic properties of BC technology may be distinguished:

- **no central authority** – there is no need for a central system manager that decides whether any operation in BC is performed in accordance with the accepted rules or regulations,
- **immutability** – the transactions saved in a chain of blocks cannot be modified, which guarantees the immutability of data stored,
- **security** – cryptographic methods are used in the consensus models and for the protection of transactions,
- **transparency** – resources and transactions of each public address are available for viewing by anyone with access to BC,

- **efficiency and higher speed** – traditional processes of concluding transactions confirmed by a central system manager are time-consuming and may fail easily because of human errors – in BC, the confirmation of a transaction is automatic, which makes the whole process much faster,
- **cost reduction** – Blockchain excludes the involvement of external parties or intermediaries in the process to provide guarantees, which may lead to a reduction in maintenance costs, for instance no need to employ personnel operating and controlling the processes of accounting for money in banks.

2.1. Blockchain Architecture

Blockchain architectural models may be classified into the following network categories: private, public and permissioned.
Private BC networks have an owner (usually a company, the society or a public entity) that decides about the access to BC nodes and data. Private BCs are usually non-decentralized networks, however cryptographic protocols are used to secure the transactions. The most popular example of such systems is Multichain BC [5].
In public BC networks, any external user is capable of reading and easily modifying the ledger of records. The most popular examples of such systems are Bitcoin [6] and Litecoin [7]. In permissioned BC networks, there is a consortium of users or a privileged user who may grant the next node the permission to write or read from the block or blocks after verification of identity. The popular example of such a system are R3 (banks) [8] or EWF (energy) [9].

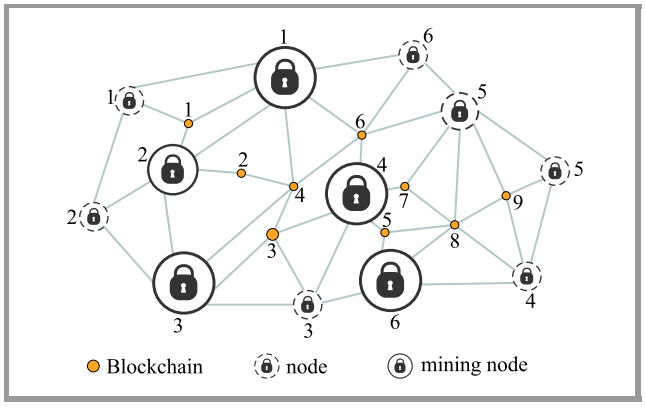


Fig. 1. Blockchain network.

Figure 1 shows an example of a BC network. One may observe that the nodes in a BC network are not always connected with all remaining nodes. There is no central unit and it is possible to connect an external, additional node to the existing network at any time. Hence, the model is very dynamic. The network consists of nodes confirming transactions (establishing the consensus), mining nodes responsible for adding blocks to BC, and users who have addresses and who upload data which are then placed in transactions.

2.2. Blocks and Merkle Tree

BC transactions may be defined by a list of the following attributes:

- transaction identifier – ID,
- transaction sender,
- transaction recipient,
- digital transaction signature,
- transaction data.

Each transaction must be approved by the majority of BC node administrators (users), usually at least 50% of the entire network.

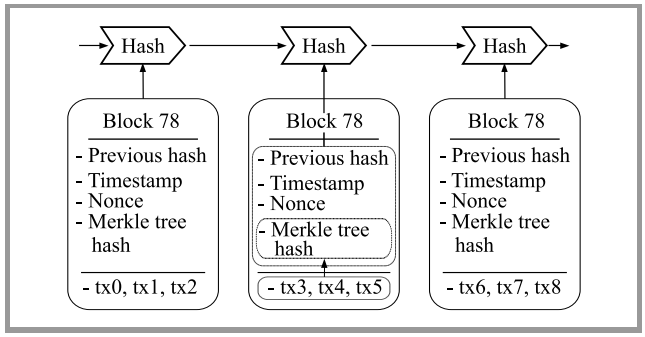


Fig. 2. Abstract model of BC blocks.

All parameters of the approved transaction are added to the block. The block is the main module of any BC node. The number of transactions in a given block (the block volume or block capacity) is defined depending on the standards defined for the entire BC system. An abstract model of a BC block is presented in Fig. 2. Each block is defined by the following components:

- block number,
- hash of current block,
- hash of previous block,
- timestamp,
- nonce – this is the number sought by the mining node, its finding usually consists in the solution of the hash function and makes it possible to add a block to the blockchain,
- the Merkle tree hash (calculations of this value are shown in Fig. 3),
- list of transactions (tx0, tx1, ..., txn) – each tx means the next transaction stored in a given block.

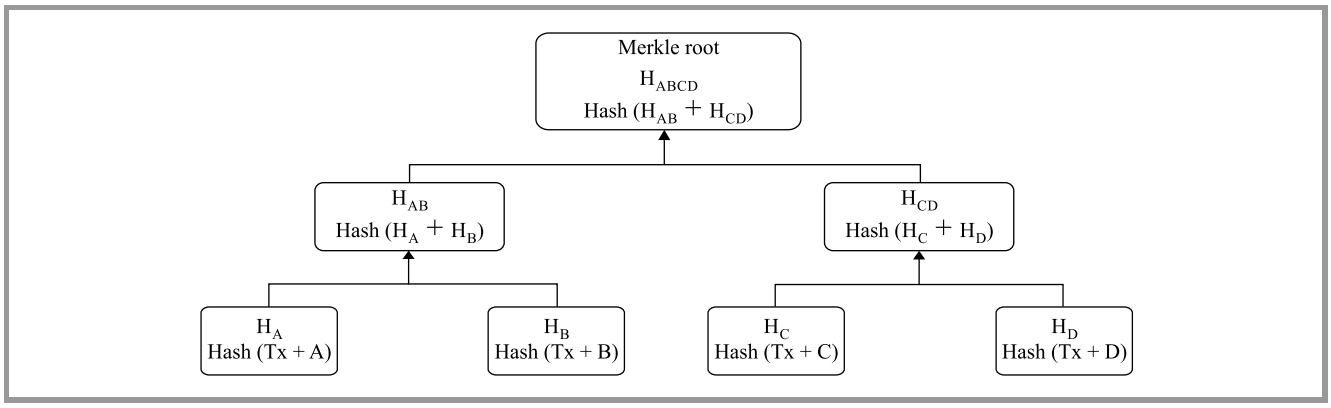


Fig. 3. Merkle tree.

A detailed description of the block components is available in [10].
The data stored in the blocks are protected and encrypted by using the cryptographic methods specified for a given BC network. Usually, these include public and private keys, digital signatures and cryptographic hash methods, such as the Secure Hash Algorithm (SHA) [11].
Each block must be hashed, thus creating a digest ID which represents the block. Any change of data stored in the block will change the hash value, which ensures data immutability [12].
The Merkle tree presented in Fig. 3 is an important component of the block model. It merges the hash values of data in the block until the root of the tree (the top hash value) is generated [10].

2.3. Conflicts and Resolutions

Once the transactions in the block have been completed and the consensus has been reached by the network, the block is added to BC. However, sometimes, when the block is being attached to BC, conflicts arise. Such situations occur if node *A* creates block *n* and distributes it to other nodes and, at the same time, node *B* also creates block *n* and distributes it to the other nodes. The blocks will not be the same in the entire network, because each of them may contain different transactions. These problems generate temporary different versions of blocks (Fig. 4).

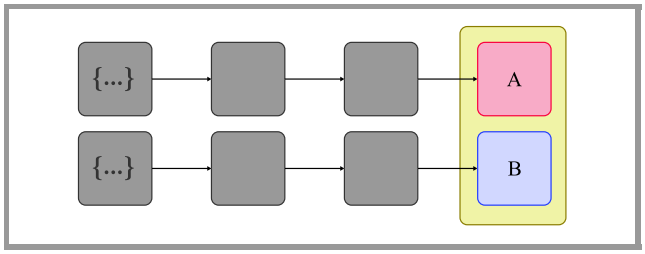


Fig. 4. Blockchain in conflict.

Blockchain systems usually deal with this problem by waiting for the next block to join BC. The longer chain wins and is treated as correct, while the shorter one is removed.

2.4. Security Aspects

Security in BC networks is usually defined as the need to protect transaction- and data-related information in a block. This means that threats and external attacks need to be detected and prevented. Joshi *et al.* in [13] present the main safety procedures in BC:

- **defense in penetration** – a strategy in which many data protection measures are used, based on the fact that many data protection layers are more effective than a single layer,
- **minimum privilege** – access to data is limited to the lowest possible level,
- **manage vulnerabilities** – checking security vulnerabilities and patching them,
- **manage risks** – identification and control of risks in the environment,
- **manage patches** – patching faulty parts of the source code.

BC systems rely on numerous techniques to achieve an adequate security level, mainly for data security purposes, and also for the verification of the nodes' ability to perform specific operations. The concept of accepting the longest chain of blocks as authentic also protects against 51% of attacks and forks problem.

2.5. Cryptographic Methods Used in BC Systems

A asymmetric key cryptography is usually used in BC systems for the authorization of processed transactions [14]. A private key is used to sign transactions, a public key to identify addresses assigned to the user and to verify the signatures generated with the use of private keys. Due to asymmetric cryptography, it is possible to determine whether the user who sends a message to another user has a private key with which the message has been signed, and thus whether he has the right to send it.
In Fig. 5 the process of signing and verifying transactions in BC systems is presented. The transaction is signed with

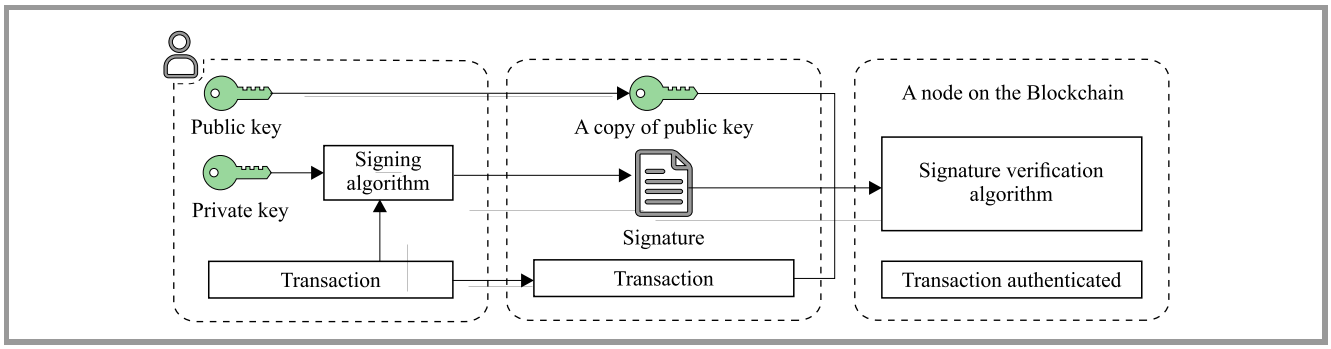


Fig. 5. Asymmetric key cryptography.

a private key, then it is forwarded, together with the signature and the public key, to the recipient. Based on this information, using the verification algorithm, a node in the network may authorize the received transaction.

3. Consensus Model

The acceptance of BC system joining procedure by an external user results in the user's adaptation to the initial state of such a system. The initial BC state is recorded in the genesis block [10], which is always a "head" component in the chain of the blocks. This means that every block must be added to BC after the genesis block, based on consensus method that has been agreed upon. Regardless of the method, each block may be validated independently by each external user (the block is valid). Having the initial state and the ability to verify every block, the external users can agree on the system's current state.
The following procedure should be implemented in the process of defining of the chain of blocks [10]:

- the initial state is defined globally and must be accepted by all external users,
- the external users agree to the consensus method by means of which blocks are added to the BC system,
- each block is linked to the previous block with a specified hash value,
- users may verify each block.

Note that the genesis block is the initial block in the chain and its hash value is set to 0. Through block validations, external users may easily verify the integrity of the BC system. This renders the system distributed and there is no need to have any third-party authority for setting/defining the system's current state. The agreement (consensus) of the active nodes and users in the system is necessary for adding new blocks into the system. The consensus method must work even in the presence of potential malicious users attempting to disrupt or take over BC. The major consensus models are presented later in this section.

3.1. Proof of Work Consensus Model

The proof of work (PoW) consensus model is the most popular agreement method in BC. Here, each external user may add a new block to the existing chain after solving a computationally intensive puzzle. The solution to this puzzle is called the "proof" of the work the user has performed. The puzzle should be defined based on the following conditions:

- the process of solving the puzzle should be complex – the puzzle should be non-trivial and difficult to solve,
- verification and validation of the solution should be easy to process.

Simple validation of the puzzle solution enables the proposed blocks to be validated by other mining system nodes and users. Negative validation of the proposed block automatically rejects the blocks from the chain. The process of solving puzzles conducted by a node does not increase its probability of solving the puzzles faster in the future. Below, we present a simple example of such a puzzle, where a node using the SHA-256 [11] algorithm must find a hash value meeting the following criteria:

$$\text{SHA256}(\text{“test”} + \text{nonce}) = \text{hash value starting with “00”}$$

The string "test" is appended to the value of nonce, and hash value is calculated. Nonce is a numerical value that changes after each hash calculation. This operation is repeated until the result has the form of a hash starting with "00". Some results are presented below:

SHA256("test1") = 1B4F0E9851971998E732078
544C96B36C3D01CEDF7CAA332359D6F1D83567014
1B means "not solved"

SHA256("test2") = 60303AE22B998861BCE3B28
F33EEC1BE758A213C86C93C076DBE9F558C11C752
60 means "not solved"

SHA256("test304") = 009FA371CD0B736AB80E8D
55C5741944DD0E740BBD92C97808F740A03722576B
00 means here "solved"

The above puzzle is not difficult to solve, but with each additional "0" in the expected hash value, i.e. "000", "0000", "0000…", the degree of its complexity increases. The higher the computing power of the mining node, the greater the probability that it will find the solution faster. After finding the solution, the mining node sends the block with the correct hash to other nodes. The recipient's nodes verify that this operation has been carried out correctly. If the verification renders a correct result, they add the block to their chain of blocks and they continue to distribute it further over the network. The PoW has been designed for networks where there is no trust. Both high performance and low performance computing units are capable of solving the puzzle correctly.
However, the main disadvantage of this approach is the consumption of considerable amounts of electricity. Due to the growing difficulty with proofs of work, nodes combine into "pools" or "collectives", where they solve puzzles together and then share the reward. Sharing the problem, each of the nodes may attempt to solve the puzzle at equal intervals:

- node 1: check "test1" to "test100",
- node 2: check "test101" to "test200",
- node 3: check "test201" to "test300",
- node 4: check ""test301" to "test400".

This strategy allows to find the solution more quickly thanks to the cooperation of several nodes. The most popular systems in which PoW is applied include Bitcoin, Litecoin and Ethereum Dogecoin.

3.2. Proof of Stake Consensus Model

In the proof of stake model, the consensus between network blocks is not achieved by mining nodes, but through the minters having stake/tokens. The higher the stake of a given user, the more likely they are to join the block to BC.

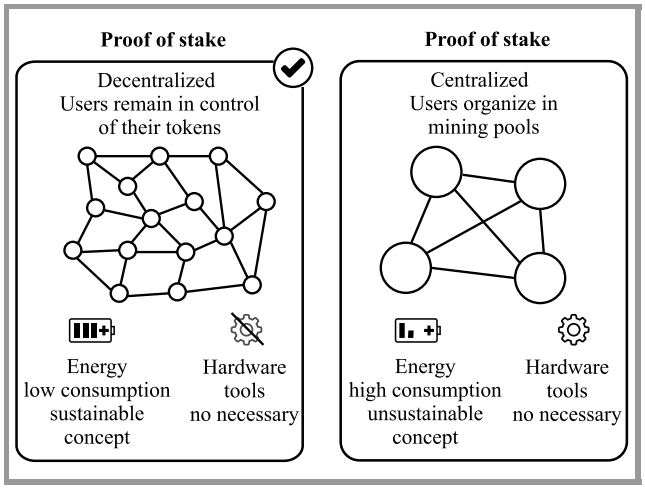


Fig. 6. PoW vs. PoS models.

Let's assume a simple network with 100 tokens, without specific minimum resources needed to participate in the mining process. With 20 tokens, we get a 20% chance to "mine" another block.
Systems using this consensus include, for example, Decred [15] or Peercoin [16]. In some implementations, older tokens have more purchasing power when mining, which may lead to monopolization of the network, i.e. a situation in which users with large resources are getting rich faster than others, and their advantage is growing continuously. There are methods to prevent such situations, which involve the introduction of limited life-time resources, for instance the user must wait, after a successful block check, a certain amount of time before proceeding to confirm the next one. This system is safe until one of the nodes takes over 51% of tokens. In Fig. 6, a simple comparison of PoW and PoS models is presented [17].

3.3. Round Robin Consensus Model

In some systems with a certain level of trust between mining nodes, there is no need of using complicated algorithms to reach the consensus, and the determination of which node will add the next block to BC may be performed alternately. This method is known as the round robin model and is usually used in private BC networks. The publishing of successive blocks is carried out alternately by nodes within the network. If a given node has the right to join the block (its turn has come), but for some reasons it does not join it or is not available, an element of randomness is introduced. This approach does not require high computational power, because there are no cryptographic puzzles to solve here. Nevertheless, a certain level of trust is required, and this model does not work well in open networks (public Blockchains).

4. Blockchain Use Cases

There are many applications that rely, to a lesser or higher degree, on the basic BC principles. Initially, BC was used in digital currency systems. Currently, it is also implemented in voting systems, identity management, smart cities and many other types of applications. Those that deserve particular attention include the following:

- Guardiam – is a token for a new global safety response network that provides a framework for distributed emergency response systems for places in the world where no emergency numbers are available [18],
- Blockchain Charity Foundation – it is a non-profit foundation whose task is to transform philanthropy by building a decentralized charity foundation, supporting sustainable development and ensuring that no one is left behind [19],
- Power Ledger – a system that allows customers to choose a source of electricity, enabling trading elec-

tricity with their neighbors and ensuring a fair return on investment, where energy is stable and affordable for everyone [20],

- EthicHub – a system whose aim is to provide all customers, with individual investors included, with the same access to traditional financial services by democratizing finances and making available investment opportunities around the world [21],
- Grassroots Economics & Bancor – decentralized BC-based community currencies in Kenya, aiming to combat poverty by encouraging local and regional trade [22],
- VeChain – decentralized platform in which companies may easily establish contacts and make transactions without intermediation [23].

The above examples show that the use of this technology not only ensures high security and quick execution of transactions, but also enables to solve problems that have not been solved in any other ways. First of all, it fosters development in areas where technological progress is very slow and where access to technology is very limited. Smart city use cases need to be taken into consideration as well, involving for instance car navigation systems, where the protection of personal data is important [24]. Current solutions, such as Google Traffic or Waze, are a specific type of a black box solution and do not offer sufficient guarantees to those concerned with their privacy.

5. Conclusions

Blockchain technology is the direction in which the industry will be heading over the coming years. The use of cryptographic algorithms ensures appropriate level of security that is required by most ITC environments. Full transparency and data integrity make it suitable for use in many data processing-related domains. Decentralization and the lack of a central supervisor makes the processes where a verification unit is needed faster and more efficient, due to the lack of the human factor and full automation. The trust built by nodes within the network ensures that all operations are carried out in accordance with the rules defined for a given network. Many systems based on Blockchain technology are already in existence. They are subject to continuous improvement and their number may be expected to grow.

References

[1] S. Ølnes and A. Jansen, "Blockchain technology as infrastructure in public sector: an analytical framework", in *Proc. of the 19th Ann. Int. Conf. on Digit. Government Res.: Governance in the Data Age DG.O 2018*, Delft, The Netherlands, 2018, Article no. 77 (doi: 10.1145/3209281.3209293).

[2] B. Marr, "A Complete Beginner's Guide To Blockchain" [Online]. Available: https://www.forbes.com/sites/bernardmarr/2017/01/24/a-complete-beginners-guide-to-blockchain/#6affecba6e60 (accessed 10 Feb. 2019).

[3] Ch. Lafaille, "What Is Blockchain Technology? A Beginner's Guide" [Online]. Available: https://www.investinblockchain.com/what-is-blockchain-technology (accessed 10 Feb. 2019).

[4] J. Seffinga, L. Lyons, and A. Bachmann, "The Blockchain (R)evolution – The Swiss Perspective", Deloitte, Feb. 2017 [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-de-innovation-blockchain-revolution.pdf

[5] G. Greenspan, "MultiChain Private Blockchain", Coin Sciences Ltd [Online]. Available: https://www.multichain.com/download/MultiChain-White-Paper.pdf

[6] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: a technical survey on decentralized digital currencies", *IEEE Commun. Surv. & Tutor.*, vol. 18, no. 3, pp. 2084–2123, 2016 (doi: 10.1109/COMST.2016.2535718).

[7] Litecoin – Open source P2P digital currency 2019 [Online]. Available: https://litecoin.org (accessed 10 Feb. 2019).

[8] r3.com [Online]. Available: https://www.r3.com (accessed 10 Feb. 2019).

[9] Energy Web Foundation, [Online]. Available: http://energyweb.org (accessed 10 Feb. 2019).

[10] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview", Draft NISTIR 8202, National Institute of Standards and Technology, 2018 [Online]. Available: https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf (accessed 5 Feb. 2019).

[11] D. Rachmawati, J. T. Tarigan, and A. B. C. Ginting, "A comparative study of Message Digest 5(MD5) and SHA256 algorithm", *J. of Physics: Conference Series, Conf. Series*, vol. 978, 012116, 2018 (doi: 10.1088/1742-6596/978/1/012116).

[12] J. Kołodziej, A. Wilczyński, D. Fernandez-Cerero, and A. Fernandez-Montes, "Blockchain secure cloud: a new generation integrated cloud and blockchain platforms – general concepts and challenges", *Eur. Cybersecur. J.*, vol. 4, no. 2, pp. 28–35, 2018.

[13] A. P. Joshi, M. Han, and Y. Wang, "A survey on security and privacy issues of Blockchain technology", *Mathem. Foundat. of Comput.*, vol. 1, no. 2, pp. 121–147, 2018 (doi: 10.3934/mfc.2018007).

[14] D. Pointcheval, "Asymmetric cryptography and practical security", *J. of Telecommun. and Inform. Technol.*, no. 4, pp. 41–56, 2002.

[15] B. Garner, "What Is Decred (DCR)? A Guide on Decentralized Blockchain Governance" [Online]. Available: https://coincentral.com/decred-lowdown-decentralized-blockchain-governance/ (accessed 9 Feb. 2019).

[16] Peercoin [Online]. Available: https://peercoin.net (accessed 9 Feb. 2019).

[17] "An Introduction to consensus algorithms: Proof of Stake and Proof of Work" [Online]. Available: https://cryptocurrencyhub.io/an-introduction-to-consensus-algorithms-proof-of-stake-and-proof-of-work-cd0e1e6baf52 (accessed 9 Feb. 2019).

[18] Guard Global Decentralized Emergency Response Network, [Online]. Available: https://guardtoken.net (accessed 5 Feb. 2019).

[19] Blockchain Charity Foundation [Online]. Available: https://www.binance.charity (accessed 5 Feb. 2019).

[20] Power Ledger [Online]. Available: https://www.powerledger.io (accessed 5 Feb. 2019).

[21] EthicHub [Online]. Available: https://ethichub.com (accessed 5 Feb. 2019).

[22] "Bancor To Launch First Blockchain-Based Community Currencies in Kenya", [Online]. Available: https://www.businesswire.com/news/home/20180621005727/en/Bancor-Launch-Blockchain-Based-Community-Currencies-Kenya (accessed 5 Feb. 2019).

[23] J. Zwanenburg, "What Is VeChain (VEN)?" [Online]. Available: https://www.investinblockchain.com/what-is-vechain (accessed 5 Feb. 2019).

[24] H. Liviu-Adrian, C. Dobre, "Blockchain privacy-preservation in intelligent transportation systems", in *Proc. IEEE Int. Conf. on Comput. Sci. and Engin. CSE 2018*, Bucharest, Romania, 2018 (doi: 10.1109/CSE.2018.00032).

Andrzej Wilczyński is an Assistant Professor at the Cracow University of Technology and a Ph.D. student at AGH University of Science and Technology. The topics of his research include Blockchain-based modeling in distributed computing, cloud computing and, in particular, data and resource virtualization, tasks scheduling in cloud computing and broadly defined security issues in these domains.

https://orcid.org/0000-0001-6774-3667
E-mail: and.wilczynski@gmail.com
AGH University of Science and Technology
Mickiewicza 30, 30-059 Cracow, Poland

Tadeusz Kosciuszko Cracow University of Technology
Warszawska 24, 31-155 Cracow, Poland

Adrian Widłak majored in Computer Science at Cracow University of Technology, Poland, received his B.A. and M.A. degrees in 2016 and 2017, respectively. He has been a researcher and teacher at Cracow University of Technology, Institute of Computer Science, since 2017. His interests include point cloud processing, artificial intelligence, computational geometry and data visualization.

https://orcid.org/0000-0001-9256-0061
E-mail: adrian.widlak@pk.edu.pl
Tadeusz Kosciuszko Cracow University of Technology
Warszawska 24
31-155 Cracow, Poland

Paper

CL-mWSNs: Cross Layer Model-Based QoS Centric Routing Protocol for Mission-Critical Cooperative Communication in Mobile WSNs

Kummathi Chenna Reddy[1], Geetha D. Devanagavi[1], and Thippeswamy M. N.[2]

[1] *School of Electronics & Communication, REVA University, Bangalore, India*
[2] *Department of Computer Science, Nitte Meenakshi Institute of Technology, Bangalore, India*

https://doi.org/10.26636/jtit.2019.129318

Abstract—The paper presents a robust QoS centric routing protocol for mission-critical communication over mobile Wireless Sensor Networks (CL-mWSN) that exploits dynamic network states from the different layers of the IEEE 802.15.4 protocol stack to make the routing decision. The CL-mWSN protocol exploits three key layers: application layer, network layer and MAC layer. It exhibits proactive network and node table management, service differentiation, fair resource scheduling and congestion detection, avoidance at the network layer, as well as dynamic link quality estimation and packet injection rate estimation at the MAC layer to assess its candidature as the best forwarding node for QoS-centric mission-critical communication. Simulation reveals that the proposed routing model exhibits higher throughput, minimum loss and deadline miss ratio that augments QoS provision in mobile WSNs.

Keywords—cross-layer signaling, link quality estimation, quality of service, wireless sensor networks.

1. Introduction

Over the past few years, the development of wireless communication technologies has demanded mobile Wireless Sensor Networks (WSNs) to serve numerous applications in which assuring QoS-centric and reliable communication is a must. The application-specific demands and customer preferences have turned Quality of Service (QoS) demands into the decisive selection criterion. Such demands have motivated the academia sector to design a more effective and cost-efficient communication system, with WSNs being considered a broad research domain.

Unlike classic WSN systems with static network deployment, mobile WSNs received more attention in terms of their further optimization. Relevant augmentation could turn mobile WSNs into a low-cost and efficient alternative for the classic ad-hoc networks or mobile ad-hoc networks (MANETs). Mobile WSNs may rely on random deployment of nodes across the network, enabling the nodes to communicate in an ad-hoc manner. However, such node deployment and mobility patterns might impose variations in topology, network states and node characteristics, such as congestion, buffer unavailability, data drop, link outage, etc. These adverse effects could cause a deterioration in QoS and unreliability of communication. In mobile WSNs, some or even all nodes may function as a router to support communication between two hosts in typical communication environments. This may be achieved by employing multi-hop transmissions. Noticeably, being a decentralized network solution, the inclusion of mobility in mobile WSNs could make network management highly complicated and, hence, could adversely affect the satisfaction of required QoS levels.

In mobile WSNs, each node relies on a routing model to perform communication with neighboring nodes, or forwards data to the next hop towards the destination. If two sensor nodes are within radio range, they may communicate directly. Otherwise, multi-hop transmission is used to forward data to the next hop node to ensure that it is reliably received at the destination. In static WSNs, routing may be performed through reactive node management, while in mobile WSNs classic reactive routing cannot be applied due to network parameter changes, meaning that a well-defined proactive network management approach and good network awareness are required. In mobile WSNs, the selection of the best forwarding node (BFN) plays a vital role.

With the aforementioned motivations taken into consideration, the emphasis of this research paper is placed on developing a novel and robust BFN for communication purposes. In WSNs, the communicated data may be of two types: real-time data (RTD) and non-real-time (NRT) data, where the delivery of RTD, which commonly has the form of event-driven critical data, often dominates the prioritization process to assure timely data delivery at the destination. On the other hand, NRT data may also be of significance for meeting user demands. QoS-centric resource provision to RTD while ensuring the maximum possible availability of resources for NRT may be of utmost significance for maintaining the optimized trade-off between these two types of data communication. In such cases, identification

of RTD among the data sequence containing NRT may play a decisive role in QoS-centric resource allocation and prioritization.

To meet this demand, various service differentiation (SD) approaches may be applied. The use of a well-planned SD scheme can assure both RTD as well as NRT data classification that, in turn, may help in optimal resource allocation to meet QoS needs. This may help the MAC and network layers understand the nature of the data and perform optimal resource scheduling. For the provision of QoS, the other key demand is timely data delivery, where selecting a node with the shortest holding period or considering packet velocity may be suitable for BFN. In addition, this may assist the PHY layer in performing dynamic power management (DPM) and link-adaptive transmission scheduling [1].

The other shortcomings of mobility include congestion and link vulnerability. Hence, assessing these two parameters at the node level can help MAC select only the node with optimum parameters (congestion-free and higher link quality) to make the transmission decision. Therefore, retrieving these key parameters (link quality, congestion, resource availability, packet velocity, etc.) and sharing them across the layers of the protocol stack may ensure optimal BFN selection to guarantee the provision of QoS over mobile WSNs. In practice, these dynamic network parameters can be estimated at the different layers of the protocol stack, and can be shared, at a later phase, with other layers to make the optimized routing decision. The use of a cross-layer network design (CND) may be a novel solution enabling to achieve the desired results.

In this paper, a robust and efficient routing protocol named "QoS-centric routing protocol for mission-critical communication over mobile WSNs (CL-mWSN)" has been developed. As a QoS-centric solution, our proposed CL-mWSN intends to achieve high packet delivery ratio (PDR), higher throughput, minimum packet drop, low latency and end-to-end delay, as well as maximum possible resource (i.e. bandwidth) utilization [2]. The proposed CL-mWSN can be stated as a geographical forwarding routing protocol, as it exploits dynamic network parameters to make the routing decision. To ensure network awareness, CL-mWSN applies the proactive network management approach, where node parameters are estimated dynamically and updated proactively to make optimized BFN selection. Unlike classic routing protocols, where single parameters – such as residual energy, link quality, signal to noise ratio (SNR), etc. – are used to perform BFN selection, CL-mWSN applies multiple parameters obtained from the different layers of the protocol stack for routing-related tasks. Here, CL-mWSN exploits the following key parameters: buffer capacity, packet velocity, link quality, distance, etc. to perform BFN selection, in order to ensure reliable data transmission with a minimum probability of data drop (due to the minimum or negligible probability of link outage), and a minimum deadline miss ratio (DMR). CL-mWSN intends to develop a highly robust resource scheduling scheme that could ensure optimal resource provision to event-driven RTD data, while ensuring that a maximum amount of resources is available to NRT data. Undeniably, it may play a significant role in managing the optimized QoS trade-off for both RTD and NRT data. The CL-mWSN protocol incorporates enhanced service differentiation and fair resource scheduling, proactive network management, congestion detection and routing decision model at the link layer, dynamic link quality and packet injection rate estimation at the MAC layer, and power switching at the PHY layer of the IEEE 802.15.4 protocol stack. The overall routing has been developed using the Matlab simulation platform, where the simulation output has exhibited higher PDR, packet loss ratio (PLR) and DMR results compared to other state-of-art technologies.

Table 1
List of used abbreviations

Variable	Description
$\mathbb{N}_{Table}$	Proactive node table
$BFNi$	Best forwarding node
$\mathbb{N}_j$	Number of nodes (one hop distant nodes)
$Eucl_d$	Euclidean distance in between the best forwarding node to the nearest destination
$Eucl_F$	Euclidean distance in between the best forwarding node and the source node
$\mathcal{T}_{d\_j}$	Residual deadline time
d_i^j	Euclidean distance between the forwarding node i and the nearest sink j
CNI_r	Cumulative congestion degree
CNI_{NRTMem}	Minimum buffer available in NRT traffic with FIFO based storage
CNI_{RTDMem}	Minimum buffer available in RTD traffic with prioritized queuing-based storage
$CNI_{NRTMemMax}$	Maximum buffer capacity of NRT traffic
CNI_{RTDMax}	Maximum buffer capacity of RTD traffic
$\mathbb{N}$	Total nodes in the network
CNI_{ri}	Cumulative congestion degree for i-th node
η	Dynamic link quality
α	Weight parameter
$\mathbb{N}_{rx}$	Total number of the received packets
$\mathbb{N}_{tx}$	Total number of the transmitted packets
$\mathbb{V}_t$	Speed factor
$\mathbb{D}_{ESD}^i$	Distance between source to destination
$\mathbb{D}_{ENS}^i$	Distance between one hop neighbor node to the destination
$ARTT_{Ti}$	Average round trip time
CRM_i	Cumulative rank matrix
$\omega_1/\omega_2/\omega_3$	Weight parameters

The remaining sections of the paper are structured as follows. Section 2 discusses the related work, while the proposed routing model and its implementation are presented in Section 3. Section 4 discusses the results obtained and is followed by conclusions and future work recommendations.

The list of abbreviations used in this paper is presented in Table 1.

2. Related Work

To achieve energy-efficient cooperative MIMO networks, Peron *et al*. [3] developed a cross-layer architecture where they applied PHY and MAC layers. In their proposed method, the authors estimated the outage probability based on power transmission estimation at PHY layer. In addition, at MAC layer, they examined different channels taking more time and energy, based on which they performed energy-efficient cooperative MIMO communication. Su *et al*. [4] developed a cross-layered cooperative transmission model which was applied in an interference channel in conjunction with cooperative interference between transmitters to achieve cell-edge throughput optimization. To assist efficient resource allocation in cooperative communication, they introduced an enhanced dirty paper coding at the PHY layer which rendered a better achievable rate region. Furthermore, they developed a cooperative transmission scheduling model at the MAC layer that enabled cooperative nature as per channel condition variation. Their model was found to be better in terms of throughput.

Rao *et al*. [5] performed optimum power allocation and resource management by exploiting the cross-layer model for throughput optimization in WSNs. Chen *et al*. [1] focused on ensuring reliable data transmission over WSNs, where they recommended a scalable, energy-efficient, and error-resilient routing model. To achieve the desired result, the authors developed a cross-layer model-based distributed energy-efficient and reliable routing protocol, where they amalgamated the network layer and power allocation policy at the PHY layer. To perform BFN selection, the authors considered the route with minimum power consumption and higher end-to-end reliability.

Mythrehee *et al*. [2] developed a cross-layered underwater wireless sensor networks (UWSNs) routing protocol that applied the adaptive neuro fuzzy-based interference system for measuring the depth of the sensor nodes, and the game theoretic model for localization of the sensor nodes at the upper layer of the sea.

Patil *et al*. [6] focused on throughput optimization of WSNs using the cross-layer routing model. The authors recommended maintaining a timely data delivery capacity in WSNs and, therefore, they developed an integrated cross-layer model. The cross-layer model they proposed focused primarily on memory allocation and power allocation functions for WSNs. Imen *et al*. [7] focused on energy-efficiency and increased life span of WSNs. The authors stated that the available zone routing protocols (ZRP) cannot deal with the adverse factors affecting the network, especially in large scale networks, and hence proposed a hierarchical cross-layer model based on the routing protocol (H-ZRP). Their model was found better in terms of packet loss rate and transmission rate.

Wan *et al*. [8] developed the QoE-oriented cross-layer resource allocation model for open wireless networks (OWN), with a mapping function applied between the service rate and the mean opinion score for best effort services. Ozen *et al*. [9] developed a two-tier SD and multi-rate transmission model for the cross-layered MAC design, which was used for QoS-centric communication over multimedia sensor networks (WMSNs). Wang *et al*. [10] developed an adaptive-opportunistic aloha (A-OAloha) for the UAV-WSN system to support network efficiency. A-OAloha was in fact a cross-layer model developed for successful data transmission and energy optimization over WSNs.

Chen *et al*. [11] developed novel wireless networked control systems (WNCSs) for which a cross layer network design was suggested to achieve network awareness under critical real-time traffic variations. Their proposed cross-layer model adaptively adjusted the control period to achieve improved resource utilization while maintaining timely data delivery. Mezouary *et al*. [12] developed a cross-layer model-based SD scheme to classify data as RTD and NRT traffic in WSNs. They combined the parameters from the MAC layer and the network layer to augment throughput. Peng *et al*. [13] focused on balancing the trade-offs between different activities, such as energy consumption and packet collision, proposing a cross-layer routing model in conjunction with a directed spanning tree routing algorithm. The algorithm they proposed resolved the key issue of undesired energy exhaustion during the transmission.

Xiong *et al*. [14] developed a cross-layer architecture-based MAC optimization model for WSNs. The authors applied a special inference ruler for MAC by employing computational geometry methods. Mishra *et al*. [15] also recommended the cross-layer WSN design to achieve QoS in WSNs. Neela *et al*. [16] developed an adaptive cross-layer model to augment the functions of the different layers. In opposition to classic routing and MAC layer (RMC) protocols using clustering, they proposed Enhanced-RMC (E-RMC) to achieve a higher network lifetime. Singh *et al*. [17] developed a cross-layer contention-based synchronous MAC protocol for WSN with multi-hop transmission. Considering the limitations of multi-hop transmission, such as reduced PDR and higher end-to-end delay, the authors proposed a cross-layer contention-based synchronous MAC protocol that collects the request-to-send data process in the data window and the confirmation-to-send data process in the sleep window to increase efficiency.

Anugraha *et al*. [18] focused on augmenting cooperative relaying in interference-limited multi-hop networks to achieve multi-rate transmission and power control. They developed a cross-layer flow-based routing model that jointly augments the routing parameters for better scheduling. Peng *et al*. [19] focused on congestion avoidance in multi-hop transmission-based WSNs and proposed a cross-layer model-based information exchange over a cross-layer design established between MAC and routing layers. Yuan *et al*. [20] developed a multi-hop virtual multiple-input-

multiple-output (VMIMO)-based cross-layer routing protocol design that augments energy efficiency, reliability and end-to-end QoS provision over WSNs. They achieved better energy exhaustion and an optimized set of transmissions. A similar effort was made by Shan *et al*. [21] who developed a QoE driven cross-layer resource allocation model for high traffic services over the OWN downlink. Similarly, the cross-layer model has been applied for ad-hoc and MANET purposes as well [22]–[29].

In [22], Gawas *et al*. developed a cross-layer model-based cooperative routing model over vehicle ad-hoc networks (VANETs). The authors developed the cross-layer model to ensure reliable data transmission for safety-related messages, with minimum end-to-end delay. Their model focused on achieving one-hop relay node, to ensure a reliable message broadcast. Rath *et al*. [23] proposed a QoS-oriented cross-layer routing model using network layer information and relying on exchange with other layers. They derived the rate monotonic algorithm (RMA) and earliest-deadline-first (EDF) scheduling to achieve a low deadline miss rate.

Shafi *et al*. [24] developed a cross-layer design-based cooperative routing model over VANET to achieve higher throughput and low loss ratios. Unlike [22], Gawas *et al*. focused, in [25], on achieving multilayer functionality from the PHY layer to the routing layer, to accomplish cooperative communication over MANET. They developed an adaptive cross-layered cooperative routing algorithm (ACCR) which exploits channel state variations to select the cooperative MAC model by employing spatial diversity information. Similarly, in [26] they proposed the IEEE 802.11e enhanced distributed channel access (EDCA) routing protocol for QoS-centric multimedia transmission. They focused on MAC optimization and MULTI-metric link disjoint multi-path routing (CMMR). They used MAC queue utilization, node density degree, and mobility to achieve channel-state awareness and routing decision capabilities.

In [27], PHY and MAC layers were used to design a cross-layer routing model for VANET. Nithya *et al*. [28] developed a QoS-centric multi-hop ad-hoc routing protocol by amalgamating MAC layer contention resolution and TCP layer congestion control. To achieve congestion control, they the applied Fibonacci sequence. Elias *et al*. [29] developed a random network coding (RNC)-based routing model for cooperative communication over VANET. They proposed the RECMAC model to achieve higher transmission reliability and throughput values.

3. Proposed CL-mWSN Protocol

To ensure QoS and reliable data communication over mobile WSNs, optimized forwarding path selection is vital. Excessively high topological variations may occur, predominantly under dynamic topology conditions, which may force the network and the nodes to undergo severe transitions, and may result in network parameter changes. BFN selection is a highly intricate task under such conditions. While performing BFN selection under such conditions, maintaining efficient (network) information is a must, which may help in making optimized, proactive routing decisions. BFN plays an important role in QoS-centric and reliable transmission over mobile WSNs. To achieve it, we assume that each deployed node has information about nodes located at the distance of one-hop. Here, to deal with dynamic topology, a proactive node management and routing protocol has been proposed.

In the proposed routing protocol, each node possesses a routing protocol that assists it in obtaining node information from different layers of the protocol stack. With QoS objectives considered, the proposed model exploits dynamic link quality, congestion probability at the node, buffer availability, packet velocity, packet injection rate or velocity, etc. These parameters may be applied to examine the suitability of a given node to become BFN for reliable data transmission. On the other hand, selection of the BFN depends, primarily, on multiple parameters, such as buffer capacity, packet injection rate, link quality, etc. The proposed routing protocol exploits those parameters from the different layers and enables reliable data transmission. In addition, considering mission critical communication purposes, where enabling timely data delivery is of utmost significance a novel service differentiation and fair resource scheduling model is developed in this research paper. The proposed SD model is capable of classifying data as RTD and NRT – a feat that has been augmented further by a novel QoS-centric fair resource allocation strategy.

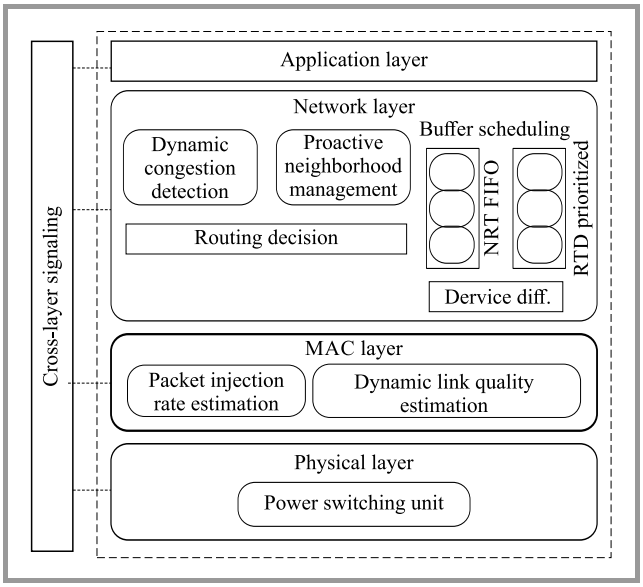


Fig. 1. Proposed cross-layer architecture-based QoS-centric routing protocol for mobile WSNs (CL-mWSN).

A snippet of the proposed cross-layer architecture is given in Fig. 1. CLmWSN exploits the network layer and the MAC layer of the IEEE 802.15.4 protocol stack. At the network layer, the CL-MWSN protocol is capable of service differentiation and fair resource scheduling (SDFRS),

dynamic congestion detection (DCD) and proactive network/node table management. Similarly, at the MAC layer of the IEEE 802.15.4 standard, packet injection rate of velocity (per node) and dynamic link quality have been estimated.

As stated in Fig. 1, CL-mWSN exploits primarily the application, network and MAC layers of the IEEE 802.15.4 protocol stack. The CL-mWSN model applies different functions to different layers. The key functions of the CL-mWSN routing protocol are:

- proactive network table management,
- service differentiation and fair resource allocation,
- congestion detection and avoidance model,
- dynamic link quality measurement,
- packet velocity measurement,
- cumulative rank matrix estimation and best forwarding path selection.

3.1. Proactive Network Table Management

Typically, nodes in classic mobile WSNs having their parameters, such as energy capacity, maximum buffer capacity, radio range, etc. defined, and due to the dynamic topology of the network, key parameters, such as link connectivity and buffer availability may change over time. Such changes may even be triggered by varying payload conditions, varying signal-to-noise ratio or link connectivity changes. In certain situations a node might may be forwarding data for a long time, which prevents data from reaching its destination within the defined time limit. Under varying topological conditions, a node may suffer from buffer deficiency and may require an additional buffer to ensure a reliable data transfer. Similarly, over the simulation period in mobile WSNs, the inter-node distance may vary and link connectivity may be subject to change as well. In such conditions, static or predefined parameter-based routing decisions can lead to link outages.

Due to considerable variations in network parameters, updating these parameters pro-actively is unavoidable. In other words, to cope with their dynamic topology, mobile WSNs require robust, proactive network management and a node table updating strategy. With this motivation in mind, the CL-mWSN protocol proposed in this paper relies on proactive network and node table management that enables dynamic network or/and node parameter updates to assist reliable BFN selection and routing decision process. It leaves out the continuous node discovery phase – an approach that reduces signaling overhead and energy consumption. In the proposed routing approach, node parameters are updated dynamically, which facilitates swift routing decision making. Each node maintains details of the single-hop neighboring node by transmitting a beacon message. The message comprises significant information about the node, along with its characteristics, such as NodeID, highest buffer capacity, current (available) buffer status, node position, packet holding period, current packet velocity, dynamic or current link quality, etc.

The three parameters: NodeID, node position and current link quality are communicated through the beacon message or ACK. This reduces computational cost and memory usage. Each control packet comprises 42 bytes and is split into three fields; NodeID (16 bits), current node status (192 bits to store link quality, current buffer availability) and node position field (128 bits). Each transmitting beacon message collects information on the on-hop neighboring node, which is updated continuously. One of the key issues in mobile WSNs is packet collision during transmission and, therefore, to avoid it, the node multicasts a beacon message that operates in coordination with an offset timer. In the proposed CL-mWSN routing protocol, the use of the offset timer is based on a normal homogeneous distribution approach. Once a request for packet transmission has been received, the node resets its off-set timer. Here, a node located at the one-hop distance updates the nearest destination in the table.

Let $\mathbb{N}_j$ be the one-hop distant neighbor and BFN_i be the potential or most suitable forwarding node. The node table is updated using Eq. (1), where $Eucl_F$ and $Eucl_d$ signify the Euclidean distance in between the best forwarding node and the source node to the nearest destination:

$$\mathbb{N}_{Table} = \{BFN_i \in \mathbb{N}_j | Eucl_d - Eucl_F \geq 0\} \ . \qquad (1)$$

3.2. Service Differentiation and Fair Resource Scheduling

To ensure QoS-centric communication, data awareness and associated resource scheduling play a decisive role. There are numerous application environments where the provision of sufficient resources (i.e. buffer) for a successful or QoS-centric transmission is a must. In mobile WSNs different data types may be communicated, including RTD and NRT data. The provision of sufficient buffer or bandwidth for RTD data is a must. However, maintaining an optimized amount of resources for NRT data may be of utmost significance as well. In the CL-mWSN routing protocol, both RTD and NRT data have been considered. Here we assume that data could be classified into two broad types, RTD and NRT. Once the data has been identified, CL-mWSN intends to allocated resources to each data type, while maintaining an optimized amount of resources for RTD data and the maximum possible amount of resources for NRT data.

Each node is assigned with two distinct types of equal capacity buffers for RTD and NRT data. In the CL-mWSN model, where a node experiences a complete buffer exhaustion for RTD data and requires additional buffer capacity for a successful transmission, it may borrow the supplementary buffer capacity from the NRT buffer, where the data are stored in the normal FIFO manner. In mobile WSNs, both RTD and NRT buffers may be filled. In that

case, CL-mWSN applies a fair resource scheduling approach (i.e. SDFRS), in which to meet the buffer-related demand for RTD data, NRT drops the recently added data to the FIFO queue. Although the data elements are stored in FIFO, the fact that a few recently connected elements are dropped cannot affect the overall performance in a significant manner. On the contrary, in major classic approaches, to provide additional buffer for RTD, the buffer for NRT is cleared or emptied completely, which is in violation of network QoS. Meanwhile, the proposed routing protocol enables optimal resource provision to RTD, while ensuring the maximum possible amount of resources for NRT, therefore balancing the resource utilization trade-offs to assure proper QoS. This mechanism allows to avoid long waiting times or holding periods at the, which ultimately augments overall network performance.

3.3. Congestion Detection and Avoidance Model

During a transmission over mobile WSNs, there is always the probability of a data flow that may as a result may impose congestion on a node. The probability of congestion increases considerably when we are dealing with mobile topology, which in turn increases the probability of a packet drop and retransmission, thus causing a QoS violation and energy exhaustion. To deal with this problem, the authors have recommended a timer-based transmission. In this mechanism, each node may transmit a beacon message to multiple nodes in the network whose frequency could be controlled through a predefined timer called the offset timer. Upon receiving a transmission request, CL-mWSN at first resets the associated timer, which eliminates ACK from the node. this also makes the proposed system computationally efficient and reduces signaling overheads. In addition, CL-mWSN avoids the storage of any significant paths or node-related information. Due to the dynamic topology, a node may receive more request to carry payload, exceeding its maximum carrying capacity, and buffer availability may vary over the simulations period, thus increasing the probability of congestion. This often results in a data drop and retransmission, causing energy exhaustion. To alleviate this problem, the CL-mWSN model implements a congestion detection and avoidance model (CDAM) that continuously assesses dynamic buffer capacity and the remaining buffer availability of node to detect congestion. It exploits the maximum buffer capacity of a node and the current buffer availability to assess the congestion probability at a node in a mobile WSN.

Upon transmitting the beacon message, the node may retrieve resource availability (i.e. buffer availability) of a one-hop distant node. To ensure the provision of QoS and a reliable transmission, a node with sufficient buffer availability may be efficient enough.

Upon identifying a node whose buffer availability is lower than the memory expected or required for data transmission, CDAM avoids that node to assist the CL-mWSN-based BFN selection. Only a node with a sufficient buffer availability and with the congestion-free status is selected for BFN formation. This reduces any likelihood of a data drop, retransmission, end-to-end delay and energy consumption, which, in turn, augments QoS assurance in mobile WSNs.

In addition, the proposed CL-mWSN model functions in conjunction with the above stated SDFRS model that applies two distinct buffers for RTD and NRT data for each node, which fosters better resource management and allows to avoid congestion. As already discussed, in the SDFRS model, RTD data is stored in a prioritized manner, while NRT data is stored based on the FIFO methodology. As each packet is assigned in a real time application, with a predefined deadline, it requires the data to reach it within that deadline to make an optimized decision. TheCL-mWSN model offers a higher priority to RTD data, while offering the maximum amount of resources to NRT data. In this model, to ensure delay the respective deadline time. To achieve this objective, CL-mWSN considers the distance between the source sensor node and the sink. Noticeably, to facilitate the highest possible priority for event-driven RTD delivery over mobile WSNs, it is inevitable to have the minimum value of $\mathcal{T}_{Ratio}$:

$$\mathcal{T}_{Ratio} = \frac{\mathcal{T}_{d\_i}}{d_i^j} \ , \tag{2}$$

where $\mathcal{T}_{d\_i}$ signifies the residual deadline time, while d_i^j states the Euclidean distance between the forwarding node i and the nearest sink j. The deadline time is estimated by using the arrival time of the individual packet. $\mathcal{T}_{d\_i}$ is updated for each packets before transmitting, and the queue time is subtracted from $\mathcal{T}_{d_i}$. Here, we use current buffer availability information to estimate the congestion probability at a mobile WSN node. In addition, the CL-mWSN model introduces a parameter called node congestion index (NCI), which comprises node information along with its association with a neighboring node subset $\mathbb{S}_n$. We estimate NCI using Eq. (3), where CNI_{NRTMem} and CNI_{RTDMem} signify the memory available in the NRT-related normal FIFO queue, and the RTD-related buffer in the prioritized queue, correspondingly. CNI_{RTDMax} and $CNI_{NRTMemMax}$ signify the highest memory or buffer capacity of the RTD and the NRT data. Thus, the overall CNI for connecting nodes in $\mathbb{S}_n$ may be obtained as:

$$CNI_r = \frac{CNI_{NRTMem} + CNI_{RTDMem}}{CNI_{NRTMemMax} + CNI_{RTDMax}} + \sum_{i-1}^{\mathbb{N}} CNI_{ri} \ . \tag{3}$$

Estimating the memory or the buffer available at each node and the associated congestion probability, the routing model decides whether that node qualifies to become the forwarding node. A congestion-free node with sufficient buffer availability is considered to be used as a forwarding node or for path selection purposes. This assures reliable data transmission over mobile WSNs with the lowest possibility of data drops and overflows. In addition, such an approach avoids the problem of packet collision.

3.4. Link Quality Measurement

To ensure the provision of QoS in mobile WSNs, one needs to assess the quality of the link between the resilient communication, RTD transmission is scheduled based on participating nodes dynamically, in order to characterize the suitability of a node for becoming a BFN. Mobility could result in topological changes and, hence, inter-node distance variations. Fixed radio range dynamics may cause link quality variations based on inter-node distance. In such conditions, assessing link quality dynamically to decide its suitability for selecting a reliable forwarding path may be vital. The CL-mWSN model applies a proficient dynamic link quality estimation model at the MAC layer of the IEEE 802.15.4 protocol stack. Details of the dynamic link quality estimation model can be found in [30]. The CL-mWSN model applies the current ratio of received packets to estimate link quality:

$$\eta = \alpha\,\eta + (1-\alpha)\,\frac{\mathbb{N}_{rx}}{\mathbb{N}_{tx}}\ . \tag{4}$$

In the above equation, η represents dynamic link quality. The packet received ratio defines the efficiency of the communication link. The remaining parameters $\mathbb{N}_{rx}$ and $\mathbb{N}_{tx}$ represent the total number of received and transmitted packets, respectively. Here, α remains within the range of 0 to 1.

3.5. Packet Injection Rate Estimation

Selecting a node and, hence, the path with the minimum holding period specific for each node may be vital to reduce latency or end-to-end delay that eventually determines the provision of QoS. In the CL-mWSN model, we estimate the packet injection rate or the holding period of a given node, i.e. the time over which the node withholds data before forwarding it. A node with a minimum holding period or a maximum packet velocity or injection rate is considered for BFN selection. Here, we have applied the packet delay parameter to estimate packet velocity at each node. In CL-mWSN, packet delay is applied to estimate the inter-node distance between neighboring nodes and the nearest destination. CL-mWSN applies Euclidean distance and relative distance, round trip time ($ARTT_{Ti}$), etc., to estimate packet velocity. The Euclidian distance is obtained between the source and the nearest destination, while the relative distance is obtained between the neighboring node and the nearest destination.

A speed factor $\mathbb{V}_t$ is obtained using:

$$\mathbb{V}_t = \frac{\mathbb{D}^i_{ESD} - \mathbb{D}^i_{ENS}}{ARTT_{Ti}}\ . \tag{5}$$

Applying Eq. (5), we have estimated the packet velocity ($\mathbb{V}_{packet}$), using Eq. (6). $\mathbb{V}_{packet}$ signifies the highest rate of data transmission at a given transmission power rating ($\mathbb{P}tx$):

$$\mathbb{V}_{packet} = \frac{\mathbb{V}_t}{\mathbb{R}_{MaxSpeed}}\ . \tag{6}$$

In Eq. (6), D^i_{ESD} signifies the Euclidean distance between source i and the destination node. D^i_{ENS} represents the distance between the source and the (nearest) sink. $R_{MaxSpeed}$ denotes the maximum possible speed of radio signal in air. In CL-mWSN the speed of radio signal is assumed to be equal to the speed of light, and round trip time is estimated as the time difference in time between packet transmission and reception of the acknowledge (ACK) signal:

$$ARTT_{Ti} = \frac{\sum_{i=0}^{N} R^i_{At} - v^i_{Pt}}{\mathcal{N}}\ . \tag{7}$$

In Eq. (7), variables R^i_{At} and v^i_{Pt} signify the time of receiving ACK and of packet transmission, respectively. The $\mathcal{N}$ states the total packets transmitted. Thus, estimating the packet velocity for each node we have used it as a node specific parameter to decide its suitability to be a BFN or path.

3.6. Cumulative Rank Matrix Estimation and Best Forwarding Path Formation

Once the dynamic network parameters of the participating nodes, as referred to above, have been estimated, they were used to select BFN. for this purpose, we estimated a (node) rank parameter called cumulative rank matrix (CRM) – Eq. (8). As already stated, CL-mWSN applies three key network parameters: congestion probability, dynamic link quality and packet injection rate or velocity, to select the best forwarding path. This is followed by best forwarding path formation and data transmission. The proposed CRM value is obtained using:

$$CRM_i = \omega_1\,\eta_i + \omega_2 CNI_i + \omega_3\,V_{packet_i}\ . \tag{8}$$

In the above equation, ω denotes the weight parameter which can be decided based on network preferences or based on a specific environment. CRM signifies the cumulative rank of node i. Noticeably, ω is assigned in such a manner that $\sum_{i=1}^{3} \omega_i = 1$. The variable η denotes the dynamic link quality.

Algorithm 1: Best forwarding node selection

1. **Input**: $\mathbb{N}_{Table}$, CNI_r, $\mathbb{V}_{packet_i}$, η_i, single – hop node information
2. **Output**: CRM_i, BFN_i
3. Initiate threshold ($CRM_{Max} = -1$);
4. **Foreach** node i in $\mathbb{N}_{Table}$ **do**
5. Calculate $CRM_i - \omega_1.\,\eta_i \cdot Single - hop\ Node[i].\,\eta + \omega_2.\,CNI_i \cdot Single - hop\ Node[i].\,CNI_i + \omega_3.\,\mathbb{V}_{packet_i} \cdot Single - hop\ Node[i].\,V_{packet_i}$;
6. **If** $CRM_Max \leq CRM_i$ **then**
7. Select $BFN_{ID} = i$;
8. **End**
9. **End**

Table 2
CL-mWSN protocol parameters with their function

802.15.4 OSI layer	Parameter	Function
Network layer	Proactive node table – Eq. (1)	Proactive network table management
	Buffer availability-congestion – Eq. (3)	Congestion detection avoidance model
	Data type classification (RTD & NRT)	Service differentiation and fair resource scheduling
MAC layer	Dynamic link quality – Eq. (4)	Link quality measurement
	Packet velocity – Eq. (6)	Packet rate injection estimation

Upon estimating CRM of each participating node, the estimated rank $CRM_{i \in TotalNodes}$ is updated in the decreasing order, and a node with the maximum CRN is considered as BFN for further data transmission over mobile WSNs. Algorithm 1 for BFN selection is then prepared for simulation purposes.

4. Results and Discussion

To examine the efficiency of the proposed CL-mWSN, we have compared its performance with other existing state-of-the-art cross-layer architecture-based routing protocols considering the parameters shown in Table 2.

The majority of the existing approaches rely on single parameter-based routing decision-making schemes, where the emphasis is placed on augmenting PHY and MAC [3], [4], [9], [12], SD functions [9], congestion avoidance at MAC [19] etc. However, very few efforts have been made to make the routing decision while considering the type of data and its priority, to ensure deadline sensitive communication [12]. On the contrary, it is a fact that inclusion of these all factors, network condition-aware routing with synchronized cross-layer information may improve BFN selection and routing decisions.

With this motivation, in this research a reference model has been developed that combines the major efficacies of multiple contributions made, such as in [3], [4], [9], [12], [19], [22]. Although in [3], the authors considered only the MAC and PHY layers where throughput and link-outage probability (at MAC) were used to perform PHY switching control, they could not address other aspects, such as packet transmission rate or packet velocity of a node, which is a must for deadline-sensitive, mission-critical communication. Similarly, in [9], the focus was on employing the SD model to achieve multi-rate transmission for data-specific transmission; however, they could not address such issues those referred to in [3], or even in our work. In addition, they applied a classic prioritization scheme, which offered less or even no concern to fair resource scheduling for NRT data. Even the existing cross-layer protocols have failed to assess whether and how (i.e. up to what extent) their proposed resource scheduling affects QoS-centric delivery of NRT data. Similarly, authors in [22] developed cross-layer based cooperative routing model, where they focused on achieving a minimum delay. Therefore, they estimated the one-hop relay node to ensure reliable message broadcast over VANET. They also applied MAC and transport layers to perform adaptive transmission rate control. However, they could not deal with other adverse effect caused by mobility. The work done in [31] looks better, as the have tried to implement multiple network parameters (of static WSN), such as velocity, energy to perform one-hop relay node identification or selection. This model could not offer the provision of better SD. Noticeably, the aforementioned routing cross-layer models [3], [4], [9], [12], [19] have implemented a cross-layer model, but for static WSNs only. They have not addressed the exceedingly dynamic topology of a mobile WSN. Under such conditions, development of a suitable reference model based on certain existing works referenced in [3], [4], [9], [12], [19], [22], [30] is inevitable, as it may help in assessing proposed model by applying common performance characteristics. With this motivation, a reference model, similar to the method suggested in [30], has been designed, amalgamating almost all features of or intentions referred to in [3], [4], [9], [12], [19]. Thus, the reference model [31], hereinafter re-

Table 3
Experimental setup

Parameter	Specification
Operating system	Windows 2010, 8 GB RAM, Intel Core i5 processor
Simulation tool	Matlab 2012b
Protocol	CL-mWSN
Data link	CSMA
Physical	IEEE 802.15.4 PHY
MAC	IEEE 802.15.4 MAC
Mobile nodes	60
Radio range	100 m
Packet deadline time	10 s
Mobility	Circular
Weight parameters	$\omega_{1(LQE)} = 0.4$, $\omega_{2(Cong)} = 0.3$, $\omega_{3(P\_Vel)} = 0.3$,
Simulation period	480 s
Payload	250, 500, 750, 1000, 1250, 1500, 1750, 2000, 2250, 2500, 2750, 3000

ferred to as the "existing system", combines the efficacies of other models and implements the SD model, packet velocity etc. to perform RTD and NRT data delivery. The performance comparison has been done for both CL-mWSN and existing systems [31]. Before discussing performance results obtained, the key parameters used in the experimental setup are presented in Table 3.

As depicted in Fig. 2, the CL-mWSN protocol exhibits higher PDR (98.4%) for RTD - a result that is higher than in the existing model [31]. The existing cross-layer model, say real-time power aware routing protocol (RPAR), has exhibited a PDR of 93.1%. Therefore, CL-mWSN has exhibited approximately 5.3% more PDR than the existing routing protocol.

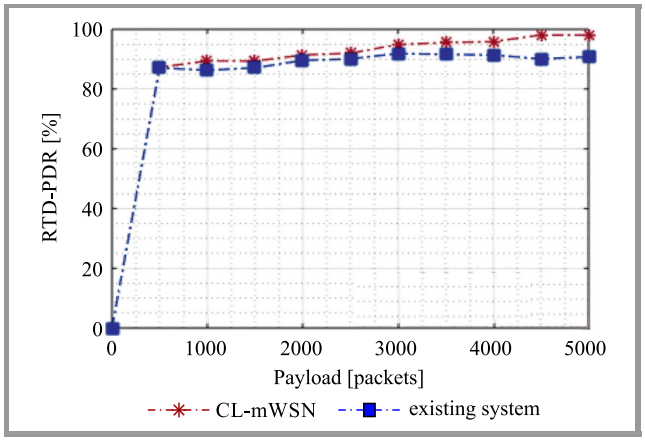


Fig. 2. PDR performance for RTD data.

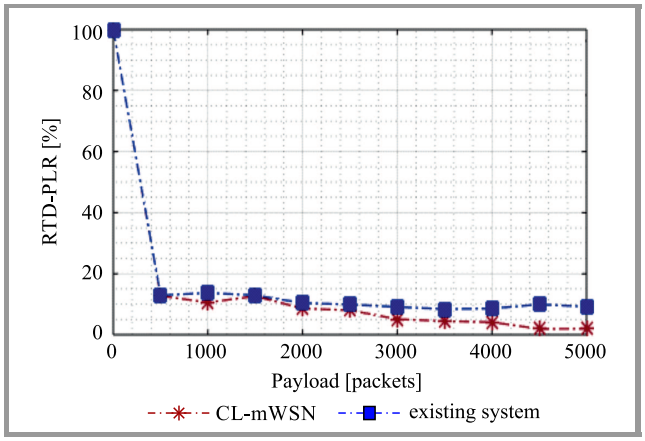


Fig. 3. PLR performance for RTD data.

As far as NRT-related performance is concerned, Fig. 3 shows the PDR value of the proposed routing model (93.8%). This result reveals that CL-mWSN exhibits higher PDR while ensuring the maximum possible resource allocation and, hence, preserving QoS for NRT transmission. This signifies the robustness of the proposed routing model. Noticeably, even in mobile scenarios, PDR performance (98.4%) for RTD traffic over mobile WSNs confirms robustness of the proposed routing model. Such a result allows to avoid the probability of retransmission and, hence, ensures proper QoS with minimum bandwidth utilization and transmission-related energy consumption.

PLR performance for RTD traffic typical of our proposed CL-mWSN model is depicted in Fig. 3. The CL-mWSN protocol exhibits a lower PLR (1.6%) than the existing cross-layer routing protocol, RPAR (6.9%). This efficacy backs up the robustness introduced in the proposed routing model. Unlike existing routing protocols, CL-mWSN employs different and dynamic network parameters to perform BFN or neighbor relay node selection, which eventually allows it to exhibit higher QoS provision levels. The higher throughput or PDR performance by CL-mWSN results in more successful data delivery and, hence, alleviates the probability of retransmission, which makes it energy efficient as well as resource efficient. The use SDRCRF makes CL-mWSN efficient and robust enough to ensure higher PDR for RTD, and guarantees uncompromised performance for NRT traffic.

PDR performance for NRT traffic is shown in Fig. 4. PLR for NRT traffic is presented in Fig. 5, where CL-mWSN has outperformed RPAR. CL-mWSN has exhibited PLR of merely 6.2% for NRT traffic.

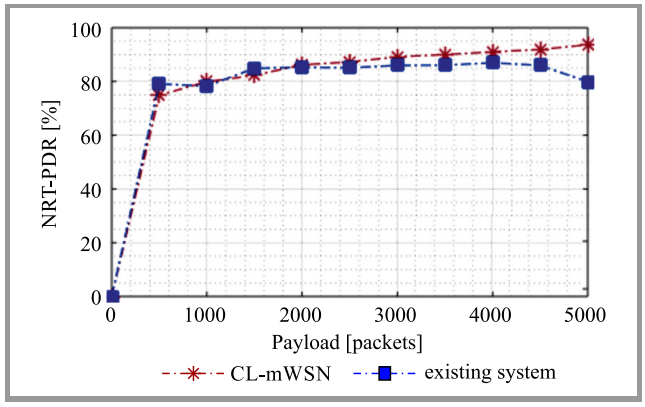


Fig. 4. PDR performance for NRT data.

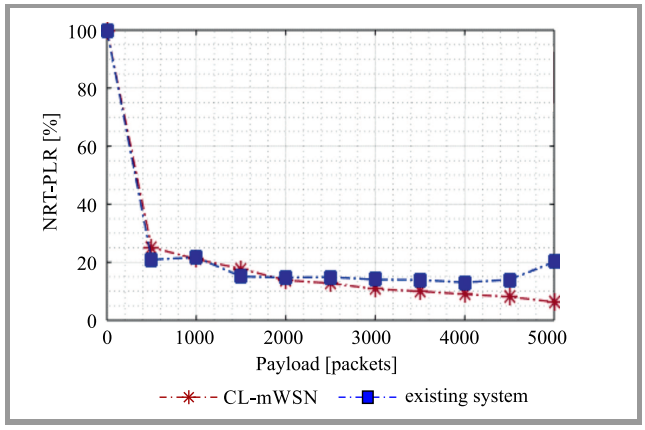


Fig. 5. PLR performance for NRT data.

The use of the novel SD model has strengthened CL-mWSN ensuring optimized resource allocation for RTD traffic, while maintaining the maximum possible resources for NRT traffic under congestion and resource-constrained

conditions. FIFO-based scheduling for NRT and last packet drop for accommodating RTD traffic are the parameters that allow CL-mWSN to exhibit a minimum drop of NRT data. This makes the proposed system robust for both RTD and NRT traffic transmissions.

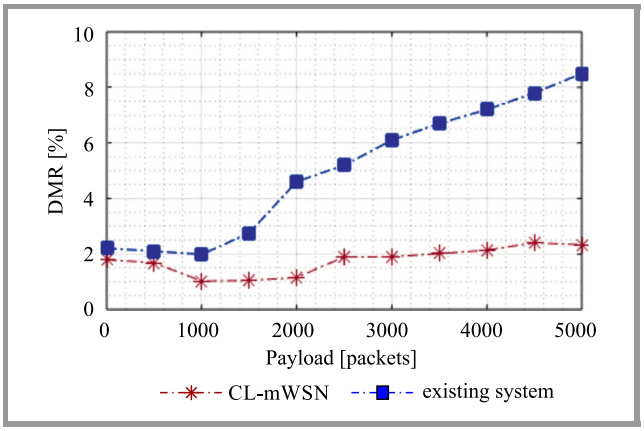


Fig. 6. DMR performance of routing protocol.

DMR performance is depicted in Fig. 6. Based on the results obtained, one may easily visualize that CL-mWSN exhibits lower DMR than the existing routing models [30]. This can be the result of deadline time (per packet) based data prioritization and resource allocation. Now, taking into consideration of all results discussed above and their respective significance, one may conclude that CL-mWSN performs better than other routing models, with its efficacy being relevant for used in real-time mobile WSN applications.

5. Conclusion

It may be stated that the proposed routing model offers a number of contributions, such as enhanced service differentiation and fair resource scheduling for different traffic types, while ensuring optimal PDR for RTD with allocating the maximum possible amount of resources to NRT. This allows the proposed system to achieve an optimized tradeoff for RTD and NRT transmissions over WSNs. Similarly, the inclusion of packet velocity of each node, describing the rate at which a given node may transmit data, has helped CL-mWSN ensure timely data delivery. Congestion avoidance and selection of the best forwarding note based on dynamic link quality also enabled the proposed routing protocol to achieve a maximum packet delivery ratio, a minimum packet loss ratio and, hence, a minimum retransmission probability, which eventually makes it energy-efficient. Therefore, the overall performance of the proposed routing protocol makes it robust enough to satisfy QoS demands in mobile WSN communication systems, which may be great significance for the IoT ecosystem as well. Although the proposed system attempts to add the greatest value to the routing model, it could not address the issue of dynamic power management and multi-rate switching control, which could have resulted in ensuring more bandwidth-efficient routing and in achieving higher energy efficiency.
In the future, efforts need to be made to incorporate the cross-layer design model with QoS-centric PHY switching or dynamic power management, in order to increase energy and resource efficiency.

References

[1] Y. Chen, L. Gao, Y. Xing, and W. Yi, "Cross-layer design for energy-efficient reliable routing in wireless sensor networks", in *Proc. 11th Int. Conf. on Mob. Ad-hoc and Sensor Netw. MSN 2015*, Shenzhen, China, 2015, pp. 31–36 (doi: 10.1109/MSN.2015.44).

[2] H. Mythrehee and A. Julian, "A cross layer UWSN architecture for marine environment monitoring", in *Proc. Global Conf. on Commun. Technol. GCCT 2015*, Thuckalay, India, 2015, pp. 211–216 (doi: 10.1109/GCCT.2015.7342654).

[3] G. Peron, G. Brante, R. D. Souza, and M. E. Pellenz, "Physical and MAC cross-layer analysis of energy-efficient cooperative MIMO networks", *IEEE Trans. on Commun.*, vol. 6, no. 5, pp. 1940–1954, 2018, (doi: 10.1109/TCOMM.2018.2796601).

[4] G. Su, B. Cui, and X. Wang, "Cross-layer approach to joint transmitter selection for cooperative transmission", in *Proc. 16th Int. Symp. on Commun. and Inform. Technol. ISCIT 2016*, Qingdao, China, 2016, pp. 426–430 (doi: 10.1109/ISCIT.2016.7751666).

[5] K. P. Rao and P. V. Sridevi, "An integrated cross layer approach for throughput improvement in wireless sensor networks", in *Proc. 10th Int. Conf. on Intell. Syst. and Control ISCO 2016*, Coimbatore, India, 2016, pp. 1–6 (doi: 10.1109/ISCO.2016.7727114).

[6] A. K. Patil and A. J. Patil, "Integrated cross layer controlling for wireless sensor network", in *Proc. Int. Conf. on Pervasive Comput. ICPC 2015*, Pune, India, 2015, pp. 1–6 (doi: 10.1109./PERVASIVE.2015.7087160).

[7] B. Imen and M. Abdellaoui, "Hierarchical organization by crossing between different layers for WSN energy saving", in *Proc. 15th Int. Conf. on Sci. and Techniq. of Autom. Control and Comp. Engin. STA 2014*, Hammamet, Tunisia, 2014, pp. 1020–1023 (doi: 10.1109/STA.2014.7086772).

[8] M. Wan, Z. Lu, L. Wang, X. Xia, and X. Wen, "A QoE-oriented cross-layer resource allocation scheme for mobile service over Open Wireless Network", in *Proc. Int. Symp. on Wirel. Pers. Multim. Commun. WPMC 2014*, Sydney, NSW, Australia, 2014, pp. 186–191 (doi: 10.1109/WPMC.2014.7014814).

[9] Y. Ozen, C. Bayilmis, N. Bandirmali, and I. Erturk, "Two tiered service differentiation and data rate adjustment scheme for WMSNs cross layer MAC", in *Proc. 11th Int. Conf. on Electron., Comp. and Comput. ICECCO 2014*, Abuja, Nigeria, 2014 (doi: 10.1109/ICECCO.2014.6997561).

[10] H. Li, L. Wang, S. Pang, and M. Towhidnejad, "A cross-layer design for data collecting of the UAV-wireless sensor network system", in *Proc. 12th IEEE Int. Conf. on Embedded and Ubiquit. Comput.*, Milano, Italy, 2014, pp. 242–249 (doi: 10.1109/EUC.2014.43).

[11] Y. L. Chen, G. Tian, J. Gao, and Y. C. Tian, "Cross-layer design for traffic management in wireless networked control systems", in *Proc. 9th IEEE Conf. on Indust. Electron. and Appl.*, Hangzhou, China, 2014, pp. 187–192 (doi: 10.1109/ICIEA.2014.6931156).

[12] R. El Mezouary, A. Loutfi, and M. El Koutbi, "A cross-layer architecture for service differentiation in wireless sensor networks with multiple sinks", in *Proc. Int. Conf. on Multim. Comput. and Syst. ICMCS 2014*, Marrakech, Morocco, 2014, pp. 843–848 (doi: 10.1109/ICMCS.2014.6911279).

[13] J. Peng, J. Jingqi, S. Qiushuo, and Z. Songyang, "A noble cross-layer protocol for QoS optimization in wireless sensor networks", in *Proc. 26th Chinese Control and Decision Conf. CCDC 2014*, Changsha, China, 2014, pp. 2430–2434 (doi: 10.1109/CCDC.2014.6852581).

[14] Q. Xiong and X. Li, "Cross-layer design of MAC and application semantics in wireless sensor networks", in *Proc. 4th Int. Conf. on Commun. Syst. and Netw. Technol.*, Bhopal, India, 2014, pp. 147–150 (doi: 10.1109/CSNT.2014.38).

[15] M. Mishra, G. S. Gupta, and X. Gui, "A review of and a proposal for cross-layer design for efficient routing and secure data aggregation over WSN", in *Proc. 3rd Int. Conf. on Computat. Intell. and Netw. CINE 2017*, Odisha, India, 2017, pp. 120–125 (doi: 10.1109/CINE.2017.30).

[16] N. Neela and O. B. V. Ramanaiah, "A comprehensive cross-layer framework for optimization of correlated data gathering in wireless sensor networks", *in Proc. IEEE 6th Int. Conf. on Adv. Comput. IACC 2016*, Bhimavaram, India, 2016, pp. 582–587 (doi: 10.1109/IACC.2016.113).

[17] R. Singh, B. K. Rai, and S. K. Bose, "A low delay cross-layer contention based synchronous MAC protocol for a multi-hop WSN", in *Proc. IEEE Region 10 Conf. TENCON 2016*, Singapore, 2016, pp. 1821–1824 (doi: 10.1109/TENCON.2016.7848335).

[18] M. Anugraha, A. Anitha, and J. J. Kumari, "Throughput optimization using cross layer flow-based framework in cooperative wireless multihop networks", in *Proc. Global Conf. on Commun. Technol. GCCT 2015*, Thuckalay, India, 2015, pp. 366–370 (doi: 10.1109/GCCT.2015.7342685).

[19] Q. Peng *et al.*, "Multipath routing protocol based on congestion control mechanism implemented by cross-layer design concept for WSN", in *Proc. IEEE 17th Int. Conf. on Computat. Sci. and Engin.*, Chengdu, China, 2014, pp. 378–384 (doi: 10.1109/CSE.2014.98).

[20] Yong Yuan, Zhihai He, and Min Chen, "Virtual MIMO-based cross-layer design for wireless sensor networks", *IEEE Trans. on Veh. Technol.*, vol. 55, no. 3, pp. 856–864, 2006 (doi: 10.1109/TVT.2006.873837).

[21] L. Shan, Q. Liao, Q. Hu, S. Jiang, and J. Zhao, "A QoE-driven cross-layer resource allocation scheme for high traffic services over open wireless network downlink", in *Proc. IEEE 82nd Veh. Technol. Conf. VTC2015-Fall 2015*, Boston, MA, USA, 2015 (doi: 10.1109.VTCFall.2015.7390811).

[22] M. A. Gawas, L. J. Gudino, and K. R. Anupama, "Cross layer approach for effective multi hop broadcast in VANET", in *Proc. 9th Int. Conf. on Commun. Syst. and Netw. COMSNETS 2017*, Bangalore, India, 2017, pp. 403–404 (doi: 10.1109/COMSNETS.2017.7945414).

[23] M. Rath, B. Pati, and B. K. Pattanayak, "Cross layer based QoS platform for multimedia transmission in MANET", in *Proc. 11th Int. Conf. on Intell. Syst. and Control ISCO 2017*, Coimbatore, India, 2017, pp. 402–407 (doi: 10.1109/ISCO.2017.7856026).

[24] S. Shafi, B. N. Bhandari, and D. V. Ratnam, "An improved cross layer cooperative routing for vehicular networks", in *Proc. Int. Conf. on Res. Adv. in Integr. Navig. Syst. RAINS 2016*, Bangalore, India, 2016 (doi: 10.1109/RAINS.2016.7764427).

[25] M. A. Gawas, L. J. Gudino, and K. R. Anupama, "Cross layered adaptive cooperative routing mode in mobile ad hoc networks", in *Proc. 22nd Asia-Pacific Conf. on Commun. APCC 2016*, Yogyakarta, Indonesia, 2016, pp. 462–469 (doi: 10.1109/APCC.2016.7581425).

[26] M. A. Gawas, L. J. Gudino, and K. R. Anupama, "Cross layer multi QoS metric routing for multimedia traffic in 802.11E over MANETs", in *Proc. 8th Int. Conf. on Ubiquit. and Fut. Netw. ICUFN 2016*, Vienna, Austria, 2016, pp. 582–587 (doi: 10.1109/ICUFN.2016.7537099).

[27] S. Rehman, M. A. Khan, and T. A. Zia, "Cross layer routing for VANETs", in *Proc. of IEEE Int. Symp. on a World of Wirel., Mob. and Multim. Netw. 2014*, Sydney, NSW, Australia, 2014 (doi: 10.1109/WoWMoM.2014.6919006).

[28] B. Nithya, C. Mala, and E. Sivasankar, "A novel cross layer approach to enhance QoS performance in multihop ad-hoc networks", in *Proc. 17th Int. Conf. on Netw.-Based Inform. Syst.*, Salerno, Italy, 2014, pp. 229–236 (doi: 10.1109/NBiS.2014.13).

[29] E. C. Elias, S. Zhang, E. Liu, E. N. Nweso, and E. C. Joy, "REC-MAC: Reliable and efficient cooperative cross-layer MAC scheme for vehicular communication based on random network coding technique", in Proc. 22nd Int. Conf. on Autom. and Comput. ICAC 2016, Colchester, UK, 2016, pp. 342–347 (doi: 10.1109/IConAC.2016.7604943).

[30] O. Chipara *et al.*, "Real-time power-aware routing in sensor networks", in *Proc. 14th IEEE Int. Worksh. on Qual. of Serv.*, New Haven, CT, USA, 2006 (doi: 10.1109/IWQOS.2006.250454).

[31] A. Woo and D. Culler, "Evaluation of efficient link reliability estimators for low-power wireless networks", Tech. Rep. UCB/CSD-03-1270, EECS Department, University of California, Berkeley, 2003 [Online]. Available: https://www2.eecs.berkeley.edu/Pubs/TechRpts/2003/CSD-03-1270.pdf

Kummathi Chenna Reddy is working as a Research Scholar at the Department of Electronics and Communication Engineering at REVA University. He received his M.E. and B.Tech. degrees in Electronics and Communication Engineering. His research interests include wireless sensor networks and neural networks.

Email: chenna.cr@gmail.com
School of Electronics & Communication
REVA University
Bangalore, India

Geetha D. Devanagavi received her Ph.D. M.Tech. and B.E. degrees in 2014, 2005, and 1993, respectively. She is currently working as a Professor at Reva University. She has 21 years of teaching experience. Her research interests include wireless sensor networks, network security, and computer networks.

Email: dgeetha@reva.edu.in
School of Electronics & Communication
REVA University
Bangalore, India

Thippeswamy M. N. is currently a Professor at CSE, NMIT, Bangalore, holds a B.E. degree in Computer Science and Engineering from Kuvempu University, India, M.Tech. degree in Computer Science and Engineering from VTU, India and Ph.D. in Engineering from the School of Engineering (Electrical, Electronic and Computer Engineering), Howard college campus, University of KwaZulu-Natal, Durban, South Africa. His interests focus currently on the Internet of Things, big data analytics, wireless ad hoc & sensor networks and cognitive radio, with a particular emphasis placed on design and analysis of MAC and routing protocols.

Email: thippeswamymn@nmit.ac.in
Department of Computer Science
Nitte Meenakshi Institute of Technology
Bangalore, India.

Paper

Autonomous Navigation Control of UAV Using Wireless Smart Meter Devices

Kiyoshi Ueda[1] and Takumi Miyoshi[2]

[1] *College of Engineering, Nihon University, Koriyama, Japan*
[2] *College of Systems Engineering and Science, Shibaura Institute of Technology, Saitama, Japan*

https://doi.org/10.26636/jtit.2019.132319

Abstract—In preparation for the upcoming home delivery services that rely on Unmanned Aerial Vehicles (UAVs), we developed a new multi-hop radio network that is laid over a smart meter network transferring electric energy information only. In this network, a UAV follows, for navigation purposes, the topology of a virtual network overlaid on the physical smart meter network. We established a service management control method which does not rely on image analysis or map information processing, i.e. processes that consume precious power resources of the UAV. Instead, navigation is based on the routing technology. The current distance between the UAV and a node of the smart meter network is measured by means of the radio transmission loss value, therefore determining the position of the UAV. A two-layer network model has been proposed. One layer consists of a network of nodes in a residential area with scattered buildings – a location that is safer to navigate – while the other is an access network of nodes in a densely populated area. Then, we proposed methods to determine the direction of movement towards the next hop node on the data-link layer and the end node on the network layer, which is the target destination. We implemented a software-based test system and verified the effectiveness of the proposed methods.

Keywords—ad-hoc network, routing, smart meter network, UAV delivery.

1. Introduction

Unmanned Aerial Vehicle (UAV) control technology has been attracting a lot of attention recently. Introduction of UAVs is expected to bring about a reduction in labor costs and an improvement in the efficiency of home delivery services. The number of home deliveries increases every single year, and methods guaranteeing that the deliveries will be made in a secure and rapid manner need to be developed. Road traffic jams become an ever more burdensome phenomenon, as the volume of goods distributed grows. Workforce shortages caused by a decrease in the number and the aging of truck drivers become a serious social problem as well. The unmanned home delivery technology relying on mobile equipment is expected to be able to solve such problems. Home deliveries performed without visual observation of UAVs become ever more efficient. However, navigation management systems and crash prevention technologies still need to be improved. Methods used to determine the position of UAVs and to ensure identical delivery routes using enormous amounts of mapping and GPS data, as well as images sourced from UAV-mounted cameras and requiring real-time analysis, have been researched. Also, some methods used to pinpoint the position of the destination are known, but they include image analysis and map information processing, which consumes precious power resources of any UAV.

On the other hand, wireless devices known as "smart, next-generation electricity meters" [1] have been installed in each house in Japan. These wireless devices are installed to transfer electric billing information to utility companies, relying on a energy efficient, multi-hop radio (920 MHz) network. Such devices may be considered to be nodes of a stable multi-hop radio network, as they are present all over the country. In Japan, they were introduced in large quantities between 2016 and 2018, and according to plan, will be installed in all houses by 2023. We study to establish a method allowing to navigate UAVs safely and automatically based on the new multi-hop radio network between these wireless device nodes (Fig. 1).

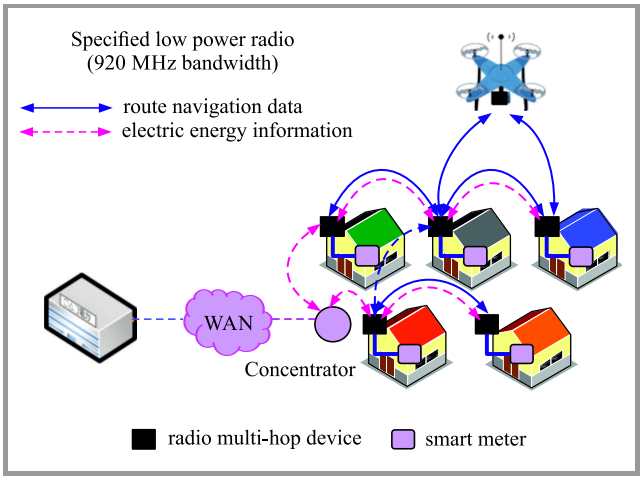


Fig. 1. Navigation based on a multi-hop radio network.

In this paper, we propose a route control protocol to build a multi-hop radio network topology in a safe, scattered res-

idential area rather than in a densely populated area. The wireless device measures the value of radio transmission loss of the received signals. Based on the radio transmission loss value, we are able to calculate the distance to the node by applying the Friis transmission equation. The position of the UAV within the network may be determined based on the distance between the UAV and the wireless devices. We also propose a method for controlling UAVs, so that they follow a specific route. Software has been developed to enable autonomous, distributed processing by each node, without any centralized functionalities, in order to account for the scalability of the number of nodes.

Although elderly people tend not to use the Internet as often, as they find it difficult to conclude a contract with and to get the connection settings from their ISP, they usually use electricity and have smart meters installed at their homes. It is important that home delivery services are available for each house. Using the location of a smart meter is more practical than pinpointing the latitude and longitude with the use of GPS. This method is suitable not only for home delivery, but also for such services as autonomous driving.

In addition, when location-related information based on smart meters is available all over the country, even if a serious disaster, such as an earthquake occurs, and telephones and the Internet cannot be used, the said information may be expected to be used in various domains, such as searching for a smart, wireless meter of a specific house, conveying its position to the city hall, or directing the rescue services.

In Section 2 of this paper related work is presented and problems related to autonomous navigation of UAVs are shown. Three methods to solve the problems described are identified in Section 3. In Section 4, we explain, in detail, the autonomous navigation control procedure. Section 5 shows the implementation and validation results. Section 6 is devoted to a discussion and contains several suggestions.

2. Related Works

Amazon announced that it is planning a rapid delivery service of lightweight commercial products using UAVs [2]. Google also revealed it had been testing UAVs for two years now as part of the "Project Wing" [3] scheme, to produce drones that are capable of delivering larger items. These systems need a camera recording the surroundings all the time, which means that the protection of privacy becomes a big problem. Therefore, a method for navigating UAVs without taking photographs is required. Indoor positioning and navigating systems relying on radio systems (Wi-Fi) were studied for accuracy [4]. But these are not suitable for navigating UAVs outdoors.

The communication layer used to establish a link with numerous wireless devices has been studied as well. It relied on a radio mobile ad-hoc network (MANET) technique. The reactive type (AODV [5]) and the proactive type (OSLR [6]) have established the shortest route between the nodes of a network.

A mobile ad-hoc network is based on the two-layer model with a node cluster. In the cluster, the network layer and the upper layer are distinguished, established by the cluster-by-cluster routing method [7]. Clustering is an effective method for improving the capacity to deal with node mobility, and to limit long distance communications by cascading short route messages.

3. Proposed Method

We propose a routing protocol to establish a safe route along a network of smart meters. The solution may be used for performing home deliveries with UAVs. We propose a control method in which the UAV communicates with the nodes, acquires information necessary for sensing the position and navigates by following the route, as if the UAV were a data packet within the network.

3.1. Network Topology for Routing of UAVs

The UAV route should be established with the principles of safe air travel taken into consideration. A two-layered network model has been adopted; a network of nodes in a scattered residential area (relay node), which is a safer navigation route (relay network), and an access network of nodes in a densely populated area. The overview of the network topology is presented in Fig. 2.

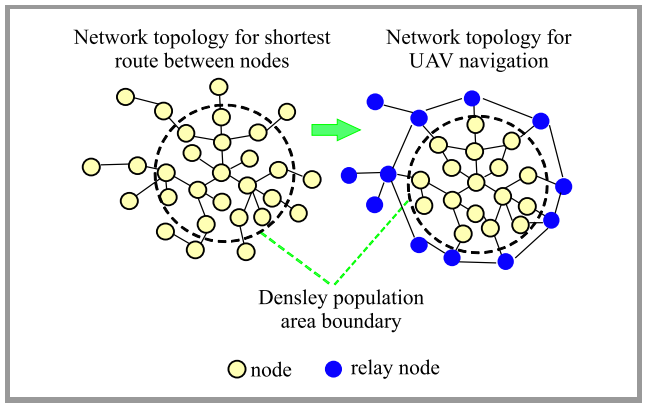


Fig. 2. UAV navigation network topology scheme.

3.2. Routing Protocol for UAV Navigation Network Topology scheme

Because no single delivery route is reused within a short period time for home delivery purposes, we investigated our routing protocol based on AODV – a masterpiece of the reactive type, creating a route list on demand. The route establishment process is shown in Fig. 3.

At first, information about the densely populated or the scattered residential area is set in all nodes. A parameter counting the number of passage areas is added to RREQ header of AODV. When a node transfers RREQ, the passage area counter of RREQ is incremented.

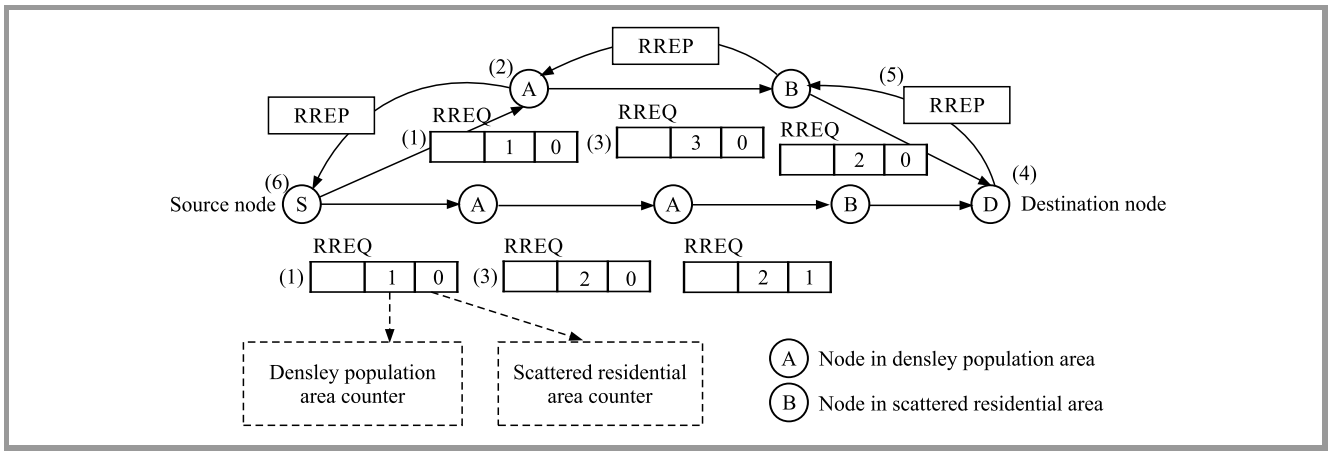


Fig. 3. Route establishment diagram.

When RREQ reaches the destination node, the number of densely populated areas and that of scattered residential areas along the route are stored. The destination node transmits RREP to the route with the smallest number of hops within densely populated areas. That is how a route avoiding densely populated areas is established. For calculating the distance between nodes, each node shall store the radio transmission loss value in the routing table, when the node receives RREQ or RREP:

1. The source node sends RREQ.
2. The node which receives RREQ adds the area count in RREQ header.
3. At step 2 above, the node which receives RREQ also records and sends the best RREQ with a lower value of densely populated area counts, compared with previous best RREQ (each node records RREQ, it received the first time, as the most suitable RREQ).
4. When RREQ signal reaches the destination node, the best route candidate is selected with the lowest number of densely populated area and residential area counts, from the numerous RREQs received.
5. The destination node repeats step 4 until time out, then it handles the elaborate route as the best root at that time. The destination node transmits RREP through that route.
6. RREP reaches the source node, and the most suitable route is established.

3.3. Autonomous Navigation Control Method

The proposed method maps a physical navigation route onto the virtual network model of nodes and links. UAV is connected to the multi-hop radio network and identifies the distance to each node based on the radio transmission loss value. UAV acquires information about the route to the destination node from the network, and proceeds to a position above the next hop node. When the next hop node cannot be detected due to instability of the wireless connection, UAV sends a new route request to the destination house node and another route is established. Thus, a network that is most suitable for navigation purposes is constructed based on the routing technology. Details of this approach are presented in following section.

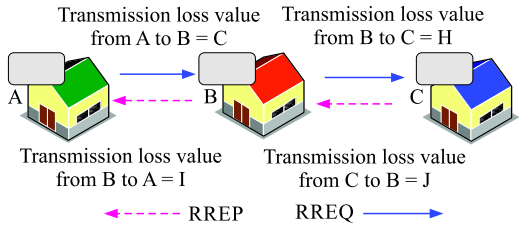
4. Autonomous Navigation Control Processing

4.1. Conditions

The smart meter of each house is considered to be a node. Each node compiles a routing table using a routing protocol and performs home delivery based on that table. Using the routing protocol shown in Section 3.2, each node may choose the home delivery route based on the high priority of a safe, scattered residential area. The value of radio transmission loss experienced between nodes is stored in a routing table (Fig. 4).

The node that received RREQ (node B) sets the address of the RREQ sending node (node A) to next hop in the column where the destination is the source node (node A) in the routing table of the node itself (node B). The node (node B) acquires the inter-node radio transmission loss value (G from node A to node B) from the received RREQ and sets it in that column. When the node receives RREP (node A) transmitted by the destination node from the previous node (node B), the node (node A) sets the address of the RREP transmitting node (node B) to the next hop of the column where the destination is the destination node (node C) in its own (node A) routing table. The node (node A) acquires inter-node radio transmission loss value (I from node B to node A) from the received RREP and sets it in that column.

As UAV communicates with the smart meter based on the routing table, it may complete the delivery without using map information, by simply following the same delivery route that would be taken by a data packet traveling along the network. Vertical UAV movements are identified along



Routing table of node A

Destination	Next hop	Transmission loss value
Null	Null	Null
C	B	I

Routing table of node B

Destination	Next hop	Transmission loss value
A	A	G
C	C	J

Routing table of node C

Destination	Next hop	Transmission loss value
A	B	H
Null	Null	Null

Fig. 4. Routing table.

the z axis, horizontal movements along the y axis, while back and forth movements along the x axis. The UAV shall be given the address of the source node and the destination node beforehand and, it is assumed that the UAV flies at a constant height Δz. We call the source node S, the destination node D, and the UAV M.

4.2. Navigation Control Flow

UAV acquires route information from the current node. It receives information necessary for position sensing and information about navigating to the next node. UAV starts moving to the next node while sending its position repeatedly. On the way to the next node, the UAV receives position information from the current node, the next node, and the previous node to obtain the movement direction. UAV follows the route from the source node to the destination node by repeating this process.

4.3. Proposed Signal Specifications

Route information request. UAV sends this signal to the current node for collecting the address of the next node and the radio transmission loss value between the current node and the next node. The route information request signal stores the address of the destination node that is necessary for UAV to request information about the next node. The ID of this signal is 1.

Route information response. The node receiving the route information request signal checks the destination node's address from the route information request signal to establish whether the specific node is the destination node or not. If the node is not the destination node, it sends a response signal to UAV, using the routing table data. The signal includes, in the data section, the address of the next node and the radio transmission loss value between the current node and the next node. The ID of this signal is 2.

End of delivery. The node receiving the route information request signal checks the destination node's address in the route information request signal, to determine whether the node is the destination node or not. If the node is the destination node, it sends the end of delivery signal to UAV. The signal does not have a data section and the ID of this signal is 3.

ϕsend. This is a signal that the UAV is transmitting to the node requiring the radio transmission loss value. The signal does not have a data section and the ID of this signal is 4.

ϕreply. This is a signal by means of which the node which is receiving the ϕsend signal is sending the radio transmission loss value to UAV. The signal does not have a data section and the ID of this signal is 5.

4.4. Route Information Request

Data from the routing table of the current node is necessary for UAV to acquire route information. Therefore, UAV transmits the route information request signal to the current node (Fig. 5). The current node, which received the signal, transmits the route information response signal, including information about the next node, to UAV. UAV, which received the route information response signal, stores

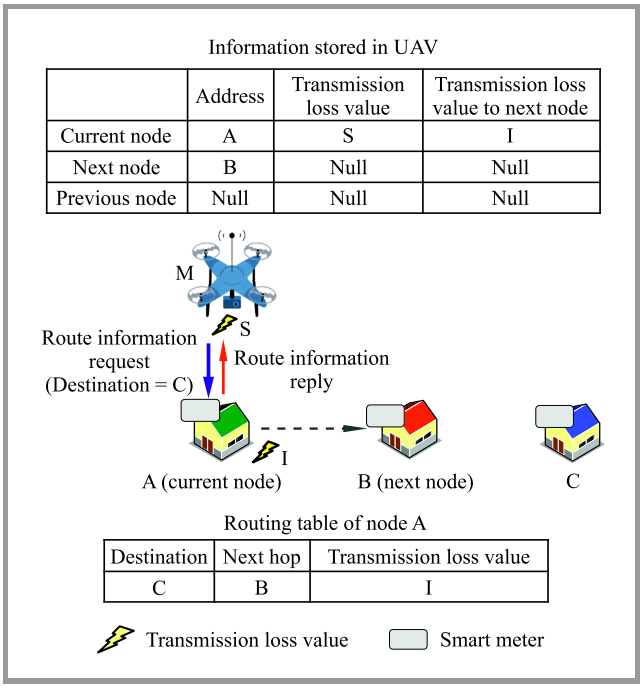
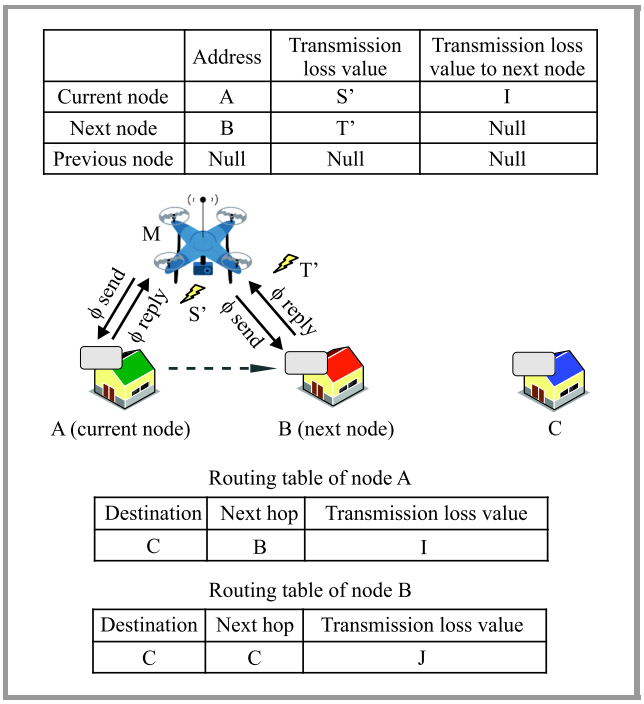


Fig. 5. Route information request.

the radio transmission loss value to the current node, as retrieved from the packet header, as well as information in the received signal data.

4.5. Radio Transmission Loss Value Request

To obtain the radio transmission loss value, UAV sends the ϕsend signal to the current node and the next node. Then, UAV receives the ϕreply signal from each node (Fig. 6). When UAV does not move, it does not send information about its position to the current node, after reception of the route information response signal, UAV obtains the value of radio transmission loss experienced while communicating with each node from the header of the ϕreply signal received.



	Address	Transmission loss value	Transmission loss value to next node
Current node	A	S'	I
Next node	B	T'	Null
Previous node	Null	Null	Null

Routing table of node A

Destination	Next hop	Transmission loss value
C	B	I

Routing table of node B

Destination	Next hop	Transmission loss value
C	C	J

Fig. 6. Radio transmission loss value request.

4.6. Calculating Distance from Radio Transmission Loss Value

UAV converts the acquired radio transmission loss value into distance. The radio transmission loss value changes as the power rating becomes lower due to increasing radio transmission distance. In free space, the radio transmission loss value is calculated using the Friis transmission equation (1). At first, we determine free space transmission gain $\left(\frac{\lambda}{4\pi d}\right)^2$ using the Friis transmission equation, and $\left(\frac{4\pi d}{\lambda}\right)^2$, which is the reciprocal number of the free space transmission gain, is the free space transmission loss L_B:

$$P_R = P_D A_R = \left(\frac{\lambda}{4\pi d}\right)^2 G_T G_R P_T \ , \qquad (1)$$

where P_R and P_T mean electric power, A_R means practical antenna area, G_R and G_T mean antenna absolute gain, P_D is power density, d is communications distance, λ is wavelength.

The radio transmission loss L_B is $10 \log \frac{P_T}{P_R}$, where the terms G_T and G_R of the equation for obtaining L_B are zero, assuming that an isotropic antenna (absolute gain = 1) is used. Wavelength λ is represented by $\frac{c}{f}$ using frequency f. Distance may be established based on radio transmission loss value by solving the expression after its conversion to distance d (2):

$$d = \frac{4\pi f}{c} 10^{\frac{20}{-L_B}} \ , \qquad (2)$$

where c is speed of the electric wave and f is frequency. In this way, UAV may calculate the distance between nodes, as well as that between the UAV and each node.

4.7. Establishing Position Based on Distance

We use the Pythagorean theorem to find the length of side AM' and side BM' from Δz of UAV height, side AM is the distance to the current node, and side BM is the distance to the next node (Fig. 7). Then, we calculate Δx, which is the distance between point B and the current position of the UAV, projected onto the ground, as well as horizontal gap Δy from the lengths of side AB, side AM' and side BM' by using Eq. (3). In this way, we identify the position of the UAV (Fig. 8).

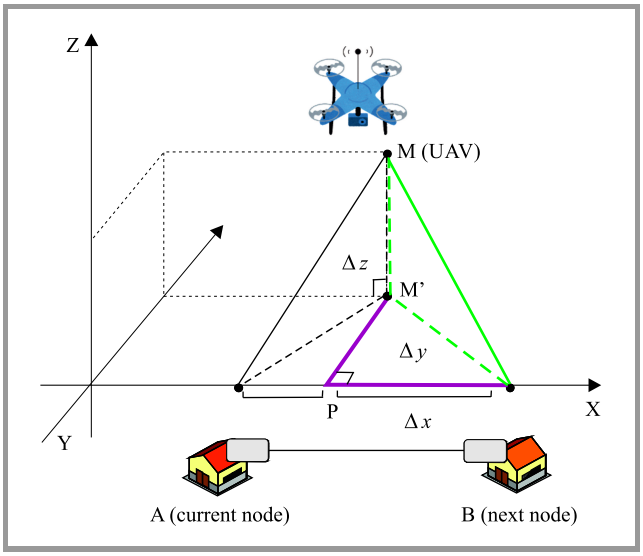


Fig. 7. Establishing the position of UAV in network 1.

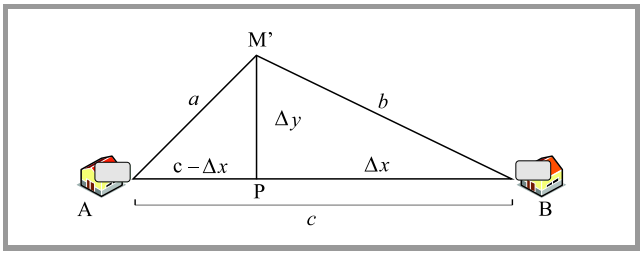


Fig. 8. Establishing the position of UAV in network 2.

$$\begin{cases} (c-\Delta x)^2+\Delta y^2=a^2 \\ \Delta x^2+\Delta y^2=b^2 \end{cases}, \tag{3}$$

$$\Delta x=\frac{-a^2+b^2+c^2}{2c}, \tag{4}$$

$$\Delta y=\sqrt{b^2-\Delta x^2}. \tag{5}$$

UAV stores the Δx and Δy values as old_x, old_y until the next measurement.

4.8. Navigation Control

After detection of the position has been accomplished, UAV moves to the next node after time unit Δt and detects its position again. UAV adjusts the position and moves in the right direction by comparing old_x with Δx and old_y with Δy.

Movement control along y axis. The tolerance threshold of Δy (right and left movements) has been set in UAV beforehand. When the Δy calculated is higher than the threshold value, UAV moves Δy to the right or to the left, until Δy becomes lower than the threshold set, before sensing its next position. The first movement is always to the right, and then the value of Δy is compared with the value of old_y. Where $old\_y > \Delta y$, the value of Δy is decreasing and UAV is moving in the right direction. Where $old\_y < \Delta y$, the value of Δy is increasing. This means that UAV is moving in the opposite way, and it should change the direction.

Movement control along x axis. UAV adjusts its movement along x axis comparing the value of Δx with the value of old_x, as it did in the scenario with y axis. If $old\_x > \Delta x$, the value of Δx is decreasing and UAV is moving to the right direction. If $old\_x < \Delta x$, that means the value of Δx is increasing, therefore, the UAV is moving in the opposite way. Then, UAV repeats position sensing, calculates the movement and approaches the next node.

4.9. Updating Current and Next Node

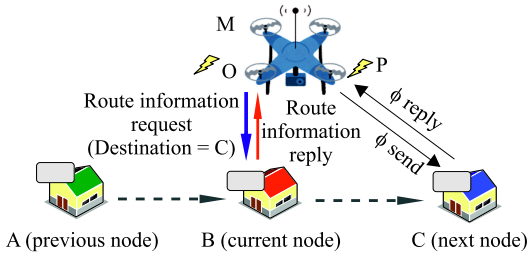
When Δx becomes "0", UAV may arrive at the next node. Then, the current node should be updated. At first, UAV stores the current node's address as the previous node's address, sends a route information request signal to the next node, then receives the route information response signal from the next node (Fig. 9).
With this procedure, UAV considers the node to route information request signal has been sent as the new current node, and then UAV finds the new next node based on the route information response signal. After that, UAV measures the radio transmission loss value, establishes its position based on distance and moves to the next node.

4.10. Turns

After updating the current and the next nodes, UAV turns toward the next node. At this time, UAV may receive radio

Information stored in UAV

	Address	Transmission loss value	Transmission loss value to next node
Current node	A	O	J
Next node	C	P	Null
Previous node	A	Q	I



Routing table of node A

Destination	Next hop	Transmission loss value
C	B	I

Routing table of node B

Destination	Next hop	Transmission loss value
C	C	J

Fig. 9. Updating current and next node.

waves from the previous node, the current node and the next node. At first, UAV moves from the position above the current node to the inside of the angle between the previous and the next node. UAV moves a little to the left or the right (y axis direction), which is the direction that the radio transmission loss value decreases, and then moves the same distance backward along axis x. At that position, UAV calculates the lengths of sides AM', BM' and CM' using the Pythagorean proposition, with height Δz and distances from UAV to the previous and the next node taken into consideration (Fig. 10).

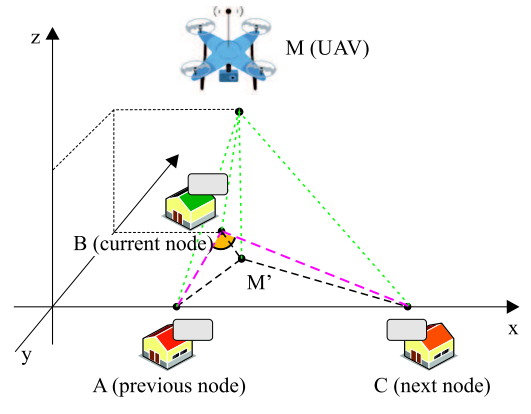


Fig. 10. Turns.

Then, UAV is capable of calculating ∠ABM' using the Law of cosines (6), based on lengths of side AB, side AM', and

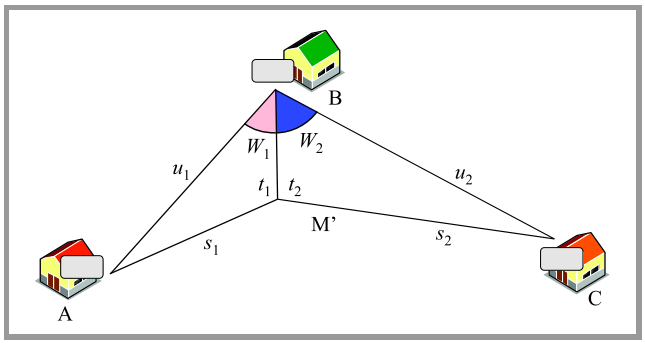


Fig. 11. Calculation of the angle by the law of cosines.

side BM' (Fig. 11). Similarly, UAV may calculate ∠M'BC based on lengths of side BC, side BM', and side CM':

$$\cos W = \frac{t^2 + u^2 - s^2}{2tu}. \tag{6}$$

The angle of rotation of UAV may be calculated by subtracting the sum of two angles calculated above from 180 degrees, enabling UAV to make the turn autonomously.

4.11. Delivery End

When the route information request signal has been transmitted to the next node and the node address matches the destination address, UAV has arrived at the target destination. In this case the node transmits a end of delivery signal to UAV and UAV descends to finish the delivery.

5. Implementation and Validation

5.1. Implementation

Before programming, we performed experiments concerning radio transmission loss values in real world, derive an expression to identify distances between UAV and the nodes. We prepared two sets of a Raspberry Pi 3 and a radio device and considered them to be UAV and smart meters installed in the house. We moved UAV device away from the house, 1 meter at a time, and recorded the radio transmission loss value L_B, which UAV acquired at

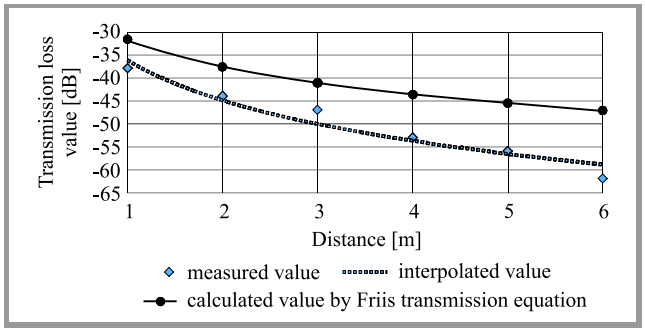


Fig. 12. Radio transmission loss value and distance.

the reception of the signal. The calculated radio transmission loss value, the distance in the free space of Eq. (2) presented in Section 4.6 and the value measured in real world are shown in Fig. 12. It was confirmed that the radio transmission loss differed from the theoretical value due to the influence of the atmosphere that acts as the transmission loss medium [8]. This time we measured it in fine weather, but rainfall increases transmission losses even further [9], so it is expected that the loss values will be higher. We assume that UAVs will perform the home delivery service in fine weather, so the effects of rain do not have to be taken into consideration.

If the distance is short, the difference between the calculated value and the measured radio transmission loss values is small. The longer the distance, the larger the difference between the calculated and the measured values. While the results are inaccurate when UAV is far away from the node, it has been confirmed that this distance measuring method may be applied for the purpose of home deliveries performed by UAV.

We derived an approximate curve from the measurement data and defined an expression (7), where e is a bottom of the natural logarithm:

$$d = \mathrm{e}^{\frac{L_B + 36.084}{-12.69}}. \tag{7}$$

We wrote programs to implement the position sensing smart meter radio devices, using Eq. (7) obtained in the above experiment. For the UAV side, we handled sending and receiving signals, programmed positioning and movement control of mobile devices, and enabled the provision of results of navigation control calculations. As far as radio devices of house node side are concerned, we implemented functions enabling them to generate, send and receive those signals.

5.2. Validation

We setup four sets comprising a Raspberry Pi 3 and a wireless device each. One set is considered to be UAV, while three remaining sets are used as smart house meters (network nodes). The question was whether UAV and the nodes are capable of transmitting right signals to the specific address. We also validated that the calculation results were correct and that the movement control signals were generated and worked as intended. We run the program and checked the output. In addition, a reverse calculation using spreadsheet software was performed to check whether the output results are correct. The reverse calculation was possible without acquiring the radio transmission loss value, by setting it in each node beforehand.

The result shows that right signals were transmitted and received between the designated nodes (Figs. 13 and 14). The results of positioning and turning calculations were almost the same as the forecast value. Because the discrepancies originate from the difference in the number

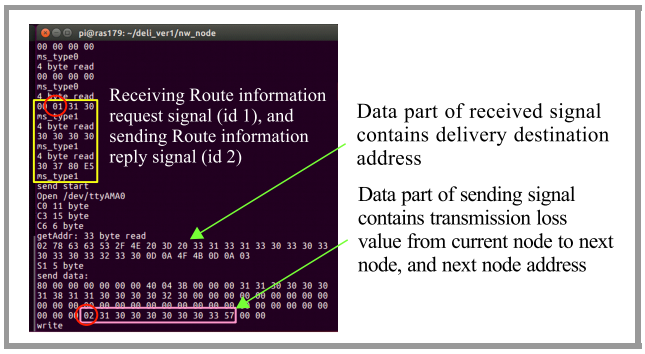


Fig. 13. Validation result 1.

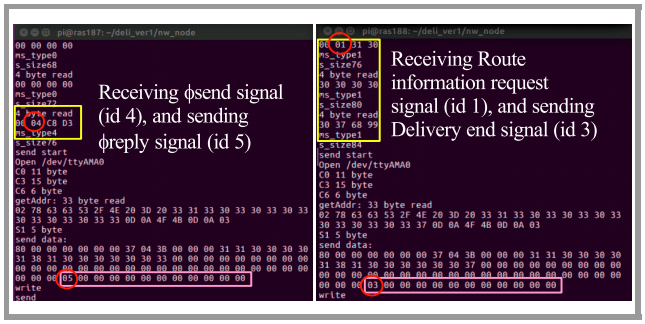


Fig. 14. Validation result 2.

of significant digits, the result indicates that the program we implemented is able to confirm that our proposal has worked well.

6. Conclusion

We proposed a routing protocol to establish a safe route for UAV navigation, using a smart meter network. We also proposed methods for position measurement and movement control, enabling UAVs to perform autonomous home deliveries. In the proposed method, distances between UAV and nodes are calculated from the radio transmission loss value. UAV is controlled by determining distance based on the severity of radio transmission loss that occurs while exchanging signals.

Some issues still exist that need to be solved before implementing this system. For example, procedures applied in a scenario in which no electric waves sent by nodes can be detected must be worked out, as must be procedures relied upon to reduce UAV's altitude, track its position or search for another route when no signal is received at all. Safe take-offs and landings are a source of concern as well. We will also establish a method that will change the route if any abnormalities are detected, in order to avoid crashing UAV. All those issues need to be addressed before an autonomous home delivery service relying on UAVs is commissioned.

For future work, we will implement all functions of the proposed method and will experimentally confirm power consumption achieved while using the proposed method and while relying on GPS and map-based navigation.

References

[1] "IPv6 routing protocol for low power and Lossy networks (RPL)", Routing Over Low power and Lossy networks (ROLL) WG, IETF, RFC 6550, March 2012 [Online]. Available: https://tools.ietf.org/html/rfc6550

[2] "Amazon Prime Air" [Online]. Available: https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011 (accessed Oct. 29, 2018).

[3] "Wing", Google Project [Online]. Available: https://x.company/projects/wing/ (accessed Oct. 29, 2018).

[4] K. Miyazaki, M. Mochizuki, K. Murao, and N. Nishio, "Cross-assistive approach for PDR and Wi-Fi positioning", in *Proc. of the 2014 ACM Int. Joint Conf. on Pervas. and Ubiqui. Comput. UbiComp'14*, Seattle, WA, USA, 2014, pp. 777–786 (doi: 10.1145/2638728.2641303).

[5] "Ad hoc On-Demand Distance Vector (AODV) Routing", IETF, RFC 3561, July 2003 [Online]. Available: https://tools.ietf.org/html/rfc3561

[6] "Optimized Link State Routing Protocol (OLSR)", IETF, RFC 3626, Oct. 2003 [Online]. Available: https://tools.ietf.org/html/rfc3626

[7] H. Narumi, Y. Shiraishi, and O. Takahashi, "A reliable cluster-based routing algorithm for MANET", *in Proc. of the Int. Worksh. on Informat. IWIN 2009*, Honolulu, Hawaii, USA, 2009, pp. 44–51, 2009 [Online]. Available: http://www.infsoc.org/conference/iwin2009/IWIN2009-Proceedings_v2.pdf

[8] Rec. ITU-R P.676-5, "Attenuation by atmospheric gaps", ITU, 2001 [Online]. Available: https://itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.676-5-200102-S!!PDF-E.pdf

[9] Rec. ITU-R P.838-2, "Specific attenuation model for rain for use in prediction methods", ITU, 2003 [Online]. Available: https://itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.838-2-200304-S!!PDF-E.pdf

[10] K. Ueda and T. Miyoshi, "Autonomous navigation control of UAV using wireless smart meter devices", in *Proc. of the Inform. and Commun. Technol. Forum ICTF 2018*, Graz, Austria, 2018.

Kiyoshi Ueda received his B.E. and M.E. degrees in Electrical Engineering from Keio University, Yokohama, Japan, in Electrical Engineering from Keio University, Yokohama, Japan, in 1987 and 1989, respectively. He received his Ph.D. degree in Information Science and Electrical Engineering from Kyushu University in 2010. After joining NTT in 1989, he was engaged in research and development work focusing on digital switching software, with a particular emphasis placed on designing distributed switching node management software. He was an active member of ITUT SG11 and SG4, where he contributed to TMN. He was also responsible for research and development of peer-to-peer network service software. Since 2014, he has been a professor at the College of Engineering, Nihon University. He received the Best Paper Award from the IEICE communication society in 2008. He is a member of IEEE, IEICE and IPSJ.

E-mail: ueda.kiyoshi@nihon-u.ac.jp
College of Engineering
Nihon University
Koriyama, Japan

Takumi Miyoshi received his B.E., M.E., and Ph.D. degrees in Electronic Engineering from the University of Tokyo, Tokyo, Japan, in 1994, 1996, and 1999, respectively. He started his career as a research associate at the Global Information and Telecommunication Institute, Waseda University, where he worked from 1999 to 2001. He is currently a Professor at the Department of Electronic Information Systems, College of Systems Engineering and Science, Shibaura Institute of Technology, Saitama, Japan. He was a visiting scholar in Laboratoire d'Informatique de Paris 6 (LIP6), Sorbonne Université, Paris, France, from 2010 to 2011. His research interests include content delivery networks, overlay networks, as well as mobile ad hoc and sensor networks.

E-mail: miyoshi@shibaura-it.ac.jp
College of Systems Engineering and Science
Shibaura Institute of Technology
Saitama, Japan

Paper

Infrastructure and Energy Conservation in Big Data Computing: A Survey

Ewa Niewiadomska-Szynkiewicz and Michał P. Karpowicz

Institute of Control and Computation Engineering, Warsaw University of Technology, Warsaw, Poland

https://doi.org/10.26636/jtit.2019.132419

Abstract—Progress in life, physical sciences and technology depends on efficient data-mining and modern computing technologies. The rapid growth of data-intensive domains requires a continuous development of new solutions for network infrastructure, servers and storage in order to address Big Data-related problems. Development of software frameworks, include smart calculation, communication management, data decomposition and allocation algorithms is clearly one of the major technological challenges we are faced with. Reduction in energy consumption is another challenge arising in connection with the development of efficient HPC infrastructures. This paper addresses the vital problem of energy-efficient high performance distributed and parallel computing. An overview of recent technologies for Big Data processing is presented. The attention is focused on the most popular middleware and software platforms. Various energy-saving approaches are presented and discussed as well.

Keywords—Big Data, cloud, cluster, energy-efficient computation, grid, HPC, software platform.

1. Introduction

A truly explosive growth in the volume, variety and speed of digital data created and collected on a daily basis may be observed from the very onset of the Internet era. Big Data computing is a critically difficult challenge for High-Performance Computing (HPC). The main goal is to develop efficient technologies for transforming massively large and often unstructured or semi-structured data - firstly into valuable information, and then into meaningful knowledge. Raw data that are gathered by numerous sources including sensors, mobile devices, open and commercial datasets and archives, social networks, etc. have to be processed, often in the on-line mode. The challenge consists in the ability to integrate, store and analyze such data while satisfying fewer software and hardware-related requirements that may apply to huge collections of data sets generated by and gathered from distributed sources. Therefore, Big Data problems require continuous improvement of processors, servers, as well as storage and network infrastructure in order to enable the efficient processing of data through remote data management applications. The main challenge is to design and develop complete frameworks for intelligent management and communication, data filtration, aggregation, correlation and fusion. Moreover, reduction in energy consumption is another technological challenge arising with the development of computing infrastructures for Big Data-related applications. The programming abstractions and data processing techniques must therefore be designed for:

- seamless implementation of applications with efficient levels of virtualization of computing resources such as servers, storage and networks,
- effective normalization, unification and merging of various types of data into a consistent format,
- energy conservation in data centers and communication infrastructure.

Distribution transparency, reliability, scalability, information sharing, fast and secure exchange of information originating from remote sources and efficient management of energy consumption are the main requirements for HPC systems. The idea behind distribution transparency is to hide the distribution-related aspects of a system from its users and applications, i.e. to provide a single system view. Transparency is often described in terms of unification of the process, memory, distributed file systems and input/output device space. A unified process space is implemented by providing visibility of and control over all processes running across the whole computing system. Unification of memory space applies to globally addressable shared memory and process-level distributed shared memory. Distributed file systems are used to provide an aggregated hierarchy of file collections stored across the computing nodes. Unification of input/output devices provides transparency and performance. Reliability and scaling are achieved through distribution, replication and caching techniques. Distributed file systems and non-relational (NoSQL) databases, fast and secure data networks aim to improve the efficiency of information sharing and remote data exchange. Modern, energy-efficient hardware components, mechanisms and methods relied upon to ensure energy-aware management of computation and communication processes foster energy conservation.

Numerous mechanisms, algorithms, computing infrastructures, software platforms and middleware for high performance computing have been developed during the past decades. Many surveys are available on recent technologies for Big Data applications (e.g. [1], [2]). However, due to their rapid development, reviews quickly become outdated. In this paper we present and discuss the most popular infrastructures, platforms and middleware that may be used for Big Data processing, modeling and simulation.

The remainder of this paper is organized as follows. A short survey of infrastructure and middleware for Big Data-related problems is presented in Section 2. Primary attention is focused on computing clusters, grids and clouds. A brief description of job scheduling and load balancing methods and algorithms is presented in Section 3. Widely used Big Data processing, visualization and machine learning platforms are discussed in Sections 4 and 5. Some frameworks for modeling and simulating Big Data problems are described in Section 6. A general overview of approaches to energy-aware computation is presented in Section 7. Finally, conclusions are drawn in Section 8.

2. Infrastructure and Middleware for Big Data Problems

During the past three decades, software for parallel computers focused on providing powerful mechanisms for managing communication between processors and environments for parallel machines and computer networks. High Performance Fortran (HPF), OpenMP, OpenACC, Parallel Virtual Machine (PVM) and Message Passing Interface (MPI) were designed to support communications for scalable applications. Application paradigms were developed to perform calculations on shared memory machines and clusters of machines. Moreover, the architecture of computing nodes may be different (a single processor or a symmetric multiprocessor), and types of methods relied upon to access storage devices may vary as well.

On the other hand, easy access to information offered by the Internet has spawned a new idea, i.e. extending the connection between computers. Thanks to such an approach, distributed resources, including applications, computing power, storage, etc., can be accessed as easily as information on Web pages. The idea was implemented in various forms, but three computing environments have been dominating recently: computing clusters, grids and clouds.

2.1. Computing Cluster

A cluster is a group of cooperating, off-the-shelf commodity computers and resources that serves as one virtual machine [3], [4]. The efficiency of a cluster depends on the speed of processors of separate nodes and the efficiency of network technology. Each computing node may have different characteristics, i.e. may be of the single processor or the symmetric multiprocessor design, and may offer various types of storage devices. In advanced computing clusters, simple local networks are substituted by very fast communication channels – dedicated networks made up of low latency and high speed switches.

Numerous software tools supporting cluster computing have been developed. Most of them rely on the single system image (SSI) computing paradigm, where a group of computing and storage resources is aggregated and is seen by the user as a single system. SSI technology involves a broad variety of techniques, from custom hardware and hypervisors to dedicated operating systems and user-level tools. A survey of classification schemes and implementation techniques is provided in [1]. Notable hardware, hypervisor and kernel level techniques are discussed. The focus is on distributed operating systems, both dedicated operating systems and adaptations of existing operating systems. MOSIX [5] is one of the oldest and most commonly known SSI kernel patches that provides transparent process migration and automatic load balancing within the cluster. MOSIX does not provide full SSI. All processes which were launched on a given node are displayed, even if they have been moved to remote nodes. However, processes initiated on other nodes are not displayed. The unique space of process IDs is preserved in OpenSSI [6] and Kerrighed [7] systems. OpenSSI allows the migration of transparent processes and groups of threads and enables load balancing within the cluster. Kerrighed provides transparent migration of processes, as well as single threads. All kernel-level implementations mentioned above are accompanied by a complementary suite of user-level software tools.

2.2. Computing Grid

A grid [8] is a collection of loosely coupled, geographically distributed, heterogeneous computational resources and devices. Initially, the idea of a grid was to expand the parallel computing paradigm from tightly coupled clusters onto geographically distributed computing systems. However, in practice, grids are utilized more often as a platform for integration of loosely coupled applications. Nowadays, computational grids enable the sharing and the aggregation of a wide variety of geographically distributed computing resources. Moreover, they present them as a unified resource for solving large-scale computation problems.

The resources that are taken into account in these definitions include the following: computer clusters, supercomputers, databases and storage systems, visualization devices and dedicated software. To facilitate the creation and maintenance of grids, several features have been assumed. The most important of them are: scalability, adaptability, data transfer, process scheduling and allocation, use of open standard protocols, interfaces, and often processes migration. The calculation and data space are in fact heterogeneous, but virtually they are homogeneous. A broad spectrum of grid computing activities and scientific projects have been carried out, e.g. a uniform interface for comput-

ing resources Unicore [9], Globus Toolkit [10] – a software toolkit used for building grids and many others described in literature [11], [12].

2.3. Computing Cloud

In general, both grid and cloud computing offer similar functionalities and serve the same purpose. However, their implementations are different. The cloud computing model offers facilities and common resources, on an on-demand basis, over the Web [13], [14]. A typical cloud computing provider delivers common business applications online. The applications are accessed from a Web service or a Web browser, while the software and data are stored on servers. Most cloud computing infrastructures consist of services delivered through common centers and are built on servers. Cloud often appears as a single point of access for the customers' computing needs. Quality of service (QoS) and service level agreements (SLAs) are generally expected. Cloud computing provides three remarkable services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Resource virtualization is generally at the heart of cloud architectures. The concept of virtualization provides an abstract, logical overview of the physical resources and includes networks, servers and data stores. The basic idea is to join physical resources and manage them as a whole. However, it should be noted that in classic HPC applications, some performance degradation may occur while working in a virtualized environment.

2.4. GPU Computing

A Graphics Processing Unit (GPU) is a specialized massively parallel graphics processor that may be used as a general purpose computing accelerator that is a low-cost, highly accessible alternative to supercomputers [15]. GPU-enabled parallel computing has become extremely popular over the past decade. The GPU-based model for parallel computing has rapidly increased its advance into different areas of technology and is currently used to solve complex scientific and engineering problems. GPUs allow to perform massively parallel computations. Therefore, those computation tasks which may be divided into large numbers of independent parts are of special interest.

This technology may be specifically exploited for massive data processing purposes. Using CPU and GPU jointly, along with CUDA or OpenCL parallel computing platforms, many real-world applications may be easily implemented and are capable of running significantly faster than on multicore or multiprocessor systems. Nowadays, GPU clusters are one of the most progressive branches of HPC. However, problems associated with the optimization of memory management are still experienced when it is necessary to provide fast access to data chunks exceeding the size of the local GPU's memory.

3. Job Scheduling and Load Balancing

Job scheduling and load balancing are one of the most important characteristics of distributed systems. Techniques such as checkpointing, as well as placement and migration of processes allow for transparent load balancing across computing nodes. An efficient load balancing algorithm is triggered when loads of nodes are not balanced or when local resources are limited. Numerous static and dynamic load balancing techniques have been developed for cluster, grid and cloud systems. A survey on load balancing algorithms is provided in [16]–[18].

There are many software tools for supporting job scheduling and management in distributed systems. Torque [19] is a distributed resource manager that provides control over batch jobs and distributed computing resources. Torque allows also to work in an interactive mode. Torque expands the original PBS system [20] offering scalability, fault tolerance and better functionality. It may be integrated with the Moab Cloud smart workload manager that is responsible for load balancing and for optimizing application performance. Torque is customizable to match the needs of the computing system and the specific application. Slurm [21] is a fault-tolerant and highly scalable open source cluster management and job scheduling system for Linux clusters of various sizes. Slurm provides a framework for starting, executing and monitoring allocated jobs. Moreover, the Slurm system manages a queue of pending tasks. MapReduce and YARN represent two different approaches to job scheduling and managing cluster resources. MapReduce [22] is a framework that provides and implements a programming model. It simplifies the processing of massive volumes of data by using two subsequent functions that handle data computations. The MapReduce processing scheme is composed of a map method, which performs data filtering, sorting and splitting, and a reduce method, which performs a summary operation - processes intermediate output data. In fact, the idea is to design data for easy scheduling and cluster management. The YARN resource management and job scheduling technology [23] is more generic than MapReduce. YARN allows multiple data processing engines, such as batch processing, real-time streaming, interactive SQL and data science to handle data stored on a single platform. Unlike MapReduce, YARN enhances efficiency by splitting two main functionalities of the job tracker into two separate daemons responsible for allocation and management of cluster resources, and for task scheduling and monitoring, respectively.

4. Platforms for Big Data Processing

Various software platforms for supporting large scale and massive data distributed processing have been developed during the past decade. Apache Hadoop ([23], [24]), is a framework that enables distributed, scalable processing of large data sets across clusters of computers utilizing a simple programming model. It is designed to scale up from

single servers to many (thousands) machines, each offering local storage and processing capabilities. The power of the Hadoop platform is based on the Hadoop Distributed File System (HDFS), the HBase distributed and scalable non-relational database and programming models. Hadoop delivers a highly-available service on top of a cluster of computers, each of which may be prone to failures. The failures are detected and handled at the application layer. The Hadoop community has contributed to enriching its ecosystem both with open source projects and a wide range of commercial tools and solutions. Some of the best-known open source examples include:

- Pig – a framework for the generation of a high level scripting language (Pig Latin),
- Hive – a data warehouse system that is designed to simplify the use of Hadoop frameworks,
- JAQL – a declarative language designed to convert high level queries into MapReduce jobs,
- Sqoop – software that provides a command-line interface and moves relational data into HDFS,
- Oozie – a workflow scheduler system,
- Mahout – a framework for scalable machine learning, etc.

A variety of commercial tools can be used for specific Hadoop development, production, and maintenance tasks. Hadoop is designed for batch processing.

Apache Spark [25] is a unified engine for Big Data processing. Spark can run in a standalone mode or with a Hadoop cluster serving as the data source. It is both a programming and computing model. Spark provides an alternative to MapReduce that enables workloads to be executed in memory, instead of on disk, thus eliminating resource-intensive disk operations that MapReduce requires. It processes data in RAM. The implemented data model is based on the Resilient Distributed Dataset (RDD) abstraction. The Spark framework consists of components for memory management, fault recovery, data exchange, task scheduling, etc. The main Apache Spark use cases include the following: streaming data, machine learning, fog computing, etc.

Apache Storm [26] is a scalable, rapid, fault-tolerant and easy-to-use platform for distributed computing that has, unlike Hadoop, the advantage of handling real time data processing. A Storm interface may potentially support any incoming data, hence data from real time synchronous and asynchronous systems can be downloaded. It can process one million tuples per second using a simple programming model and hiding the complexity of the Big Data application. Typical use cases include real-time analytics, online machine learning, IoT, continuous computation, etc.

Apache Flink [27] is a framework for batch and stream processing, event-time processing and stateful computations. It can run in all common cluster environments, perform computations at in-memory speed and on a high scale. Similarly to Storm, it may be successfully used to develop software systems for fraud and anomaly detection, monitoring, as well as real-time and discrete-event simulation.

5. Platforms for Big Data Visualization and Machine Learning

A number of tools for Big Data analysis, visualization and machine learning are available in the network. RapidMiner Studio [28], Orange [29] and Weka [30] belong to this group of solutions. Numerous novel applications have been designed and developed for browsing, interpreting, visualizing and analyzing large-scale sequencing data. Several of these, including Tablet [31] have been designed specifically for the visualization of genome sequence assemblies. Other tools, such as BamView [32] have been developed specifically to visualize mapped read alignment data in the context of the reference sequence. Artemis is a freely available integrated platform for visualization and analysis of large-scale experimental data. It is an established genome annotation tool [33] that has been used in many genome projects. It is an effective tool for visualization, analysis, interpretation and inspection of high-throughput sequence-based experimental data [34].

Plenty of platforms and packages have been developed for social network analysis and visualization. The survey of most popular ones, which find a wide range applications, including network theory, finance, biology, sociology, etc., is presented in [35].

6. Simulation Frameworks

Simulation of large scale systems is another issue requiring attention. Simulation and Big Data analytics produce the most value when used together. Methods for Big Data analytics process simulation data, extract valuable information and convert it into proper decisions or predictions of future behavior – all in a short period of time. The combination of efficient and reliable simulation software and specialized (purpose-built) hardware optimized for simulation workloads is crucial to fully exploit the value of simulating Big Data problems. The simulation power can be increased by deploying both HPC infrastructures and computing models that enable fast job execution and deliver the highest possible computing performance for the simulation workloads. Synchronous and asynchronous distributed simulation is one of the options that may improve the scalability of a simulator, both in terms of application size and execution speed, enabling large-scale systems to be simulated in real time [36], [37].

Investigations conducted in the field the development of modern simulation technologies have led to the design of general-purpose and problem-oriented software tools for Big Data systems simulations. ScalaTion [38] serves as a modeling and simulation testbed. It provides comprehensive support for discrete event simulation, and offers

an easy-to-use framework for Big Data analytics and many optimization solvers that may be successfully used to solve simulation-optimization problems. A software framework for federated simulation of WSN and mobile ad-hoc networks is presented in [39]. Paper [40] reviews several large-scale military simulations producing Big Data and describes two software frameworks for simulation and Big Data management, based on layered and service-oriented architectures.

GPU-based simulation platforms are mainly dedicated to massive data processing, e.g. high performance neural network simulators [41], [42], simulation of P systems – computational models that perform calculations using a biologically-inspired process [43], large scale volume of data visualization [44], and more.

Some software platforms have been designed to simulate large-scale distributed data centers and computer networks. Jade [45] is a heterogeneous multiprocessor design simulation environment that allows to simulate inter-chip networks, network-on-chips and intra-rack networks utilizing optical and electrical interconnects. Jade supports memory hierarchy, cache coherence and low-power technologies. SimGrid [46] can be used to simulate grids, clouds, HPC or P2P systems, as well as to evaluate heuristics or prototype applications. CloudSim [47], [13] is a Java framework for modeling and simulating cloud computing infrastructures and services. It is one of the most popular open source cloud simulators in the research and academia community. Multi2Sim [48] is a software platform for simulation of CPU and GPU technologies, used to test and validate new hardware designs before they are physically manufactured.

7. Energy-Aware Infrastructure for HPC Computing

7.1. Energy Conservation and HPC Computing

Nowadays, energy efficiency in all sectors, including HPC infrastructure, is a key part of European energy policies for the upcoming decade [49], [50]. Energy awareness is an important aspect of design and management processes involving large-scale data centers. Over the past decade, the amount of energy used by data centers has grown rapidly. This stems primarily from the growing demand for HPC services and computing clouds. Thus, progress in HPC systems depends on energy-efficient data mining and computing technologies.

Indeed, data centers, supporting both HPC applications and cloud services, consume enormous amounts of energy. Over the period of five years (2005–2010), the amount of energy consumed by data centers has increased by 56%, which accounts to 1.5% of the total electrical energy used in 2010. Growing energy consumption increases operating costs of data centers and contributes CO_2 (carbon dioxide) production. According to the analysis of current trends presented and discussed in [51], CO_2 emissions generated by the ICT industry are expected to exceed 2% of the global emission levels [52], [53]. Data centers are very energy intensive. Typical power densities in commodity data centers equal 538–2153 W/m^2 [54], and are even higher in the case of classic HPCs, exceeding 5000 W/m^2 [55]. High energy consumption is attributed primarily to the computing and networking demands and to cooling equipment. The cooling system may use, on average, up to 40% of the energy consumed by a given data center.

Energy efficiency (FLOPS/W) of ICT systems continues to improve. However, the rate of improvement does not match the growing demand for large scale computing. Unless new energy-aware technologies are introduced, both in hardware and software domains, it seems that it will not be possible to meet DARPA's 20-MW exaflop goal (50 GFLOPS/W) by the year 2020 (50 GFLOPS/W) by the year 2020 [3]. Computational power improvements are, in fact, heavily constrained by energy budgets that are necessary for driving computing grids, clouds and data centers. Limiting power consumption and related thermal emissions has become a key problem. Based on technology development-related projections, it has been argued that the continued scaling of the available systems will eventually lead to data centers consuming more than a gigawatt of electrical power (at Exaflop level), a value that violates the economic rationale for the provision of cloud or HPC services. Optimization of energy consumption in data centers must be addressed in response to environment protection and market needs.

As an answer to the momentum that has been created, considerable research efforts devoted to energy-efficient computing and networking technologies have been undertaken both in the research domain and on the ICT market. The rapid increase in energy demand, generated by data centers and network infrastructures, may be mitigated on software and hardware levels. According to [56], the following interrelated approaches and solutions can be distinguished:

- design and development of energy-efficient hardware components (CPUs/GPUs, disks, memory units, network interface cards, etc.),
- development of energy-saving systems for controlling hardware components (servers, routers, etc.),
- introduction of energy-efficient control frameworks for task scheduling and workload balancing.

New computing components, i.e. CPUs/GPUs, disks, memory units, network line cards, have been developed to operate in multiple (performance and idle) modes and at differentiated energy consumption levels (ACPI). Mode switching and high-frequency performance monitoring functions have also been exposed by co-designed Application Program Interfaces (API) [57]. Development of APIs and management tools is essential for optimized use of computing resources. On the other hand, system-wide regulation of power consumption needs to be controlled by a centralized management framework, capable of collecting and processing energy consumption measurements,

and taking, in real time, coordinated actions across the data center infrastructure.

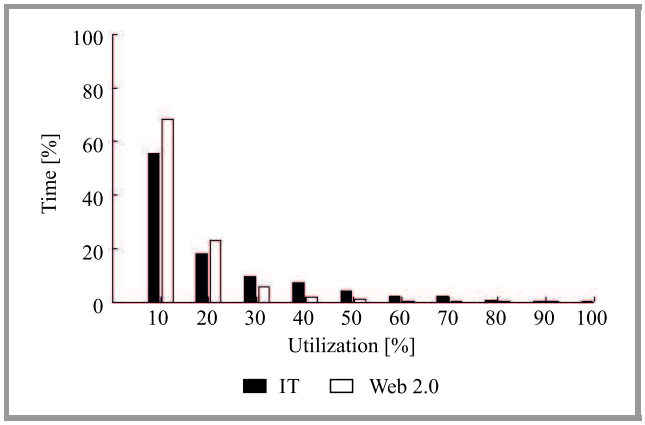


Fig. 1. Server utilization histogram [58].

According to [58], data center server utilization rate rarely approaches 100% (see Fig. 1). Most of the time the servers operate at 10–50% of their full capacity. This results from the requirements of providing sufficient quality of service (QoS) provisioning margins. The over-subscription of computing resources is applied as a sound strategy to eliminate potential breakdowns caused by traffic fluctuations or internal disruptions stemming from hardware or software faults. A fair amount of slack capacity is also required for the purpose of performing maintenance tasks. However, the strategy of resource over-provisioning is clearly a source of energy waste, i.e. the provisioned power supply is less than the sum of the possible peak power demands of all the servers [59]. This highlights the problem of distributing power throughout the entire data center. To keep the total power consumption within the available power range, servers are equipped with power (ACPI-based) budgeting mechanisms capable of limiting their power use. The challenge of energy-efficient data center or cloud control is, therefore, to design a control structure improving the utilization of computing resources and reducing energy usage in accordance with QoS constraints in a highly stochastic environment, capable of providing fast responses to fluctuations in application workloads. To reduce energy consumption, the control system is required to dynamically deactivate and reactivate (by switching between low-power modes) physical computing elements (CPU/GPU, memory, interconnect) to meet the observable resource demand.
Moreover, data intensive computing, and especially Big Data processing, requires advanced methodologies to efficiently allocate resources (CPU, memory and network capacity) to user applications. In general, the idea is to reduce the gap between the capacity provided by data centers and networking environments, and the requirements of users, especially during low workload periods. Nowadays, the main challenge is to arrange and adapt all available methods and techniques to develop energy-efficient and flexible power control systems encompassing all elements of cluster, grid and cloud infrastructures.

7.2. Energy-Saving Technologies

Improvement of energy efficiency of data centers and network infrastructures includes, as it has been already mentioned, optimization of performance of CPU units and network interfaces. For an overview of recent design trends and a detailed discussion on related technical issues concerned with the energy conservation approaches and solutions, see e.g. [56], [60]–[63]. A commonly used direction is to apply novel measurement technologies and utilize assessment of energy consumption characteristics exposing power management functionality through APIs. A detailed study of energy monitoring mechanisms for data centers can be found in [64]. A discussion of power consumption identification problems has been presented in [65], [66].
A survey of memory power management has been presented in [67], [68].
The second approach focuses on control systems and mechanisms adjusting performance of devices to their short-term workload. Two main technologies are distinguished in this context, namely, low power idle and service rate adaptation. They are discussed in [69], [66]. The first one allows a device to switch off for a short period of time whenever there is no workload to be processed, while the other one allows a device to lower its service rate – dynamic voltage frequency scaling (DVFS) mechanisms can be used whenever reduced workloads are observed. The 802.3az Ethernet standard [4] is an example of the implementation of the low power idle technology. The service rate adaptation of Ethernet links has been presented and discussed in [70]. Two mechanisms implementing low power idle and adaptive rate concepts to control the performance of CPUs are delivered by Linux kernel:

- cpuidle governor [71],
- cpufreq governor [61], [56], [72].

In [73], a design of a feedback controller for solving the problem of low utilization of servers in a data-center running I/O-intensive applications is proposed. To adjust CPU frequency, the controller relies on energy-related system-wide feedback rather than on CPU utilization levels. A technique to reduce memory bus and memory bank contention by DVFS-based control of thread execution on each core is presented in [74]. The process model identification technique applied for the purpose of designing CPU frequency control mechanisms has been presented in [61]. A feedback control design methodology that leads to stochastic minimization of performance loss is described in [75]. The optimal design of a controller is formulated as a problem of stochastic minimization of runtime performance error for selected classes of applications. A supervised learning technique is used to predict the performance state of the processor for each incoming job and to reduce the overhead of state observation (see [76]). A hardware-level implementation and performance of power management mechanisms, allowing for independent DVFS of the cores of a multi-core processor that integrates 48 cores and 4 DDR3 memory channels is given in [77].

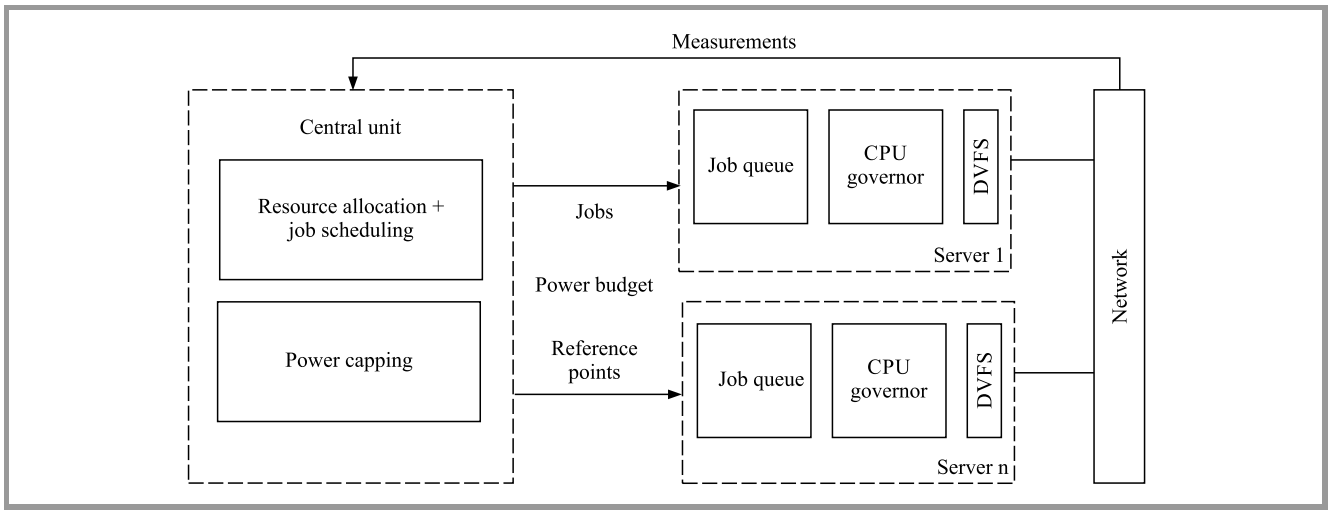


Fig. 2. General control framework architecture.

A DVFS technique that makes use of adaptive update intervals for optimal frequency and voltage scheduling has been proposed in [78]. An optimized control strategy was developed to meet the workload processing deadlines. Papers [61], [79], and [56] address issues concerned with the structure of optimized energy-aware CPU frequency scaling rules. A class of CPU frequency switching rules, exploiting DVFS, is discussed. A benchmarking methodology derived from the RFC2544 specification for identification of models of CPU workload dynamics is proposed and discussed.

Next, it is demonstrated how the proposed models can be applied in the design of customized energy-aware controllers that dynamically adjust CPU frequency to application-specific workload patterns. The numerous experiments referred to above show that customized controllers may outperform standard general-purpose governors of the Linux kernel, both in terms of server performance and power saving capabilities.

The third approach to energy conservation in HPC systems has been focusing on the development of mechanisms for energy management in data centers and networks linking computing nodes. Performance metrics for green data centers have been discussed in [80], [64]. It is believed that considerable energy savings may be achieved in this scenario if only operations of computing and network devices are coordinated and adjusted to workload and traffic patterns observed. In some scenarios, the energy consumed by clusters and network infrastructures may be minimized by switching off or idling servers, routers or line cards [81], [82]. The ability to control the activity of computing nodes is provided by various tools and platforms described in Sections 3 and 4, for instance by Slurm. Moreover, various efforts have been undertaken to develop energy-efficient task scheduling, load balancing and green routing protocols [83]–[85], [72]. However, optimized task scheduling and allocation becomes much more difficult with the classic makespan criterion with energy-efficiency and user-perceived QoS [86], [87] taken into consideration.

Figure 2 shows an overview of a general computer system for an energy-aware data center. The system introduces dynamic power and performance control technologies, based on standby and performance scaling capabilities, improving energy efficiency of computing devices. The idea is to combine the ability of setting the adequate energy states of the computing devices using CPU frequency switching rules, exploiting DVFS implemented along with a control mechanism for optimization of the allocation of resources used by the central unit. The knowledge of the expected computing workload and network traffic matrix leads to considerable and comprehensive optimization problem formulations that have to be solved by the central dispatcher.

A literature survey of green cloud computing is provided in [88]. The paper demonstrates the main achievements in energy-aware computing clouds. The recent developments are summarized, as well as future research directions and open problems related to green cloud computing are presented. Other novel solutions in the field of cluster, grid and cloud energy use optimization are surveyed in [89], [90].

8. Summary and Conclusions

HPC facilities and technologies are required in a rapidly increasing number of data-intensive domains – from life and physical sciences to socioeconomic systems. Thus, the Big Data era offers HPC striking opportunities to expand its range and to strengthen its societal and economic impact. A broad spectrum of activities concerned with the development of HPC infrastructure and middleware for solving Big Data problems have been undertaken. Much of the research has been devoted to the development of methods, algorithms and techniques for energy conservation in data centers, grids, clouds and computer networks. To meet the increasing demand for computing power, a holistic approach to energy-aware design of hardware, middleware and data processing applications is proposed. This paper

presents an overview of middleware, software platforms and simulation platforms for solving Big Data problems. Particular attention is paid to techniques developed to improve energy efficiency of HPC infrastructure. We have taken a look at power-saving algorithms utilizing low power idle and service rate adaptation mechanisms and algorithms for task scheduling and energy-efficient load balancing. However, although numerous energy conservation strategies and systems have been proposed and described in literature, development of scalable, energy-efficient infrastructures for HPC still remains a challenging task.

Acknowledgments

This work was supported by the Polish National Science Centre's grant 2015/17/B/ST6/01885.

References

[1] P. D. Healy, T. Lynn, E. Barrett, and J. P. Morrison, "Single system image: A survey", *J. Parallel Distrib. Comput.*, vol. 90–91, pp. 35–51, 2016 (10.1016/j.jpdc.2016.01.004).

[2] A. Oussous, F. Z. Benjelloun, A. A. Lahcen, and S. Belfkih, "Big data technologies: A survey", *J. of King Saud Univer. – Comp. and Inform. Sci.*, vol. 30, no. 4, pp. 431–448, 2018 (doi: 10.1016/j.jksuci.2017.06.001).

[3] ETP4HPC Strategic Research Agenda achieving HPC leadership in Europe [Online]. Available: www.etp4hpc.eu

[4] IEEE 802.3az-2010 – IEEE standard for information technology [Online]. Available: https://standards.ieee.org/standard/802_3az-2010.html

[5] Mosix home page [Online]. Available: www.mosix.org

[6] OpenSSI home page [Online]. Available: www.openssi.org/cgi-bin/view?page=openssi.html

[7] Kerrighed home page [Online]. Available: www.kerrighed.org

[8] F. Berman, G. Fox, and A. J. G. Hey, Eds., *Grid Computing: Making the Global Infrastructure a Reality*. Wiley, 2003 (ISBN: 978-0-470-85319-1).

[9] Unicore home page [Online]. Available: www.unicore.eu

[10] Globus toolkit home page [Online]. Available: toolkit.globus.org

[11] M. Cannataro, *Handbook of Research on Computational Grid Technologies for Life Sciences, Biomedicine, and Healthcare*. Hershey, PA, USA: IGI Global, 2009 (ISBN-13: 978-1605663746).

[12] R. J. Walters, S. Crouch, and P. Bennett, "Building computational grids using ubiquitous Web technologies", in *Collaborative Networks in the Internet of Services. 13th IFIP WG 5.5 Working Conference on Virtual Enterprises, PRO-VE 2012, Bournemouth, UK, October 1-3, 2012. Proceedings*, L. M. Camarinha-Matos, L. Xu, and H. Afsarmanesh, Eds. *IFIPAICT*, vol. 380, pp. 254–261. Berlin, Heidelberg: Springer, 2012 (doi: 10.1007/978-3-642-32775-9_26).

[13] S. Chaudhary, G. Somani, and R. Buyya, Eds., *Research Advances in Cloud Computing*. Springer, 2017 (doi: 10.1007/978-981-10-5026-8).

[14] N. Sehgal and P. Ch. P. Bhatt, *Cloud Computing. Concepts and Practices*. Springer, 2018 (ISBN: 978-3-319-77839-6).

[15] W.-M. Hwu, Ed., *GPU Computing Gems Emerald Edition*. Morgan Kaufman, 2011 (ISBN: 9780123849885).

[16] A. B. Singh, J. S. Bhat, R. Raju, and R. D'Souza, "Survey on various load balancing techniques in cloud computing", *Adv. in Comput.*, vol. 7, no. 2, pp. 28–34, 2017 (doi: 10.5923/j.ac.20170702.04).

[17] A. Thakur and M. S. Goraya, "A taxonomic survey on load balancing in cloud", *J. of Netw. and Comp. Appl.*, vol. 98, pp. 43–57, 2017 (doi: 10.1016/j.jnca.2017.08.020).

[18] J. Zhang *et al.*, "Load balancing in data center networks: A survey", *IEEE Commun. Surv. Tutor.*, vol. 20, no. 3, pp. 2324–2352, 2018 (doi: 10.1109/COMST.2018.2816042).

[19] G. Staples, "TORQUE resource manager", in *Proc. of the 2006 ACM/IEEE Conf. on Supercomput. SC'06*, Tampa, FL, USA, 2006, Article no. 8 (doi: 10.1145/1188455.1188464).

[20] Portable batch system home page [Online]. Available: www.pbspro.org

[21] Slurm workload manager home page [Online]. Available: slurm.schedmd.com

[22] E. Mohamed and Z. Hong, "Hadoop-mapreduce job scheduling algorithms survey", in *Proc. 2016 7th Int. Conf. on Cloud Comput. and Big Data CCBD 2016*, Macau, China, 2016, pp. 237–242, 2016 (doi: 10.1109/CCBD.2016.054).

[23] T. White, *Hadoop: The Definitive Guide*. O'Reilly Media, 2015 (ISBN: 9781491901687).

[24] Apache Hadoop home page [Online]. Available: https://hadoop.apache.org

[25] Apache Spark home page [Online]. Available: spark.apache.org

[26] Apache Storm home page [Online]. Available: storm.apache.org

[27] Apache Flink home page [Online]. Available: https://flink.apache.org

[28] Rapidminer studio home page [Online]. Available: https://rapidminer.com/

[29] Orange home page [Online]. Available: orange.biolab.si

[30] E. Frank, M. A. Hall, and I. H. Witten, *Data Mining: Practical Machine Learning Tools and Techniques*. Morgan Kaufmann, 2016 (ISBN: 9780123748560).

[31] I. Milne, M. Bayer, L. Cardle, P. Shaw, G. Stephen, F. Wright, and D. Marshall, "Tablet – next generation sequence assembly visualization", *Bioinformatics*, vol. 26, no. 3, pp. 401–403, 2010 (doi: 10.1093/bioinformatics/btp666).

[32] T. Carver, T. D. Bohme, U. Otto, J. Parkhill, and M. Berriman, "Bamview: viewing mapped read alignment data in the context of the reference sequence", *Bioinformatics*, vol. 26, no. 5, pp. 676–673, 2010 (doi: 10.1093/bioinformatics/btq010).

[33] K. Rutherford *et al.*, "Artemis: sequence visualization and annotation", *Bioinformatics*, vol. 16, no. 10, pp. 944–949, 2000 (doi: 10.1093/bioinformatics/16.10.944).

[34] T. Carver, S. R. Harris, M. Berriman, J. Parkhill, and J. A. McQuillan, "Artemis: an integrated platform for visualization and analysis of high-throughput sequence-based experimental data", *Bioinformatics*, vol. 28, no. 4, pp. 464–469, 2012 (doi: 10.1093/bioinformatics/btr703).

[35] D. Desale, Top tools for social network analysis and visualisation, 2018 [Online]. Available: https://www.kdnuggets.com/software/social-network-analysis.html

[36] A. Sikora and E. Niewiadomska-Szynkiewicz, "A federated approach to parallel and distributed simulation of complex systems. *Int. J. of Appl. Mathem. and Comp. Sci.*, vol. 17, no. 1, pp. 99–106, 2007 (doi: 10.2478/v10006-007-0009-0).

[37] A. Inostrosa-Psijas, V. Gil-Costa, M. Marin, and G. Wainer, "Semi-asynchronous approximate parallel DEVS simulation of Web search engines", *Concurr. and Comput.: Pract. and Exper.*, vol. 30, no. 7, 2018 (doi: 10.1002/cpe.4149).

[38] J. A. Miller, M. E. Cotterell, and S. J. Buckley, "Supporting a modeling continuum in scalation: from predictive analytics to simulation modeling", in *Proc. of 2013 Winter Simulations Conference WSC 2013*, Washington, DC, USA, 2013, pp. 1191–1202 (doi: 10.1109/WSC.2013.6721507).

[39] E. Niewiadomska-Szynkiewicz and A. Sikora, "A software tool for federated simulation of Wireless Sensor Networks and mobile ad hoc networks", in *Applied Parallel and Scientific Computing 10th International Conference, PARA 2010, Reykjavík, Iceland, June 6-9, 2010, Revised Selected Papers, Part I*, K. Jónasson, Ed. *LNCS*, vol. 7133, pp. 303–313. Berlin, Heidelberg: Springer, 2012 (doi: 10.1007/978-3-642-28151-8_30).

[40] X. Song, Y. Wu, Y. Ma, Y. Ciu, and G. Gong, "Military simulation big data: Background, state of the art, and challenges", *Mathem. Problems in Engin.*, vol. 2015, Article ID 298356, pp. 1–20, 2015 (doi: 10.1155/2015/298356).

[41] A. K. Fidjeland, E. B. Roesch, M. P. Shanahan, and W. Luk, "Nemo: A platform for neural modelling of spiking neurons using GPUS", in *Proc. 2009 20th IEEE Int. Conf. on Appl.-specif. Syst., Architec. and Process.*, Boston, MA, USA, 2009, pp. 137–144 (doi: 10.1109/ASAP.2009.24).

[42] P. Szynkiewicz, "A novel GPU-enabled simulator for large scale spiking neural networks", *J. of Telecommun. and Inform. Technol.*, no. 2, pp. 34–42, 2016 [Online]. Available: https://www.itl.waw.pl/czasopisma/JTIT/2016/2/34.pdf

[43] M. A. Martinez-del Amor *et al.*, "Accelerated simulation of P systems on the GPU: A survey", in *Bio-Inspired Computing – Theories and Applications. 9th International Conference, BIC-TA 2014, Wuhan, China, October 16-19, 2014. Proceedings*, L. Pan, G. Păun, M. J. Pérez-Jiménez, and T. Song, Eds. *Communications in Computer and Information Science*, vol. 472, pp. 308–312. Springer, 2014 (doi: 10.1007/978-3-662-45049-9_50).

[44] J. Beyer, M. Hadwiger, and H. Pfister, "A survey of GPU-based large-scale volume visualization" in *Proc. of the Eurograph. Conf. on Visual. Eurovis 2014*, Swansea, UK, 2014, pp. 1–19 (doi: 10.2312/eurovisstar.20141175).

[45] R. K. V. Maeda *et al.*, "JADE: a heterogeneous multiprocessor system simulation platform using recorded and statistical application models", in *Proc. of the 1st Int. Worksh. on Adv. Interconn. Solutions and Technol. for Emerg. Comput. Syst. AISTECS'16*, Prague, Czech Republic, 2016 (doi: 10.1145/2857058.2857066).

[46] H. Casanova, A. Giersch, A. Legrand, M. Quinson, and F. Suter, "Versatile, scalable, and accurate simulation of distributed applications and platforms", *J. of Parallel and Distrib. Comput.*, vol. 74, no. 10, pp. 2899–2917, 2014 (doi: 10.1016/j.jpdc.2014.06.008).

[47] R. N. Calheiros, R. Ranjan, A. Beloglazov, C. A. F. De Rose, and R. Buyya, "CloudSim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms", *Software: Pract. and Exper. (SPE)*, vol. 41, no. 1, pp. 23–50, 2011 (doi: 10.1002/spe.995).

[48] Multi2sim workload manager home page [Online]. Available: www.multi2sim.org

[49] Energy Efficiency [Online]. Available: https://ec.europa.eu/energy/en/topics/energy-efficiency

[50] Code of Conduct for Energy Efficiency in Data Centres [Online]. Available: https://ec.europa.eu/jrc/en/energy-efficiency/code-conduct/datacentres

[51] Carbon Abatement Handbook [Online]. Available: https://gesi.org/report/detail/carbon-abatement-handbook

[52] M. Avgerinou, P. Bertoldi, and L. Castellazzi, "Trends in data centre energy consumption under the European code of conduct for data centre energy efficiency", *Energies*, vol. 10, no. 10, pp. 1–18, 2017 (doi: 10.3390/en10101470).

[53] B. Subramaniam, W. Saunders, T. Scogland, and W. Feng, "Trends in energy-efficient computing: A perspective from the Green500", in *2013 Int. Green Comput. Conf. Proc.*, Arlington, VA, USA 2013, pp. 1–8 (doi: 10.1109/IGCC.2013.6604520).

[54] D. L. Beaty, "Internal IT load profile variability", *ASHRAE J.*, vol. 55, no. 2, pp. 72–74, 2013.

[55] J. S. Vetter, *Contemporary High Performance Computing: From Petascale toward Exascale*. Chapman and Hall/CRC Computational Science series, CRC Press, 2013 (ISBN: 9781466568341).

[56] M. P. Karpowicz, P. Arabas, and E. Niewiadomska-Szynkiewicz, "Energy-aware multilevel control system for a network of Linux software routers: Design and implementation", *IEEE Systems J.*, vol. 12, no. 1, pp. 571–582, 2018 (doi: 10.1109/JSYST.2015.2489244).

[57] ETSI ES 203 237 v1.1.1 (2014-03) standard [Online]. Available: www.etsi.org

[58] L. A. Barroso and U. Holzle, "The case for energy-proportional computing", *Computer*, vol. 40, no. 12, pp. 33–37, 2007 (doi: 10.1109/MC.2007.443).

[59] H. Lim, A. Kansal, and J. Liu, "Power budgeting for virtualized data centers", in *Proc. of the 2011 USENIX Ann. Tech. Conf. USENIX ATC'11*, Portland, OR, USA, 2011 [Online]. Available: https://www.microsoft.com/en-us/research/wp-content/uploads/2011/06/VPSUsenix11.pdf

[60] L. Chiaraviglio, M. Mellia, and F. Neri, "Reducing power consumption in backbone networks", in *Proc. of the 2009 IEEE Int. Conf. on Commun. ICC'09*, Piscataway, NJ, USA, 2009, pp. 2298–2303 (doi: 10.1109/ICC.2009.5199404).

[61] M. Karpowicz, "Energy-efficient CPU frequency control for the Linux system", *Concurr. and Comput.: Pract. and Exper.*, vol. 28, no. 2, pp. 420–437, 2016 (doi: 10.1002/cpe.3476).

[62] R. Bolla *et al.*, "Large-scale validation and benchmarking of a network of power-conservative systems using ETSI's green abstraction layer", *Trans. on Emerg. Telecommun. Technol.*, vol. 27, no. 3, pp. 451–468, 2016 (doi: 10.1002/ett.3006).

[63] P. Arabas, "Energy aware data centers and networks: a survey", *J. of Telecommun. and Inform. Technol.*", no. 4, pp. 26–36, 2019 (doi: 10.26636/jtit.2018.129818).

[64] A. Y. Zomaya and J. Ch. Lee, Eds., *Energy-Efficient Distributed Computing Systems*. Wiley, 2012 (ISBN: 978-0-470-90875-4).

[65] J. C. McCullough, Y. Agarwal, J. Chandrashekar, S. Kuppuswamy, A. C. Snoeren, and R. K. Gupta, "Evaluating the effectiveness of model-based power characterization", in in *Proc. of the 2011 USENIX Ann. Tech. Conf. USENIX ATC'11*, Portland, OR, USA, 2011 [Online]. Available: https://www.synergylabs.org/yuvraj/docs/Agarwal_USENIX11_Evaluating-Power-Models.pdf

[66] J.-M. Pierson, *Large-scale Distributed Systems and Energy Efficiency: A Holistic View*. Wiley, 2015 (ISBN: 9781118864630).

[67] S. Mittal, "A survey of architectural techniques for DRAM power management", *Int. J. of High Perform. Syst. Archit.*, vol. 4, no. 2, pp. 110–119, 2012 (doi: 10.1504/IJHPSA.2012.050990).

[68] K. Chalmers *et al.*, Eds., *Communicating Process Architectures 2015 & 2016: WoTUG-37 & WoTUG-38*. Concurrent Systems Engineering Series, vol. 69. IOS Press, 2018 (ISBN 978-1-61499-885-3).

[69] R. Bolla, R. Bruschi, A. Carrega, and F. Davoli, "Green network technologies and the art of trading-off", in *Proc. 2011 IEEE Conf. on Comp. Commun. Worksh. INFOCOM WKSHPS 2011*, Shanghai, China, 2011, pp. 301–306 (doi: 10.1109/INFCOMW.2011.5928827).

[70] V. Pallipadi, S. Li, and A. Belay, "cpuidle: Do nothing, efficiently...", in *Proc. Linux Symposium*, Ottawa, Ontario, Canada, 2007, vol. 2, pp. 119–125.

[71] V. Pallipadi and A. Starikovskiy, "The ondemand governor", in *Proc. Linux Symposium*, Ottawa, Ontario, Canada, 2006, vol. 2, pp. 215–230.

[72] M. Karpowicz, E. Niewiadomska-Szynkiewicz, P. Arabas, and A. Sikora, "Energy and power efficiency in cloud", in *Resource Management for Big Data Platforms: Algorithms, Modelling, and High-Performance Computing Techniques*, F. Pop, J. Kołodziej, and B. Di Martino, Eds. Springer, 2016, pp. 97–127 (doi: 10.1007/978-3-319-44881-7_6).

[73] I. Manousakis, M. Marazakis, and A. Bilas, "FDIO: A feedback driven controller for minimizing energy in I/O-intensive applications", in *Proc. of the 5th USENIX Conf. on Hot Topics in Storage and File Syst. HotStorage'13*, San Jose, CA, USA 2013 [Online]. Available: https://www.usenix.org/system/files/conference/hotstorage13/hotstorage13-manousakis.pdf

[74] M. Kondo, H. Sasaki, and H. Nakamura, "Improving fairness, throughput and energy-efficiency on a chip multiprocessor through DVFs", *SIGARCH Comp. Archit. News*, vol. 35, no. 1, pp. 31–38, 2007 (doi: 10.1145/1241601.1241609).

[75] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges", *J. of Internet Serv. and Appl.*, vol. 1, no. 1, pp. 7–18,

[76] H. Jung and M. Pedram, "Supervised learning based power management for multicore processors", *IEEE Trans. on Comp.-Aided Design of Integr. Circ. and Syst.*, vol. 29, no. 9, pp. 1395–1408, 2010 (doi: 10.1109/TCAD.2010.2059270).

[77] J. Howard *et al.*, "A 48-core IA-32 processor in 45 nm CMOS using on-die message-passing and DVFs for performance and power scaling", *IEEE J. of Solid-State Circ.*, vol. 46, no. 1, pp. 173–183, 2011 (doi: 10.1109/JSSC.2010.2079450).

[78] M. E. Salehi *et al.*, "Dynamic voltage and frequency scheduling for embedded processors considering power/performance tradeoffs", *IEEE Trans. on Very Large Scale Integr. (VLSI) Syst.*, vol. 19, no. 10, pp. 1931–1935, 2011 (doi: 10.1109/TVLSI.2010.2057520).

[79] M. Karpowicz, P. Arabas, and E. Niewiadomska-Szynkiewicz, "Design and implementation of energy-aware application-specific CPU frequency governors for the heterogeneous distributed computing systems", *Future Gener. Comp. Syst.*, vol. 78, pp. 302–315, 2018 (doi: 10.1016/j.future.2016.05.011).

[80] L. Wang and S. U. Khan, "Review of performance metrics for green data centers: a taxonomy study", *J. of Supercomput.*, vol. 63, no. 3, pp. 639–656, 2003 (doi: 10.1007/s11227-011-0704-3). 2010 (doi: 10.1007/s13174-010-0007-6).

[81] I. T. Cotes-Ruiz *et al.*, "Dynamic voltage frequency scaling simulator for real workflows energy-aware management in green cloud computing", *PLoS ONE*, vol. 12, no. 1, 2017 (doi: 10.1371/journal.pone.0169803).

[82] Y. Chiang, Y. Ouyang, and C. Hsu, "An efficient green control algorithm in cloud computing for cost optimization", *IEEE Trans. on Cloud Comput.*, vol. 3, no. 2, pp. 145–155, 2015 (doi: 10.1109/TCC.2014.2350492).

[83] E. Niewiadomska-Szynkiewicz, A. Sikora, P. Arabas, M. Kamola, M. Mincer, and J. Kołodziej, "Dynamic power management in energy-aware computer networks and data intensive systems", *Future Gener. Comp. Syst.*, vol. 37, pp. 284–296, 2014 (doi: 10.1016/j.future.2013.10.002).

[84] J. Kołodziej, S. Khan, L. Wang, and A. Zomaya, "Energy efficient genetic-based schedulers in computational grids", *Concurr. and Comput.: Pract. and Exper.*, vol. 27, no. 4, pp. 809–829, 2015 (doi: 10.1002/cpe.2839).

[85] M. Kamola and P. Arabas, "Shortest path green routing and the importance of traffic matrix knowledge", in *Proc. 2013 24th Tyrrhenian Int. Worksh. on Digit. Commun. – Green ICT TIWDC 2013*, Genoa, Italy, 2013 (doi: 10.1109/TIWDC.2013.6664215).

[86] K. Govindarajan, V. S. Kumar, and T. S. Somasundaram, "A distributed cloud resource management framework for high-performance computing (HPC) applications", in *Proc. 2016 8th Int. Conf. on Adv. Comput. ICoAC 2017*, Chennai, India, 2017, pp. 1–6 (doi: 10.1109/ICoAC.2017.7951735).

[87] E. Niewiadomska-Szynkiewicz and P. Arabas, "Resource management system for HPC computing", in *Automation 2018. Advances in Automation, Robotics and Measurement Techniques*, R. Szewczyk, C. Zieliński, and M. Kaliczyńska, Eds. *Advances in Intelligent Systems and Computing*, vol. 743, pp. 52–61. Springer, 2018 (doi: 10.1007/978-3-319-77179-3_5).

[88] L.-D. Radu, "Green cloud computing: A literature survey", *Symmetry*, vol. 9, no. 12, pp. 1–20, 2017 (doi: 10.3390/sym9120295).

[89] N. Akhter and M. Othman, "Energy aware resource allocation of cloud data center: review and open issues", *Cluster Comput.*, vol. 19, no. 3, pp. 1163–1182, 2016 (doi: 10.1007/s10586-016-0579-4).

[90] T. Mastelic, A. Oleksiak, H. Claussen, I. Brandic, J.-M. Pierson, and A. Vasilakos, "Cloud computing: survey on energy efficiency", *ACM Comput. Surv.*, vol. 47, no. 2, Article no. 33, 2015 (doi: 10.1145/2656204).

Ewa Niewiadomska-Szynkiewicz, D.Sc., (2005), Ph.D., (1995), Professor of Control and Computer Engineering at the Warsaw University of Technology, head of the Complex Systems Group. She is also the Research Director of the Research and Academic Computer Network (NASK). Niewiadomska-Szynkiewicz is the author and co-author of 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 group activities and has overseen the organization of a number of national-level and international conferences.

https://orcid.org/0000-0003-4782-3816
E-mail: ens@ia.pw.edu.pl
Institute of Control and Computation Engineering
Warsaw University of Technology
Nowowiejska 15/19
00-665 Warsaw, Poland

Michał P. Karpowicz, Ph.D. (2010), Assistant Professor of Computer Science with Warsaw University of Technology, Warsaw, and NASK Research Institute. He is the author and co-author of over 50 journal and conference papers and is involved in several national and international research projects. He is also a coauthor of one book. His research interests focus on stochastic control theory, control engineering, game theory, network optimization and cybersecurity.

https://orcid.org/0000-0003-1431-3078
E-mail: m.karpowicz@elka.pw.edu.pl
Institute of Control and Computation Engineering
Warsaw University of Technology
Nowowiejska 15/19
00-665 Warsaw, Poland

Paper

Optimized Energy Aware Resource Allocation Algorithm Using Software Defined Network Technology

Ranya Al-Musawi and Obada Al-Khatib

Faculty of Engineering and Information Sciences, University of Wollongong, Dubai, UAE

https://doi.org/10.26636/jtit.2019.129418

Abstract—The number of data centers (DCs) used for storing and processing data has evolved rapidly in recent years. However, the operations held by DCs may relate to a number of disadvantages, primarily presuming in excessive energy and power consumption due to the poor management standards applied. This may lead to a situation in which many devices within the DC operate at full capacity without any tasks assigned for actual execution. A Software Defined Network (SDN) is a network architecture where the control plane is an independent entity from the data plane, yielding to a higher controllability and flexibility over the network. Through the utilization of SDN architecture, a highly functional energy aware network may be established. In this paper, we propose a heuristic algorithm that monitors the current status of an SDN network (in addition to all ingoing and outgoing traffic), in order to dynamically and efficiently allocate network resources by ensuring that only the necessary network devices are active and by turning the idle ones off. The results show that the proposed algorithm reduces energy consumption of the network compared to existing solutions.

Keywords—computer network management, network servers, software defined networking, virtual machines.

1. Introduction

The data center (DC) is considered to be the heart of any organization or company, since it is responsible for all networking operations and for the handling of all ingoing and outgoing data [1], [2]. The hardware that may be found inside a data center includes servers, switches, routers, storage devices, etc., with all of them interconnected via a backbone network to create a comprehensive solution enabling global information exchange [3], [4]. Thus, the term data center often relates to an enormous area or an entire building that houses networking equipment and infrastructure [3], [5]. The exponential increase in Internet traffic calls for the construction of more DCs to ensure that massive storage capacities and fast processing speeds are guaranteed. However, building more DCs will increase the operational costs due to increased energy consumption [6]–[8].

Extensive research has been conducted to ensure energy efficient operation of DCs [7], [9]–[11], taking into consideration various, energy-intensive DC systems, such as the cooling installation, for instance [5], [6]. Researchers have proposed the use of renewable energy sources to power DCs [6], [12], [13]. However, these sources do not offer sufficient reliability levels due to their dependency on weather conditions (sun or wind) [6], [14]. Others have proposed creating a hybrid system that integrates non-renewable and renewable energy sources to balance energy expenses and pollution level [6], [12]–[14].

Excessive energy consumption of DCs may also be caused by poor allocation of DC resources. For example, many devices in a DC may be actively operating at full capacity without being assigned any tasks [5], [6]. Therefore, optimized resource allocation algorithms are proposed in order to handle traffic efficiently and to turn idle devices off [7], [10], [15], [16]. However, switching off some devices might cause degradation in Quality of Service (QoS) and Quality of Experience (QoE), especially during the peak load periods. Thus, such algorithms must consider maintaining acceptable QoS and the QoE levels [8], [10], [11].

The primary aim of this paper is to highlight and resolve the underlying consequences of the failure to manage DC resources in an efficient manner – a phenomenon that leads to high energy consumption, loss of packets, delays, as well as degraded QoS and QoE levels. The solution focuses on optimizing resource allocation and traffic routing procedures within the DC. The proposed network topology is based on Software Defined Networking (SDN) which separates the control plane from the data plane. By doing so, SDN offers good programming flexibility and enables dynamic adjustment based on the current network state and on the network's incoming traffic.

The network will function in the following manner. The main server will be used as a controller unit to manage and supervise all network operations, while other servers will be used to process the traffic and execute the appropriate actions based upon the commands that they receive from the host controller. The controller is responsible for monitoring and analyzing the network's status, in order to take optimized decisions on managing the data flow and alternating the on/off state of the network devices. Physical servers are consolidated and reconfigured into multiple

virtual machines (VMs). This is done for the purpose of reducing the number of active devices within the network and, therefore, decreasing the amount of energy and power drawn by the DC. Servers are able to host multiple VMs to make full use of their capacity, where each VM represents a process/task requested by a client. The capacity of each VM is adjusted based on the volume of traffic emerging from the client. Likewise, the controller prioritizes incoming traffic by providing more resources to the client with a higher traffic volume. This approach is used to assure that no overload is encountered for the purpose of minimizing the chances of experiencing packet loss or delays, and to maintain satisfactory QoS and QoE levels. To avoid overload, the controller will not route traffic to a network device if its load exceeds a specified threshold value.
The rest of this paper is organized as follows. Section 2 discusses different research papers addressing the proposed issue. Section 3 presents detailed information about the methodology used while developing the proposed energy saving system. Section 4 focuses on the results retrieved from the emulated network, to prove the successful operation of the proposed solution.

2. Literature Review

The cost of electricity used by DCs is expected to approach 8% of the overall cost of electric power used worldwide by 2020 [5], [7]. Therefore, energy saving techniques have evolved, with main advances achieved in the area of chip-, infrastructure- and system-level energy saving technologies [17].
The chip-level energy saving approach highlights a dynamic adjustment of CPU frequency and voltage supply to decrease overall power consumption [17]. The infrastructure-level energy saving technology consists in installing efficient cooling and heat dissipation systems to avoid high temperatures in DCs [17], [18]. Moving forward, the system-level energy saving method consists in dynamically arranging and distributing workload and tasks between the available devices [17]. However, the underlying question is whether those methods would compromise QoS or QoE offered to end users. The answer would be positive in some cases. However, novel solutions have appeared to address the issue of low QoS and QoE [4].

2.1. Minimizing Cost While Going Green

Going green refers to consuming the minimum amount of energy and reducing carbon dioxide emissions. Experts suggest that renewable energy should be used as source of power for data centers [6]. However, renewable energy systems, e.g. those relying on the sun, require clear skies in order to operate efficiently. Wind is another source of renewable energy, yet its prevalence cannot be guaranteed [6]. To use both renewable and non- renewable energy sources increases the cost of data centers. In addition, the issue of overloads caused by massive traffic waves has not been addressed, resulting in low levels of quality experience by end-users, as well as in packet loss, delays and high latency levels.

2.2. Traffic

Statistics reveal that the amounts of power drawn by data centers during peak traffic loads are staggering [19]. However, since traffic intensity fluctuates between day and night, some of the network devices may be turned off to save power during light traffic conditions [20]. On the other hand, if some of the devices are to be turned off, this may cause serious issues and complications affecting data processing. For example, in the case of a traffic strike, the data center will be unable to handle the surge due to some of its devices being inactive [1], [20]. To resolve this matter, the controller should continuously monitor traffic loads and make decisions to switch devices on or off accordingly [10], [20], [21]. This process should be dynamic, in order not to affect ongoing operation of the center [20].

2.3. Routing Algorithms

It is important to maintain an approach that unravels how each task should be transmitted through the ideal path, in the sense of going through the minimum number of devices to get to the final destination that possesses the appropriate capacity to execute the task at hand. Ideal capacity refers to CPU and memory demands that are to be preserved according to the amount of traffic. Such an approach allows to use the resources rapidly to avoid packet loss and delays [4]. To achieve this, a mechanism should be available in the network to enable it to calculate the CPU power and other requirements of a given task, and to prioritize it accordingly [4]. A high priority task is provided with relevant resources and is given priority over other tasks, so that it may be processed faster. In addition, the algorithm that searches for the shortest path to direct traffic to the appropriate server for execution, should make sure that the server is unoccupied [21], [22]. For instance, when a server is overloaded, the SDN controller uses another node to migrate the traffic to an unoccupied server for processing.

2.4. QoS and QoE

QoS and QoE are two important factors when considering end user satisfaction and when rating DC capacity. QoS is determined by diminishing packet loss, delay and high latency levels [8], [23]. When subjected to any of those factors, the service offered to the end user subject to deterioration, due to the distorted or damaged nature of information received [23]. Delay, especially when receiving any type of visual information, may occur easily if the transmission time is not synchronized between the source and the client. High latency occurs mainly when the data center suffers from traffic overload and is unable to process data in an efficient and rapid manner. This causes late responses experienced by the end user. QoE depends on all

three factors listed pertaining to QoS. However, delay and packet loss play a huge role in affecting QoE [8]. Two experiments in [8] were conducted to prove how packet loss and delay negatively affect the quality of a video stream.

2.5. Network Function Virtualization

In network function virtualization (NFV), hardware components are replaced by a software algorithm [8]. Such an approach results in less hardware being used in data centers. Hence, the reduced amount of energy consumed. Cost is also cut down, as DCs are no longer required to purchase expensive hardware, and providing maintenance is no more a consideration [8], [10]. Unlike traditional data centers, NFV technology enables easy control and surveillance of the execution of processes and facilitates the routing of traffic, especially when integrated with SDN technology [8], [10].

2.6. Software Defined Network

Software Defined Network (SDN) offers infrastructure providers (InPs) better control over the network. It enables easy modification of all components present within the network using a software algorithm [8], [10], [24]–[26].

The control plane offers full control over all components within a given network. It is able to monitor traffic, analyze work loads, migrate traffic, turn off idle servers and prioritize tasks in a dynamic manner using SDN technology [4], [27]. Statistical data about traffic load and analyses of the work processes are updated periodically in order to make dynamic decisions and to identify the necessary network changes accordingly [4], [7], [27], [28]. The control plane calculates CPU and bandwidth requirements of the tasks/requests in order to route them to the appropriate server that has the required capacity to process them rapidly. The requirements of various tasks are sorted based on priority. The higher the CPU and bandwidth requirement, the higher the priority granted to the task in order to process it quicker [4], [7], [27], [28]. This helps decrease latency within the data center, and also facilitates dealing with workloads in a dynamic manner. Interaction between the control plane and the data plane and the sending of control signals are based on the standard SDN protocol known as Open Flow, where cooperation with the forwarding plane is established to manage the data as per the main controller's instructions [8], [10], [24].

What distinguishes SDN technology from other existing network architectures is the flexible programmable interface. It may be effortlessly upgraded by updating the algorithm to suit the changing needs of the data center. This is in contrast with existing networks, where numerous changes need to be introduced on hardware and software levels if the data centre acquires an upgrade [7], [8], [10], [24]–[26].

SDN and NFV are two technologies that are highly similar. The main difference lies in the scope of responsibility of each technology. SDN is liable for global control, resource allocation, routing decision making and work flow process within a network, while NFV is an algorithm that executes those processes instead of having a hardware device to perform the task [8], [10], [26].

Implementing both technologies together creates a hybrid data center with flexible control over a network that is programmable [7], [27], [29], and conserves energy.

2.7. CPU Frequency

In [30] extensive research and tests have been conducted to construct a dynamic mechanism that changes the router's CPU frequency on single-core and multi-core processors, based on incoming traffic intensity. With low traffic intensity, CPU frequency is lowered to reduce power consumption. When incoming traffic intensity increases, CPU frequency is increased dynamically to meet the network's demands. This mechanism allows to save power while ensuring efficient traffic handling and management [30].

CPU frequency may be manipulated via hardware- or software-based methods [12]. In hardware, the logical processor's request to achieve a specific frequency rate is stored in a register, and then the processor with the highest required frequency will be chosen. The main drawback of the hardware method is the frequency difference between the processors, where one processor may experience a high load while running on a low CPU frequency, because the decision of other lightly loaded processors to maintain the low CPU frequency has been complied with. The solution is to implement software that utilizes the hardware-provided information about the load and provides the appropriate CPU frequency to each processor independently. Alternatively, it may balance the running load of the applications in a manner that evenly distributes them amongst the processors to provide an equivalent dynamic frequency rate for all processors [12].

3. Methodology

The factors that cause excessive energy consumption may be divided into two categories: internal and external. External causes include poor placement of network components inside the data center, where many active devices are purchased and used to accommodate the incoming traffic and to avoid overload. Internal causes related to inefficient resource allocation inside the network, leading to overloads. This may cause glitches, where some network devices stop responding, yielding to delays, high latencies and packet loss. Here, we focus on internal resource allocation, with its purpose being to evade overload and to ensure maximized use of all network device resources. This ensures that no energy is dissipated without being used. The number of physical active devices inside the DC network is minimized as well.

3.1. Proposed Energy Saving System

The proposed energy saving approach consists in employing an optimized dynamic resource allocation heuristic

algorithm that controls the flow of traffic and manages it in a dynamic manner. Dynamic management refers to creating a system that has the ability to monitor traffic and analyze the workload inside the DC based on information collected and processed, with traffic being then routed to the appropriate destination.

The network system will be designed and created using C++, relying both on SDN and NFV technologies. The system will have the form of a small network for demonstration purposes; however, the heuristic may be incorporated into large scale networks as well. The aim is to attain results that reveal a huge reduction in energy consumption, while accomplishing a network resource utilization rate. The results may be verified by monitoring statistical data available after the programs were executed multiple times, as the process of the users' arrival to the system is random. The success of the algorithm heuristic will also be confirmed through the comparison of the amount of energy consumed in the proposed approach and in other solutions found in traditional DCs. The network has a main server, which will be considered as the controller shown in Fig. 1. The other servers in the network are responsible for executing and processing data based upon the command signals that they receive from the controller. The controller has the privilege of supervising all of the network devices, such as switches, hosts and virtual machines. The network has two switches, each connected to two servers or hosts, where each host has a number of virtual machines (Fig. 1).

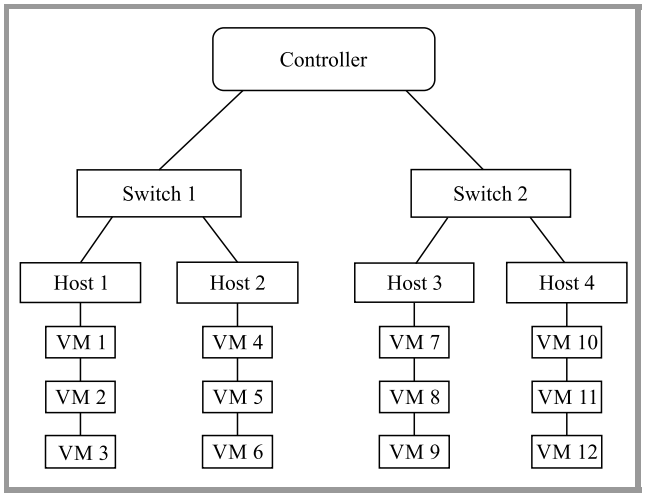


Fig. 1. The proposed network architecture.

The switches are of the Cisco Catalyst 4948 WS-C4948-S variety. When in the idle state, the power drawn by the switch is 176 W, which equals approximately 58.6% of the full load power of 300 W. To avoid unnecessary energy dissipation, idle switches are dynamically turned off when they are not in use. However, when a huge wave of traffic enters the network, they are turned back on. To avoid overload on the switches and to reduce the power consumed by them, a maximum threshold for power and capacity is set at 95% of the original power and capacity, translating to 285 W at 253 MHz. The controller will take into consideration the threshold as the highest permitted capacity and power consumption value which should not be exceeded when calculating and routing traffic towards the designated switch.

The servers (hosts) are based on Intel Xeon Quad Core processors, and operate at 2.27 GHz. The power consumed by idle servers amounts to 100 W a piece, which equals 71.4% of the full load power of 140 W. To avoid energy dissipation, idle servers or servers with no traffic are dynamically turned off. Similarly, when a huge wave of traffic enters the network, those servers are turned back on to accommodate the workload. The maximum power and capacity threshold for the servers is set at 95% of the original power and capacity level, translating to 133 W at 2.16 GHz. This allows to avoid overload and surges in energy and power consumption.

3.2. Algorithm Insights

The controller maintains the maximum threshold values for the switches/servers and ensures that they are not exceeded by continuously monitoring the available capacity and the incoming workload, and by calculating the power of the server/switch k as:

$$P_k = r P_{\max} + (1-r) P_{\max} U_k(t) b_k \ , \tag{1}$$

where $0 \leq r \leq 1$ is the percentage of time in which the server is idle, $P_{\max}$ is the maximum power of the server/switch at full load, $U_k(t)$ denotes the utilization of server/switch k, and b_k is a Boolean number that is zero if server/switch k does not have any assigned tasks and it will be set to one if switch/server k has been assigned a task for execution. The utilization, $U_k(t)$, is calculated as:

$$U_k(t) = \frac{C b_k}{\text{Original capacity}} \ , \tag{2}$$

where C represents the utilized capacity of switch/server k. The number of the incoming clients is preset. However, the amount of traffic that each client conveys is random.

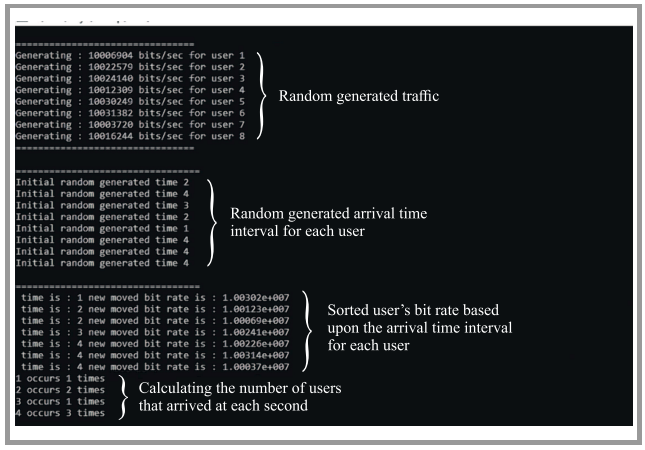


Fig. 2. Users with random bitrates initially enter at random times and are then sorted in an ascending order.

In addition, the arrival time of each client is also random. After completion of the network analysis process, the controller monitors the incoming traffic and sorts the users according to their arrival times, as shown in Fig. 2, and then calculates the remaining available capacity on each switch/server through Eqs. (1) and (2) to assure that the capacity is sufficient for all users arriving at the same time. If the bitrate of all users arriving at the same time is greater than the available capacities of all the switches and servers, the controller will allow the entrance of only some of the users, which the network components can accommodate without getting overloaded for the purpose of processing them, while other users will be terminated/blocked to avoid overload. Users who have been blocked/terminated may establish a new connection request later.

The aim of sorting the users' arrival times in an ascending order is to apply the FIFO management technique, where users who arrive first get served first, which is a crucial step towards assuring that the clients will not experience significant delays. Eliminating the overload problem eradicates session timeouts that lead to delays and loss of packets by the network. Figure 2 is a simple representation that deliberates the processes going on inside the network, assuming that eight random users with random bitrates ranging from 10 to 99 Mbps are generated with random arrival times ranging from 1 to 4 s. The algorithm will primarily sort the users in an ascending order based on their arrival time and will then determine the number of users entering at the same instant. It then starts with the second one and observes how many users arrived at that time (in Fig. 2, it is only one user). It compares the bitrates of those users against the available capacity on the switch. If the switch has enough capacity, the user is allowed to enter and is served. The user processing time will be calculated and when the traffic is processed inside the switch, the users exit and are be transported to the appropriate host destination, down to a virtual machine inside the host, where appropriate capacity is provided based upon the user's demands.

3.3. Power and Energy Saving

To reduce the number of active devices and energy consumption, servers are consolidated into VMs. This ensures maximum utilization, while keeping the rest of the servers/hosts off. When traffic comes from multiple clients, the controller will observe which client has the most vol-

Stage 1	1. Incoming traffic gets sorted in an ascending order based upon the user's arrival time. 2. The heuristic examines the number of user entering at each instance of arrival time.
Stage 2	1. The heuristic compares the capacity of the network components against the incoming traffic at each arrival time instance. 2. Users having a capacity that exceeds the network capacity threshold or may cause an overload, are terminated/blocked immediately.
Stage 3	1. The amount of process time for each user on the switch/host is calculated preliminarily. 2. User's traffic (data rate) is guided to one of the switches based upon previous stages analysis. 3. Available capacity left after the users enter the switch is displayed. 4. Idle switches/hosts are turned off.
Stage 4	1. Traffic exits the switch and is forwarded to one of the hosts based upon the available capacity. 2. Traffic is assigned to a virtual machine inside the host and is offered with the appropriate CPU capacity to accommodate the workload. 3. Available capacity left after the users enter the host is displayed. 4. Idle hosts are turned off.
Stage 5	1. Traffic exits the hosts. 2. The number of terminated/blocked (if any) users is displayed. 3. The amount of power consumed at each time interval on each network component is displayed

Fig. 3. Network stages of the proposed algorithm.

ume of traffic to move the data to the appropriate VM, granting it a higher CPU rate and providing priority over others to assure that no packet loss or delays occur. If the network faces a low traffic wave, it will direct the traffic through one of the switches while keeping the other switch off, and the same applies to the hosts. Subsequently, if the network components are finished with processing traffic and become idle, the controller will dynamically turn them off to decrease energy and power consumption. However, they will get turned back on if a huge amount of traffic enters the network. A feasible representation of the individual stages of the algorithm applied to incoming users is shown in Fig. 3.

3.4. Testing Procedure

The assessment of the proposed heuristic algorithm is an essential measure for revealing the reliability and the success of the new algorithm. Results may be observed as the program is executed, presenting a clear map of all processes going on inside the network at each stage. Starting from the moment the users enter the network at each time instant, until the time they exit. Statistics are also provided throughout the execution process to reveal how much capacity was used by each user on each switch and host. Furthermore, the algorithm displays the capacity left after each user has entered and exited the network device concerned. Likewise, at the end, the algorithm indicates the number of users that were terminated for the purpose of avoiding overloading the network. It also previews how much power has been consumed in each second and on each switch/host, as the users enter at different times.

4. Results and Findings

In this section, we disclose the results and findings based on the examination of the algorithm concerned. The emulated proposal employs random inputs, such as traffic and arrival times for each of the users. To validate functionality of the heuristic algorithm, a mapping representation may be drawn up showing user's progress through all routing stages inside the network, as shown in Fig. 3.

4.1. Resource Allocation and Mapping

In stage one, when the incoming traffic is processed and enters stages 2–4, the outcome may be clearly seen in Fig. 4. The program output is based on a sample of 108 different users who enter at random times ranging from 1 to 4 s. The observation that can be made is concerned with how the users are served the moment they enter the network and how the switches are turned on and off based upon the number of users and the amount of their traffic.

Primarily, the number of users and their traffic amount entering at each time instant are noted and then the available capacity on the network devices is computed. As a result, each user's traffic is routed to the device which has sufficient capacity to serve the user and the total time required to serve the user is calculated. For example, as depicted in Fig. 4, the users entering in second one are served by a switch and then they are directed out of the switch before the new users arrive at second two. The algorithm goes on until all users have been served and have exited the switch towards the hosts.

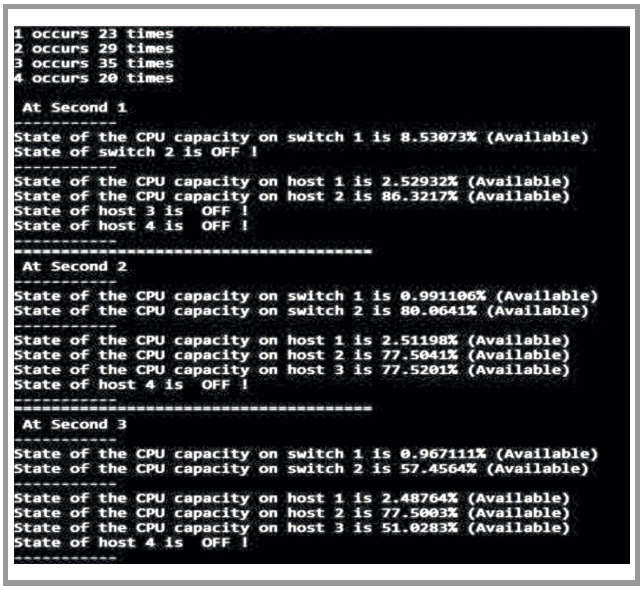


Fig. 4. Traffic handling and routing inside the network.

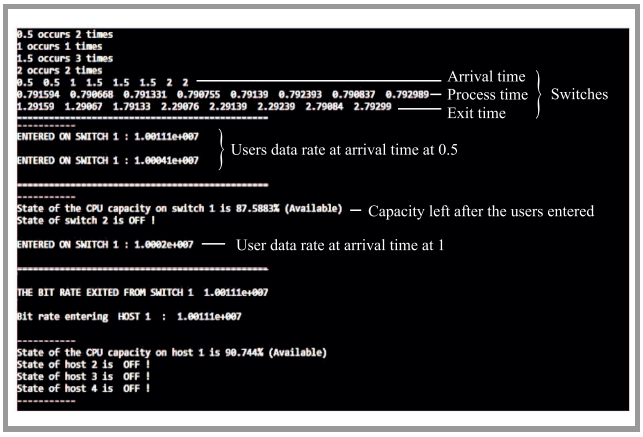


Fig. 5. Illustration of traffic with overlapping intervals between exit time and new arrival time are guided.

Another example is concerned with a situation in which the exit time of the current user(s) overlaps with the arrival time of new incoming user(s), as illustrated in Fig. 5. The controller took the users arriving at 0.5 s and guided them to switch one, after it has realized that their exit time is beyond second one, which is the arrival time of the next incoming user(s). The controller granted access to switch one to the user(s) arriving at second one and it has also turned off switch two because it state is idle. Notice that the controller keeps track of the available capacity of each switch on a continuous basis, after each arrival or exit of

a new user. another observation may be made in Fig. 5, showing that as one user exits switch one at 0.5 s, it immediately enters host one, while keeping idle hosts 2–4 off. After the user has entered host one, it will be assigned to a virtual machine, where appropriate CPU capacity will be dynamically provided to accommodate the workload and to process it efficiently. This process continues until the traffic of all users has been processed and guided out of the network.

Fig. 6. Blockage rate.

The number of blocked users who were not served inside the network due to network capacity constraints and the threshold set to avoid overload, are displayed at the end, as shown in Fig. 6. QoS is maintained through the illustration on how the users are served. As shown in Fig. 5, all users who have been served by the network have not experienced any delays. That is, they have exited the network as per the expected exit time calculated initially when they entered the network. For the considered simulation parameters, the network has also not experienced any overload, and the blockage constraint in the proposed algorithm is incorporated for the purpose of avoiding bottlenecks, overload and delays. As these issues are evaded, it can be confirmed that the proposed algorithm does not compromise QoS.

4.2. Confirming Energy and Power Conservation

A test was conducted on the designed network with 204 random users and random incoming bit rates. Figure 7 unveils energy consumption, in J/s, after the users have passed through all network stages and have exited the network. Since switch two was turned off (energy is zero) throughout the entire test, due to the fact that no incoming traffic has entered it as switch one was able to accommodate all incoming traffic, it may be clearly noted how the system is able to save energy in an efficient manner thanks to the proposed algorithm.

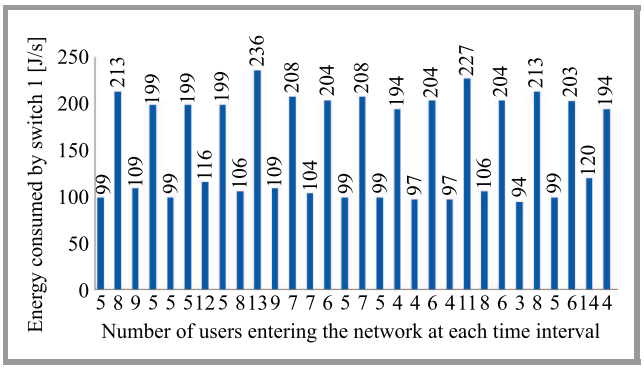


Fig. 7. Amount of energy consumed by the users entering the network after being sorted.

4.3. Comparison with Traditional Data Center Networks

Traditional data centers, such as [8], are mainly concerned with processing data in an efficient manner to guarantee good QoS and QoE levels experienced by the end user, while neglecting the extensive amounts of power and energy being dissipated. Another proposal that suggests a dynamic resource allocation approach but neglects QoS and QoE rates is [7]. However, the algorithm proposed in this paper aims to assure that both problems arising in [7] and [8] are resolved at once. QoS and QoE are dependent upon packet loss rate, delays and high latencies. The proposed algorithm proves that quality may be maintained (unlike in [7]) through avoiding overload and dynamically allocating traffic while granting it with the resources required to accommodate the workload. The problem with [8] is that the network devices remain active at all times. To prove the distinct nature of the proposed algorithm, the following values retrieved from Fig. 8 are compared against a sys-

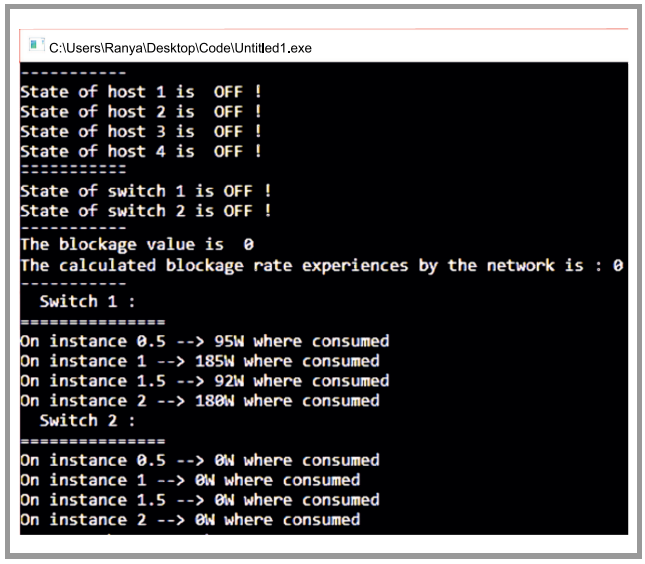


Fig. 8. Statistics concerning the power consumed at each instance after all clients have been served and directed out of the network switches (network components are turned back off).

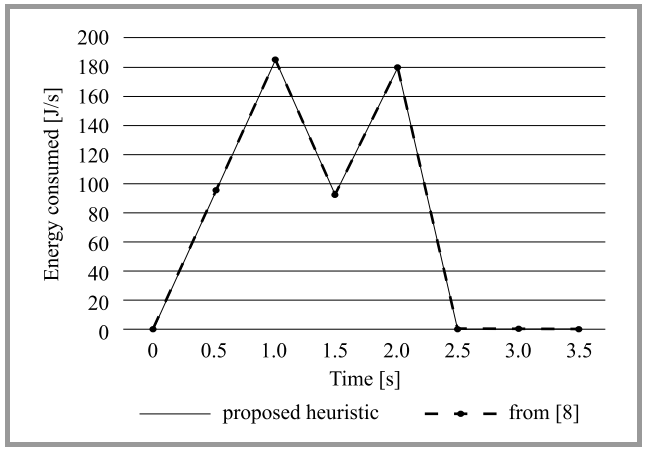


Fig. 9. Energy consumed by switch one by the proposed algorithm and the algorithm described in [8].

tem that relies on principles similar to those of [8], meaning that it employs an optimized resource allocation plan to avoid overload but fails to conserve energy. Since the switches are turned off when they are not in use, switch two dissipates zero watts, while switch one handles all of the incoming traffic. A simple graph representation may be seen in Figs. 9 and 10, where a comparison between [8] and the proposed algorithm has been shown.

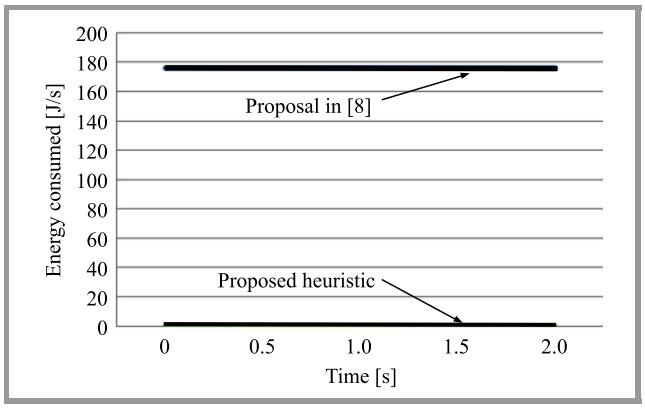


Fig. 10. Difference in energy consumption between the proposed algorithm and the solution proposed in [8], for switch two.

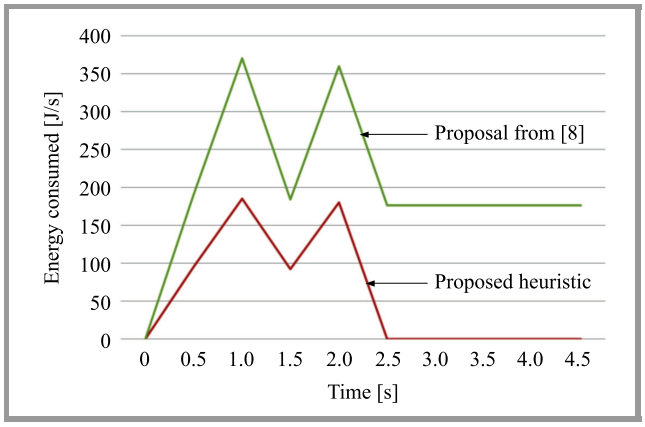


Fig. 11. Total energy consumed by the proposed algorithm and the algorithm described in [8].

Assuming that both solutions proposed in this paper and in [8] are tested on the same network devices chosen for simulation purposes, the following results may be observed. Both proposals are concerned with avoiding overload and routing traffic within the network in a studied manner. As shown in Fig. 9, energy consumption is hypothetically similar in both scenarios. However, in Fig. 10, with observations focused on switch 2, [8] consumes more power, as illustrated in Fig. 11, since it is always on.

5. Conclusion and Future Work

The proposed heuristic algorithm has been proved to attain the expected outcomes discussed in the earlier sections, with energy consumption confirmed to decrease drastically and with quality maintained due to the fact that no packet loss or delays are experienced within the network. Future work may be concerned with incorporation of a mechanism that is able to save the data and reallocate them in the case in which a physical host from the data center suffers a failure.

References

[1] C. Mastroianni, M. Meo, and G. Papuzzo, "Analysis of a self-organizing algorithm for energy saving in data centers", in *Proc. 2013 IEEE Int. Symp. on Parallel Distrib. Process., Worksh. and Phd Forum*, Cambridge, MA, USA, 2013, pp. 907–914 (doi: 10.1109/IPDPSW.2013.184).

[2] D. A. Alboaneen, B. Pranggono, and H. Tianfield, "Energy-aware virtual machine consolidation for cloud data centers", in *Proc. 2014 IEEE/ACM 7th Int. Conf. on Util. and Cloud Comput.*, London, UK., 2014, pp. 1010–1015 (doi: 10.1109/UCC.2014.166).

[3] I. Widjaja, A. Walid, Y. Luo, Y. Xu, and H. J. Chao, "Small versus large: Switch sizing in topology design of energy-efficient data centers", in *Proc. 2013 IEEE/ACM 21st Int. Symp. on Qual. of Serv. IWQoS 2013*, Montreal, QC, Canada, 2013, pp. 51–56 (doi: 10.1109/IWQoS.2013.6550264).

[4] J. Perel *et al.*, "All-optical packet/circuit switching-based data center network for enhanced scalability, latency, and throughput", *IEEE Network*, vol. 27, no. 6, pp. 14–22, 2013 (doi: 10.1109/MNET.2013.6678922).

[5] M. Seymour, "Is energy efficiency enough? Filling the engineering gap in data center design and operation", in *Proc. 15th IEEE Intersoc. Conf. on Thermal and Thermomech. Phenom. in Electron. Syst. ITherm 2016*, Las Vegas, NV, USA, 2016, pp. 702–709 (doi: 10.1109/ITHERM.2016.7517616).

[6] A. Amokrane, M. F. Zhani, R. Langar, R. Boutaba, and G. Pujolle, "Greenhead: Virtual data center embedding across distributed infrastructures", *IEEE Trans. on Cloud Comput.*, vol. 1, no. 1, pp. 36–49, 2013 (doi: 10.1109/TCC.2013.5).

[7] B. Yu, Y. Han, X. Wen, X. Chen, and Z. Xu, "An energy-aware algorithm for optimizing resource allocation in software defined network", in *Proc. IEEE Global Commun. Conf. GLOBECOM 2016*, Washington, DC, USA, 2016, pp. 1–7 (doi: 10.1109/GLOCOM.2016.7841589).

[8] E. Grigoriou, A. A. Barakabitze, L. Atzori, L. Sun, and V. Pilloni, "An SDN-approach for QoE management of multimedia services using resource allocation", in *Proc. IEEE Int. Conf. on Commun. ICC 2017*, Paris, France, 2017, pp. 1–7 (doi:10.1109/ICC.2017.7997261).

[9] B. Pavithra and R. Ranjana, "Energy efficient resource provisioning with dynamic VM placement using energy aware load balancer in cloud", in *Proc. Int. Conf. on Inform. Commun. and Embedded Syst. ICICES 2016*, Chennai, India, 2016, pp. 1–6 (doi: 10.1109/ICICES.2016.7518919).

[10] S. Subbiah and V. Perumal, "Energy-aware network resource allocation in SDN", in *Proc. Int. Conf. on Wirel. Commun., Sig. Process. and Netw. WiSPNET 2016*, Chennai, India, 2016, pp. 2071–2075 (doi: 10.1109/WiSPNET.2016.7566506).

[11] X. Wen, Y. Han, H. Yuan, X. Zhou, and Z. Xu, "An efficient resource embedding algorithm in software defined virtualized data center", in *Proc. IEEE Global Commun. Conf. GLOBECOM 2015*, San Diego, CA, USA, 2015, pp. 1–7 (doi: 10.1109/GLOCOM.2015.7417556).

[12] Q. Zhang, Q. Zhu, M. F. Zhani, and R. Boutaba, "Dynamic service placement in geographically distributed clouds", in *Proc. IEEE 32nd Int. Conf. on Distrib. Comput. Syst.*, Macau, China, 2012, pp. 526–535 (doi: 10.1109/(ICDCS.2012.74).

[13] S. Padma, K. Vijayalakshmi, and G. Sangameshwaran, "Power generation using hybrid renewable energy resources for domestic applications", in *Proc. Int. Conf. on Wirel. Commun., Sig. Process. and Netw. WiSPNET 2016*, Chennai, India, 2016, pp. 1993–1998 (doi: 10.1109/WiSPNET.2016.7566491).

[14] A. Qureshi, R. Weber, H. Balakrishnan, J. Guttag, and B. Maggs, "Cutting the electric bill for internet-scale systems", *SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 4, pp. 123–134, 2009 (doi: 10.1145/1594977.1592584).

[15] M. Rahnamay-Naeini, S. S. Baidya, E. Siavashi, and N. Ghani, "A traffic and resource-aware energy-saving mechanism in software defined networks", in *Proc. Int. Conf. on Comput., Netw. and Commun. ICNC 2016*, Kauai, HI, USA, 2016, pp. 1–5 (doi: 10.1109/ICCNC.2016.7440553).

[16] T. Yang, Y. C. Lee, and A. Y. Zomaya, "Energy-efficient data center networks planning with virtual machine placement and traffic configuration", in *Proc. IEEE 6th Int. Conf. on Cloud Comput. Technol. and Sci.*, Singapore, 2014, pp. 284–291 (doi: 10.1109/CloudCom.2014.135).

[17] K. Zhang, T. Wu, S. Chen, L. Cai, and C. Peng, "A new energy efficient VM scheduling algorithm for cloud computing based on dynamic programming", in *Proc. IEEE 4th Int. Conf. on Cyber Secur. and Cloud Comput. CSCloud 2017*, New York, NY, USA, 2017, pp. 249–254 (doi: 10.1109/CSCloud.2017.46).

[18] M. K. Patterson, "The effect of data center temperature on energy efficiency", in *Proc. 11th Intersoc. Conf. on Thermal and Thermomech. Phenom. in Electron. Syst.*, Orlando, FL, USA, 2008, pp. 1167–1174 (doi: 10.1109/ITHERM.2008.4544393).

[19] N. T. Hieu, M. D. Francesco, and A. Yl-Jski, "Virtual machine consolidation with usage prediction for energy-efficient cloud data centers", in *Proc. IEEE 8th Int. Conf. on Cloud Comput.*, New York, NY, USA, 2015, pp. 750–757 (doi: 10.1109/CLOUD.2015.104).

[20] A. Markiewicz, P. N. Tran, and A. Timm-Giel, "Energy consumption optimization for software defined networks considering dynamic traffic", in *Proc. IEEE 3rd Int. Conf. on Cloud Netw. CloudNet 2014*, Luxembourg, 2014, pp. 155–160 (doi: 10.1109/CloudNet.2014.6968985).

[21] D. Henni, Y. Hadjaj-Aoul, and A. Ghomari, "Probe-SDN: A smart monitoring framework for SDN-based networks", in *Proc. Global Inform. Infrastruc. and Netw. Symp. GIIS 2016*, Porto, Portugal, 2016, pp. 1–6 (doi: 10.1109/GIIS.2016.7814940).

[22] C. Zhang, X. Huang, G. Ma, and X. Han, "A dynamic scheduling algorithm for bandwidth reservation requests in software-defined networks", in *Proc. 10th Int. Conf. on Informa., Commun. and Sig. Process. ICICS 2015*, Singapore, 2015, pp. 1–5 (doi: 10.1109/ICICS.2015.7459856).

[23] K. Liu, Y. Cao, Y. Liu, G. Xie, and C. Wu, "A novel min-cost QoS routing algorithm for SDN-based wireless mesh network", in *Proc. 2nd IEEE Int. Conf. on Comp. and Commun. ICCC 2016*, Chengdu, China, 2016, pp. 1998–2003 (doi: 10.1109/CompComm.2016.7925051).

[24] S. Tomovic, I. Radusinovic, and N. Prasad, "Performance comparison of QoS routing algorithms applicable to large-scale SDN networks", in *Proc. IEEE EUROCON 2015 – Int. Conf. on Comp. as a Tool EUROCON 2015*, Salamanca, Spain, 2015, pp. 1–6 (doi: 10.1109/EUROCON.2015.7313698).

[25] Y. Guo, Z. Wang, X. Yin, X. Shi, and J. Wu, "Optimize routing in hybrid SDN network with changing traffic", in *Proc. 26th Int. Conf. on Comp. Commun. and Netw. ICCCN 2017*, Vancouver, BC, Canada, 2017, pp. 1–8 (doi: 10.1109/ICCCN.2017.8038397).

[26] Y. Han, J. Li, J.-Y. Chung, J.-H. Yoo, and J. W. Hong, "SAVE: Energy-aware virtual data center embedding and traffic engineering using SDN", in *Proc. of the 2015 1st IEEE Conf. on Netw. Softwariz. NetSoft 2015*, London, UK, 2015, pp. 1–9 (doi: 10.1109/NETSOFT.2015.7116142).

[27] A. Ishimori, F. Farias, E. Cerqueira, and A. Abelm, "Control of multiple packet schedulers for improving QoS on OpenFlow/SDN networking", in *Proc. 2nd Eur. Worksh. on Software Defined Netw.*, Berlin, Germany, 2013, pp. 81–86 (doi: 10.1109/EWSDN.2013.20).

[28] J. Pang, G. Xu, and X. Fu, "SDN-based data center networking with collaboration of multipath TCP and segment routing", *IEEE Access*, vol. 5, pp. 9764–9773, 2017 (doi: 10.1109/ACCESS.2017.2700867).

[29] A. Bentaleb, A. C. Begen, R. Zimmermann, and S. Harous, "SDNHAS: An SDN-enabled architecture to optimize QoE in HTTP adaptive streaming", *IEEE Trans. on Multimed.*, vol. 19, no. 10, pp. 2136–2151, 2017 (doi: 10.1109/TMM.2017.2733344).

[30] P. Desmond, "5 contributors to data center energy inefficiency", 2011 [Online]. Available: https://blog.schneider-electric.com/datacenter/2011/09/06/5-contributors-to-data-center-energy-inefficiency/

Ranya Al-Musawi is currently a student at the University of Wollongong (Australia), perusing her final year to receive a B.Sc. degree in Computer Engineering. She was a representative of engineering students at the representative council for the year of 2017 at Wollongong. Her main interests are in automation, embedded systems and telecommunication networks.
E-mail: rmmam836@uowmail.edu.au
Faculty of Engineering and Information Sciences
University of Wollongong Dubai
Dubai Knowledge Park
P.O. Box 20183, Dubai, UAE

Obada Al-Khatib received his B.Sc. degree in Electrical Engineering (Honors) from Qatar University, Doha, Qatar, in 2006, M.Eng. degree in Communication and Computer Technology (Honors) from the National University of Malaysia, Bangi, Malaysia, in 2010, and Ph.D. degree in electrical and information engineering from the University of Sydney, Sydney, Australia, in 2015. From 2006 to 2009, he was an Electrical Engineer with the Consolidated Contractors International Company, Qatar. In 2015, he joined the Centre for IoT and Telecommunications at the University of Sydney, as a Research Associate. Since 2016, he has been with the Faculty of Engineering and Information Sciences, University of Wollongong in Dubai, UAE, as an Assistant Professor. His current research interests are in the areas of smart grid communication, wireless resource allocation and management, cooperative communications and wireless network virtualization.
https://orcid.org/0000-0001-9473-2365
E-mail: obadaalkhatib@uowdubai.ac.ae
Faculty of Engineering and Information Sciences
University of Wollongong Dubai
Dubai Knowledge Park
P.O. Box 20183, Dubai, UAE

Paper

Multimedia Mathematical Communication in a Diverse Group of Students

Jolanta Brzostek-Pawłowska

Research and Academic Computer Network (NASK), Warsaw, Poland

https://doi.org/10.26636/jtit.2019.132819

Abstract—The article tackles the problem of improving mathematical communication in a group of students with different visual impairment levels, under the guidance of a group leader or a teacher. Visually impaired persons face a problem while learning mathematics. The said problem results from the specific nature in which mathematical content (formulas, function graphs, geometrical figures and projections of solids) is recorded and presented. The effectiveness of learning mathematics is boosted when students work in a group moderated by a leader. This requires them to share documents, with the leader being able to keep track of the individual work of each participant, and with the group discussing specific solutions. In order for a visually impaired student to be able to participate in and contribute to the work of the group, either remotely or locally, all participants must use universal IT tools that support visually impaired students without complicating the work of others. This paper presents interactive multimedia solutions developed under two research projects carried out by the author. The said solutions support communication in mathematics. Results of qualitative surveys on new solutions are presented, confirming their usefulness and the measurable impact they exert on the efficiency of the group's work concerning mathematical problems.

Keywords—efficiency of communication in learning mathematics, mathematical formula notations, semantic readout of formulas.

1. Introduction

The problem of communication-related capabilities in mathematics that are necessary for transferring, acquiring, consolidating and using mathematical knowledge in everyday life, was tested on a group of secondary school students and is described in paper [1]. Low percentage results were obtained with regard to the following: (i) ability to described a situation, an idea or a mathematical correlation using algebraic expressions, graphics, images (35%), (ii) use of mathematical language in everyday life (35%), (iii) use of images or diagrams to express a mathematical concept (53,3%). The results confirmed existence of the low level of communication skills in the field of mathematics. The surveyed consisted of students without sight impairments. Visually impaired students (particularly blind ones) encounter even more serious problems concerning mathematical communication. This is mainly due to such spatial elements as formulas, function graphs, diagrams and geometric objects.

As shown by research presented in [2], one of the effective forms of teaching and learning mathematics is by working on a project, a problem or a mathematical task in a group of several people. The conclusions from these studies indicate a positive effect of, inter alia, the factor of mutual assistance of the group members, and of individualized assistance. Similar, individualized assistance is provided to a student in a two-person teacher-student group, e.g. during compensatory, additional classes or during remote, online consultations. A problem appears when a group learning mathematics, either on its own or with the help of a teacher, comprises visually impaired students. Such groups are, by definition, the norm in inclusive education. The problem of the students' poor mathematical communication skills overlaps with the problem of the efficiency of communication with a visually impaired member of the group who is often using a different user interface, e.g. Braille technology and other mathematical tools, such as equation editors. For a diverse group to be able to cooperate efficiently and for the student's self-help factor or the teacher's assistance to work, the group must be equipped with IT tools that facilitate communication concerning mathematical problems. The tools that may be helpful in creating, presenting and exploring mathematical content, as well as in communicating by exchanging mathematical documents, include chats and remote voice conversations. A set of such software tools supporting the teacher or the group leader, as well as visually impaired and blind students, known under the name of PlatMat OPTY, has been developed under two research projects.

The paper presents selected solutions that have been developed and implemented in the tools comprising the PlatMat OPTY platform, used to enhance efficient communication concerning mathematical content containing formulas, within a group of students that is diverse in terms of the visual capabilities of its members. The users may create and share their math-related texts and audio content relying on audio-visual and tactile senses. The users may create and control a new way of communication using this system, in addition to conducting traditional, single medium-based conversations. In order to overcome interaction lim-

itations, we have proposed, in PlatMat OPTY, the use of integrated senses. Solutions enabling quick recognition of mathematical graphics have also been developed[1], as have been tools allowing to perform arithmetic calculations in a written form [3]. They are intended for students with visual impairments but are not discussed in this paper.

2. Accessibility Problems in Mathematical Communication

The problems whose solutions have been sought through research and development activities include the following:

1. compatibility of various interfaces used for editing and presenting mathematical formulas, enabling a group made up of sighted and visually impaired people to cooperate while working on mathematical issues;
2. creating a single version of electronic mathematical documents – accessible both to sighted persons and to those with visual impairments, simplifying the process and shortening the time devoted by the author to creating e-documents, and avoiding stigmatization of visually impaired persons cooperating within the same group with sighted persons;
3. sharing information and e-mathematical documents in a group that is diversified in terms of visual acuity, working remotely via the Internet or locally, with or without access to Wi-Fi networks.

A special case of a group that is diversified in terms of visual acuity of the participants, is one made of students and a teacher of an integration class in a public school implementing the idea of inclusive education. Another case is a two-person group: a sighted teacher and a visually impaired pupil, working locally during compensatory classes, or remotely, via the Internet.

2.1. Various Mathematical Notations and User Interfaces

The first problem concerns various notations (languages) used for writing formulas, and various user interfaces applied to save and read them, by means of which sighted, blind and low vision persons create and present formulas. Sighted people use spatial and graphical visualization of formulas, and usually write formulas with the help of popular formula editors available in MS Word, Open Office, Libre Office, offering spatial formula structures to be filled by the user, for example: $\frac{\sqrt{\square^{\square}}}{\square}$, $\sum_{\square}^{\square}\square^{\square}$.
While preparing scientific publications with a large number of formulas, academics use the LaTeX system [4]. For writing and reading formulas, blind and low-vision persons with serious visual disability can use the linear Braille mathematical notation, based on the 7-bit, 128 character ASCII standard available via a QWERTY keyboard, for example AsciiMath (AMS) notation [5], Wiskunde Notatie Dedicon (WND) [6], or an extended notation using multi-byte characters, such as Lambda notation [7], as well as UnicodeMath notation developed in PlatMat, based on AsciiMath. The difference between the latter and the AsciiMath notation is that the mathematical symbols not accessible from a QWERTY keyboard, and are entered using a keyboard shortcut or a mouse click on the symbol displayed in the formula editor. These symbols are saved using Unicode, not ASCII. In Poland, non-digitized, tactile convex printing Braille Mathematical Notation (BNM) is used [8]. In other countries, due to the lack of standardization, other mathematical Braille notations are used. It is worth mentioning, however, that such an approach hinders the interoperability of documents and prevents international cooperation of visually impaired people in the field of mathematics. In Poland, linear mathematical notations, other than BNM, are not widely used. The educational system for blind students is based on Braille notation and technology. The problem with linear notations, both of the Braille and ASCII variety, lies in the fact that the formulas in these notations are longer and require more characters than in spatially visualized forms.
An exemplary expression of a fraction with a root in the numerator, presented in a spatial form, looks as follows:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} .$$

While the same expression presented in selected linear notations looks as follows:

BNM:	_x=;-b!-CbO;"-#d_ac 8 #b_a<	(29 characters),
Lambda:	x=//-b+-√b^2-4ac/2a\\	(19 characters),
LaTex:	$$x=\frac{-b+-\sqrt{b^{2}-4ac}}{2a}$$	(37 characters),
AsciiMath:	x=(-b+-sqrt(b^2-4ac))/(2a)	(26 characters),
WND:	x=(-b+-sqrt(b^2-4ac))/(2a)	(26 characters),
UnicodeMath:	x=(-b+-√(b^2-4ac))/(2a)	(23 characters).

It is worth noting that in some linear notations, for example in Lambda, operating systems include fonts developed specifically for marking the structure of the formula. These fonts are accessible via a keyboard shortcut or a mouse click in the formula editor of a given notation. In Lambda, these characters are marked in red, indicating the beginning and the end of the fraction and the end of the numerator. As it may be noticed in the examples provided, the formulas are lengthy, both in Braille and in other line notations. The advantage that non-Braille linear notations (hereinafter: linear QWERTY notations) have over Braille, especially when the form of the formula is not, for printing purposes, converted to a mathematical Braille notation, consists in the possibility of editing and reading formulas using commonly available computer hardware with a QWERTY keyboard.
Formulas in QWERTY linear notations, unless otherwise programmed, are read character by character, using assistive software, such as screen readers, e.g. NVDA or Jaws

[1] Paper under preparation.

installed at the operating system layer. This method of reading is not friendly for a blind user and makes it difficult for them to recognize the structure of the formula and its transformation. However, it is often used by persons with seriously impaired vision, who find structural editors, for example MS Word, too difficult to use. Nevertheless, in the Netherlands, at schools teaching blind students, the WND linear notation (an example of a WND record is shown above), similar to the AsciiMath notation standard, has been used for 20 years, and the Braille mathematical notation is not used at all. Formulas are read by a screen reader, character by character, while convex printouts are created with Braille fonts whose codes correspond to the characters in the linear formula record. This way of teaching mathematics to visually impaired students does not require the teacher's and the pupil's knowledge of complex the Braille mathematical notation system, and does not require expensive specialist Braille equipment, such as Braille lines and notebooks. This technology is adapted to inclusive education purposes in accordance with the basic assumption stating that mainstream schools should be prepared to teach visually impaired students (and those with other disabilities). However, students using linear formula notations cannot work at the same pace as their sighted peers.

To recapitulate, quick conversion of formulas (e.g. during group discussions) commonly used by sighted persons into the Braille line notation used by blind persons is a problem that is partly solved by semantic formula reading and AsciiMath notation, used by low vision students.

2.2. Universality and Availability of Mathematical E-documents

The second problem that we tried to solve, taking into account the first challenge of various user interfaces relied upon while creating and exploring formulas, is the rapid exchange of information and electronic documents containing formulas, occurring on a continuous basis during the work of a group made up of persons with various visual acuity. These needs have to be addressed in educational settings – in the classroom, during supplementary activities, remote e-consultations and e-tutoring, and in publishing houses during cooperation concerning mathematical documents, e.g. in the preparation of mathematical textbooks. Problems faced in the last of the scenarios above are described in detail in [9]. An electronic document containing formulas, projected spatially on a screen, is not accessible to blind people, unless it has been specifically processed. In general, formulas in electronic publications have the form of raster images, inaccessible to the blind, or are saved in the form of structural MathML notations, based on XML. The MathML standard may be supported by most browsers (based on Gecko and WebKit engines), which means that it displays the formula spatially (graphically), which is inadequate for people with a high level of visual impairment. A semantic readout of the formula may be of assistance here. This solution is easier to implement for formulas written in MathML than for linear notations. Semantic formula readers operating in many native languages are available, based on plug-ins for browsers, e.g. for Firefox and Internet Explorer (MathPlayer) but they do not operate in the Polish language.

As textbooks assume the form of apps and electronic exams replace traditional their paper predecessors, the demand for ICT tools is growing. We observe a continuous development of multimedia e-publications, also those of mathematical character, but no measurable development of supporting IT technologies that facilitate the absorption of mathematical content users with a serious visual impairment may be observed in Poland. Educational publications and auxiliary materials, especially in the field of mathematics, require user's interactivity in solving problems and mathematical tasks. This applies, for instance, to notebooks, work sheets, examples in textbooks and tests. The level of interactivity offered by e-books is insufficient in relation to the needs of mathematical education, not only in the case of visually impaired students, but also in the case of sighted users. Interactivity of e-books boils down to navigating the document, selecting fragments of content, making tabs and notes. Few e-publications use MathML notation, due to the poor rendering of formulas saved in MathML by browsers other than Firefox. An example of misinterpretation of entries in MathML is presented below:

- the cube root in the expression x+1: $\sqrt[3]{x}+1$,
- the root of minus one-third degree of x+1: $\sqrt[-13]{x+1}$.

It is safer for the publisher to place a raster image of a specific formula in an e-book. The effect is that it is not possible to edit the formula or navigate the structure of the formula to better understand it or to reach the element of the structure that is to be modified.

To ensure that a group of visually impaired people may operate efficiently, facilities are necessary that increase the accessibility of formulas, such as semantic reading of a formula or of its selected fragments, quick selection of a fragment of the formula and its edition by means of a preferred method (Braille or QWERTY notation), in combination with a readout. The possibility of creating a mathematical e-document in one universal version which may be used by both sighted and visually impaired persons, and which may also be relied upon for transferring their e-work between them, is a condition that needs to be fulfilled for ensuring efficient work, within a group, of its sighted, visually impaired and blind members. All that is related to the need of solving a third problem, namely efficient exchange of universal mathematical e-documents and information.

2.3. Efficient Exchange of Mathematical e-documents and Information

The exchange of information and documents within the group should be ensured regardless of the environmental

conditions related to the availability of the network or its lack. The first example may be the work of students in the classroom, performed under the guidance of a teacher, where it is necessary to monitor both the workflow of each student and the exchange of documents between the teacher and students. The teacher should be able to remotely monitor the work of each pupil, in order to be able to react quickly to any mistakes made by students. Students should be able to pass, to the teacher, their work along with any comments. The teacher should be able to send back, to the student, the corrected work with mistakes pointed out and described, and with guiding and explanatory comments included. The teacher should be able to show selected solutions to the students and to discuss them. But this is where specific problems need to be tackled.

In a classroom which is not, for example, an IT room, access to a network and/or the Internet may not be available, as the author of the paper has experienced while pursuing various projects. Teachers should have the tools to carry out these educational operations without barriers caused by the diversity of the group (visual acuity of the participants or limitations concerning access to the network). In order to implement these educational operations, the teacher needs to be able to organize an ad-hoc Wi-Fi network, locally in the room, and to connect all computers used by the teacher and students, including an interactive whiteboard. In the case of an interactive whiteboard, there is a need of connecting the whiteboard to the teacher's computer, as this will provide the teacher and the students with access to tools required for creating and exchanging universal mathematical e-documents.

Online assistance provided to students working at home, in a dormitory or in hospital, ensuring that they are not left behind in their schoolwork or are able to make up for any losses as soon as possible, is another example. To offer this type of help, in addition to the Internet, there is a need for a remote method of viewing the pupil's work, exchanging e-documents and conversing via written or spoken mediums.

The problems discussed above are related to the provision of efficient classwork communication means, i.e. those between the teacher and students. Internet-based systems facilitating the provision of teacher-student communication exist and are used, as it transpires from research conducted within the EuroMath project under the Erasmus+ program [10]. Google Classroom [11], Impero [12] and Desmos Classroom Activities [13] are systems used in Ireland and the Netherlands, for example. According to research conducted, they have not been used in Polish schools for teaching visually impaired students. The authors' analysis of the accessibility of these systems intended for visually impaired users, the results of which were included in paper [14], showed that only Google Classroom is fully available to this group of users. However, in relation to the three problems discussed above, it only partially solves the third problem by enabling the teacher and the students to share documents.

3. Development of Accessible Communication Media

This section of the paper presents solutions that have been developed within PlatMat OPTY, addressing the three problems discussed in the previous section: the use of various languages and mathematical interfaces; creation of universal and accessible mathematical e-documents; efficient distribution and exchange of e-documents and mathematical information.

3.1. Media for Editing, Reading and Exploring Formulas

Each participant of the group may edit a given formula using their preferred formula editor, and may use an accessible user interface. Five different formula editors that may be deployed by teachers and students have been developed:

- for teachers and sighted students – a structured editor similar to the MS Word (Fig. 1a),
- for teachers and sighted students – a customized version of a Windows-based editor for manual edition of formulas (Fig. 1b),
- for low vision students as well as for teachers and sighted students – UnicodeMath editor, based on the AsciiMath notation, with a shortened linear visualization of the formula, e.g. instead of "sqrt", the square root symbol $\sqrt{}$ is displayed (Fig. 1c),
- for blind students – AsciiMath notation editor (Fig. 1d),
- for blind students – BNM notation editor (Fig. 1e).

The interfaces which may be used to edit formulas include the following:

- QWERTY keyboard and mouse,
- keyboard shortcuts for entering mathematical symbols,
- keyboard shortcuts for navigating the formula structure,
- touch gestures with one and two fingers to navigate the formula structure while editing the formula (at the beginning/end of the formula, by one character to the right/left, one step up/down in the hierarchy structure),
- Braille keyboard emulated on a QWERTY keyboard (f, d, s, l, j, k, l keys for the six-point edition in BNM),
- physical Braille keyboard and keyboard shortcuts,
- aural reading of the formula characters (and text characters) entered.

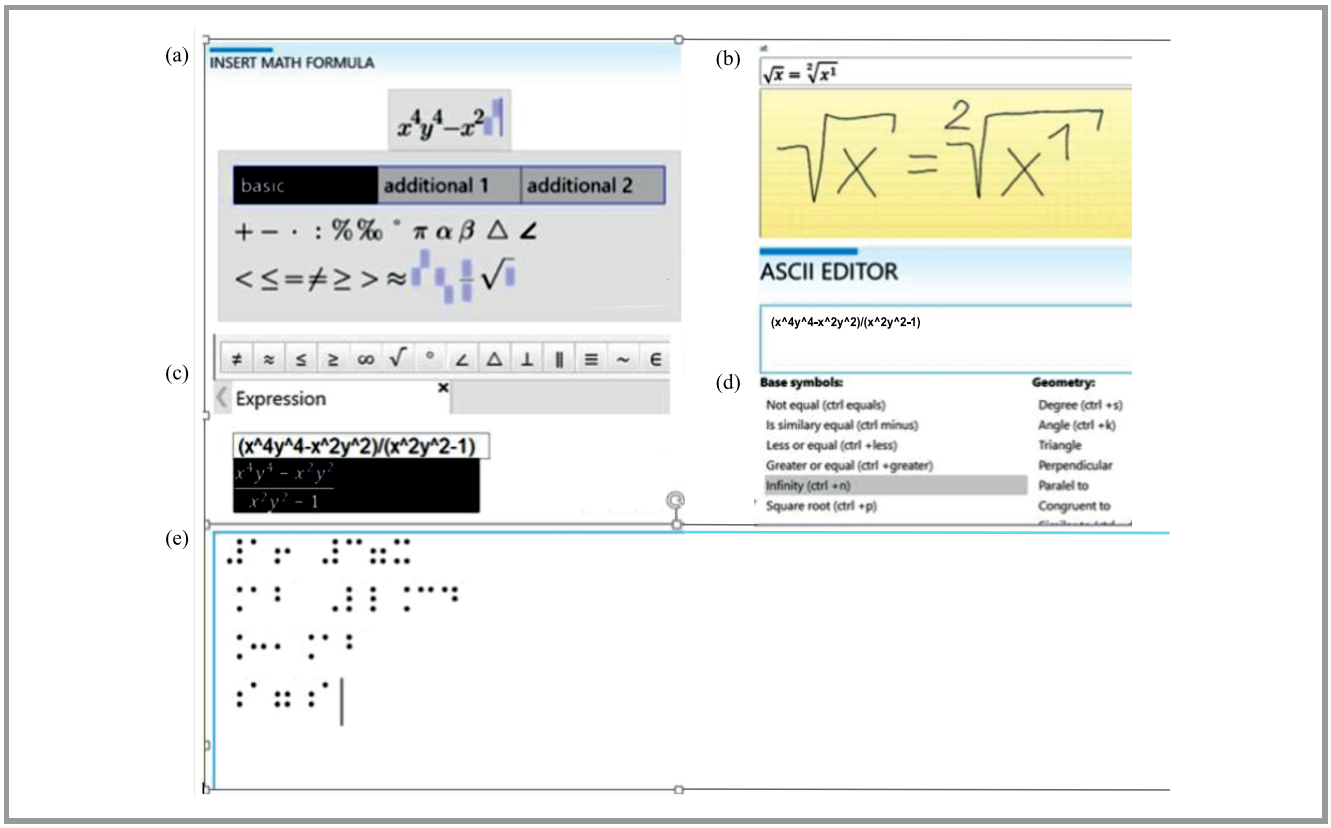


Fig. 1. Five editor formulas available in PlatMat OPTY for sighted users and users with a sight dysfunction.

The interfaces that may be used while reading formulas include the following:

- a screen where formulas are always visualized spatially for the teacher's needs and, depending on the user's needs and preferences, also linearly in AsciiMath, UnicodeMath and BNM,
- Braille line (also known as Braille monitor), on which BNM or AsciiMath characters are activated by touch, by moving pins,
- semantic reading of a formula or of a selected fragment of a text including the formula, in Polish,
- keyboard shortcuts and touch gestures with one and two fingers for reading and detailed exploration of a given formula.

The record of the formula obtained in a notation that is different than the one used by the original user must be – without a noticeable delay – converted into the notation which he/she uses. The following five converters cooperating with each other on an on-going basis via programming interfaces (API) have been developed:

- BNM into MathML,
- MathML into BNM,
- MathML into AsciiMath,
- UnicodeMath into AsciiMath,
- AsciiMath into UnicodeMath.

In addition, a ready-made library in the JavaScript language for converting AsciiMath to MathML was used.

In order for a formula, regardless of the editor and notation it was written in, to be spatially displayed by a browser for the needs of sighted users and to be semantically read out for the needs of visually impaired users, it must be saved in MathML notation. Other notations (AsciiMath, UnicodeMath, BNM) are converted to MathML. For the purpose of editing formulas, the inverse conversion from MathML to the required notations is performed. As mentioned above, some browsers have trouble with correctly displaying formulas saved in MathML. The MathML notation is correctly interpreted by Firefox. It is worth noting that this set of converters cooperating with each other on an on-going basis, has been developed for the first time; although many attempts have been made in relation to conversion of various mathematical notations, and despite the fact that their results are available in the form of online services [15], [16] and local solutions [17], [18], they fail to include the Polish version of BNM notation.

Automatic translation covering four methods of expressing mathematical language (BNM, AsciiMath, UnicodeMath and MathML) is a rather complex problem. The development of BNM converters poses a particularly major research challenge due to the problem of semantic inter-

Table 1
Mathematical communication based on exchanging .epub files between users relying on various mathematical notations and user interfaces

Participants	Direction of communication	Participant interface	Participant's notation	Mathematical notation	Conversion
W, S	W→S	W	Structural editor	MathML	MathML→epub
		S	UnicodeMath editor	UnicodeMath	epub→MathML/AsciiMath/UnicodeMath
	S→W	S	UnicodeMath editor	UnicodeMath	UnicodeMath/AsciiMath/MathML→epub
		W	Structural editor	MathML	epub→MathML
W, N	W→N	W	Structural editor	MathML	MathML→epub
		N	Ascii editor	AsciiMath	epub→MathML/AsciiMath
	N→W	N	Ascii editor	AsciiMath	AsciiMath/MathML→epub
		W	Structural editor	MathML	epub→MathML
	W→N	W	Structural editor	MathML	MathML→epub
		N	BNM editor	BNM	epub→MathML/BNM
	N→W	N	BNM editor	BNM	BNM/MathML→epub
		W	Structural editor	MathML	epub→MathML
S, N	S→N	S	UnicodeMath editor	UnicodeMath	UnicodeMath/AsciiMath/MathML→epub
		N	BNM editor	BNM	epub→MathML/BNM
	N→S	N	BNM editor	BNM	BNM/MathML→epub
		S	UnicodeMath editor	UnicodeMath	epub→MathML/AsciiMath/UnicodeMath
	S→N	S	UnicodeMath editor	UnicodeMath	UnicodeMath/AsciiMath/MathML→epub
		N	Ascii editor	AsciiMath	AsciiMath/MathML→epub
	N→S	N	Ascii editor	AsciiMath	AsciiMath/MathML→epub
		S	UnicodeMath editor	UnicodeMath	epub→MathML/AsciiMath/UnicodeMath
Key: W – sighted user, S – low vision user, N – blind user					

Table 2
Examples of rules applied while translating formula elements into texts of their semantic readout

Item	Formula elements	Readout rule
1	Integers	The integers are read as they are pronounced in Polish, e.g. 121 'sto dwadzieścia jeden' (English: *hundred twenty one*)
2	Floating-point numbers	Numbers with a coma (*point in English notation*) e.g. 5,26, are read as 'pięć przecinek dwadzieścia sześć' (English: *five coma twenty six*)
3	Letters – vowels	The vowels are read unchanged
4	Letters – consonants	The consonants are read phonetically, e.g. b as beh. Big letters are preceded by the word capital
5	Greek letters	Greek letters are read phonetically, e.g. α as alpha
6	Subscripts	The subscripts are read, e.g. '… with subscript end of subscript'. If the subscript contains only one element, then the text 'end of the subscript' is omitted. Area subscripts such as Pb are read (in Polish) as pe be (English pronunciation: *peh beh*) and Pp as pe pe (English pronunciation: *peh peh*)
7	Superscripts	The superscripts are read, e.g. '… to the power … end of superscript'. If the superscript contains only one element, then the text 'end of the superscript' is omitted. If the superscript is 2, and it is the only element, then the text read is: „… kwadrat (English: *square*). If the index is 3 and it is the only element, then the text read is '… sześcian' (English: *cube*)
8	Fractions	The fractions are read as follows: a fraction numerator … denominator … end of a fraction. Numeric fractions are read literally, e.g. 1/6 – one sixth

pretation of particular symbols, which often depends on the context (appearing in connection with other symbols, a space place before or after the symbol etc.).
The set of converters developed enables instant, on-going communication between people using various mathematical notations and different user interfaces. The term "on-going communication" relates to three communication scenarios:

- an .epub file being generated (in the EPUB 3 standard discussed below) by one of the users and sent to another user or to other users, containing formulas recorded in MathML notation, regardless of the notation in which the formulas were edited,
- transferring them to the interactive whiteboard, displaying them spatially on the group leader's screen, regardless of the notation used in the edition phase,
- displaying on the screen of the leader, and possibly on the interactive whiteboard, the content of the remote screen of the selected group member, editing the formulas in the preferred notation, with the said formulas being then saved in MathML and visualized spatially.

Table 1 shows the conversion processes taking place when exchanging .epub files, depending on the notations preferred by the the sender and recipient of mathematical content. In the remaining two situations, the conversions are similar, as in each case the conversion leads to creating a MathML notation, or a user-preferred notation based on MathML notation. It is worth noting that in order for a blind user to see the content on the interactive whiteboard receiving data from another user's screen, the screen contents must be sent to the blind user as an .epub file that will be unpacked, and then the MathML notation of the formulas included in the content will be converted to BNM or AsciiMath.
In order to increase the chances of blind and low-vision students working in a group at a pace that would not interfere with the work of the entire, in addition to the ability to read formulas by sight or by touch on the Braille line, another option to improve mathematical communication has been introduced. It allows a formula or its fragments to be read in Polish, semantically, in a manner adopted in Poland for that specific purpose. To offer this functionality, Poland's semantic formula reader relying on synthetic speech has been developed. The basic module of the reader has the form of a translator of the formula structure recorded in MathML notation, converting it into the text to be read out. The MathML notation is based on XML tag language [17]. With the introduction of HTML 5, MathML has superseded, in the browsers, the AsciiMath notation, which was used on the Internet at that time. The structured, hierarchical nature of MathML enables reliable spatial visualization of formulas. An example of a fraction with the root in the numerator, which was shown above in several linear notations, saved in MathML, is presented in Listing 1.

Listing 1. MathML example

```
<math mode="display"
xmlns="http://www.w3.org/1998/Math/MathML">
 <semantics>
  <mrow>
    <mi>x</mi>
    <mo>=</mo>
    <mfrac>
      <mrow>
        <mo form="prefix">&#x2212;<!-- ? --></mo>
        <mi>b</mi>
        <mo>&#x00B1;<!-- &PlusMinus; --></mo>
        <msqrt>
          <msup>
            <mi>b</mi>
            <mn>2</mn>
          </msup>
          <mo>&#x2212;<!-- ? --></mo>
          <mn>4</mn>
          <mo>&#x2062;<!-- &InvisibleTimes; --></mo>
          <mi>a</mi>
          <mo>&#x2062;<!-- &InvisibleTimes; --></mo>
          <mi>c</mi>
        </msqrt>
      </mrow>
      <mrow>
        <mn>2</mn>
        <mo>&#x2062;<!-- &InvisibleTimes; --></mo>
        <mi>a</mi>
      </mrow>
    </mfrac>
  </mrow>
  <annotation encoding="TeX">
     x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}
  </annotation>
  <annotation encoding="StarMath␣5.0">
     x={-b plusminus sqrt {b^2 - 4 ac}} over {2a}
  </annotation>
 </semantics>
</math>
```

A table used for translating formula templates into texts to be read out has been developed based on predetermined readout rules. Texts and readout rules have been developed for formulas introduced by primary and secondary school curricula. The readout texts have been agreed upon with mathematics teachers. The translator, the rules developed and the problems encountered during translation were presented in [20]. Some examples of translation rules are presented in Table 2.
For example formula

$$y^{a^{b_c}} \neq y^{b^b \cdot c}$$

is read as 'igrek do potęgi a do potęgi be z indeksem dolnym ce koniec wykładnika koniec wykładnika nie równa się igrek do potęgi a do potęgi be koniec wykładnika ce koniec wykładnika' (In English: *wai to the power ei to the power bi end of superscript with a subscript si end of subscript end of superscript is not equal to wai to the power ei to the power bi end of superscript si end of superscript*). Figure 2a shows the structure of this formula (and the text of the readout) visualized in the formula navigator, while Fig. 2b,c shows the structure of selected fragments of the formula during navigation and the texts of their readouts. The texts of the readouts which do not appear in real conditions on the screen, have been included in the drawings for illustrative purposes.
The texts of readouts from the translation tables are passed to the NVDA screen reader synthesizer, which PlatMat cooperates with in its part intended for blind users.

3.2. Universally Accessible Medium for Recording Mathematical Content

In search of an electronic medium recording mathematical content and enabling its distribution and exchange within a group of participants with diverse visual acuity, the increasingly popular EPUB e-publication standard has been chosen over its competitor – Amazon's commercial AZW standard (an extension of the MOBI standard). EPUB is an open standard for the distribution and exchange of digital publications and documents that is based on the structured XML markup language [21].

EPUB version 3.1 (EPUB3) relies on the following standards: HTML5 – content, CSS3 – style, SVG – vector graphics, MathML – formulas, MPEG4 – video and sound, OTF – fonts, JS – scripts. The EPUB3 container, which is a ZIP file, integrates various types of files that can create multimedia, interactive, mathematical content. The features and properties of individual formats may be effectively used to increase the accessibility of EPUB3 content. In particular, MathML for writing formulas and SVG vector graphics standards, based – just as EPUB3 – on the structural language of XML markups, are essential for improving the accessibility of mathematical content. The structure of the recording allows detailed exploration of an EPUB3 document and of the formulas and graphics contained therein, in a manner accessible to people with visual impairments. Active elements – JS scripts, which may be included in the EPUB3 container, can be used to increase the accessibility of a mathematical document, e.g. to read, using synthetic speech, a part of the formula and also to support the user's interactivity, for instance by means of a touch gesture or a keyboard shortcut. JS scripts improve the interactive capability of a user working with an EPUB3 document, beyond the typical interactivities available in e-publications, such as note taking, selecting text fragments, creating tabs or navigating the document structure.

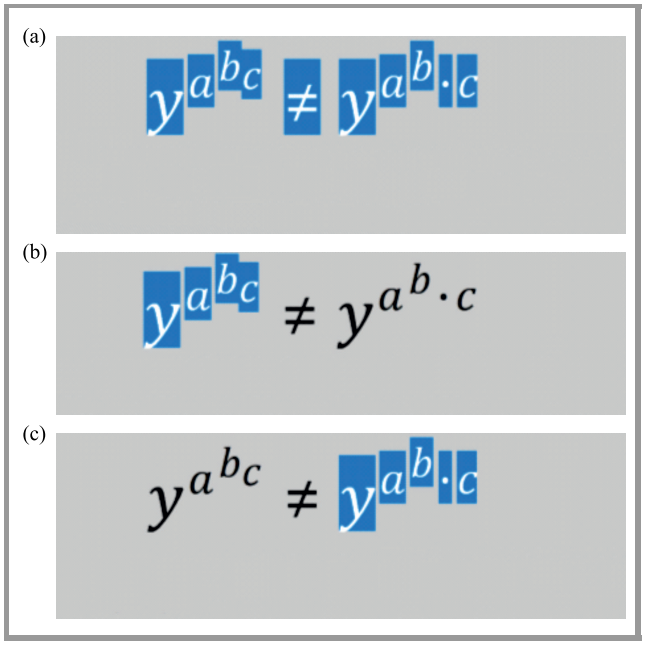


Fig. 2. Visualization of the formula structure and texts of its readouts (a), and formula fragments while navigating the formula (b) and (c).

The ability to enter formulas into an e-document, or to edit formulas contained in the text using the user-preferred notation, as well as to convert them to MathML notation, with the prospect of subsequent conversion when the document reaches a user whose preferred notation differs from that of the original one, is a good example of enhanced interactivity. These types of interactivities are very much needed, for example in mathematical education (solving tasks/tests, improving student's work) or in cooperation on publishing mathematical e-publications. Scripts may also be used for additional navigation, beyond navigation functionalities offered by browsers, among such elements of the mathematical e-document as formulas, text or voice comments, test questions, and mathematical graphics.

Conversion of mathematical notations specified in Table 1, as well as exploration of the entire e-document and the formulas contained therein, handled by JS scripts, enables the creation of a universal, mathematical EPUB3 e-document that is accessible to every participant of the cooperating group, regardless of the level of their visual acuity. It should be emphasized that universality is a useful feature for the creator of a mathematical e-document, because it means that the document may be created once, in one version, for all group members, and accessibility is a useful feature for the e-document recipient who receives the same e-document as other group members and may read, modify and explore it in a manner tailored to his/her needs.

Theoretically, browsers would be the most convenient way to handle EPUB3 documents. There are browser add-ons (plug-ins) extending their functionalities, so as enable them to tackle e-documents, e.g. EPUBReader for Firefox, but these are typical readers of documents not containing mathematical content and they do not or only partially support the MathML standard. They play the role of typical e-publication readers and offer, as mentioned above, a limited scope of interactive support.

Due to the lack of interactive software supporting mathematical content stored in EPUB3, the installable PlatMat software that is based on the Gecko engine, was and still remains the only software for creating, reading, modifying and exploring mathematical EPUB3 e-documents. It is also a tool for disseminating, exchanging and collecting e-documents and mathematical information – functionalities that are discussed in the following part of this paper.

4. Media for Sharing Mathematical E-documents and Information

The third problem discussed earlier, which was taken up in the works on PlatMat, is the question of an efficient, ongoing exchange of EPUB3 mathematical e-documents and information in a group that is diversified in terms of visual

acuity of its members, in various environmental conditions concerning the availability of local Wi-Fi and Internet connections.

4.1. Mathematical Communication in a Wi-Fi Network

Each member of the group, equipped with the PlatMat software, can create an EPUB3 document and save it locally. The leader can also save the document in a remote repository on the www.platmat.pl portal, so as to have it generally available. In order for the document placed in the repository to be published, it must undergo a verification process. The verification process takes place between the verifier and the author of the document. After successful verification, the portal administrator places a positive verification flag in the document's metadata. Then, the document becomes public, visible to the users and available for download. Each group participant may download the document published in the repository to his/her own local disk. In the local network the leader may send a document to each member of the group. Each group member may send/send back a document to the leader.

The applications of the leader and those of group members communicate with each other via the local Wi-Fi network. The group is connected forming the topology of a star, with the leader's computer serving as the central node. Group members do not communicate with each other directly. The exchange of documents between group members is possible through the leader. The star topology was adopted, in consultation with teachers, as the most suitable for the working conditions of a school group – with the teacher and the students in a classroom.

To connect the group members' applications with the leader and to enable them to exchange documents, it must be made sure that both applications operated on the same subnet. The subnet is identified by the first 3 digits of the IPv4 address – they are identical within the same subnet. After launching the application on the leader's computer and starting up the applications of the group members, the latter begin to actively search for the leader's application. When the searching process comes to an end (after about 10–20 s), the application of each group member will connect to leader's application it has identified, or it will ask the user to select the appropriate leader if more than one leader application has been found in a given network. If no leader has been found, the search will continue indefinitely. The same will occur in the event of a loss of connection.

Where no local Wi-Fi network is available, it is possible to set up a hot spot on the leader's computer, provided that the network card supports such a functionality (it must operate in the AccessPoint mode). Some classrooms have no access to a Wi-Fi network, and the option of becoming unrestricted by this limitation while communicating within the group is very useful. In addition to exchanging documents, a local Wi-Fi network allows the leader to activate the remote desktop of a selected group member, for example a student in a classroom, and to monitor the student's work by displaying a picture of the student's screen on the leader's computer to support the student if any problems in solving tasks are encountered. The leader may display, on the interactive whiteboard, the content of their own screen

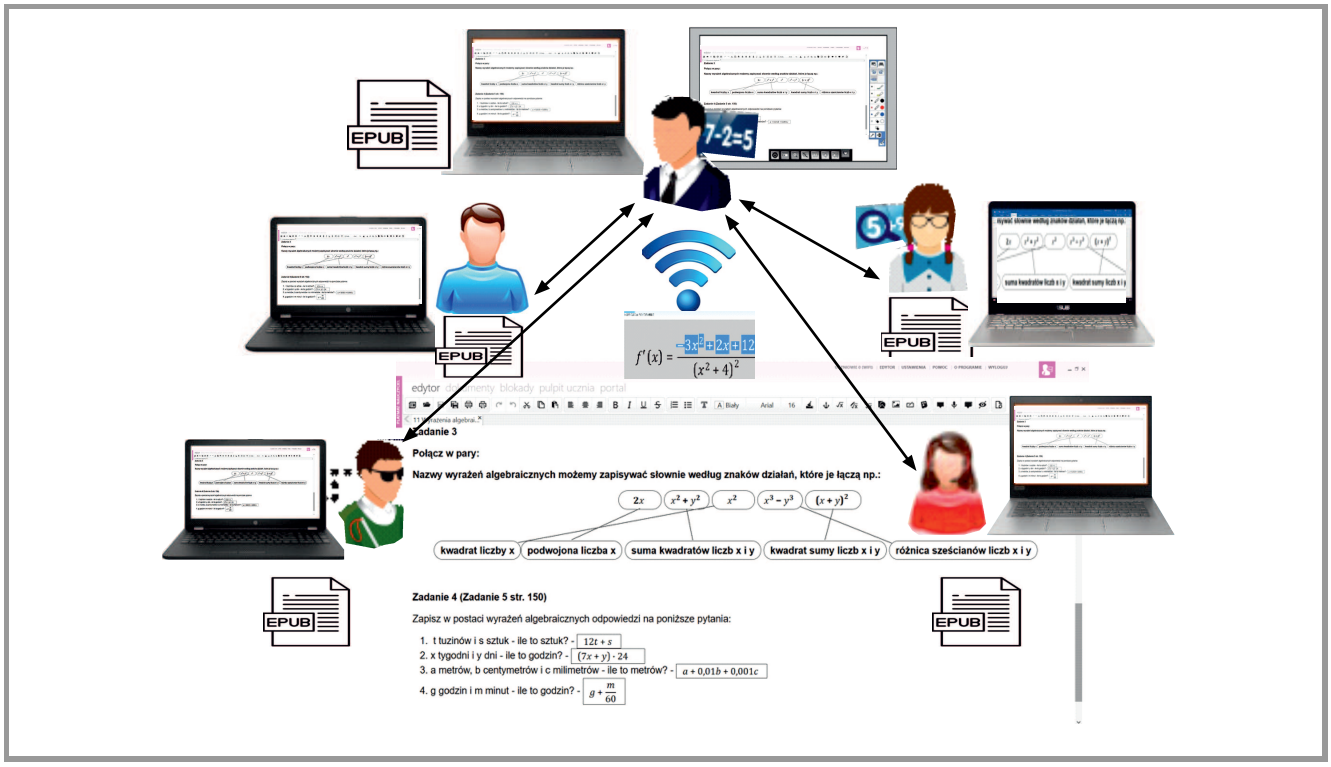


Fig. 3. Mathematical communication in a diverse group of participants, relying on a local Wi-Fi network.

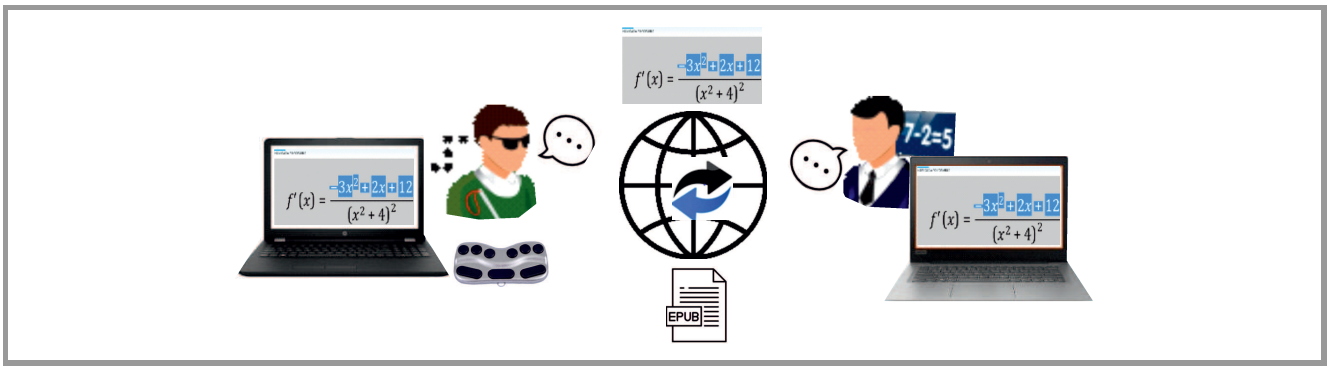


Fig. 4. Mathematical communication of a leader and a group member via the Internet (chat, Braille, voice, EPUB3 documents exchange, remote desktop).

Table 3
Mathematical communication via a Wi-Fi network and the Internet

		Role in the group		Network	
Item	Operation	Group leader	Group member	Local Wi-Fi	Internet
1	Creating/modifying EPUB3 e–documents	+	+	–	–
2	Collecting locally EPUB3 e–documents	+	+	–	–
3	Publishing EPUB3 e–documents in a remote repository for publication	+	–	–	+
4	Downloading published EPUB3 e–documents from a remote repository	+	+		+
5	Sending an EPUB3 e–document to a group member	+	–	+	+
6	Sending an EPUB3 e–document to the group leader	–	+	+	+
7	Initiating a chat	–	+	–	+
8	Chat with a group member	+	+	–	+
11	Remote desktop of a group member viewed by the leader	+	–	+	+

or of the screen of a group member, received via the remote desktop function. The Wi-Fi based communication model is illustrated in Fig. 3.

4.2. Mathematical Communication via the Internet

PlatMat-based online communication was developed for the purpose of remote consultations and is useful for mathematics as it offers the following functionalities: chat (also in Braille), voice calls, exchange of documents, remote desktop monitoring. Examples of educational activities that require remote assistance include the following: helping a student who is behind in his/her work, one who is poor at maths or is home-schooled. Another example involves editorial cooperation concerning a mathematical document, with the blind person using Braille technology. Chat typed in six-point Braille font is received by the sighted person in the form of plain text, a mathematical .epub document, while formulas edited in mathematical Braille notation are received by a sighted person in MathML notation and are displayed spatially (graphically). On the remote desktop of a blind person working in Braille technology (BNM editor) or in ASCII technology (Ascii editor), the formulas are visualized spatially thanks to the conversion process presented in Table 1. Such an approach ensures there are no problems in communication between two people using different mathematical languages, whether they cooperate via the Internet or within a group, using a local network. Mathematical communication via the Internet is presented in Fig. 4.

Table 3 presents communication-related operations carried out in PlatMat by the leader and by group members in a local Wi-Fi network and via the Internet.

5. Surveys on the Usefulness of New Solutions

Research on the impact and usefulness of the solutions proposed in PlatMat was conducted at three different points during the process of developing the new technology. We shall focus on the most recent surveys conducted in 2017 among math teachers and their students at 3 educational institutions in Warsaw, Kraków and Siedlce (Poland) attended by sighted, low-vision and blind students. 5 mathematics teachers and 11 students took part in the qualitative surveys that were combined with individual interviews. The aim of the survey was to determine the measurable benefits enjoyed by mathematics teachers, blind students and low-vision students, resulting from the use, both in the class-

room and at home, of the PlatMat tools with new ICT solutions. The research was carried out after pilot phase under which PlatMat tools were implemented at those facilities over a period of several months. Because not all students had access to laptop computers in the classroom, the pilot-phase classes were conducted primarily as compensatory lectures, one a one-on-one basis or in small groups with 2–3 students. The compensatory activities were also carried out via the Internet. Similarly to the compensatory classes, on-going consultations concerning homework were also offered remotely. The questionnaires were divided into three parts, concerning: the teacher's work, the blind student's work and the low-vision student's work. The fourth part presented the criteria and assessment methodologies used. The questionnaires covered all new solutions implemented in PlatMat, including those supporting the work performed by a group of students diversified in terms of their visual acuity, as described in this paper.
The opinions about formula editors were not focused on any particular editor. Teachers, depending on their preferences and needs, used a structured editor, a UnicodeMath editor or a handwriting editor. Low vision students preferred the UnicodeMath editor. Blind students preferred the BNM Braille editor. No attempt was made to work on the AsciiMath editor, which is a functional option available in software for blind students. Students participating in the survey studied in upper grades of technical schools and high schools, were well skilled and experienced in using Braille. An opinion has been reached that the new technologies replacing Braille must be introduced at the very early stages of education.
The primary measurable benefits offered by the presented solutions, as identified in the survey, are as follows:

- improvement of IT efficiency of younger students, which shortens the time required for performing mathematical operations (mastery of keyboard shortcuts),
- less time spent on mathematical operations by low-vision students,
- increased self-reliance of students, inter alia thanks to the semantic reading of formulas, recognizing the structure of a formula, own records that are clear for their author (low-vision students),
- the number of mistakes made by students was not larger, and it was clearly lower in 'pairing' tasks and tasks with a narrative containing parameters for calculations,
- better ability to communicate, grater level of students' comfort while working and higher effectiveness of the teacher's support, as the student's screen could be monitored by the teacher,
- greater capacity for providing support to a student and for making it more precise,
- time needed by teachers to prepare worksheets, especially with tasks involving fractions, roots, equation systems and special characters, the writing of which is quite troublesome while using Word.

The research – surveys, criteria, measures and results – is described in detail in the Research Report submitted to PFRON [22].

6. Conclusions

The paper presents a selected range of new solutions proposed in the PlatMat system. Their aim is to support work in the field of mathematics, performed in a group of participants with diverse visual acuity. The groups for which PlatMat is primarily intended include groups of students at regular or special needs schools, attended by blind and low-vision students. The solutions discussed, aimed at facilitating the work and communication in the field of mathematics include the following: a sequence of conversions, performed on an on-going basis, of various mathematical notations (languages), enabling the use of mathematical notation and formula editing tools preferred by users, as well as on-going cooperation; universal, accessible and interactive mathematical documents in the EPUB3 e-publication standard, enabling the exchange of mathematical content and information; setting up the exchange of mathematical documents and information via a Wi-Fi network and via the Internet, in various environments and between users using different math languages and interfaces. Qualitative research/surveys listing the opinions of mathematics teachers and their students on the usefulness of the presented solutions, were conducted among groups of 2–3 students having personal computers. The ability to create a single version of lesson materials in the form of an epub document – an interactive document for all students, and the ability to monitor students' work via a Wi-Fi network or via the remote desktop function, was very well received by teachers. Among students, the greatest satisfaction was expressed by low-vision students who could now edit formulas using the UnicodeMath editor. Previously, they had been using the MS Word formula editor – a feature that is difficult to operate due to the precision of movements required when entering values into formula template fields.
In order to assess the usefulness of the discussed solutions in large groups (meaning, under real-world conditions, that a lesson needs to be conducted in a classroom), the first requirement that has to be met is that all students need computers. Research performed in 2018 as part of the abovementioned EuroMath project and concerned with ICT tools used to support teaching maths, showed that few students use laptops or any other computer equipment (apart from smartphones) in the classroom. It would be worthwhile to organize, for experimental purposes, a class of students equipped with laptops and PlatMat tools for teaching mathematics, to carry out research on the effects of computerization of mathematical education and to disseminate the

positive results that are likely to be obtained. This will create an incentive for other schools and will contribute to the promotion of PlatMat technologies.

Acknowledgments

This work is a part of two research projects:

1. "Towards professional activation of blind people: PlatMat platform increasing the effectiveness of inclusive education in the field of mathematics and physics", no. BEA/000021/BF/D, co-financed by PFRON, 2014–2015,
2. "OPTY: Studies on the effectiveness of computerization of mathematical education of students with visual impairments using the optimized PlatMat" tools, no. BEA/000027/BF/D, co-financed by PFRON, 2016–2017.

References

[1] D. S. Sari, K. Kusnandi, and S. Suhendra, "A cognitive analysis of students' mathematical communication ability on geometry", *J. of Phys. Conf. Series*, vol. 895, no. 1, 012083, 2017 (doi: 10.1088/1742-6596/895/1/012083).

[2] G. M. Tinungki, "The role of cooperative learning type team assisted individualization to improve the students' mathematics communication ability in the subject of probability theory", *J. of Educ. and Pract.*, vol. 6, no. 32, pp. 27–31, 2015 [Online]. Available: https://www.iiste.org/Journals/index.php/JEP/article/view/27313/27996

[3] D. Mikułowski, G. Terlikowski, and J. Brzostek-Pawłowska, "Virtual cubarithms – innovative assistive technology for teaching the blind and visually impaired students traditional columnar layout operations", *Studia Inform.*, vol. 1–2, no. 20, pp. 17–25, 2016.

[4] LaTeX notation [Online]. Available: https://www.latex-project.org/ (accessed Feb. 3, 2019).

[5] ASCII-Mathematikschrift AMS – Anleitung zur Umsetzung mathematischer Formeln [Online]. Available: http://chezdom.net/wp-content/uploads/2008/11/ams.pdf (accessed Feb. 1, 2019).

[6] A. Van Leendert, "WND Wiskunde Notatie Dedicon, Voortgezet Onderwijs" [Online]. Available: https://www.eduvip.nl/cms/files/WND_VO_juni_2016.pdf (accessed Dec. 10, 2018).

[7] Lambda notation [Online]. Available: http://www.lambdaproject.org/the_lambda_code (accessed 04.02.2019).

[8] J. Świerczek, Ed., *Brajlowska notacja matematyczna fizyczna i chemiczna*. Krakow, Laski, Łódź, 2011 [Online]. Available: http://pzn.org.pl/wp-content/uploads/2016/07/brajlowska_notacja_matematyczna_fizyczna_chemiczna.pdf [in Polish].

[9] J. Brzostek-Pawłowska and D. Mikułowski, "Research on improving communication between the blind and the sighted in the area of mathematics, and related requirements", in *Proc. of the Federated Conf. on Comp. Sci. and Inform. Syst. FedCSIS 2012*, Wrocław, Poland, 2012, pp. 1065–1069 [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6354311

[10] Research project "EuroMath – increasing support for teachers and vision-impaired students with innovative ICT in inclusive education", co-financed by the Erasmus+ program, no. 2017-1-PL01-KA201-038548, implementation period 2017–2020, coordinator NASK PIB.

[11] Google Classroom System [Online]. Available: https://classroom.google.com (accessed Feb. 13, 2019).

[12] Impero System [Online]. Available: https://www.imperosoftware.com/uk/ (accessed Feb. 10, 2019).

[13] Desmos Classroom Activities System [Online]. Available: https://teacher.desmos.com/ (accessed Feb. 10, 2019).

[14] J. Brzostek-Pawłowska, M. Rubin, and D. Mikułowski, "Technologie informacyjno-komunikacyjne zwiększające dostępność treści matematycznych", Wydawnictwo Adam Marszałek (published in the first half of 2019) [in Polish].

[15] K. Miesenberger *et al.*, "MathInBraille online converter", in *Proc. of the 13th Int. Conf. on Comp. Helping People with Special Needs ICCHP 2012*, Linz, Austria, 2012, pp. 196–203 (doi: 10.1007/978-3-642-31522-0_29).

[16] L. B. Christensen, S. J. Keegan, and T. Stevns, "SCRIBe: A model for implementing robobraille in a higher education institution", in *Proc. of the 13th Int. Conf. on Comp. Helping People with Special Needs ICCHP 2012*, Linz, Austria, 2012, pp. 77–83 (doi: 10.1007/978-3-642-31522-0_12).

[17] D. Archambault and F. Guyon, "UMCL transcription tools: Universal Maths Conversion Library", *Assist. Technol. Res. Series*, vol. 29, pp. 416–423, 2011 (doi: 10.3233/978-1-60750-814-4-416).

[18] F. Alonsoi *et al.*, "SBT: A translator from Spanish mathematical braille to MathML", in *Proc. of the 10th Int. Conf. on Comp. Helping People with Special Needs ICCHP 2006*, Linz, Austria, 2006, pp. 1207–1214 (doi: 10.1007/11788713_174).

[19] MathML specification, version 3.0 [Online]. Available: https://www.w3.org/TR/MathML3/ (accessed Feb. 3, 2019).

[20] Specification of EPUB 3 electronic publication standard [Online]. Available: http://idpf.org/epub/30 (accessed Feb. 10, 2019).

[21] A. Salamończyk and J. Brzostek-Pawłowska, "Translation of MathML Formulas to Polish Text, Example Applications in Teaching the Blind", in *Proc. of the 2nd IEEE Int. Conf. on Cybernetics CYBCONF 2015*, Gdynia, Poland, 2015, pp. 240–244 (doi: 10.1109/UBConf.2015.7175939).

[22] M. Rubin, "Raport z badań o potrzebach i informatycznych technikach ich zaspokojenia w zakresie wspomagania niewidomych i słabowidzących w edukacji i nabywaniu kompetencji kluczowych (matematyka) prowadzonych w 2016 r. – 2017 r. w ramach projektu badawczego "OPTY: Badania efektywności informatyzacji edukacji matematycznej uczniów z dysfunkcjami wzroku z zastosowaniem zoptymalizowanych narzędzi PlatMat" dofinansowanego przez PFRON", Mathematical Machines Institute, 2017, access: NASK NRI Projects Archive.

Jolanta Brzostek-Pawłowska Ph.D., graduate of the Faculty of Electronics and Information Technology at the Warsaw University of Technology, assistant professor at NASK – PIB. She has been conducting research and development work on e-learning, assistive technologies and alternative user interfaces for many years. She managed research projects that resulted in the creation of new technologies such as TeleEdu LMS, PlatMat platform supporting mathematical education for visually disabled students. She is currently conducting the EuroMath (EU Program Erasmus+) project adapting the best solutions of the PlatMat to educational conditions in other European countries.

https://orcid.org/0000-0002-9870-0480
E-mail: jolanta.brzostek-pawlowska@nask.pl
Research and Academic Computer Network (NASK)
Kolska 12
01-045 Warsaw, Poland

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 authors JTIT LATEX style file is available:
http://www.nit.eu/for-authors

Papers published should contain up to 10 printed pages in LATEX authors style (Word processor one printed page corresponds approximately to 6000 characters).

The manuscript should include an abstract about 150200 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. 262264, 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. 301314.

Biographies and photographs of authors. A brief professional authors 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.

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 worlds 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 Publishings 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
http://www.nit.eu

JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY 2/2019