JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY

4/2014

(Contents Continued on Back Cover)

Editorial Board

Editorial Advisory Board

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

Circulation: 300 copies

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

JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY

Preface

For the last decades, we witness an explosive growth in the volume, velocity, and variety of the data available on the Internet and other global networks. Terabytes of data originated from multitude of sources including mobile devices, sensors, individual archives, social networks, Internet of Things, enterprises, cameras, software logs, is created on a daily basis. Modern intelligent networks cannot be considered in today's data-aware computing as the systems for such data storage and transmission. Network end-users and devices can also generate the data, such as in the smart city environment, where most of the data is generated by the sensors. Thus, the recent challenging research issues in today's intelligent networking include the effective and optimal management techniques of such a large amount of data and information processing methodologies, as well as new ways to analyze large amounts of data for unlocking information.

One of the most important problem in global and highly distributed networks is a huge traffic generated by billions of connected devices. This devices amount is expected to triple or even quadruple over the next several years as connectivity rapidly expands beyond phones and tablets. The impact on the existing infrastructure will create profound challenges for equipment providers and network operators alike. In such a case, scalability and reliability of the whole infrastructure in massive data processing are the major issues.

Recently, Cloud Computing gives application developers the ability to marshal virtually infinite resources with an option to pay-per-use and as needed, instead of requiring upfront investments in resources that may never be optimally used. Once applications are hosted on cloud resources, users are able to access them from anywhere at any time, using devices ranging from wide class of mobile devices (smartphones, tablets) to desktop computers. The data centre cloud provides virtual centralization of application, computing, and data. While cloud computing optimizes the use of resources, it does not (yet) provide an effective solution hosting the massive data applications.

Despite the above technological advances in intelligent networking and data processing paradigms, large-scale reliable system-software for massive data applications are yet to become commonplace. There are multiple reasons for this state of affairs including: (i) lack of system-software frameworks that allow portability of such applications across multiple distributed data hosts and data centers, (ii) inefficient fault-tolerance mechanism for the improvement of the network reliability and security, (iii) manual approaches leading to

non-optimal hardware and software resource provisioning, data and application management and network monitoring; and (iv) lack of a right set of programming abstractions, which can extend the capability of existing information and data processing paradigms to large-scale dynamic network infrastructures with mobile and remotely accessed services and devices and mobile users.

This issue contains thirteen research papers reporting the recent results on models, solutions, and techniques from a wide area of data-intensive computing and intelligent networking, ranging from conceptual and theoretical developments to advanced technologies and innovative applications and tools.

In the first five papers, the authors present the novel solutions for the improvement of the fault detection and fault-tolerant mechanism in various types of distributed networks and infrastructures. Iacono and Marone in the first paper addressed the problem of Web service selection and integration in Internet. Nita *et al.* developed a Fault Injector Module for cloud systems. Both models are responsible for supporting the cloud developers in the validation of their infrastructure. Nita *et al.* work on CloudSim simulator, where the system faults are generated by using various statistical distributions. In the experimental section, the impact of the statistical distributions on the cloud failures has been analyzed. Careful Web data scanning can improve the efficiency of the malware detection in large-scale networks. Malware can disrupt or even damage the whole infrastructure and is especially dangerous in massive data processing. Kruczkowski and Niewiadomska-Szynkiewicz investigated a novel malware detector based on three supervised learning methods for data mining, namely Support Vector Machine, Naive Bayes and k-Nearest Neighbors techniques. They evaluated their model on realistic data originated from the devices located in several units, organizations and monitoring systems serviced by CERT Poland. Similar problem has been studied by Conti *et al.* defined the new biometric authentication technology for mobile devices with Android system. They showed that their technology can rapidly increase the security of the data and messages exchanged between the mobile telecommunication network nodes. Finally, Lokesh and Nalini developed the novel fault detection and recovery to achieve fault tolerance mechanisms in Distributed Sensor Network (DSN) by using Bayesian Networks (BNs). It is assumed that sensors in DSN can be located randomly in the dynamic environment. Bayesian Network is used to aid reasoning and decision making under uncertainty of the generated data and resources.

The decision making is a very complex process in massive data processing in large-scale networks. There are several abstract models which can be used for supporting the users and system managers' decisions at different network levels and clusters. Multiagent systems (MAS) for instance is commonly used for simulation the users' behavior and choices, users' interactions and network management components. Mariano and Correia developed game-based model supporting the agents' decisions on the selection of the partners for collaboration based on the reputation parameters. They defined n-players game for illustration the agent's selection results in the dynamic populations (of the variable sizes), where the agents can interact with each other, reproduce and die. Such MAS model and collaboration behavior can be applied in many data-intensive processes and scenarios, which is confirmed in the paper of Tasquier and Aversa. The authors present the agent-based interaction model in smart house environment. The agents' decisions are made on the optimal (in the sense of energy consumption) selection of the electrical devices based on the current users needs and preferences, and state of the environment.

Scheduling the complex applications in highly distributed computing environments has been usually studied separately from the required data scheduling. Szmajduch developed a novel generic scheduling model in Infrastructure-as-a-Service cloud layer, where both applications and data are scheduled simultaneously in one joint process. The provided simulation results show the importance of considering various scenarios of data transfer to the computational network nodes. In the next paper, Abaev *et al.* studied the delays in message and data processing Session Initiation Protocol (SIP) proxy servers. They modeled such processing in SIP servers by using a specialized G|PH|c queuing system. A comprehensive theoretical analysis showed that measured waiting time and minimum transit time through SIP server can be approximated by acyclic phase-type distributions.

The last part of the issue is composed of four papers on miscellaneous topics related to the wide area of intelligent networking. Le, in the first paper in this part, focused on the optimization of the design of FTTH (Fiber To The Home) access points for popular telecom-

munication networks. El-Bendary and El-Tokhy address the problem of the optimization of retransmission times of Enhanced Data Rate (EDR) packets in Wireless Personal Area Networks. They performed a simple probabilistic analysis for Packet Error Probabilities over the Additive White Gaussian Noise (AWGN) and channels (with Hamming encoding method) for Bluetooth (EDR) packets. The provided experiments show high efficiency of the proposed method in the reduction of the energy utilization in the Bluetooth data transmission. Sudhir and Manvi developed for the improvement of the GPS-based global satellite navigation systems. They designed and implemented a new model of dual antenna GPS-GLONASS navigation receiver. Their receiver improved significantly the performance of the navigation system in critical realistic scenarios (lost of the link, lost of the signal). Finally, Kazakova *et al*. present a short survey of the information recovery system models based on the data generated by the monitoring systems of sensor networks. The paper contains a simple theoretical specification and analysis of the addressed problem.

I strongly believe that this issue will bring all the readers (students, researchers, and industry practitioners interested or currently working in the evolving and interdisciplinary areas of data intensive intelligent networking, and many others) new inspirations for their further research and developments.

I am very grateful to the authors for their hard work and sharing so many interesting ideas and results. My sincere thanks go to all reviewers, who have helped us to ensure the quality of the papers. I thank very much the Journal editorial team for a great support throughout the entire publication process.

Joanna Kołodziej
Guest Editor
Institute of Computer Science
Cracow University of Technology, Cracow, Poland
E-mail: jokolodziej@pk.edu.pl
URL: http://www.joannakolodziej.org

Paper

Model-Based Availability Evaluation of Composed Web Services

Mauro Iacono[1] and Stefano Marrone[2]

[1] *Dipartimento di Scienze Politiche, Seconda Universita degli Studi di Napoli, Caserta, Italy*
[2] *Dipartimento di Matematica e Fisica, Seconda Universita degli Studi di Napoli, Caserta, Italy*

Abstract—Web services composition is an emerging software development paradigm for the implementation of distributed computing systems, the impact of which is very relevant both in research and industry. When a complex functionality has to be delivered on the Internet, a service integrator can produce added value by delivering more abstract and complex services obtained by composition of existing ones. But while isolated services availability can be improved by tuning and reconfiguring their hosting servers, with Composed Web Services (CWS) basic services must be taken as they are. In this case, it is necessary to evaluate the composition effects. The authors propose a high-level analysis methodology, supported by a tool, based on the transformation of BPEL descriptions of CWS into models based on the fault tree availability evaluation formalism that enables a modeler, unfamiliar with the underlying combinatorial probabilistic mathematics, to evaluate the availability of CWS, given components availability and expected execution behavior.

Keywords—automatic model generation, Composed Web Services, fault tree, model composition, service availability.

1. Introduction

Quantitative evaluation of characteristics of distributed systems is a difficult task, due to the complexity of the systems and to the need for efficient models evaluation. In many fields, classical mathematical evaluation frameworks have been structured into higher level methods that hide the complexity of the mathematical approach by encapsulating it into graphical (or other kinds of) formalisms, easier to manage, with the aim of enabling the use by non-expert users.

Two classical examples of such high level methods are given by Fault Trees and Stochastic Petri Nets. Fault Trees[1] (FT) is a graphical formalism to model the combined probability of a complex event (called fault, since the technique is typical in reliability/availability engineering), given the interrelation of (statistically independent) basic events, that are characterized by a known (fault) probability, specified by a number of intermediate events that result by elementary conjunctions or disjunction of basic events. Such a high-level method allows an expert in system engineering to exploit the benefits of probability computation in large systems, without the need for explicit knowledge in the field and with the additional benefit that, whatever the model complexity, the modeling process is less error-prone than writing the actual equations and scales better. Stochastic Petri Nets (SPN) [1] is a graphical formalism to model the dynamic behavior of concurrent systems that can be evaluated by Markov chains. In SPN the system is modeled by places, characterized by a marking in terms of tokens that represent a part of the system state, and transitions that modify the markings of the places to which they are connected according to exponentially distributed firing rates. Such a method allows a modeler that has a very good knowledge about the system to represent and evaluate it by Markov chains without the need for being familiar with them. Analogously, other methods can be found in literature enabling different ways the use of complex mathematical tools while hiding their details behind a user-friendly framework.

The stratification and the articulation of modern distributed systems, that are built after a system-of-systems logic, pose a second level complexity problem, that consists in modeling such systems by aggregating (sub-)models in order to cope with the explosion of their extension by exploiting the same compositional logic. The availability of higher level methods is not sufficient to enable efficient modeling processes, so additional conceptual tools are needed to supply proper approaches that can scale to more complex and extended system architectures. In this paper we propose a structured approach for the construction of high level probabilistic availability models (based on exponentially distributed variables) for a very common and spread class of distributed systems, such as Service Oriented Architecture (SOA) compliant systems, that are based on the Service Oriented Computing (SOC) paradigm.

The paper is organized as follows. Section 2 presents a brief introduction to FT and their evaluation; Section 3 introduces the SOA and related problems. Section 4 introduces service composition; Section 5 shows the general approach to obtain availability models from BPEL (Business Process Execution Language) documents and is complemented by the description of supporting tool and an example in Section 6 and Section 7. Final considerations and future works complete the paper.

2. Fault Trees

FT is based on the idea that independent undesired events influence the general behavior of a complex system according to its structure. Events effects combinations are repre-

[1] Fault Trees can also be used for a qualitative analysis of the relevance of the role of basic events with respect to the complex event.

sented by two operations, analogous to OR and AND operators of Boolean algebra and logic networks. Two events are combined by an OR operator if each of their single individual contributions is effective on the system, while they are combined by an AND if their contribution is effective only if they happen both at the same time.

Let $A_1 \dots A_n$, $n \in N$ be n events, statistically independent and with probabilities $P_1 = P(A_1) \dots P_n = P(A_n)$, $Pi << 1 \forall i \in 1 \dots n$ (due to the nature of the application field). From a quantitative point of view, the probability P of the event $A = A_i$ OR $A_j, i, j \in 1 \dots n, i \neq j$, represents the probability of the case in which A_i or A_i happens, eventually simultaneously with the other. Such a probability can be computed as $P_i + P_j P_{ij}$, in which $P_i j$ is the probability of having A_i and A_j simultaneously. If A_i and A_j are mutually exclusive, $P_i j = 0$, but generally, being A_i and A_j independent and $P_i, P_i << 1, P_{ij} << P_i + P_j$ and $P \approx P_i + P_j$ (rare events approximation). The probability of the event $A = A_i$ AND $A_j, i, j \in 1 \dots n, i \neq j$, represents the probability of the case in which A_i and A_j happen simultaneously. Such a probability can be computed as $P_i \cdot P_j$, being A_i and A_j independent.

Both operators can be generalized to any number of operands. The reader will find the analysis of the generalized AND and OR operations and a more thorough introduction to FT in [2]. For the goals of this paper, it is sufficient to consider that, in the given hypotheses, by properly using the operators to aggregate together basic (and/or non basic) events to obtain non-basic events it is possible to form the different levels of a FT, until a single event (top event) is described as complex event aggregation. Given a complete FT, the analysis of its structure gives the analytical expression of the probability of the top event that can be easily obtained by mechanical substitutions whatever the complexity of the tree.

The possibility or representing as logical operations the combination of events allows for the application of boolean algebra to fault trees. Given a FT, it can be described in terms of a Boolean equation that can be transformed applying the theorems of Boolean algebra. Such transformation can result into a reduction of the model, or can be exploited, as in the following, to extend the use of FT to include fictitious events that enable for the expression of more complicated conditions. Besides AND and OR, Boolean algebra defines the NOT operator, that is not present in the description given in this section for FT. The interpretation of the NOT operator applied to an event (A, with probability P) results in the definition of the complementary event (A', with probability $1 - P$), that can be used in the FT.

3. Service Oriented Computing

The Service Oriented Computing paradigm provides a methodological foundation for the design of complex distributed applications by integrating existing components, namely services.

A service is a software component capable of interacting with other services with a loose coupling logic to provide a functionality that is performed by it in complete autonomy. A service is accessible independently from its implementation details and is designed to be reused. Services are commonly implemented by Web service technology that allows services to be discovered, integrated and used on the Internet, by running them on a server (that can run simultaneously more Web services).

Services are meant to be integrated, knowing their interfaces, in Business Processes (BP) or Workflows (WF). Among the several techniques available for such integration, BPEL [3] is the most spread solution and took the role of standard language for services orchestration. Orchestration is one of the two main strategies for service integration and is based on the idea that an application consists in a centrally specified BP or WF that operates all services involved and is run by a specific executor.

BPEL is a language for the specification of orchestrations, based on Extensible Markup Language (XML). A BPEL document can be assumed as the formal description of the desired service orchestration. The integration of services by a service integrator can produce a significant added value if the composed, more abstract, complex service is designed to provide a well defined Quality of Service (QoS), eventually better than the one offered by isolated services. Isolated services can be fine-tuned by reconfiguring their hosting servers to increase performances or availability, but in the case of Composed Web Services (CWS) basic services have to be taken as they are. In this case a reasonable measure is to evaluate the effects of the composition. In order to perform such evaluation, a quantitative analysis is needed. In the next section an analysis methodology that allows availability evaluation of CWS by transforming BPEL descriptions into FT models exploiting proper patterns is proposed.

BPEL definition of a CWS intrinsically describes the relations by which the availability of component basic services influences the availability of the composed one. Systematic analysis of BPEL language elements allows the definition of equivalent FT patterns that represent their composition effects. With this premises, it is possible to obtain an evaluation method for the availability of a CWS given components availability and the expected execution CWS behavior. Such an approach offers a decision support tool for integrators.

Literature shows a great interest in formal verification of BPEL programs, mainly oriented to correctness verification. The most spread approaches are based on high-level analysis methods (both for quantitative and qualitative evaluation) to ease the understanding of such systems. An important contribution is provided by van der Aalst's transformations from BPEL to Petri Nets (PN) to perform liveness verification [4]–[6]. Studies of non-functional properties of BPEL WFs [7]–[10] by means of formal models are mainly oriented to performance and security rather than reliability and availability. The use of FT for reliability and avail-

ability models generation is consolidated [11]–[15]. In FT models have been generated from system descriptions while in a UML system model is used for automatic generation of Dynamic FT.
Recent research trends explore the applications of these techniques to the wider topic of the cloud computing. Some scientific works related to this aspect are [16]–[19].

4. Proposed Approach

Following literature general orientation, a high-level modeling approach to the stated availability modeling problem has been chosen, founded onto Fault Trees as a basic high-level probabilistic tool. According to this choice, the low-level mathematical details (related to FT) will not be considered in the following and the work will focus on high-level transformations and compositions.
The main aim of this paper is the definition of a relationship between BPEL language constructs and fault tree patterns. CWS availability must be assured in order to provide a sustainable level of QoS. A failure is an event that occurs when the delivered service deviates from correct service in value or time [20]. In this paper a CWS failing is considered if it does not reply at all to requests (delays are not relevant).
The authors apply model-driven techniques to generate formal models of critical services. In particular model-to-model transformations are applied in order to automate the generation of availability models of CWS. The compositional approach that will be used is supported by the main results of compositional failure analysis [21], [22], according to which system failure models can be constructed from component failure models using a process of composition, For a further introduction to automated safety analysis and reuse the reader can refer to [23].
The main problem in evaluating CWS availability is due to distribution and heterogeneity. Assumed the CWSs as bug-free software components, here we only consider faults due to their distributed nature and the dependence of provided service from requested ones, i.e. hosting hardware, messages delivery, timeout, network faults. Thus, faults mainly come from invoked services that run on remote servers. These faults can be reasonably represented by stochastic models. Assuming that remote services can fail and local ones generally cannot, not every fault occurrence brings CWS to a failure since BPEL can mask faults by means of Fault Handlers (FHs) and offers choice constructs. The effective contributions of faults to CWS availability are determined by the WF business logic, that describes the invocation patterns, and by its workload profile (that gives e.g. the estimated branching probability in a choice or average number of activations in a loop). Note that while for components embedded in a system nature and frequency of their failures are known or at least estimable, components of a CWS are remote services that cannot be examined or stress tested, since they do not belong to the same organization. Anyway, a coarse grain stochastic model of remote service failures can be obtained by logs or tests combined with QoS parameters declared by the providers.
In the following the authors propose FT patterns for some BPEL elements. Since this set is not complete the proposed approach must be considered an ongoing work. FTs have been chosen because of their handiness and because more complex modeling tools (multi-state variables, complex repair mechanisms and dynamic issues) are not needed at the state. For each of these constructs, the authors analyze with a top-down perspective how faults of inner activities propagate to construct failures.
Sequence is the simplest BPEL structured activity, and represents the execution of a temporally ordered sequence of activities, each of which is started only if and when the previous one is completed. A Sequence fails if at least one of the (remote) activities fails. Assuming a Sequence of A and B activities, Fig. 1a depicts the corresponding FT model. In this model A and B are characterized by their unavailability. It is important to stress that A and B are depicted as generic middle events since they can be recursively translated by another pattern. Moreover some of them can also be local activities and can be considered impossible events (unavailability equal to 0). Fig. 1b defines the translation of If construct, that branches the execution into two mutually exclusive activities (one of which can be an empty activity) according to a Boolean condition. As activities in then and else branches are mutually exclusive it can be stated that a failure of the If is possible if A fails when A is activated (events that occurs with probability pTH) or B fails when the else branch is chosen (event that occurs with probability $pELSE = 1 - pTH$). The translation is obtained by the introduction of two virtual events pTH and $pELSE$, that account for these considerations. Figure 1c introduces the FT pattern for Fault handler construct, that executes an activity if the related construct fails. As the whole construct fails if both the handled activity S and the catch process (Catch) fail, the best way to translate it into FT is a subtree with an AND gate between the fault events. Figure 1d depicts behavior of BPEL loops (Foreach, While), that repeat a certain activity a given number of times or until a certain condition is satisfied, from the point of view of unavailability. Assuming a loop of an activity S, if we evaluate (from CWS workload profile estimation) the mean number of times the loop is called, loop fails if at least one of these calls fails[2]. BPEL Flow describes the parallel concurrent execution of a certain number of activities. A Flow of $1 \dots n$ fails in the same way as loops, so Fig. 1e represents its FT pattern. The Link construct needs a deeper discussion. When a link is present in a flow construct, two activities are involved: a link source and a link target. The execution of the target activity depends on the termination condition of the source activity. While source activity failure modes are not affected by this construct, target activity execution may change according to ingoing links status and several conditions that characterize its behavior. Due

[2]This can be written under hypothesis of independence of invoked service.

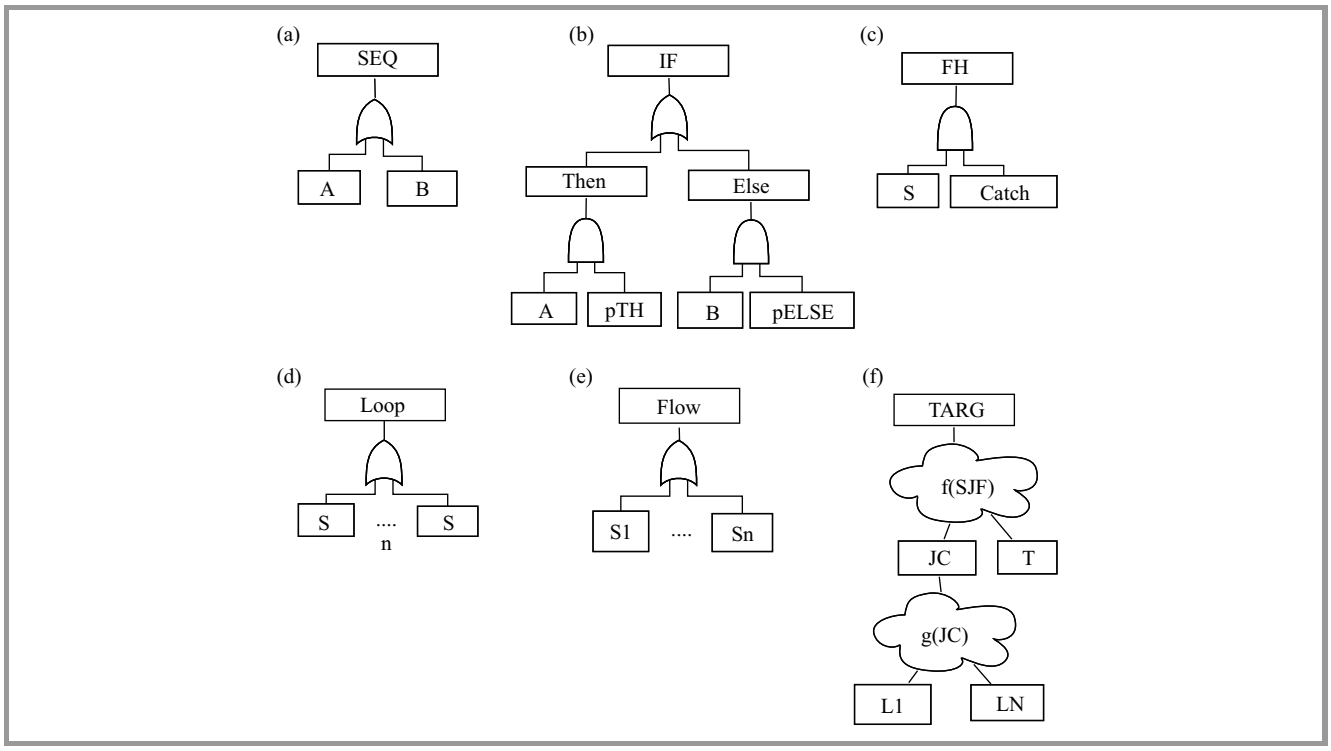


Fig. 1. Fault Tree patterns of relevant BPEL constructs.

to these reasons a different FT pattern must be used. It represents the translation of activity in flows (T) that are target of one or more links (see Fig. 1f). The parameters that influence WF control flow and that directly affect the nature of f and g functions in Fig. 1f, are: *joinCondition* (*JC*) (a logic predicate based on link conditions $1 \dots n$; as this predicate can evaluate to true, target activity is allowed to start) and *suppressJoinFailure* (*SJF*) (when this flag is true, a failure on joinCondition is suppressed, target activity does not start and the fault does not propagate through WF control flow). Otherwise, the target activity may fail on joinCondition failure or on an inner failure.
Such considerations can be summarized into the following equation (also see Table 1):

$$TARG = SJF \cdot T \cdot JC + !SJF \cdot (T + !JC),$$

where ! is the NOT operator, $\cdot$ is the AND operator, $+$ is the OR operator, and where *SJF* is the suppressJoinFailure flag, *JC* is the truth of joinCondition and T is the fault event of target activity.
According to such equation, we can state that:

- if suppressJoinFailure is true, failure of link target can be written as the conjunction of the failure of activity and the success of joinCondition so f is an AND gate while g implements the joinCondition logic predicate,
- if suppressJoinFailure is false, failure of this link target can be written as the disjunction of the failure of activity and the failure of joinCondition so f is an OR gate while g implements the negation of joinCondition logic predicate.

Table 1
Truth table for link target activity

Link Target	SJF	JC	T
0	0	0	0
1	0	0	1
1	0	1	0
1	0	1	1
0	1	0	0
1	1	0	1
0	1	1	1

In next sections these patterns are applied to evaluate and compare two example CWS.

5. Support Tools

To support the proposed methodology a tool for the automatic translation of a BPEL file into an analyzable FT has been developed. Moreover the tool takes into account some information that can not be specified into the BPEL file (e.g., probability of then-else branches in if constructs, failure rates of Invoke activities). These data are passed to the tool by a simple properties file. The steps implemented by the tool are depicted in Fig. 2. The tool has been developed in Java and relies on SHARPE [24] for the analysis of generated fault tree.
This is the workflow of the tool in presence of simple services, i.e., where there is one single Web service. In presence of more services, during the phase of properties file

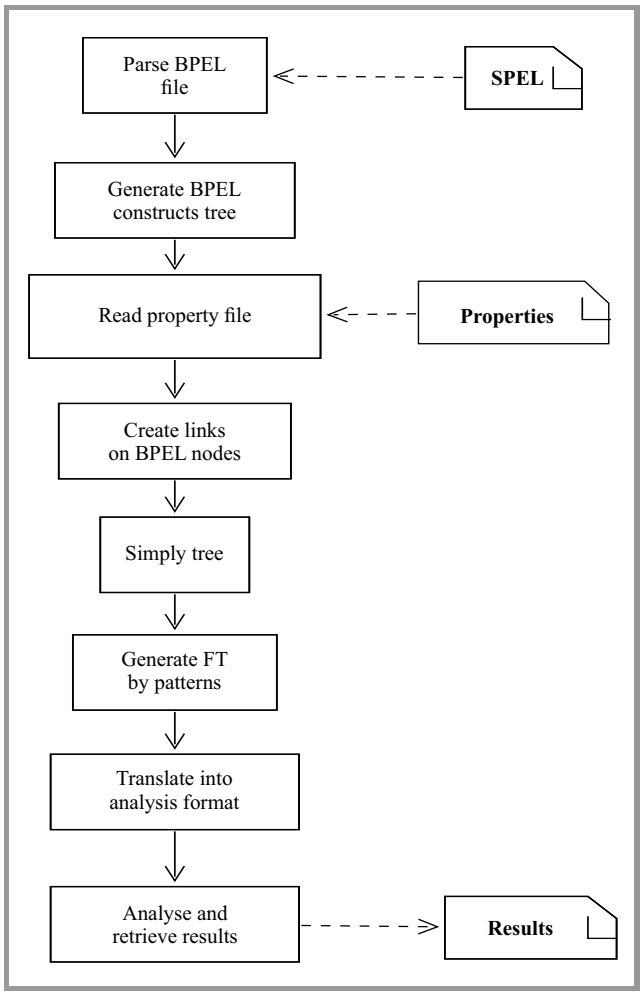


Fig. 2. Tool processing steps.

reading the BPEL constructs tree is explored. Its leaves, that are Invokes constructs, are searched in properties file. In case of an Invoke that is related to another BPEL implemented Web service, the entire analysis process is recursively repeated generating a series of Fault Trees hierarchically organized. Moreover, during the analysis phase, Fault Trees are solved from bottom to up in order to exploit modular analysis of such models.

6. Case Study

In this section proposed FT patterns to the evaluation of availability of a BPEL example WF is applied. The chosen case study is an agri-food information and tracking system. Agri-food information and tracking systems require that information about goods is registered and verified for every item that is produced or transformed in the market. Moreover data vaults are needed in order to store historical data about several aspects of goods, i.e., origin, storage, transportation, composition, processing data. Such registration has to be certified by third parties, eventually authorized and supervised by public authority if requested by the law.

The system to be analyzed requests the registration and logs every request attempt and confirmation on a centralized logging system that is shared with all other dedicated information systems of the same company. The structure of the system is shown in Fig. 3a. The system is composed by a CWS that executes the described orchestration and two subsystems, Log (based on two remote logging services) and Reg (based on three remote registries). Figure 3b describes the high-level message flow performed by the system. The CWS uses the subsystems by requesting a logging operation (Pre with PAck response), the registration (Save with a SAck response) and another logging operation (End with PEnd response).

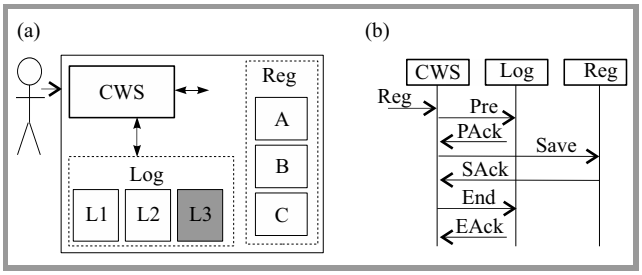


Fig. 3. UML description of case study.

The CWS BPEL implementation can be represented as in Fig. 4.

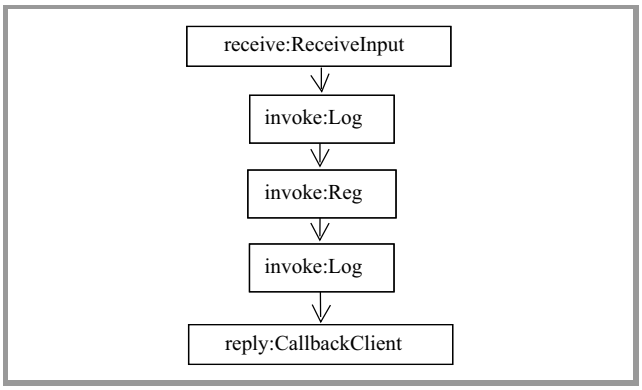


Fig. 4. CWS BPEL implementation.

The Reg subsystem is implemented by another CWS that uses 3 external (geographically distributed) certification services in parallel. Requests to services are cached locally to minimize accesses, and are then performed when the cache is full. Information about the requests that are ready to be sent, cached or processed, are checked and the calculated checksum is logged. Requests arrive in batches of 5 and it is tolerated 1 processing problem per batch.

Processing of batches is implemented by a BPEL Foreach. For each item, the local WS managing the cache is invoked to evaluate if the request can be cached (and just the logging has to be performed) or data has to be sent to registries (in this case, by invoking local services results of registration operations are validated, operations are logged

and the cache is reset). The interaction with the registries is executed by a BPEL flow.

To show the effectiveness of the approach, two versions of the CWS are presented and examined, with slight differences. The two variants are depicted in Fig. 5 (a simple version) and in Fig. 6 (the fault tolerant version).

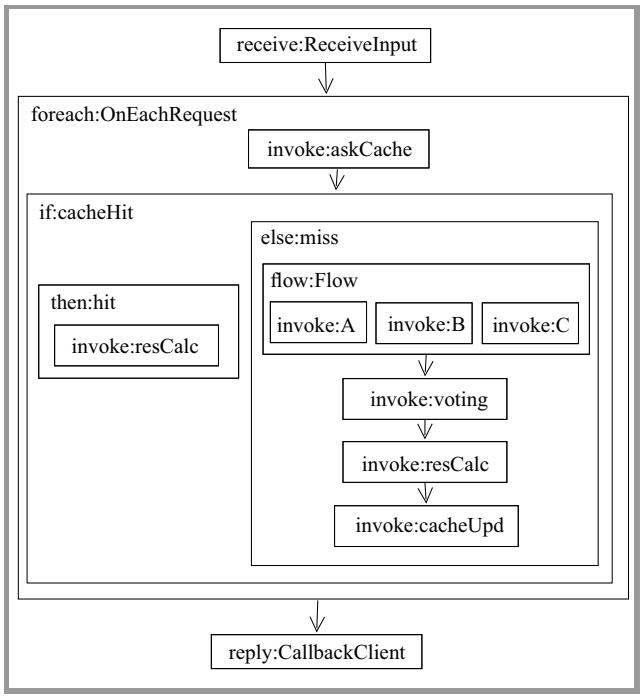


Fig. 5. Simple version of REG service.

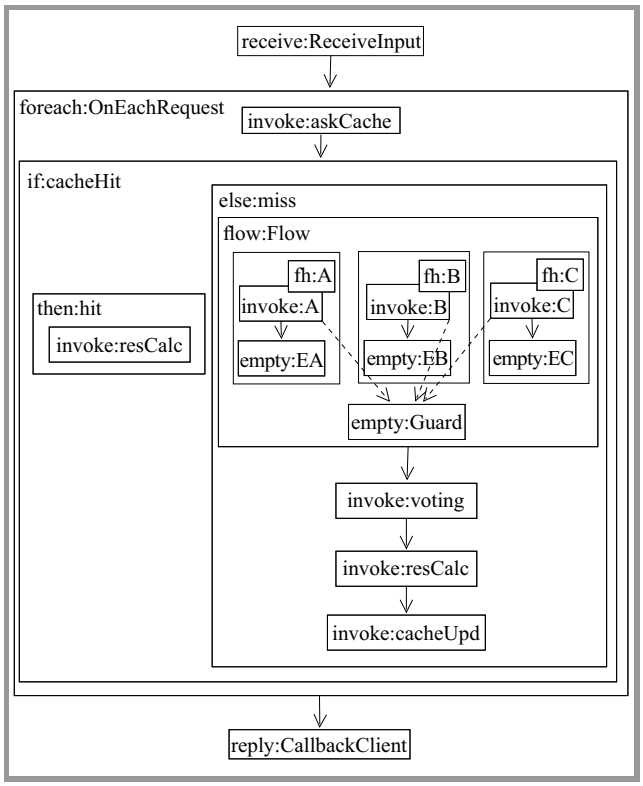


Fig. 6. Fault tolerant version of REG service.

In the first, a fault in one of the service invocations causes a fault of the Flow activity and of the CWS. The second one is designed to complete successfully if at least one of the parallel invocations is successful[3] and join failures are not suppressed[4]. To obtain the same final result, in this implementation failed registrations are externally rescheduled as off-line background operations by the Fault Handlers, if at least one external registry recorded the information so that it becomes public and official.

The second version of the CWS is clearly designed to obtain an improvement in the availability of the system, due to the introduction of fault tolerance in the registration. But how much more available is the second version?

In order to analyze availability of the two implementations, only relevant (fault prone) constructs are to be considered. The resulting FTs differ in the branch that represents the Flow construct, and are represented in Fig. 7. The askCache, resCalc, voting and cacheUpd activities are considered to be fault prone. The three remote invocations (namely A, B and C) are obviously fault prone. The common part of the FT is in Fig. 7a. In the first case, the availability of the Flow depends on the availability of A, B and C as in Fig. 7b. In the second case, by simply applying the patterns Fig. 7c is obtained. Anyway, some considerations are useful to obtain the solution in Fig. 7d, that is the correct solution. At first, Guard is not fault prone and contributes with a null fault probability to the composition, and A, B and C do not give contribution because of the presence of their Fault Handlers. Moreover a Link L_x is true when the related Invoke X is successful, so the probability of the event NOT(L_x is true) is the fault probability of X and $\mathrm{NOT}(\mathrm{OR}(L_a, L_b, L_c)) = \mathrm{AND}(A, B, C)$, that is finally the only contribution of the Flow to the FT.

According to considerations previously made, we assume that: service failure rates are $10^{-7}h^{-1}$ for *askToCache*, *resCalc*, *cacheUpdate* and *CallbackClient*, $10^{-2}h^{-1}$ for A and B, $5 \cdot 10^{-3}h^{-1}$ for C, $10^{-6}h^{-1}$ for voting. The authors are also assuming that the probability of execution of the hit then branch is 0.3. With these parameters, the two variants have a CWS MTTF of 1978000 and 2017400 hours. FT models have been evaluated by the SHARPE tool [24]. The Log subsystem is implemented by a third CWS that uses 2 external (geographically distributed) logging services in parallel. The two services are run by the company, but in a remote data center. They are config-

[3]This is obtained inserting three Empty activities in sequence with the three invocations and a fourth Empty activity, that is the destination of three Links originating in the three Invoke activities, true if the Invoke was successful. This activity is executed if the logical OR of the three Links is true. Another solution without the three Empty activities is possible, but due to ambiguities in the standard it could be not correctly supported by all BPEL interpreters. Here sequences are used to ensure that outgoing Links are set to false in case of faults.

[4]Faults generated by an Invoke activity are masked by a Fault Handler to prevent the propagation to the Flow activity, so that it, and eventually the CWS, will fail only if none of the three parallel Invoke activities is successful. Moreover Links from invoked services and a central consensus activity has been introduced in order to evaluate failures of one or more remote activities.

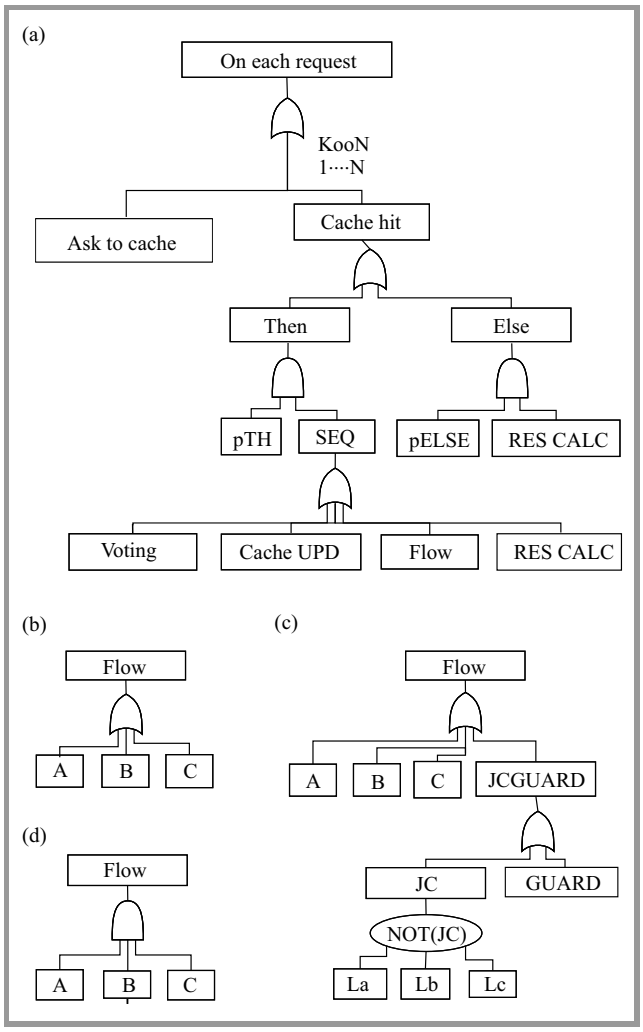


Fig. 7. Generated Fault Trees of CWSs

ured as mirrors and store the same information. Requests to services are implemented by a BPEL flow. Two versions of the CWS are presented: the first requires both the registrations to be successful in order to have a successful completion of the Log CWS (Fig. 8). The second is successful if at least one of the two registrations is successful, as a BPEL Fault Handler instructs the failed mirror to automatically retry the registration according to the other as soon as possible (Fig. 9).

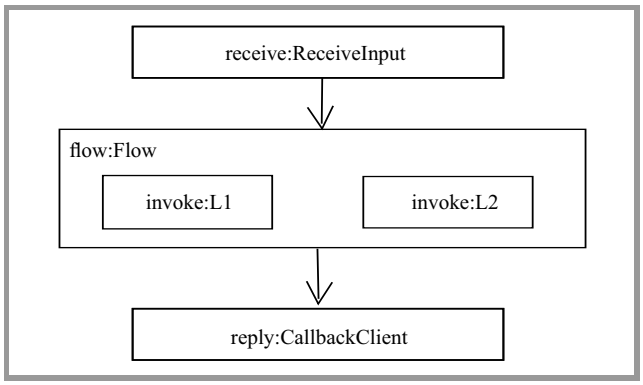


Fig. 8. Simple version of Log service.

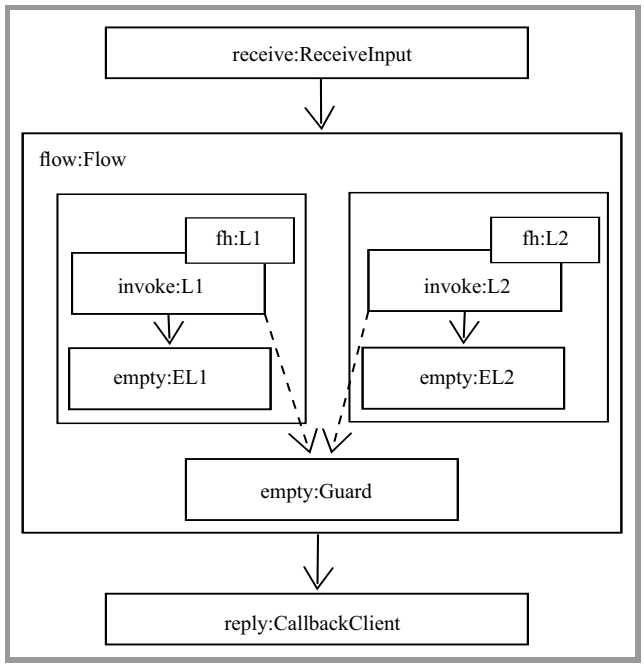


Fig. 9. Fault tolerant version of Log service.

The structure of the two alternative implementations is similar to that of the cases seen for the Reg subsystem, so no further comment will be given here.

Given the compositionality of the approach, the main CWS availability can be obtained using the results of the analyses performed on the other CWS. Four cases can be obtained by combining the two alternative implementations for each subsystem. The general FT for the CWS can be obtained by considering that two subsequent invocations of the Log CWS are completely independent, since they are enclosed in a BPEL Sequence. According to the related pattern, the CWS FT is described in Fig. 10. The complete FTs for the four cases are omitted.

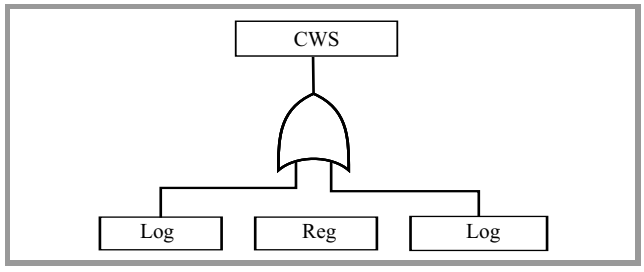


Fig. 10. Fault tolerant version of Log service.

The parameters used in our analysis are summarized in Table 2. Numerical values are failure rates and are expressed in h^{-1}.

According to such parameters, Table 3 describes the overall availability (MTTF) of composed Web service according to the four different configurations of Reg (on rows) and Log (on columns) services.

Table 2
Processes parameters

Parameter	Value
Reg service	
askToCache	10^{-7}
hit	0.8
resCalc	10^{-5}
remoteA	$5 \cdot 10^{-4}$
remoteB	$5 \cdot 10^{-4}$
remoteC	$5 \cdot 10^{-4}$
voting	10^{-9}
cacheUpd	10^{-7}
callbackClient	10^{-8}
Log service	
Log1	10^{-7}
Log2	10^{-7}
callbackClient	10^{-8}

Table 3
MTTF overall analysis

Log Reg	Simple [h]	Fault tolerant [h]
Simple	829530	1241500
Fault tolerant	836400	1256900

One can note that, since the Log process is called twice in the overall process, its influence is stronger so passing from a simple to a complex implementation of this process has a great effect on overall availability. On the other hand the adoption effect of fault tolerant version of Reg process does not give a great advance on overall availability. Such considerations are now not only intuitive and based on qualitative consideration but, by means of the described methodology and tool, can be supported by numerical data.

7. Conclusions and Future Works

In this paper a first step in the translation of a BPEL WF into a formal model in order to evaluate its availability is proposed. For this purpose a FT model is generated having as basic events invoked services whose availability can be measured by black box approaches. The structure of the FT is given by the BPEL WF by applying FT patterns. The effectiveness of proposed approach has been shown by evaluating and comparing, by means of a tool prototype that supports the translation, the availability of two similar BPEL examples, one of which introduces fault masking constructs.

Next steps in this activity will include a further validation of proposed approach by experiments and/or comparisons with models obtained by other formal tools (e.g. Generalized Stochastic Petri Nets). On the other side the authors will study the possibility to include quantitative information, provided at the moment in a separate file, into BPEL, proposing some extension of the language and providing supporting methodologies and tools.

References

[1] G. Balbo, "Introduction to stochastic petri nets", in *European Educational Forum: School on Formal Methods and Performance Analysis*, E. Brinksma, H. Hermanns, and J.-P. Katoen, Eds. *LNCS*, vol. 2090 pp. 84–155. Springer, 2000.

[2] W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasl, *Fault Tree Handbook*. U.S. Nuclear Regulatory Commission, Washington, DC, 1981.

[3] A. Alves *et al.*, "Web Services Business Process Execution Language Version 2.0 (OASIS Standard)", 2007 [Online]. Available: http://docs.oasis-open.org/wsbpel/2.0/wsbpel-v2.0.html

[4] W. M. P. van der Aalst, "The application of Petri nets to workflow management", *The J. Circ. Syst. Comp.*, vol. 8, no. 1, pp. 21–66, 1998.

[5] W. M. P. van der Aalst, "Making work flow: On the application of Petri nets to Business Process Management", in *Proc. 23rd Int. Conf. Appl. Theory of Petri Nets*, Adelaide, Australia, 2002. *LNCS*, vol. 2360, pp. 1–22. Springer, 2002.

[6] J. Dehnert and W. M. P. van der Aalst, "Bridging the gap between business models and workflow specifications", *Int. J. Cooper. Inform. Sys.*, vol. 13, no. 3, pp. 289–332, 2004.

[7] J. Xia and C. K. Chang, "Performance-driven service selection using stochastic cpn", in *Proc. IEEE John Vincent Atanasoff Int. Sym. Modern Comput. JVA 2006*, Sofia, Bulgaria, 2006, pp. 99–104.

[8] K. Bhargavan, C. Fournet, and A. D. Gordon, "Verified reference implementations of ws-security protocols", in *Proc. 3rd Int. Worksh. Web Services and Formal Methods WS-FM 2006*, Vienna, Austria, 2006, pp. 88–106.

[9] I. Kim and D. Biswas, "Application of model checking to axml system's security: A case study", in *Proc. 3rd Int. Worksh. Web Services and Formal Methods WS-FM 2006*, Vienna, Austria, 2006, pp. 242–256.

[10] *Web Services and Formal Methods, Third International Workshop, WS-FM 2006 Vienna, Austria, 2006, Proceedings*, M. Bravetti, M. Núñez, and G. Zavattaro, Eds., *LNCS*, vol. 4184. Springer, 2006.

[11] P. Liggesmeyer and M. Rothfelder, "Improving system reliability with automatic fault tree generation", in *Proc. 28th Ann. Int. Symp. Fault-Tolerant Comput. FTCS '98*, Munich, Germany, 1998, p. 90.

[12] J. P. Ganesh and J. B. Dugan, "Automatic synthesis of dynamic fault trees from uml system models", in *Proc. 13th Int. Symp. Softw. Reliab. Engin. ISSRE 2002*, Annapolis, MD, USA, 2002.

[13] A. Bobbio *et al.*, "Comparison of methodologies for the safety and dependability assessment of an industrial programmable logic controller", in *Proc. Eur. Safety and Reliab. Conf. ESREL 2001*, Turin, Italy, 2001.

[14] F. Flammini, N. Mazzocca, M. Iacono, and S. Marrone, "Using repairable fault trees for the evaluation of design choices for critical repairable systems", in *Proc. 9th IEEE Int. Symp. High-Assur. Syst. Engin. HASE 2005*, Heidelberg, Germany, 2005, pp. 163–172.

[15] D. Codetta Raiteri, M. Iacono, G. Franceschinis, and V. Vittorini, "Repairable fault tree for the automatic evaluation of repair policies" in *Proc. Int. Conf. Dependable Syst. Netw. DSN 2004*, Florence, Italy, 2004, pp. 659–668.

[16] L. Wang, "Machine availability monitoring and machining process planning towards cloud manufacturing", *CIRP J. Manufac. Sci. and Technol.*, vol. 6, no. 4, pp. 263–273, 2013.

[17] R. Aoun *et al.*, "Towards an optimized abstracted topology design in cloud environment", *Future Gener. Comp. Syst.*, vol. 29, no. 1, pp. 46–60, 2013.

[18] M. Alrifai, T. Risse, and W. Nejdl, "A hybrid approach for efficient Web service composition with end-to-end QoS constraints", *ACM Trans. on the Web*, vol. 6, no. 2, 2012.

[19] E. Barbierato, M. Iacono, and S. Marrone, "PerfBPEL: A graph-based approach for the performance analysis of BPEL SOA applications", in *Proc. 6th Int. ICST Conf. Perform. Eval. Methodol. and Tools*, Cargese, Corsica, France, 2012, pp. 64–73.

[20] A. Avizienis, J. C. Laprie, and B. Randell, "Fundamental concepts of dependability", Res. Rep. no. 1145, LAAS-CNRS, Apr. 2001.

[21] C. L. Heitmeyer, J. Kirby, B. G. Labaw, M. Archer, and R. Bharadwaj. "Using abstraction and model checking to detect safety violations in requirements specifications", *IEEE Trans. Softw. Eng.*, vol. 24, no. 11, pp. 927–948, 1998.

[22] J. D. Reese and N. G. Leveson, "Software engineering", in *Proc. 19th Int. Conf. Software Engin.*, Boston, MA, USA, 1997, pp. 250–260.

[23] I. Wolforth, M. Walker, Y. Papadopoulos, and L. Grunske, "Capture and reuse of composable failure patterns", *Int. J. Critical Comp.-Based Syst. IJCCBS*, vol. 1, no. 1/2/3, pp. 128–147, 2010.

[24] C. Hirel, R. A. Sahner, X. Zang, and K. S. Trivedi, "Reliability and performability modeling using sharpe 2000", in *Proc. 11th Int. Conf. Comp. Perform. Eval. Model. Tech. Tools TOOLS 2000*, Schaumburg, IL, USA, 2000, pp. 345–349.

Mauro Iacono is a tenured Assistant Professor in Computing Systems. He published around 50 peer reviewed scientific papers and has served as chairman, committee member and referee for many conferences, and as guest editor, editorial board member and referee for several journals. His research is mainly centered on the field of performance modeling of complex computer-based systems, with a special attention for multiformalism modeling techniques, and applications to critical systems and infrastructures, Big Data architectures and dependable systems.
E-mail: mauro.iacono@unina2.it
Dipartimento di Scienze Politiche
Seconda Università degli Studi di Napoli
Viale Ellittico, 31
81100 Caserta, Italy

Stefano Marrone is an Assistant Professor in Computer Engineering at Seconda Università di Napoli, Italy. His interests include the definition of model driven processes for the design and the analysis of transportation control systems, complex communication networks and critical infrastructures. He is currently involved in research projects with both academic and industrial partners.
E-mail: stefano.marrone@unina2.it
Dipartimento di Matematica e Fisica
Seconda Università degli Studi di Napoli
Viale Lincoln, 5
81100 Caserta, Italy

Paper

FIM-SIM: Fault Injection Module for CloudSim Based on Statistical Distributions

Mihaela-Catalina Nita, Florin Pop, Mariana Mocanu, and Valentin Cristea

Faculty of Automatic Control and Computers, Computer Science Department, University Politechnica of Bucharest, Bucharest, Romania

Abstract—The evolution of ICT systems in the way data is accessed and used is very fast nowadays. Cloud computing is an innovative way of using and providing computing resources to businesses and individuals and it has gained a faster popularity in the last years. In this context, the user's expectations are increasing and cloud providers are facing huge challenges. One of these challenges is fault tolerance and both researchers and companies have focused on finding and developing strong fault tolerance models. To validate these models, cloud simulation tools are used as an easy, flexible and fast solution. This paper proposes a Fault Injector Module for CloudSim tool (FIM-SIM) for helping the cloud developers to test and validate their infrastructure. FIM-SIM follows the event-driven model and inserts faults in CloudSim based on statistical distributions. The authors have tested and validated it by conducting several experiments designed to highlight the statistical distribution influence on the failures generated and to observe the CloudSim behavior in its current state and implementation.

Keywords—cloud simulation, continuous distributions, discrete distributions, fault injector.

1. Introduction

Cloud computing is in this moment the most used computational technology with implementations from private in-house environments (private clouds) to public clouds offered commercially to the customers and all sharing the same characteristics providing reliable services, fault tolerant hardware, and scalable computational power [1]. Born from the idea of a system that can serve seamlessly and transparently the end user, the cloud system architecture needs to be able to act like a reliable infrastructure with a high availability and degree of resource integration within.

In this context, one of the top things that a cloud provider must have in mind is the fault tolerance assurance. The literature provides various fault tolerance techniques [2], [3] and both research institutes and companies are still digging for finding complex and better solutions. The question rising at this moment is "how to better validate these models?" One of the most popular methods is cloud simulation based on a dedicated tool. A simulation represents an environment in which a system that behaves similarly to another system, but is implemented in an entirely different way [4]. It provides the basic behavior of a system but it may not reproduce the exact output as the real one. It is important to distinguish between simulation and emulation, which presents a system, that behaves exactly like another system, and it is expected to have the same output as the real one. In other words, it represents a complete replication of another system, but operating in a different environment. The cloud simulation top benefits are: flexibility, easy to customize and low cost [5], [6]. Designing, developing, testing and afterwards redesigning and retesting on the cloud can be expensive.

For this work, the authors have chosen CloudSim, a widely used and easy to integrate simulation framework together with CloudReports a graphical extension for CloudSim. The aim of this work is to create a module that can automatically inject faults into CloudSim order to verify its behavior in case of a fault. The questions rising when designing such a module are: when to inject a fault? Where to place the fault? How much time does it take?

For answering the first question, there are three different kinds of simulation systems: continuous, discrete and discrete-event systems. A continuous system modifies its state continuously in time. On the other hand a discrete system is observed only at some fixed regular time points. A real life analogy would be the health exam that we are taking every six months. In a discrete-event system, its state is determined by random event times t_1, t_2 etc. A continuous system will determine the time until the first failure, but a discrete system will found out the period between two failures. In our tool we considered both discrete and continuous distribution based event generator. The fault injection module will help the end user in determining the system reliability and drawing conclusions like: the failure caused by a network bottleneck will respect a Weibull distribution with parameters $\beta = x$ and $\theta = y$ hours. By having these variables one can find out the system reliability.

Regarding the second question, the following type of failures is considered: host failures (memory and PEs failure), VM creation failures, and high level failures like cloudlets.

For the third question the following assumptions have been made: the affected resources will be down during the rest of the simulation period and the VM creation failure for a specific host will be activate only for the moment when the event is introduced into the system.

In this context, this paper proposes a Fault Injector Module for CloudSim tool (FIM-SIM) for helping the cloud developers to test and validate their infrastructure. FIM-SIM follows the event-driven model and inserts faults in CloudSim based on statistical distributions.
This paper is structured as follows. Section 2 covers the critical analysis of exiting work, focusing on fault tolerance and various cloud simulation tools, together with CloudSim, the chosen solution. Section 3 describes the model of proposed simulation model, the statistical distribution used, system architecture and interaction with the other modules. Section 4 describes the experimental setup and results obtained. The paper ends with conclusion and future work, presented in Section 5.

2. Related Work

In order to test a system's capabilities and availability, his response in exceptional situation is analyzed and monitored [7]–[9]. Fault injection [10] is the key operation for testing and creating these abnormal situations for a system, offering him as input faulty states. The motivation around this kind of testing where the system is intentionally exposed to unwanted scenarios is that real life events are hard to collect and preferable to be avoided. With these techniques we can understand failures and validate the system availability to extreme scenarios [11].
The most common failures are: crash, time out of response, incorrect response message, arbitrary fails (byzantine failure) [12]. Beside the above classification of commonly failures we still have the hardware fails encounters, which are most of the times bypassed by redundant components of server's key items. Here it's worth to mention disks failure, network connectivity issues (network overload or adapter failure) and not least the environment incidents (fire, floods, earthquakes, etc).
To define the server availability and viability, the industry uses most of the times the indicator Mean Time To Failure (MTTF). This parameter is defined as the up-time divided by the number of failures. As a short example in cloud storage, is a Google study in which the availability propriety of a storage system is 4.3 MTTF and the most failure events (approx. 10%) last longer than 15 minutes [13]. As a result, many failures are correlated with each other and can chain to a series of critical events that can take down the system.
The arbitrary fail is by far the most difficult failure to predict due to its apparently randomness. The fault tolerant technique, designed to prevent such type of failures, is inspired by the Byzantine Generals Problem [14]. In this case, the system's components will fail in arbitrary ways and the overall system may respond in an unpredictable way unless is designed to be fault tolerant. We can take a logical example of 3 functions in which the result of the first function it will serve as an input for the second function and so on. If the first output of the first function it will have even a small round-off error this will propagate and create a much larger error until the values produced are worthless. This is a typical case of a small deviation that can cause a very powerful impact over the whole system. In real life we had two such examples: Amazon S3 was down for several hours due to a single-bit hardware error propagated through the entire system and Google – due to a code type error (";" misplaced) system was propagating no availability through servers around the world. In this case, the fault injection will help the cloud provider by injecting into the system several events, following a mathematical distribution, with the main target of failing several components, for example, the create virtual machine module.

In [8] an Adaptive Fault Tolerance in real-time cloud computing is proposed. This scheme tolerates the faults on the reliability basis of each computing node. A virtual machine is selected for computation if it has a higher reliability level and can be removed, if does not perform well for real time applications. There are two main types of nodes: a set of virtual machines, running on cloud infrastructure, and an adjudication node. The virtual machine contains the real time application algorithm and an acceptance test for its logical validity. On the adjudicator, there is a time checker, reliability assessor and some decision mechanism modules. The location of adjudication node depends on the type of the real time applications and the scenario in which they are used. It can be a part of the cloud infrastructure or can be a part of the user infrastructure. Generally, it is placed near to the sensors, actuators, and submission node.

The proposed Fault Injector Module will also help the above proposed adaptive fault tolerance module, by offering the context of determining the reliability of a resource in a certain scenario [15]. A critical analysis of existing tools for implementing fault tolerance techniques is presented in Table 1.

Cloud computing, as the successor of the grid systems, has all the attributes of the parallel system gathering a collection of virtualized nodes, dynamically provisioned and presented as one unified computing resource. The resources are allocated through the rules of service level agreements and negotiated between the service provider and consumer. Analyzing and testing the performance of a distributed system such as a public cloud has become more of a challenge. Cloud computing environments are offering a dynamically large pool of resources, configurable and optionally rebalanced. A full test of a public cloud can result in a significant cost and time, with the possibility to go to thousands of processing core involved. The most feasible option to test the service discovery performance, scheduling, monitoring, etc., of these systems without a scalable environment is a simulation tool. This tool will need to be able to reproduce the relevant tests and behavior of a real system.

iCanCloud is a modeling and simulation platform for cloud computing systems. The main purpose of the platform is to provide to the user useful information about the cost of given applications ran on the cloud specific hard-

Table 1
Existing tools for implementing fault tolerance techniques

Fault tolerance techniques	Policies	System	Programming framework	Environment	Fault detected	Application type
Self-healing, job migration, replication	Reactive/ Proactive	HAProxy	Java	Virtual machine	Process/ node failures	Load balancing/ Fault tolerance
Check-pointing	Reactive	SHelp	SQL, Java	Virtual machine	Application failure	Fault tolerance
Check-pointing, retry, self-healing	Reactive/ Proactive	Assure	Java	Virtual machine	Host, Network failure	Fault tolerance
Job migration, replication, Sguard, Resc	Reactive/ Proactive	Hadoop	Java, HTML, CSS	Cloud environment	Application/ node failures	Data intensive
Replication, Sguard, task resubmission	Reactive/ Proactive	Amazon EC2	Amazon Machine Image, Amazon Map	Cloud environment	Application/ node failures	Load balancing/ Fault tolerance

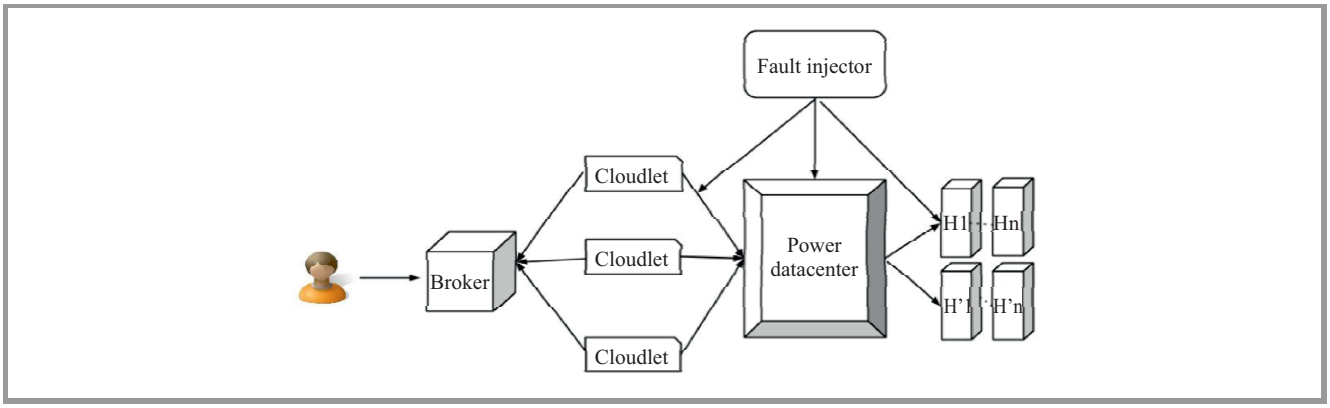


Fig. 1. FIM-SIM model system architecture.

ware and predict the trade-offs between cost and performance [16].

GreenCloud is packet-level simulator with the focus on the cloud communications, cloud computing data centers module with energy-aware modules. Also as a focus in data centers for energy saving, the tool is offering a detailed modeling for energy consumption by the IT equipment: computing nodes, network infrastructure and communication links [17].

The chosen simulation tool for proposed solution is CloudSim. The modularity of the tool made it the perfect choice. Each component is implemented as a Java class and can be extended very easy. CloudSim can provide an extensible simulation framework generalized by the main properties of the cloud concept [18].

3. FIM-SIM: Fault Injector Module for CloudSim

This section presents the proposed solution by providing further details on the implementation and the architecture.

3.1. FIM-SIM Model

The authors have developed a run-time, event driven fault injection module for cloud simulation. At random moments of time [19] it will generate an event and it will simulate a failure in the cloud system.

Its architecture is described in Fig. 1. We can notice that the Broker will send one or more cloudlets to the Datacenter and the Datacenter will schedule it, according with a Scheduling Policy, on a host. Each entity of CloudSim can send a certain event to another. In this case, the Fault Injector will send a message to the Datacenter and it will notify it about any failures that have occurred in the system. Sending the failure event is based on the following command:

```
sendNow(dataCenter.getId(),
        FaultEventTags.HOST_FAILURE,
        host);
```

One of the main characteristics of this fault injector module is the fact that it generates the events based on statistical distribution, both discrete and continuous. The fault injector is a thread that will be present for the whole simulation

period and it will try to insert faults based on a statistical method for generating random numbers.
For example at the moment t, the inject function will do the following:

```
mean = statisticalDistrbution.mean;
x = statisticalDistrbution.sample();

if (x > mean) {
    generateFault();
} else {
    Continue;
}
```

3.2. Statistical Distributions used by FIM-SIM

This section presents various statistical distributions: the ones that already exist in CloudSim plus another one – Poisson. It also presents the key concepts, implementations and further details for cloud simulation, fault tolerance and various simulation tools. We describe here only the Weibull, Poisson and Pareto distributions. The other ones used in our model are:

- Exponential distribution, used for analysis of the Poisson process,
- Uniform distribution (used very well in situation of risk analysis but also in algorithms for random generation of numbers due to its propriety of given equal probability over a known range for continuous distribution);
- Gamma distribution – model exponentially sums of random variables;
- LogNormal distribution – Galton distribution, used very often for reliability modeling of the application in order to achieve fault tolerance scenarios)
- Lomax distribution – Pareto 2 distribution, sed as an alternative to the exponential distribution with data heavily tailed;
- Zipf distribution, a discrete distribution with many applications in linguistics and modeling rare events.

Weibull distribution – for life data analysis, it is the most used statistical model [20]. As a continuous probability distribution, it is used in continuous simulations with application in economic forecasting, weather forecasting and all problems based on the solution of time dependent partial differential equations. The probability density function of a Weibull random variable is:

$$f(x;\lambda,k) = \begin{cases} \frac{k}{\lambda}\left(\frac{x}{\lambda}\right)^{k-1} e^{-(x/\lambda)^k} & x \geq 0, \\ 0 & x < 0, \end{cases} \tag{1}$$

where λ is the scale parameter and k the shape parameter of the distribution function. The Weibull distribution, in particular cases, it interpolates between two known distribution: exponential distribution (where $k = 1$) and Rayleigh distribution (where $k = 2$). If we define the random Weibull variable x as time-to-failure then we will have a distribution where the rate of failure is proportional to a power of time. In this way, the Weibull distribution changes dramatically with the value of the shape parameter k. This parameter in the interval $(0,1)$ could be interpreted as follows:

- failure rate decreases in time for $k < 1$,
- failure rate increases with time for $k > 1$, an example here could be an aging process that is likely to fail as time goes by,
- constant failure rate in time for $k = 1$ (random external events are causing the failure).

The hazard rate of the distribution or failure rate is given by:

$$h(x;k,\lambda) = \frac{k}{\lambda}\left(\frac{x}{\lambda}\right)^{k-1}. \tag{2}$$

The **Poisson distribution** is a very useful and used distribution in experiment because many random events are following the pattern of this distribution [21]. The Poisson distribution is a discrete probability distribution that can be used to calculate the probability of certain event number to occur in a fixed interval of time and space. The events considered should be independent and with a known average occurrence rate. The probability function of the Poisson distribution for a given discrete random variable has the following definition:

$$f(k;\lambda) = \Pr(X = k) = \frac{\lambda^k e^{-\lambda}}{k!}. \tag{3}$$

The notations used by the distribution are the following: $x = k$ means actual number of success resulted from the Poisson experiment, λ is the average number of successes that occurs in a certain known interval. In the Poisson experiment, the probability of a success to occur is proportional to the size on the interval/region and the smaller is the interval of time or region the probability will be close to zero.

Pareto Distribution – the distribution is named after the engineer Vilfredo Pareto and used to describe observable events in many fields of expertise. The statistical analysis [22] of the distribution can reveal the key events, which influence significantly the events chain part of the distribution. After rigorous analysis in quality control processes, charting the events based on the distribution, the Pareto rule was defined saying that 80% of the problems (events) are cause by 20% of key events/actions done wrong. The survival function is given by the probability of the Pareto random variable to be greater than some number x (x_m is the scale parameter and α is shape parameter for the Pareto distribution):

$$\overline{F}(x) = \Pr(X > x) = \begin{cases} \left(\frac{x_{\mathrm{m}}}{x}\right)^{\alpha} & x \geq x_{\mathrm{m}}, \\ 1 & x < x_{\mathrm{m}}. \end{cases} \tag{4}$$

The distribution can be used to describe many situations for equilibrium found in large/small items or events and make observations about the effectiveness of the process steps.

3.3. Integration in CloudSim

While describing CloudSim is important to mention the main entities/concepts its based on, in terms of terminology:

- **Processing element (PE)** or the unit responsible for computational execution. It can be seen as the smallest unit of the system responsible for the completion of a certain task;
- **datacenter** represents the resource provider. It is responsible for managing the available resources, i.e. hosts, PEs, VMs, memory;
- **broker** is responsible for mediating between the user and the datacenter. It represents the users needs. It sends the cloudlets for scheduling to the datacenter, monitors the cloudlets status and it informs the user about current state of his requirements;
- **cloudlet** represents the user requirement (a task for the cloud provider). It is characterized by length, PEs number (the number of PEs required for the cloudlet to be done);
- **host** is a physical resource characterized by a number of PE and RAM capacity (a computer);
- **Virtual machine (VM)** is a software-based emulation of a computer.

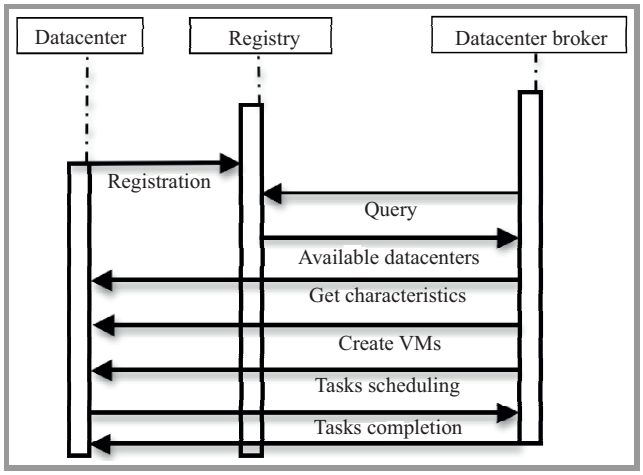


Fig. 2. CloudSim communication model.

The entities in CloudSim communicate through messages. Since host and VM are static entities, each change in their state should be realized by the datacenter. Figure 2 presents an example of the messages flow during the simulation between the broker and the datacenter. The broker, based on the simulation configuration (number of cloudlets and their specification) will request the VM creation, cloudlets scheduling and it will wait to be informed by the datacenter when the cloudlets completion is realized.
The Fault Tolerance Module is extending the CloudSim core functions with the following entities:

1. FaultInjector
   - extends the SimEntity class;
   - it will be started at simulation startup along with the other entities from the system;
   - it is responsible for inserting fault events at random moments of time;
   - the random generation of moments of time is based on a statistical distribution.
2. FaultEvent
   - extends the SimEvent class;
   - describes a fault event: source, destination, time and type;
   - tag type: HOST_FAILURE, CLOUDLET_FAILURE, CREATE_VM_FAILURE;
   - it is created in the Fault Injection Module.
3. FaultHandlerDatacenter
   - extends the datacenter class;
   - processes fault events sent by the FaultGenerator;
   - it updates the cloudlet execution/status according to the fault event type;
   - it handles VM migration;
   - since host and VM are static entities, all its state modification should be processed by the datacenter.

3.4. Fault Injector Integrated with CloudReports

The authors have chosen to integrate FIM-SIM in CloudReports, a GUI implementation for CloudSim. The module is an integrated part of CloudSim and can be further used in any other application that is based on CloudSim. CloudReports is an extension that can be used with CloudSim as a simulation tool. It's basically a graphical tool that helps to simulate distributed system environments, providing an easy interface to user and pluggable extension.
To meet all CloudSim proprieties, CloudReports can provide a number of datacenters, each been 100% customizable, and run them as a provider of services or in cloud terms as an Infrastructure as a Service (IaaS). The customers to this solution are also customizable with a full cost and resource allocation. They can modify and set the number of VMs needed as a user. The broker can allocate the resources and track down the consumptions. Virtual machines can be entirely customized from CPU processing

power to RAM and network bandwidth but can also run scheduling algorithms for tasks in place.

As this is a graphical tool, CloudReports can generate reports for each simulation from raw data to processed data. Those reports that can be displayed as HTML reports or exported for further analysis in third-party application tools. This application has been built on top of CloudSim as a framework for modeling and simulation of IaaS by Thiago T. Sa for final graduation project at Federal University of Ceara, Brazil. This software is licensed under GNU GPL 3.0.

This application have been chosen based on the fact that it provides a friendly GUI that permits easy creation, modification and removal of any cloud component. In addition, the fault injector was integrated in the graphical interface, allowing two options: enable/disable fault injector and choose the statistical method for generating the events.

As mentioned before one of the Cloud Reports benefits is its logging and reporting system, both in raw data and graphic interface. One can obtain all data types about the system performance, i.e., power consumption, storage usage, CPU performance needed and bandwidth used from provider and customer perspectives. In addition it offers information about the cloudlets successfully finished, the execution time evolution, the average start and finish time, etc.

4. FIM-SIM Evaluation

The several experiments have been conducted with the main goal of noticing CloudSim behavior in case of a failure occurrence, the overall system performance and the rate of faults generated based on the statistical distribution chosen. In performed tests the number of hosts was varied from 10 to 30 and the number of VMs from 4 to 10. The cloudlet generation is dynamic and continuous for the observation time specific to each simulation. It is realized by CloudReports broker: at every cloudlet finish it will generate another one with a random length. For this reason, the total number of cloudlets sent in a period of time t, may vary from simulation to simulation, even if all the describing parameters are the same.

The authors have inserted 2 types of failures: host failures and high level failures (cloudlet failures caused by any networking problem that CloudSim can not control). The second type of failures have been chosen for the tests where we followed only the faults generation rate or the relationship between the statistical parameters and total number of failures generated.

The experiments for VM_CREATION, VM_DESTROY and VM_SCHEDULING_ERROR faults are no relevant because the CloudReports simulations are not dynamic so it does not permit the dynamic creation of other VMs or further host integration. In this case, it was out of the target to focus on these types of failures since we have wanted to notice the system behavior during a simulation.

4.1. Poisson Failures Distribution

In the first experiment a 10 hosts, 4 VMs and an observation time of one hour have been chosen. There were failures generated for each of them and starting with $t > 50$ minutes the system failed to provide requests. When the number of hosts was modified to 30, the system continued to execute the cloudlets. It can be noticed that there is a tendency to generate more faults in the second half of the observed interval (see Fig. 3).

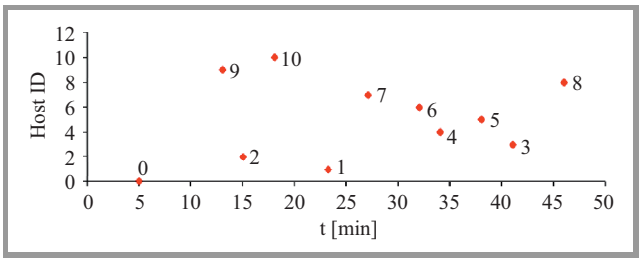


Fig. 3. Poisson failures distribution.

The host selection process was randomly for every moment that was considered a fault. It is important to mention that CloudSim has a sequential method of selecting the host that will be eligible for migration (based on a power consumption limit). In this case, if the selection of the next host to be failed is also sequential we will have a very big number of migrations generated. The overall performance of the cloud will be affected in terms of response time and resources consumption. The success rate it is not affected. Table 2 presents a short example of the number of migrations generated for several randomly host chosen simulations and for one sequential.

Table 2
Migrations generated for several simulations

Simulation ID	Number of migrations	Hosts implied
1	4	2
2	12	4
3	8	3
4	8	3
5	4	2
Sequential	44	11

As a brief conclusion, an average rate of 4/8 migrations can be expected, which will bring a better performance to the system then 44.

4.2. Weibull Failures Distribution

In this case the cloudlets failures for 2 different customers have been inserted, chosen in an alternative way, randomly each other. Here we can notice that the failures are spread

all over the interval with a frequency rate of at every 5 minutes (see Fig. 4).

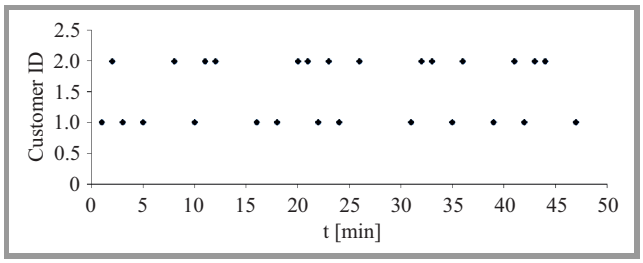


Fig. 4. Weibull failures distribution.

4.3. Exponential Failures Distribution: λ Variation

For the exponential distribution the λ is increased and growing failures number is observed (see Fig. 5).

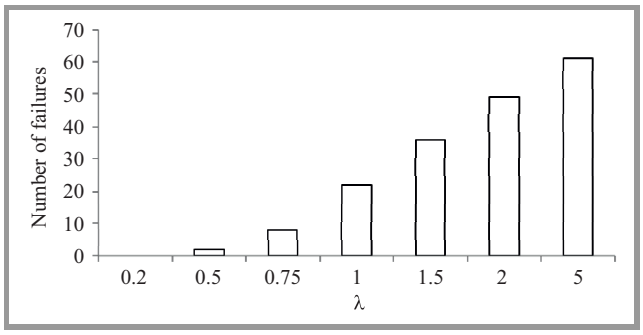


Fig. 5. Exponential distribution failure rate (λ variation).

4.4. Pareto Failures Distribution

In the case of Pareto distribution mostly the same number of failure is obtained generated without any observable relationship between the parameters and faults injected. However the maximum value of failures inserted was 22 (see Table 3).

Table 3
Pareto Distribution Results

α	x_m	Mean	Number of faults
1.5	0.5	0.15	9
2	0.5	1	14
3	0.5	0.75	20
4	0.5	0.66	21
5	0.5	0.625	22
10	0.5	0.555	22
20	0.5	0.52	22
50	0.5	0.51	22
100	0.5	0.5005	22
2	1	2	14
2	2	4	14
2	3	6	14
2	10	20	14
2	100	200	14

4.5. System Performance without VM Migration

For the last experiment the VM migration was deactivated and a 10 different simulations without any change in the initial state of the system were run. The results are presented in Fig. 6 The best success rate obtained, in case of a host failure, depending on the random sequence of failures was 52%. The events were generated based on Poisson distribution.

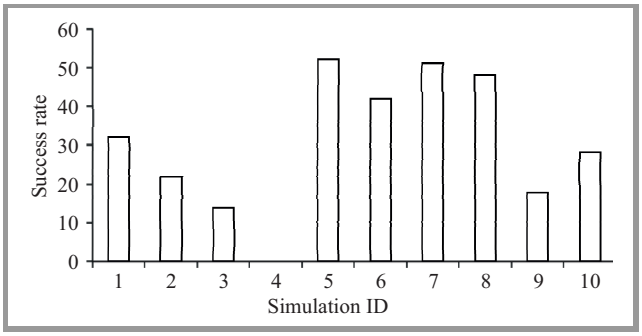


Fig. 6. System performance without VM migration.

Other observations realized during the performed experiments:

- CloudSim can assure host failures through migration;
- If a failure is sent during the execution of some cloudlets those cloudlets will fail even though a VM migration was started. A success rate of 90–100% was obtained;
- It does not resubmit the failed cloudlets;
- CloudReports is based on power aware module: it will generate migration if the power consumption has level up at certain threshold.

5. Conclusion

The work presented in this paper can be summarized as follows. A Fault Injector Module, named FIM-SIM, have been designed and implemented, on cloud simulation with the main goal to provide a helpful tool for validation and testing of various fault tolerance models or any new policy that can be faulty. In authors vision, the main characteristic of this fault injector is its intention to reproduce faults in a more natural and realistic way. We all have faced some moment in times when something went wrong and we have described it as “randomly happen”. Maybe, in some cases, randomly is not so randomly as it seems to be. Probably there are failures that tend to happen with a certain frequency or tend to respect a certain pattern in time. For these situations a Fault Injector Module have been built that tends to produce faults event according to a certain distribution.
The authors have built FIM-SIM module as a integrated part of CloudSim and it was extended with CloudReports,

a GUI solution for CloudSim. This module was designed as an event generator with various ways of "randomly" generating the events in time following distributions as: a Poisson, Weibull, Gamma, Pareto, and Exponential.

In conducted experimental results the authors have noticed some tendencies in failures distribution under Poisson and Weibull distributions. For the Poisson distribution, the failures tend to happen more in the second half of the analyzed interval but in the Weibull distribution it tends to respect a certain frequency: 3 every 5 minutes for example.

CloudSim can respect requests even if the resources are failing by activating the VM migration. There is a strong relationship between the sequence of failures and the VM migration. If the VM migration is realized based on the location criteria and there are failures that happens in a certain area, then the number of migration will increase and the overall performance will be lower. Another important observation is that CloudSim does not resubmit the failed cloudlets.

The authors think that FIM-SIM module can have a great impact in the research area for cloud providers. Sometimes is very expensive to validate a model in real life, to realize that it has many drawbacks and you have to redesign it an implement it again. As a further work, the authors intend to propose some fault tolerance techniques and try to extend the type of failures that can appear in a cloud environment.

Acknowledgements

The research presented in this paper is supported by following projects: "*SideSTEP - Scheduling Methods for Dynamic Distributed Systems: a self-* approach*", ID: PN-II-CT-RO-FR-2012-1-0084; *CyberWater* grant of the Romanian National Authority for Scientific Research, CNDI-UEFISCDI, project number 47/2012; *MobiWay*: Mobility Beyond Individualism: an Integrated Platform for Intelligent Transportation Systems of Tomorrow - PN-II-PT-PCCA-2013-4-0321; *clueFarm*: Information system based on cloud services accessible through mobile devices, to increase product quality and business development farms – PN-II-PT-PCCA-2013-4-0870.

References

[1] A. Hameed *et al.*, "A survey and taxonomy on energy efficient resource allocation techniques for cloud computing systems", *Computing*, 2014 (in Press).

[2] R. Jhawar and V. Piuri, "Fault tolerance management in Iaas clouds", in *Proc. IEEE 1st AESS Eur. Conf. Satell. Telecommun. ESTEL 2012*, Rome, Italy, 2012, pp. 1–6.

[3] M. Nastase, C. Dobre, F. Pop, and V. Cristea, "Fault tolerance using a front-end service for large scale distributed systems" in *Proc. 11th Int. Symp. Symb. Numeric Algorithms for Scient. Comput. SYNASC 2009*, Timisoara, Romania, 2009, pp. 229–236.

[4] Z. Zheng, T. C. Zhou, M. R. Lyu, and I. King, "Component ranking for fault-tolerant cloud applications", *IEEE Trans. Serv. Comput.*, vol. 5, no. 4, pp. 540–550, 2012.

[5] J. Kolodziej, H. Gonzalez-Velez, and L. Wang, "Advances in data-intensive modeling and simulation", *Future Gener. Comp. Syst.*, 2014 (in Press).

[6] C. Dobre, F. Pop, and V. Cristea, "A fault-tolerant approach to storing objects in distributed systems", in *Proc. Int. Conf. on P2P, Parall., Grid, Cloud and Internet Comput. 3PGCIC 2010*, Fukuoka, Japan, 2010, pp. 1–8.

[7] P. Das and P. M. Khilar, "VFT: A virtualization and fault tolerance approach for cloud computing", in *Proc. IEEE Conf. Inform. Commun. Technol. ICT 2013*, Jeju Island, South Korea, 2013, pp. 473–478.

[8] S. Malik and F. Huet, "Adaptive fault tolerance in real time cloud computing", in *Proc. IEEE World Congr. Serv. SERVICES 2011*, Washington, DC, USA, 2011, pp. 280–287.

[9] Y. He *et al.*, "A simulation cloud monitoring framework and its evaluation model", *Simul. Modell. Pract. and Theory*, vol. 38, pp. 20–37, 2013.

[10] S. Vilkomir, "Cloud testing: A state-of-the-art review", *Inform. & Secur.: An Int. J.*, vol. 28, no. 2, pp. 213–222, 2012.

[11] A. Boteanu, C. Dobre, F. Pop, and V. Cristea, "Simulator for fault tolerance in large scale distributed systems", in *Proc. IEEE 6th Int. Conf. Intell. Comp. Commun. and Process. ICCP 2010*, Cluj-Napoca, Romania, 2010, pp. 443–450.

[12] A. Costan, C. Dobre, F. Pop, C. Leordeanu, and V. Cristea, "A fault tolerance approach for distributed systems using monitoring based replication", in *Proc. IEEE 6th Int. Conf. Intell. Comp. Commun. and Process. ICCP 2010*, Cluj-Napoca, Romania, 2010, pp. 451–458.

[13] D. Ford *et al*., "Availability in globally distributed storage systems", in *Proc. 9th USENIX Conf. Operat. Sys. Design and Implemen. OSDI'10*, Berkeley, CA, USA, 2010, pp. 1–7. USENIX Association.

[14] Y. Zhang, Z. Zheng, and M. R. Lyu, "BFTCloud: A byzantine fault tolerance framework for voluntary-resource cloud computing", in *Proc. IEEE 4th Int. Conf. Cloud Comput. CLOUD '11*, Washington, DC, USA, 2011, pp. 444–451.

[15] F. Cappello, "Fault tolerance in petascale/ exascale systems: current knowledge, challenges and research opportunities", *Int. J. High Perform. Comput. Appl.*, vol. 23, no. 3, pp. 212–226, 2009.

[16] A. Núñez *et al.*, "A flexible and scalable cloud infrastructure simulator", *J. Grid Comput.*, vol. 10, no. 1, pp. 185–209, 2012.

[17] L. Liu *et al.*, "Greencloud: A new architecture for green data center", in *Proc. 6th Int. Conf. Industry Session on Autonomic Comput. and Communi. Industry Session ICAC-INDST '09*, Barcelona, Spain, 2009, pp. 29–38.

[18] 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", *Softw. Pract. Exper.*, vol. 41, no. 1, pp. 23–50, 2011.

[19] K. J. Lang, "Practical algorithms for generating a random ordering of the elements of a weighted set", *Theor. Comp. Sys.*, vol. 54, no. 4, pp. 659–688, 2014.

[20] A. M. Razali and A. A. Al-Wakeel, "Mixture weibull distributions for fitting failure times data", *Appl. Math. Comput.*, vol. 219, no. 24, pp. 11358–11364, 2013.

[21] G. Shmueli, T. P. Minka, J. B. Kadane, S. Borle, and P. Boatwright, "A useful distribution for fitting discrete data: revival of the Conway-Maxwell-Poisson distribution", *J. Royal Statist. Soc.: Series C (Applied Statistics)*, vol. 54, no. 1, pp. 127–142, 2005.

[22] M. E. J. Newman, "Power laws, pareto distributions and Zipf's law", *Contemporary Phys.*, vol. 46, no. 5, pp. 323–351, 2005.

Mihaela-Catalina Nita finished his M.Sc. in 2014 on Parallel and Distributed Computing Systems program at University Politehnica of Bucharest, Faculty of Automatic Control and Computers, Computer Science Department. She is an active member of Distributed Systems Laboratory. Her research interests are in cloud system and resource management, especially in fault-tolerance systems, SLA assurance, multi-criteria optimization, cloud middleware tools, complex applications design and implementation.

E-mail: catalina.nita@hpc.pub.ro
Faculty of Automatic Control and Computers
Computer Science Department
University Politechnica of Bucharest
313, Splaiul Independentei, Sector 6
060042 Bucharest, Romania

Florin Pop received his Ph.D. in Computer Science at the University Politehnica of Bucharest in 2008. He received his M.Sc. in Computer Science in 2004 and the Engineering degree in Computer Science in 2003, at the same University. He is Associate Professor within the Computer Science Department and also an active member of Distributed System Laboratory. His research interests are in scheduling and resource management, multi-criteria optimization methods, grid middleware tools and applications development, prediction methods, self-organizing systems, contextualized services in distributed systems. He is the author or co-author of more than 150 publications. He served as guest-editor for International Journal of Web and Grid Services and he is managing editor for International Journal of Grid and Utility Computing. He was awarded with "Magna cum laude" distinction from University Politehnica of Bucharest for his Ph.D. results, one IBM Faculty Award in 2012 or the project CloudWay Improving resource utilization for a smart cloud infrastructure, two Prizes for Excellence from IBM and Oracle (2008 and 2009), Best young researcher in software services Award, FP7 SPRERS Project, Strengthening the Participation of Romania at European R&D in Software Services in 2011 and two Best Paper Awards. He worked in several international and national research projects in the distributed systems field as coordinator and member as well. He is a senior member of the IEEE, a member of the ACM and a member of the euroCRIS.

E-mail: florin.pop@cs.pub.ro
Faculty of Automatic Control and Computers
Computer Science Department
University Politechnica of Bucharest
313, Splaiul Independentei, Sector 6
060042 Bucharest, Romania

Mariana Mocanu is a Professor of the Computer Science and Engineering Department of the University Politehnica of Bucharest, and has a long experience in developing information systems for industrial and economic processes, and in project management. She performs teaching for both undergraduate and master's degree in software engineering, systems integration, software services and logic design. At the University of Regensburg, as visiting professor, she thought Process Computers. She worked for ten years in a multidisciplinary research team for vehicles, being co-author of two patents. She participated in numerous research projects, implementing information systems for control/optimization of processes in various areas (transport, environment, medicine, natural resources management). Her results of research and teaching are reflected in articles published in journals, in papers presented at national and international conferences, and books. She is a member of the University Senate, at the faculty she is responsible for quality assurance and is a board member of the department.

E-mail: mariana.mocanu@cs.pub.ro
Faculty of Automatic Control and Computers
Computer Science Department
University Politechnica of Bucharest
313, Splaiul Independentei, Sector 6
060042 Bucharest, Romania

Valentin Cristea is a Professor of the Computer Science and Engineering Department of the University Politehnica of Bucharest, and Ph.D. supervisor in the domain of Distributed Systems. His main fields of expertise are large scale distributed systems, cloud computing and e-services. He is co-founder and director of the National Center for Information Technology of UPB, and has a long history of experience in the development, management and coordination of international and national research projects. He led the UPB team in COOPER (FP6), datagrid@work (INRIA "Associate Teams" project), CoLaborator project for building a Center and collabora-

tive environment for high-performance computing in Romania, distributed dependable systems project DEPSYS, and others. He co-supervised the UPB Team in European projects SEE-GRID-SCI (FP7) and EGEE (FP7). The research results have been published in more than 230 specialist papers in international journals or peer-reviewed proceedings, and more than 30 books and book chapters. Prof. Cristea organized several scientific workshops and conferences. In 2003 and 2011 he received the IBM faculty award for research contributions in e-Service and Smart City domains. He is a member of the Romanian Academy of Technical Sciences.

E-mail: valentin.cristea@cs.pub.ro
Faculty of Automatic Control and Computers
Computer Science Department
University Politechnica of Bucharest
313, Splaiul Independentei, Sector 6
060042 Bucharest, Romania

Paper

Comparative Study of Supervised Learning Methods for Malware Analysis

Michał Kruczkowski[1,2] and Ewa Niewiadomska-Szynkiewicz[1,3]

[1] *Research and Academic Computer Network NASK, Warsaw, Poland*
[2] *Institute of Computer Science, Polish Academy of Sciences, Warsaw, Poland*
[3] *Institute of Control and Computation Engineering, Warsaw University of Technology, Warsaw, Poland*

Abstract—Malware is a software designed to disrupt or even damage computer system or do other unwanted actions. Nowadays, malware is a common threat of the World Wide Web. Anti-malware protection and intrusion detection can be significantly supported by a comprehensive and extensive analysis of data on the Web. The aim of such analysis is a classification of the collected data into two sets, i.e., normal and malicious data. In this paper the authors investigate the use of three supervised learning methods for data mining to support the malware detection. The results of applications of Support Vector Machine, Naive Bayes and *k*-Nearest Neighbors techniques to classification of the data taken from devices located in many units, organizations and monitoring systems serviced by CERT Poland are described. The performance of all methods is compared and discussed. The results of performed experiments show that the supervised learning algorithms method can be successfully used to computer data analysis, and can support computer emergency response teams in threats detection.

Keywords—data classification, k-Nearest Neighbors, malware analysis, Naive Bayes, Support Vector Machine.

1. Introduction

Malicious software (malware) is software designed to disrupt or damage computer system, gain access to users or gather sensitive information. Malicious programs can be classified into worms, viruses, trojans, spywares, etc. In recent years numerous attacks have threaten the ability and operation of the Internet. Therefore, mechanisms for successive detection of malicious software are crucial components of network security systems. In this paper the use of selected data mining techniques to malware analysis is investigated. Comprehensive and extensive analysis of data on the Web can significantly improve the results of malware detection. A large number of learning based methods have been developed over the past decades and used to complex data analysis. The taxonomy and survey are provided in [1]. Recently, a class of supervised learning methods has emerged as powerful techniques for heterogenous data analysis and classification. It is obvious that most data on the World Wide Web is heterogeneous, unstructured, and often incomplete. Therefore, in presented research the authors focus on the application of the supervised methods to malware detection.

The goal is to detect malware based on classification of data taken from various computer networks that belong to various users and organizations. The objective is to classify a given program on the Web into a malware or a clean class. Hence, a problem of two-class pattern classification is considered.

The problem of identifying to which set of categories a new observation (measurement) belongs is crucial in many domains, i.e., pattern recognition, anomaly detection, similarity analysis, social networks etc. [2], [3], [5]–[8]. The individual observations usually have to be analyzed with respect to a set of quantifiable properties. Various techniques for heterogenous data classification are described in literature. The three learning methods are employed: Support Vector Machine (SVM), Naive Bayes (NB) and *k*-Nearest Neighbors (*k*NN) techniques to malware detection. The application of these methods to malware analysis and data on the Web classification is discussed in [3], [5], [9]. The novelty of presented approach is classification based on the extensive set of the malware samples features. Moreover, a large Web databases consisting of strong heterogeneous data is considered.

The paper is structured as follows. In Section 2 a brief overview of techniques to malware detection is provided. In Section 3 the problem of malicious software detected is specified. Three methods used in experiments, i.e., Support Vector Machine, Naive Bayes and *k*-Nearest Neighbors are reported in Section 4. In Section 5 the results of numerical experiments are presented and discussed. Finally, conclusions are drawn in Section 6.

2. Related Work

In recent years the important direction of research in network security is devoted to design and development of methods and tools for malware analysis and detection [3], [5]. The widely used approach to analyze malicious software is based on the extraction of information about suspicious communication with the system, the detection of Intrusion Detection System (IDS) signatures and the

generation of new IDS signatures. Honeypot systems are often employed to detect, deflect or counteract attempts at unauthorized use of information systems. Other techniques utilize algorithms inspired on human immune system to detection and prevention of Web intrusions [10], [11]. Malware samples can be used to create a behavioral model to generate signature, which is served as an input to a malware detector, acting as the antibodies in the antigen detection process. In case of malicious botnets a new trend is to use alternative communication channels, i.e., DNS-tunneling or HTTP instead of IRC to connect command & control (C&C) servers and infected hosts [12].

Malware detection can be significantly supported by a comprehensive and extensive analysis of data taken from the Internet. The common direction is to use statistic analysis [13] and data mining methods [14]. The supervised learning algorithms are successfully used to data classification taking into account the unique set of features. Wide range of applications of these techniques to malware detection is described in literature [9], [15], [16]. The focus is on anomaly detection and similarity analysis of data samples related with the malware programs [16], [17].

3. Problem Specification

Let us consider the set Ω of vectors of measurements x. The goal is to detect the malicious data among the data gathered from the Internet.

In general, the classification problem consists of two steps: training and prediction. To classify the dataset into disjoin subsets consisting of samples with similar characteristics we have to divide the whole data space Ω into training and testing sets. Each instance in the training set contains one target value (i.e., the class label) and several attributes (i.e., the features and attributes of observed variables). The goal of a classifier is to produce a model based on the training data, which can enable us to assign an object from the testing set to the appropriate class as well as possible. The decision about classification of a new object is made only based on its features and attributes.

In presented research, the authors consider a problem of two-classes pattern classification. Each data sample have to be classified into one of two categories: positive class containing normal data and negative class containing malicious data. In the following sections three methods that can be used to classify the heterogenous data are described and evaluated.

4. Classification Techniques

4.1. k-Nearest Neighbors Classifier (kNN)

The k-Nearest Neighbors (kNN) algorithm [18], [19] is widely used for regression and classification. It is one of the simplest of the machine learning algorithms. The general idea of the k-Nearest Neighbors classifier is to classify a given query sample based on the class of its nearest neighbors (samples) in the dataset. The classification process is performed in two phases. In the first phase the nearest neighbors are determined. The neighbors are taken from a set of samples, which the class is known. The optimal number of neighbors (value of k in Fig. 1) can be calculated in different ways. They are described in literature [18], [19].

The neighbors of a query sample are selected based on the measured distances. Therefore, a metric for measuring the distance between the query sample and other samples in the dataset has to be determined. Various metrics can be used: Euclidean, City-block, Chebyshev, etc. The Euclidean distance metric was used in those experiments.

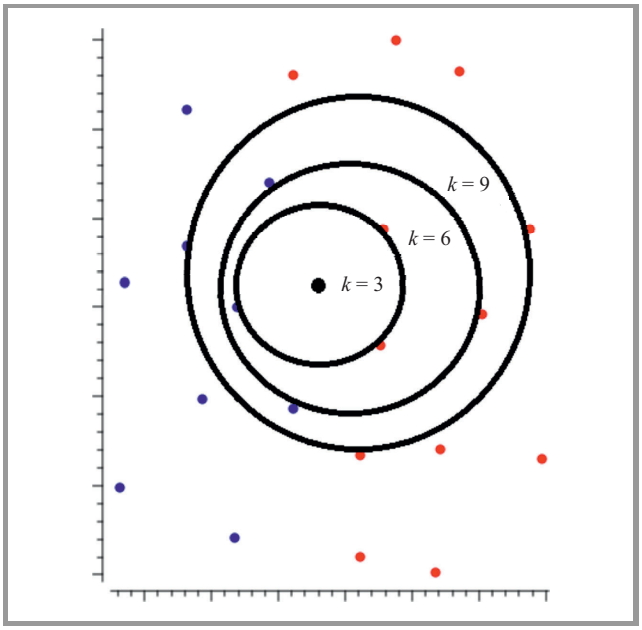


Fig. 1. k-Nearest Neighbors classification for various number of k.

The aim of the second phase is to determine the class for a query sample based on the outcomes (assigned classes) of the k selected neighbors. The decision about class is obviously straightforward in case when all determined neighbors belong to the same class. Otherwise, in case of neighbors from different classes various ways to select a class are proposed. The most straightforward solution is to assign the majority class among the k neighbors. The other widely used approach applies voting. The neighbors vote on the class, and their votes depend on their distances to the query sample.

4.2. Naive Bayes Classifier

A Naive Bayes (NB) classifier [20] employs Bayes' theorem with strong independence assumptions. In this technique, it is assumed that the presence or absence of a given characteristic of a class is unrelated to the presence or absence of any other characteristic. The learning algorithm based on Bayes classifier allows to combine prior knowledge and current measurements. It calculates explicit probabilities for

hypothesis. This method can be successfully used to the analysis of heterogeneous and high dimensionality data. Parameter estimation for naive Bayes models uses the method of maximum likelihood.

Naive Bayes classifiers can handle an arbitrary number of independent variables whether continuous or categorical. Given a set of variables, $X = x_1, x_2, \ldots, x_d$, the goal is to calculate the posterior probability for the event C_j among a set of possible outcomes $C = c_1, c_2, \ldots, c_d$. The Bayes' rule (1) can be used to perform calculations.

$$p(C_i|x_1, x_2, \ldots, x_d) \propto p(x_1, x_2, \ldots, x_d|C_j)p(C_j), \quad (1)$$

where $p(C_j|x_1, x_2, \ldots, x_d)$ denotes the posterior probability of class membership, i.e., the probability that X belongs to C_j. Since NB assumes that the conditional probabilities of the independent variables are statistically independent the likelihood to a product of terms (2) can be decomposed:

$$p(X|C_j) \propto \prod_{k=1}^{d} p(x_k|C_j), \quad (2)$$

and rewrite the posterior as (3):

$$p(C_j|X) \propto p(C_j) \prod_{k=1}^{d} p(x_k|C_j). \quad (3)$$

Using Bayes' rule described above, a new case X with a class level C_j is labeled, that achieves the highest posterior probability. Although the assumption that the predictor variables are independent is not always accurate, it does simplify the classification task dramatically, since it allows the class conditional densities $p(x_k|C_j)$ to be calculated separately for each variable, i.e., it reduces a multidimensional task to a number of one-dimensional ones. Hence, Naive Bayes reduces a high-dimensional density estimation task to a one-dimensional kernel density estimation. Furthermore, the assumption does not seem to greatly affect the posterior probabilities, especially in regions near decision boundaries, thus, leaving the classification task unaffected.

Naive Bayes can be implemented in several variants including normal, lognormal, gamma and Poisson density functions. In the experiments described in this paper the normal distribution function is considered.

4.3. Support Vector Machine classifier (SVM)

The Support Vector Machine (SVM) [21] is a widely used supervised learning model with associated learning algorithms to analyze high dimensional and sparse data and recognize patterns [2], [3], [22].

The concept of SVM is to classify each data sample into one of two categories: positive class denoted by "+1" and negative class denoted by "–1". It boils down to find a decision boundary – a plane (a hyperplane for $n > 3$), which divides data into two sets, one for each class. Next, all the measurements on one side of the determined boundary are

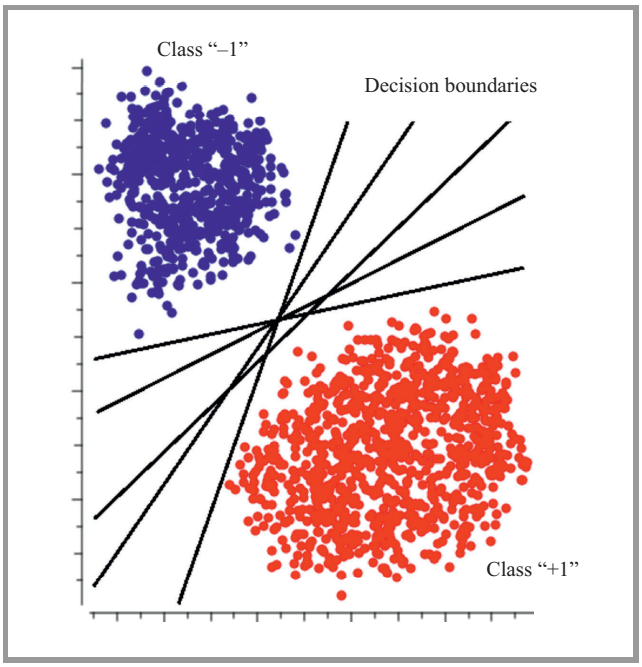


Fig. 2. Binary classification.

classified as belonging to "+1" class and all those on the other side as belonging to "–1" class.

The problem is that many hyperplanes that divides the dataset can be determined (see Fig. 2). Hence, the best one has to be selected. In general, SVM tries to learn the decision boundary, which gives the best generalization. A good separation is achieved by the hyperplane that has the largest distance to the nearest data sample of any class – a wider margin implies the lower generalization error of the classifier [1], [23] (Fig. 3). To select the max-

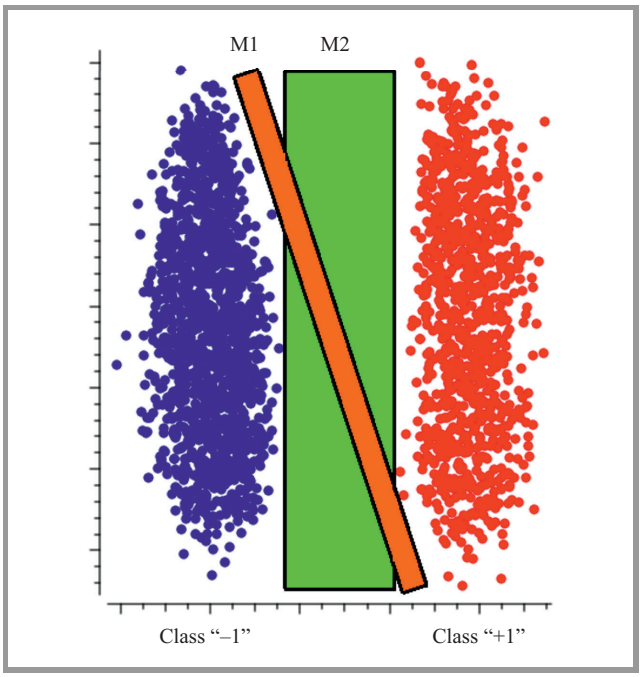


Fig. 3. Various margin hyperplane.

imum margin hyperplane the optimization problem is formulated and solved.

Let us focus on the SVM algorithm. Under the assumption that two classes +1 and –1 are considered the training set D of N pairs (x_i, y_i), $i = 1,\ldots,N$, which is used during the training process can be defined as follows [24]:

$$D = \left\{(x_i, y_i) | x_i \in R^n, y_i \in \{-1, +1\}\right\}_{i=1}^{N}, \tag{4}$$

where x_i denotes a training sample – fixed-length vector consisting of n values (measurements) and y_i is a binary label associated to the i-th vector.

Given a training dataset, the SVM algorithm searches for a plane (a hyperplane for $n > 3$) in the input space that separates the positive samples from the negative ones.

Let us focus on the original SVM model developed by Vapnik [21] – linear classifier. Assume that all hyperplane in R^n are parameterized by a vector w, and a constant b

$$w^T x + b = 0, \tag{5}$$

where w is the vector orthogonal to the hyperplane and b denotes the width of a margin.

For hyperplane (w, b) defined in Eq. (5) that separates the data the classification rule can be formulated:

$$h_w(x) = sign(w^T x + b). \tag{6}$$

The function h_w should correctly classify the training data. Moreover, it should classify the other data that has not been known yet. The problem is that many such hyperplane can be found, i.e., all expressed by pairs $(\alpha w, \alpha b)$ for each positive constant $\alpha \in R^+$, and the optimal one should be selected. Therefore, as it has already been mentioned training a binary classification SVM means solving the optimization problem, which solution should be a maximum margin hyperplane (Fig. 3). For a given training set D defined in Eq. (4) the optimization problem is formulated [21]:

$$\min_{w,b,\zeta} \left(\frac{1}{2} w^T w + C \sum_{i=1}^{N} \zeta_i\right), \tag{7}$$

subject to the constraints:

$$y_i(w^T x_i + b) \geq 1 - \zeta_i, \qquad \zeta_i \geq 0, \tag{8}$$

where ζ_i denotes the slack variable, which measures the degree of misclassification of the sample x_i. $C > 0$ is the constant value, which can be seen as a tunable parameter. The higher value of C involves more importance on classifying all the training data correctly. The lower value of C involves a more flexible hyperplane that tries to minimize the margin error. The quadratic programming can be used to calculate the optimal decision hyperplane [24], [25].

The next step is the prediction process. The goal is to classify each sample from the testing dataset on one side of the determined decision hyperplane as belonging to "–1" class and each that on the other side as belonging to "+1" class [26], [27]. Hence, the final goal of SVM is to produce a model (based on the training data), which classifies the samples from a new dataset based only on the knowledge about their features and attributes.

In practical applications, it often happens that the datasets are not linearly separable in the data space. Due to the fact that the separation is easier in the higher space the solution of this problem is to map the original finite-dimensional space into a much higher-dimensional space (even infinite). Hence, the solution to create nonlinear classifiers by applying kernel functions to maximum-margin hyperplanes was developed [28]–[30]. A kernel function $K(x_i, x_j)$ defines the similarity between a given pair of objects. A large value of $K(x_i, x_j)$ indicates that x_i and x_j are similar and a small value indicates that they are dissimilar.

Summarizing, the resulting nonlinear SVM algorithm is formally similar – every dot product in (8) is replaced by a nonlinear kernel function. Various kernel functions are employed. They are described in literature [31], [32]. The authors used the polynomial kernel function

$$K(x_i, x_j) = (\gamma x_i^T x_j + r)^d, \quad \gamma > 0 \tag{9}$$

to malware analysis. In Eq. (9) γ, r, and d denote kernel parameters. The other kernel functions widely used in the literature are as follows:

- radial basis function (RBF):
  $K(x_i, x_j) = exp(\gamma \parallel x_i x_j \parallel^2), \quad \gamma > 0,$
- sigmoid:
  $K(x_i, x_j) = tanh(\gamma x_i^T x_j + r), \quad \gamma > 0.$

5. Case Study Results

5.1. Input Dataset

The kNN, NB and SVM methods were used to classify heterogeneous data from the real malware database of the n6 platform. The n6 platform was developed in Research and Academic Computer Network (NASK) [33]. The purpose of the system is to monitor computer networks, collect, and analyze data about such events as threads, incidents, etc. [15].

Data in the n6 database are taken from a numerous sources and distributed channels. Events are detected by the devices located in many units and organizations (e.g. security organizations, software providers, independent experts, etc.) and monitoring systems serviced by CERT Poland (Computer Emergency Team Poland). Access to all collected datasets, i.e., URLs of malicious websites, addresses of infected machines, open DNS resolvers, etc., is provided through a REST API. The API exposes an unified data model. Hence, the collected data is represented as a searchable collection of atomic events with a flexible set of properties (key-value pairs) with predefined semantics. The native output extension is JSON [RFC7159], although n6 supports other extensions, i.e., CSV [RFC4180] and IODEF [RFC5070]. A fine-grained permission model

and mandatory TLS [RFC2246] with client certificates for authentication and confidentiality are provided to control the access to the system (see Fig. 4).

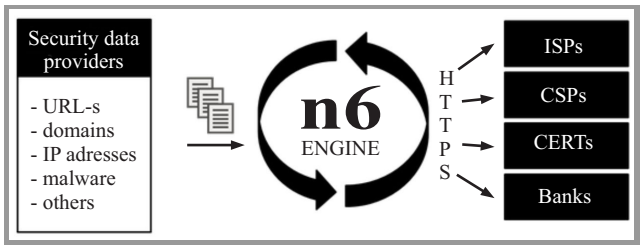


Fig. 4. The n6 database.

Most of the data collected in the n6 database is updated daily. The n6 platform provides tools for sorting the incidents. Due to a sophisticated tagging system, incidents can be assigned to unique entities (e.g. based on IP address and AS numbers). Data are collected into special package, which keeps an original source format (each source in separate file). Additionally it is possible to provide other information, e.g., about C & C servers that are not consisted in a client network, but can be utilized to detect infected computers. Information about malicious sources is transferred by the platform as URL's, domain, IP addresses or names of malware.

5.2. Training Dataset Analysis and Visualization

The preliminary analysis of the training dataset was performed. Four attributes are assigned to each sample collected in the n6 database: time, format, domain, and address. The record *time* consists of two components: date and time of inserting an event into the n6 database. To simplify the analysis two attributes were transformed to the more suitable forms. Each *domain* attribute was clustered, and converted to the numerical. Each *IP address* was described in decimal according to the formula: $W.X.Y.Z = 256^3W + 256^2X + 256Y + Z$, where W,X,Y,Z correspond with values in IP address.

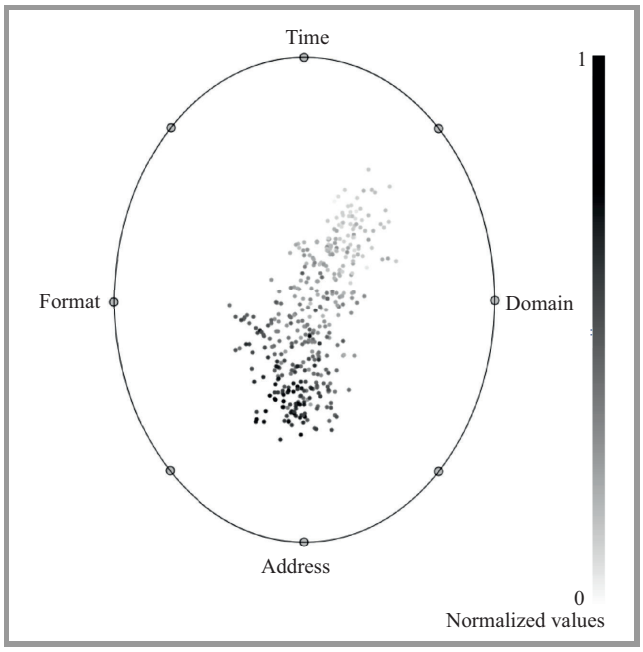


Fig. 5. n6 dataset visualization (radius visualization).

Then, the data samples from the training dataset were analyzed. The visualization of all attributes, i.e., format, time, domain, and address are displayed in Figs. 5 and 6. Prior to visualization, values of attributes are scaled to the values between 0 and 1. The widely used non-linear multidimensional visualization technique Radviz [34] was used to present the data in the four-dimensional space defined by these attributes. In this approach, all attributes are presented as anchor points equally spaced around the perimeter of a unit circle (Fig. 5). Data samples are shown as points inside the circle. Their positions are determined by a metaphor from physics: each point is held in place with springs that are attached at the other end to the attribute anchors. The stiffness of each spring is proportional to the value of the corresponding attribute and the point ends up at the position where the spring forces are in equilibrium. Data samples that are close to a given anchor have higher values of this attribute. We can determine some groups of samples with similar values of all attributes.

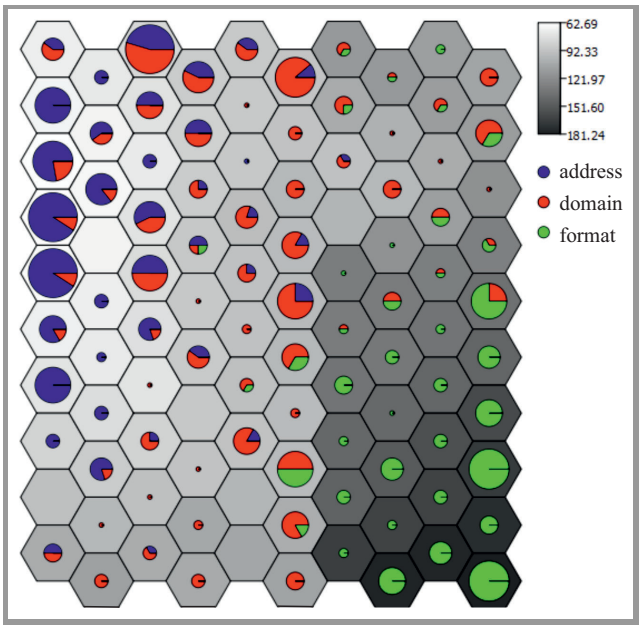


Fig. 6. n6 dataset visualization (self-organizing map).

Next, the self-organizing map (SOM) – another technique for displaying multidimensional data – was applied to investigate the general structure of the training dataset. The map depicted in Fig. 6 shows the distribution of samples in the dataset mapped into the space of all attributes.

Figure 7 presents the correlations between *time* attribute and three other, i.e., *format*, *domain* and *address*. It can be observed that all attributes are commonly correlated, and the correlation coefficient for each pair of attributes is different. Correlations between format and domain versus

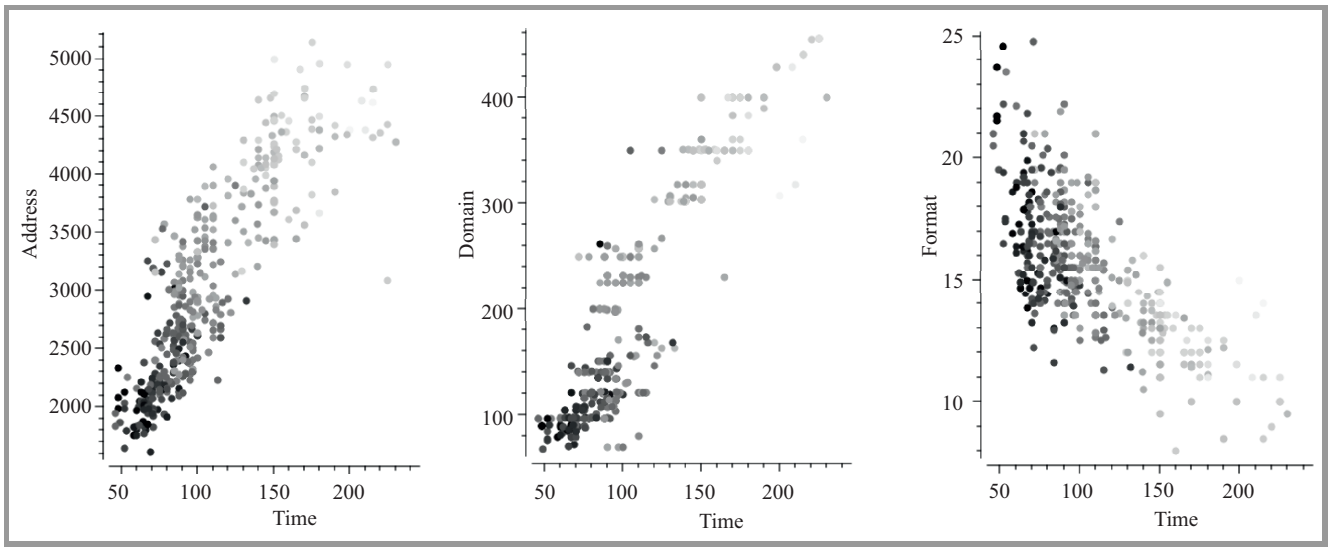


Fig. 7. Correlations between time and other attributes.

time are positive (rising), and for address versus time is negative (falling).

5.3. Validation of Classification Systems and Comparative Study

The goal of the experiments was to validate the *k*NN, NB and SVM classification systems on datasets taken from the n6 platform. Three series of experiments were performed for the same input dataset consisting of 398 samples. The goal of all tests was to classify each data sample from the input dataset into one of two categories: positive class denoted by "+1" (normal data) and negative class denoted by "–1" (malicious data). The accuracy of the classification was evaluated and efficiency of *k*NN, NB and SVM techniques was compared (Tables 1–3). Parameters of the techniques equals respectively: number of neighbors were $k = 3$ in Euclidean metrics for *k*NN, Laplace probability estimation and size of LOESS window equals 0.5 for NB and for SVM the polynomial kernel function was used with parameters $\gamma = 0.5$, $r = 1$ and $d = 3$.

Table 1
Confusion matrix for *k*NN classification

Class	CV [%]		LOO [%]		RS [%]	
	+1	–1	+1	–1	+1	–1
+1	94.4	7.6	94.3	8.3	96.0	13.7
–1	5.6	92.4	5.7	91.7	4.0	86.3

Table 2
Confusion matrix for NB classification

Class	CV [%]		LOO [%]		RS [%]	
	+1	–1	+1	–1	+1	–1
+1	96.6	6.6	96.9	7.2	96.2	8.7
–1	3.4	93.4	3.1	92.8	3.8	91.3

Table 3
Confusion matrix for SVM classification

Class	CV [%]		LOO [%]		RS [%]	
	+1	1	+1	–1	+1	–1
+1	98.1	13.9	95.4	7.3	99.2	11.8
–1	1.9	86.1	4.6	92.7	0.8	88.2

Three commonly used cross-validation methods were used for assessing how the results of the classification will generalize to an independent data sets [4], [23]: CV – Cross Validation, LOO – Leave-One-Out and RS – Random Sampling. Multiple tests for various parameters of these methods were performed. In this paper the results obtained for 5-folds cross validation and random sampling with 5 repetitions of training process and 50% of the relating training set size is presented. For these values of parameters, the authors got the best compromise between accuracy and speed of calculations.

The achieved efficiency of fitting of the testing data was from 86 to 99% respective to the given method and class (+1 or –1). The SVM method gave the best accuracy of selecting to the class "+1" (99.2% for RS technique).

Figure 8 shows the calibration plots that illustrate the quality of the *k*NN, NB and SVM based classification systems the classification systems. Figure 9 displays the receiver operating characteristic curves (ROC) for these systems.

Then, the quality of the classification systems was assessed. Five commonly used criteria were taken into consideration:

- CA – classification accuracy,
- Sens – sensitivity,
- Spec – specificity,
- AUC – area under ROC curve,
- F1 – F-measure.

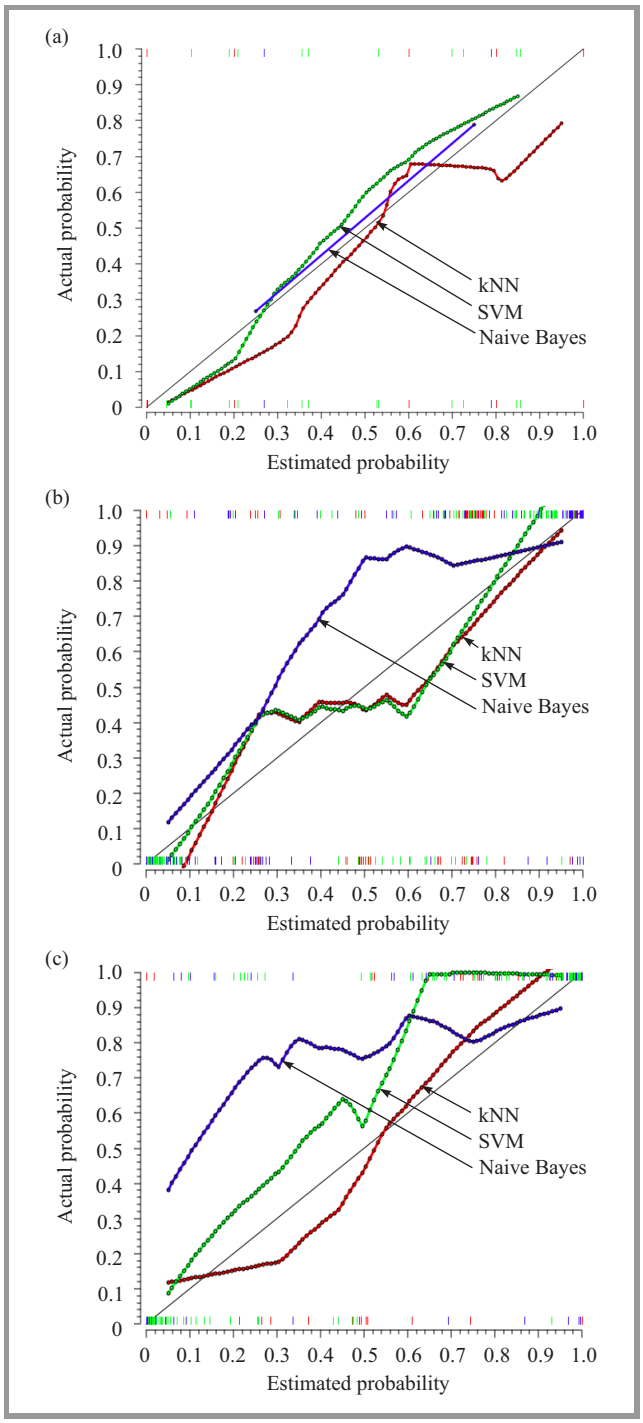


Fig. 8. Calibration plots for *k*NN, NB and SVM based systems: (a) CV, (b) LOO, (c) RS.

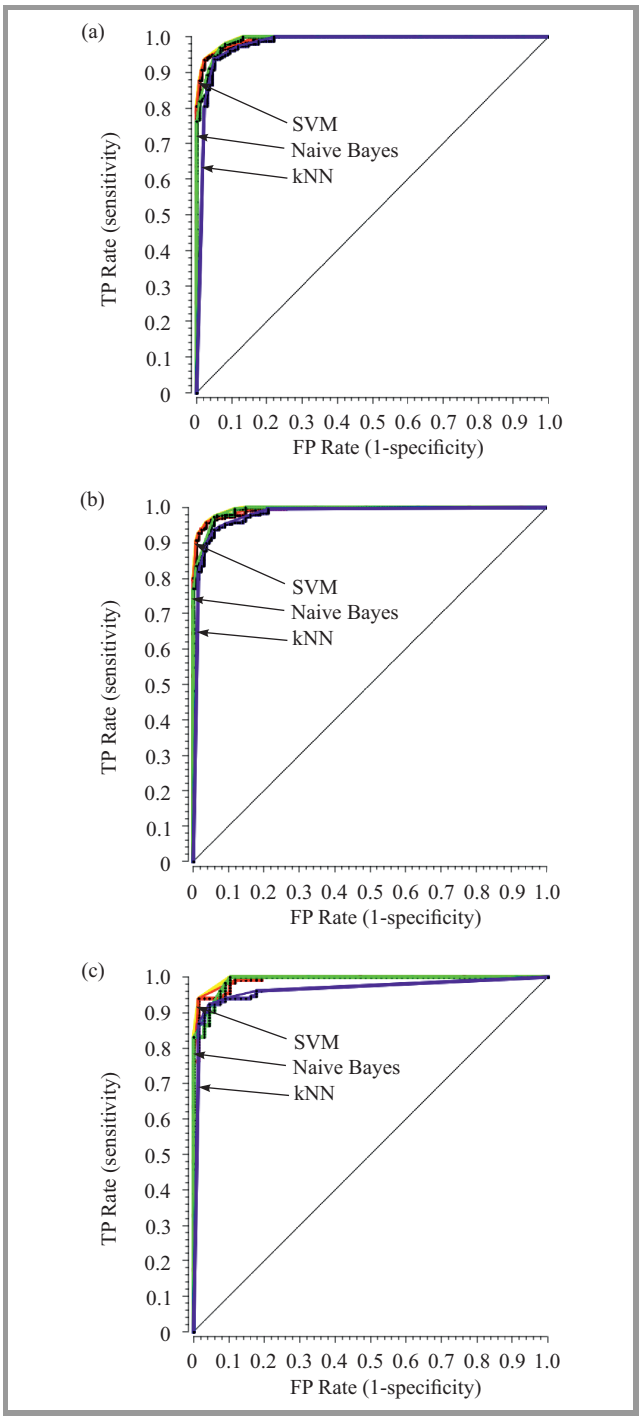


Fig. 9. Receiver operating characteristic curves for *k*NN, NB and SVM based systems: (a) CV, (b) LOO, (c) RS.

The sensitivity of learning machine (Sens) is defined as follows:

$$Sens = \frac{TP}{TP+FP}, \tag{10}$$

where TP denotes the number of true positive predictions and FP the number of false positive predictions.
The specificity of learning machine (Spec) is defined as follows:

$$Spec = \frac{TN}{TN+FN}, \tag{11}$$

where TN denotes the number of true negative predictions and FN the number of false negative predictions.
The classification accuracy (CA) is defined by the ratio of number of correctly identified samples into the size of the dataset.

$$CA = \frac{TP+TN}{TN+FN+TP+FP}. \tag{12}$$

The accuracy of a test (AUC) depends on how well the test separates the data samples being tested. The accuracy is

measured by the area under the ROC (Receiver Operating Characteristic) curve plotted in the coordinate system with x-axis corresponding to the probability of false positive selection and y-axis corresponding to the probability of true positive selection. In this research, x-axis corresponds to the false alarm and y-axis to the true malware detection. In general, an area of 1 represents a perfect test; an area of 0.5 represents a worthless test. F-measure is a measure of a test's accuracy. It considers both the precision p (ratio of the number of correct results to the number of returned results) and the recall r (ratio of the number of correct results to the number of results that should have been returned) of the test to compute the score. The F-measure can be interpreted as a weighted average of the precision and recall, where the F-measure reaches its best value at 1 and worst score at 0.

The values of CA, Sens, Spec, AUC and F1 criteria calculated for kNN, NB and SVM based classification systems are collected in Table 4.

Table 4
Evaluation of kNN, NB, and SVM classification

Method	CV	LOO	RS
kNN			
CA	0.9371	0.9347	0.9246
Sens	0.9617	0.9579	0.9237
Spec	0.8905	0.8905	0.9265
AUC	0.9776	0.9788	0.9631
F1	0.9526	0.9506	0.9416
NB			
CA	0.9548	0.9548	0.9447
Sens	0.9655	0.9617	09542
Spec	0.9343	0.9416	0.9265
AUC	0.9910	0.9912	0.9898
F1	0.9655	0.9654	0.9579
SVM			
CA	0.9398	0.9422	0.9497
Sens	0.9808	0.9732	09774
Spec	0.8613	0.8832	0.8971
AUC	0.9937	0.9927	0.9907
F1	0.9552	0.9567	0.9623

The results for all validation experiments confirm a good quality of our classification systems. The obtained classification accuracy was from about 92 to 95%, sensitivity from 92 to 98%, and specificity from 86 to 94%. All validation experiments gave the similar results. However, the slight better specificity was obtained for NB, while sensitivity was the best for SVM.

5.4. Application of Classification Systems to Malware Detection

Finally, the kNN, NB and SVM based classification systems were used to malware detection. The systems trained on the training dataset consisting of 398 samples (the same that used in the experiments described in the previous section) were used to classify dataset consisting of 10747 samples. Hence, in contrary to the validation tests the training dataset was about five times smaller than the testing one. Moreover, both training and testing datasets contained different measurements.

The results of data classification are presented in Table 5. The quality of the classification systems is presented in Figs. 10 and 11 and Table 6. Figure 10 displays the obtained receiver operating characteristic curves (ROC) for all systems. Figure 11 shows the calibration plots.

Table 5
Confusion matrices (three classification systems)

Class	kNN [%]		NB [%]		SVM [%]	
	+1	–1	+1	–1	+1	–1
+1	58.4	8.2	73.8	15.2	76.1	15.3
–1	41.6	91.8	26.2	84.8	23.9	84.7

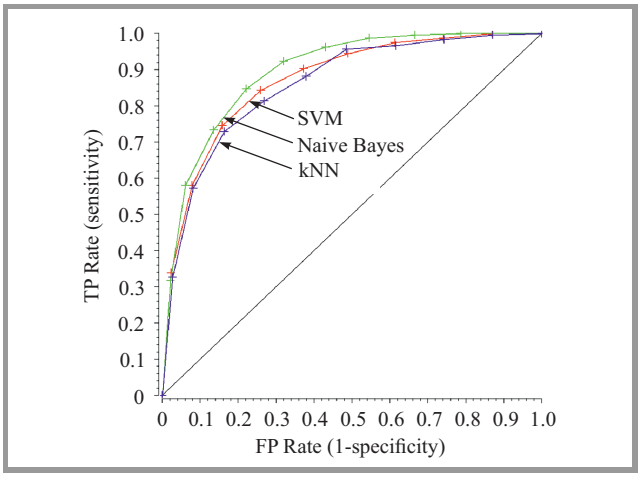


Fig. 10. Receiver operating characteristic curves for kNN, NB and SVM based systems.

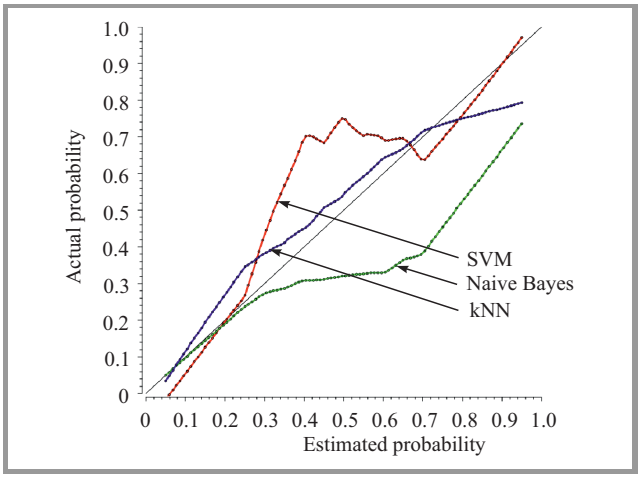


Fig. 11. Calibration plots for kNN, NB and SVM based systems.

The values of CA, Sens, Spec, AUC and F1 criteria calculated for the kNN, NB and SVM based systems are collected in Table 6.

Table 6
Evaluation of classification systems

Validation criterion	*k*NN	NB	SVM
CA	0.8117	0.8311	0.8342
Sens	0.4661	0.7669	0.4576
Spec	0.8259	0.9474	0.9641
AUC	0.8736	0.8991	0.8637
F1	0.5714	0.6630	0.5714

Next, the performance of the NB, *k*NN and SVN based classification systems was compared. Table 7 collects the training and classification times for all methods. The efficiencies of *k*NN and SVM are similar (training: 0.31–0.33 s, classification: 1.71–2.11 s). Both methods provide satisfactory results. It is obvious that the complexity of these methods depends on the assumed number of neighbors (*k*NN) and employed kernel core function (SVM). NB based classification system is much slower, and its execution time strongly depends on the size of a dataset.

Table 7
Training and classification times

Techniques	*k*NN	NB	SVM
$t_{training}$ [s]	17.21	5.91	5.03
$t_{classification}$ [s]	30.00	5.33	10.05

In general, the results presented in the tables and figures show that the classification systems employing *k*NN, NB and SVM methods provide a good accuracy classification (CA more than 80%). However, the results are of course much worse than in case of cross-validation experiments. The largest differences are observed for the specificity criterion.

6. Summary and Conclusion

In this paper the authors consider the application of three types of supervised learning methods: *k*-Nearest Neighbours, Naive Bayes, and Support Vector Machine to malware detection systems. These methods were used to the classification of data on the Web into malware and clean class. The performance of the methods was validated. The commonly used validation techniques, i.e., *k*-folds Cross-Validation, Leave One Out, and Random Sampling were applied.

Moreover, the systems were used to malware detection in real network. In general, the results of all experiments confirm that the examined classification methods achieve the relatively high level of accuracy, sensitivity, and specificity. Therefore, it can be expected that these methods could be successfully implemented in intrusion detection systems. However, the size of training dataset, selection of methods and their parameters strongly influences the results of classification. Dealing with unstructured data is the main strength of investigated methods especially in the case of computer network datasets that are frequently heterogeneous, unstructured and often incomplete. In authors opinion future work can be focused on optimization of calibration parameters in order to achieve better values of criteria.

Nevertheless, the computation of strong heterogeneous data, and pre-processing of this data is still heavy. Therefore, the classification of large dataset on the Web is still a challenging task. The further improvements of investigated methods are necessary to achieve efficient techniques for network security.

Acknowledgment

This research was partially supported by the "Nippon-European Cyberdefense – Oriented Multilayer threat Analysis (NECOMA)" FP7 grant agreement number 608533 and research fellowship within Project "Information technologies: Research and their interdisciplinary applications", agreement number UDA POKL.04.01.01-00-051/10-00.

References

[1] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning*, 2nd ed. Series in Statistics, Springer, 2009.

[2] W. S. Noble, "Support vector machine applications in computational biology", in *Kernel Methods in Computational Biology*, B. Schölkopf, K. Tsuda, and J.-P. Vert, Eds. Cambridge, USA: MIT Press, 2004, pp. 71–92.

[3] C. Wagner, G. Wagener, R. State, and T. Engel, "Malware analysis with graph kernels and support vector machines", in *Proc. 4th Int. Conf. Malicious and Unwanted Software MALWARE 2009*, Montreal, Canada, 2009, pp. 63–68.

[4] M. Krzyśko, W. Wołyński, T. Górecki, and M. Skorzybut, *Systemy uczące się* (*Learning systems*). Warszawa: Wydawnictwo Naukowo Techniczne, 2009, pp. 107–187 (in Polish).

[5] K. Rieck, T. Holz, C. Willems, P. Dussel, and P. Laskov, "Learning and classification of malware behavior", in *Proc. 5th In. Conf. DIMVA 2008*, Paris, France, 2008, vol. 5137, pp. 108–125.

[6] M. Amanowicz and P. Gajewski, "Military communications and information systems interoperability", in *Proc. Milit. Commun. Conf. MILCOM 96*, McLean, VA, USA, 1996, vol. 1–3, pp. 280–283.

[7] R. Kasprzyk and Z. Tarapata, "Graph-based optimization method for information diffusion and attack durability in networks", in *Rough Sets and Current Trends in Computing, LNCS*, vol. 6086, pp. 698–709, Springer, 2010.

[8] M. Mincer and E. Niewiadomska-Szynkiewicz, "Application of social network analysis to the investigation of interpersonal connections", *J. Telecommun. Inform. Technol.*, no. 2, pp. 81–89, 2012.

[9] M. Shankarapani, K. Kancherla, S. Ramammoorthy, R. Movva, and S. Mukkamala, "Kernel machines for malware classification and similarity analysis", in *Proc. Int. Joint Conf. Neural Netw. IJCNN 2010*, Barcelona, Spain, 2010, pp. 1–6.

[10] S. Forrest *et al.*, "Self-nonself discrimination in a computer", in *Proc. Comp. Soc. Symp. Res. Secur. and Priv.*, Oakland, CA, USA, 1994, vol. 10, pp. 311–324.

[11] I. Liane de Oliveira, A. Ricardo, A. Gregio, and A. M. Cansian, "A malware detection system inspired on the human immune system", in *Computational Science and its Applications – ICCSA 2012*, *LNCS*, vol. 7336, pp. 286–301, Springer, 2012.

[12] E. Stalmans and B. Irwin, "A framework for DNS based detection and mitigation of malware infections on a network", in Proc. *10th Ann. Inform. Secur. South Africa Conf. ISSA 2011*, Johannesburg, South Africa, 2011.

[13] M. Zubair Shafiq, S. Ali Khayam, and M. Farooq, "Embedded malware detection using markov n-grams", in *Detection of Intrusions and Malware, and Vulnerability Assessment*, T. Holz and H. Bos, Eds., *LNCS*, vol. 6739, pp. 88–107. Springer, 2008.

[14] M. Franklin, A. Halevy, and D. Maier. "From databases to dataspaces: A new abstraction for information management", *Sigmod Record*, vol. 34, no. 4, pp. 27–33, 2005.

[15] K. Lasota and A. Kozakiewicz, "Analysis of the Similarities in Malicious DNS Domain Names", in *Secure and Trust Computing, Data Management and Applications*, C. Lee, J.-M. Seigneur, J. J. Park, and R.R. Wagner, Eds. *Communications in Computer and Information Science*, vol. 187, pp. 1–6. Springer, 2011.

[16] Y. Yanfang, D. Wang, T. Li, and D. Ye, "IMDS: Intelligent malware detection system", in *Proc. 13th ACM SIGKDD Int. Conf. Knowl. Discov. Data Mining KDD'07*, San Jose, CA, USA, 2007, pp. 1043–1047.

[17] M. R. Faghani and H. Saidi, "Malware propagation in online social networks", in *Proc. Int. Conf. Malicious and Unwanted Software MALWARE 2009*, Montreal, Canada, 2009, pp. 8–14.

[18] P. Cunningham and S. J. Delany, "*k*-Nearest Neighbour Classifiers", Tech. Rep. UCD-CSI-2007-4, UCD School of Computer Science and Informatics, Dublin, 2007, pp. 1–17.

[19] J. M. Keller, "A fuzzy *k*-Nearest Neighbor algorithm", *IEEE Trans. Syst., Man, and Cybernet.*, vol. 15, no. 4, pp. 580–585, 1985.

[20] L. Jiang, H. Zhang and Z. Cai "A Novel Bayes Model: Hidden Naive Bayes", *IEEE Trans. Knowl. Data Engin.*, vol. 21, no. 10, pp. 1361–1371, 2009.

[21] V. N. Vapnik, *The Nature of Statistical Learning Theory*. New York: Springer, 1995.

[22] A. Borders and L. Bottou, "The Huller: a simple and efficient online SVM", in *Machine Learning: ECML-2005*, J. Gama, R. Camacho, P. Brazdil, A. Jorge, and L. Torgo, Eds., *LNCS*, vol. 3720, pp. 505–512. Springer, 2005.

[23] J. Koronacki and J. Ćwik, *Statystyczne systemy uczące się* (*Statistical learning systems*). Warsaw: Exit, 2008 (in Polish).

[24] T. Joachims, "Support Vector and Kernel Methods", SIGIR-Tutorial, Cornell University Computer Science Department, 2003.

[25] N. Cristianini and J. Shawe-Taylor, *An Introduction to Support Vector Machines*, 1st ed. Cambridge University Press, 2000, pp. 25–29.

[26] E. Ikonomowska, D. Gorgevik, and S. Loskovska, "A survey of stream data mining", in *Proc. 8th Nat. Conf. Int. Particip. ETAI 2007*, Ohrid, Republic of Macedonia, 2007, pp. 16–20.

[27] T. Joachims, "Training linear SVMs in linear time", in *Proc. 12th ACM SIGKDD Int. Conf. Knowl. Discov. Data Mining KDD 2006*, Philadelphia, PA, USA, 2006 pp. 217–226.

[28] Kernel Machines homepage [Online]. Available: http://www.kernel-machines.org/

[29] C. Burges, "A Tutorial on Support Vector Machines for Pattern Recognition", *Knowledge Discovery and Data Mining*, vol. 2, no. 2, pp. 121–167, 1998.

[30] T. Jebara, "Multi-task feature and kernel selection for SVMs", in *Proc. Int. Conf. on Machine Learning*, Banff, Canada, 2004, pp. 55–63.

[31] F. R. Bach, G. Lanckriet, and M. Jordan "Multiple kernel learning, conic duality and the smo algorithm", in *Proc. 21st Int. Conf. Machine Learning ICML'04*, Banff, Canada, 2004, pp. 6–13.

[32] F. R. Bach, R. Thibaux, and M. I. Jordan, "Computing regularization paths for learning multiple kernels" in *Advances in Neural Information Processing Systems*, L. K. Saul, Y. Weiss, and L. Bottou, Eds. MIT Press, 2005, pp. 73–80.

[33] N6 Platform homepage [Online]. Available: http://www.cert.pl/news/tag/n6

[34] G. M. Draper, "Interactive radial vizualizations for information retrieval and management", Ph.D. Thesis, Univertity of Utah, 2009, Chapter 3.

Michał Kruczkowski received his M.Sc. in Electronics and Telecommunications from the Gdańsk University of Technology in 2011. Currently he is a Ph.D. student at the Institute of Computer Science, Polish Academy of Sciences. Since 2013 he works at the Research and Academic Computer Network (NASK). His research interests focus on artificial intelligence, analysis of strongly heterogeneous datasets, advanced statistical models, machine learning.

E-mail: Michal.Kruczkowski@nask.pl
Research and Academic Computer Network (NASK)
Wąwozowa st 18
02-796 Warsaw, Poland

E-mail: M.Kruczkowski@phd.ipipan.waw.pl
Institute of Computer Science
Polish Academy of Sciences
Jana Kazimierza st 5
01-248 Warsaw, Poland

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 Director for Research of Research and Academic Computer Network (NASK). The author and co-author of three books and over 140 journal and conference papers. Her research interests focus on complex systems modeling, optimization and control, computer simulation, parallel computation, computer networks and ad hoc networks. She was involved in a number of research projects including EU projects, coordinated the Groups activities, managed organization of a number of national-level and international conferences.

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

E-mail: ewan@nask.pl
Research and Academic Computer Network (NASK)
Wąwozowa st 18
02-796 Warsaw, Poland

Paper

Usability Analysis of a Novel Biometric Authentication Approach for Android-Based Mobile Devices

Vincenzo Conti[1], Mario Collotta[1], Giovanni Pau[1], and Salvatore Vitabile[2]

[1] *Faculty of Engineering and Architecture, Kore University of Enna, Cittadella Universitaria, Enna, Italy*
[2] *Department of Biopathology and Medical and Forensic Biotechnologies, University of Palermo, Palermo, Italy*

Abstract—Mobile devices are widely replacing the standard personal computers thanks to their small size and user-friendly use. As a consequence, the amount of information, often confidential, exchanged through these devices is raising. This makes them potential targets of malicious network hackers. The use of simple passwords or PIN are not sufficient to provide a suitable security level for those applications requiring high protection levels on data and services. In this paper a biometric authentication system, as a running Android application, has been developed and implemented on a real mobile device. A system test on real users has been also carried out in order to evaluate the human-machine interaction quality, the recognition accuracy of the proposed technique, and the scheduling latency of the operating system and its degree of acceptance. Several measures, such as system usability, users satisfaction, and tolerable speed for identification, have been carried out in order to evaluate the performance of the proposed approach.

Keywords—fingerprints authentication, mobile device security, operating system, usability.

1. Introduction

In the actual technological scenario, where Information and Communication Technologies (ICT) provide advanced services, mobile computing systems need strong procedures to protect data and resource access from unauthorized users. The continuous advances of technology require high security levels, especially in mobile devices. More and more users are urged to enter proprietary data on these devices, in order to access to a greater number of services [1], [2].

Authentication procedures, based on the simple PIN or username/password pair, are not sufficient to provide a suitable security level for applications requiring high protection of data and services. Biometric based authentication systems represent a valid alternative to conventional approaches [3]. In this field, the identity management is related to the manipulation, storage and protection of personal biometric templates inside an electronic environment. Biometry represents a secure approach for identity management and personal authentication [4]. For trusted authentication, a secure infrastructure where each user could be reliably authenticated is required. Trustiness is an essential requirement when transactions must be executed without limits and compromises. Critical ICT services supplied to people (e.g. e-commerce or e-banking) need a high level of security [5]. A trusted biometric authentication system has to reduce the point-of-attacks in the recognition chain and has to give the capability to authenticate people with a high level of certainty. So, the eventual release of an application or a service is made through a biometric module (fingerprints control) on the basis of who the user is.

The main aim of this paper is to evaluate the feasibility and the acceptability of a biometric authentication system on a mobile device, addressing user reactions for the fingerprint acquisition, processing, and verification time. The results of these tests may be useful for future developers in order to find the optimization limit and the right trade-off for future biometric system implementations on mobile devices.

The paper has been structured as follows. Section 2 discusses the related works about authentication techniques and systems used on mobile devices. Section 3 describes the proposed approach. Section 4 reports the human-machine interaction evaluation techniques and the related experimental results in terms of user satisfaction. Finally, some concluding remarks are reported in Section 5.

2. Related Works

Android offers several techniques to protect the mobile device. These techniques are all related to screen lock and not to each application start. To configure this protection mode is enough to manage security settings. The latest versions of Android offer different possibilities to unlock:

- none – when the power button is pressed (even accidentally) the screen turns on and provides access to all device features (no security);
- numerical code (PIN) – the user chooses a numerical sequence of at least 4 digits. When the power button is pressed, the user must enter the sequence in the right way, in order to access to all device functions (medium security);

- password – the user chooses an alphanumeric case sensitive password. To unlock the device, the user must enter the characters in the exact sequence. In the event that the user enters an incorrect password five times, the device will be blocked for 30 seconds, in order to avoid attempts to unlock the device with brute force methods (high security);
- sequence type – this is a graphic unlock method. A grid with nine elements (3×3) is shown to the user. The release occurs only if the elements are touched in the right order and without lifting the finger from the screen (medium-low security);
- scrolling – when the button is pressed, different unlocking options are shown to the user in order to directly access to some device features, such as the camera or the homepage. This mode only protects against in adverting break outs (no security);
- face unlock (beta) – through a facial recognition algorithm and using the device's camera, the face of the user is recorded, specifically the eyes and mouth positions. Google considers this feature "unsafe" as the level of facial recognition has been lowered in order to enhance usability. In addition, after many users' reports related to the possibility to unlock the device using a photo of the owner, Google and Samsung have solved this problem by putting a parameter called "vitality control". In practice after facial recognition, the user must wink to unlock the device. In addition, this unlock function provides several customizations. For example it allows the user to enter four self-portraits in different conditions (with glasses, beard, with low light). In this way the user does not have to reconfigure the device to any appearance change.

The lock screen has various functions for security and it protects the mobile device from involuntary pressures of keys (for example when the device is in a pocket or in a purse). At the same time the lock screen provides protection both in case in which the device is left unattended and in case of theft or loss. In case of theft, the lock screen does not provide any protection against the device formatting, which determines all data loss and security settings reset.

In order to provide higher security, the unlock password should be saved online. The access to this password should happen only after the user enters the same password. This can make the devices theft more difficult but not impossible, because a formatting done by an experienced user could transform the device into another. In [6] the authors describe the permission-based security models. This system uses a computer security technique that allows the administrator and operating system to restrict applications to access specific resources. Throughout the analysis, they discover several phenomena that verify past research, and new potentials in permission-based security models that may provide additional security to the users. In [7] the authors, in cooperation with a security expert, carried out a case study with the mobile phone platform Android, and employed the reverse engineering tool-suite Bauhaus for this security assessment. During the investigation they found some inconsistencies in the implementation of the Android security concepts.

In [8], the authors present the current state of smartphone security mechanisms and their limitations in order to identify certain security requirements for proposing enhancements for smartphones security models. In [9] the authors present their upgraded Lock Screen system, which is able to support authentication for the user's convenience and provide a good security system for smartphones. They also suggest an upgraded authentication system for Android smartphones. All these considerations have led many researchers to study innovative techniques to improve security on all kind of devices. Different studies and implementations of biometric authentication systems based on different features were published in the literature. Usually, both software and hardware standard approaches are based on three main steps: image enhancement phase, extraction of biometric identifiers, and matching phase. In what follows, the most meaningful works are briefly described. In [10] the authors present a multimodal biometric identification system based on the combination of geometry and fingerprint features of the human hand. Hand images are acquired with a commercial scanner (150 dpi resolution) while support vector machines technique is used as verifier. In [11] the author makes new observation about fingerprint recognition that uses state of the single steak in the fingerprint image, because patterns of the veins in the fingerprint without notice of the fingerprint about person, and can be used for identified person. This algorithm can work on gray scanned photo and also its work very fine on the binary images. Whereas the insecurity of a system can be easily exaggerated even with little minor vulnerability, the security is not easily demonstrated.

In [12] the authors represent the system in terms of a state machine, elucidate the security needs, and show that the specified system is secure over the specified states and transitions. The authors expect that this work will provide the basis for assuring the security of the Android system. Multi-modal biometric fusion is more accurate and reliable compared to recognition using a single biometric modality, as said by author of [13]. Their goal is to advance the state-of-the-art in biometric fusion technology by providing a more universal and more accurate solution for personal identification and verification with predictive quality metrics. In [14] the authors focus their attention on the technical details and performance comparison of various available fingerprint sensors and explore the future direction and system development that states using similar techniques for chance or latent fingerprint enrolment. The study and experiments carried out indicate that the error occurred due to poor calibration causes a greater impact on the generated overall system output and serious usabil-

ity issues with respect to handling of fingerprint sensors. In [15] the authors proposed a novel fingerprint matching algorithm based on minutiae sets combined with global statistical features. The approach has the advantage of considering both local and global features for the fingerprint matching task. The above feature improves the accuracy of matching score without increasing of time and memory consuming.

In [16] the authors realized a software authentication system that refers to classical methods for fingerprint enhancement. Fingerprint is processed with two filters in order to enhance images quality. The first filter is based on two-dimensional Fourier transform for reducing low and high frequency noise. The second filter equalize fingerprint image grey levels. The last elaboration is then related to minutiae extraction. All the minutiae are sorted as to the distance by the image center. The processing time using a standard general purpose PC is 11.4 s. In [17] the authors proposed a hardware system using the pipeline technique to increase the final throughput. Various tasks were implemented on Altera FLEX10KE FPGA. An initial Gaussian filtering is used to enhance fingerprint quality and an edge-detection algorithm is applied to segment fingerprint ridges. Finally, a thinning algorithm is applied before the minutiae extraction task. The execution time is of 589.93 ms. In [18] the authors developed a prototype for fingerprint authentication through a Xilinx Virtex-II FPGA based board. The proposed architecture can be broken in 3 levels, where the lower level is constituted by hardware platform. In the enrollment phase, the extracted biometric template is stored into the FPGA memory. The execution time is about 5 s. In [19] the author presents and analyses the typical and known attacks against biometric systems and outlines several solutions to protect and design a secure biometric system. The advantages and disadvantages of each proposed technique was then discussed.

In [20] the authors make a biometric secured mobile voting. This is a novel technology and also first of its kind at present. Using fingerprint based biometric control information and encryption along with SSL using VeriSign would make the software involved in the voting process well secured. In addition tying the credentials to a mobile device will make the system even more robust. The next generation of banking applications won't be on desktop or mainframes but on the small devices we carry every day. In [21] authors have focused on how biometric mechanism provides the highest security to the mobile payment. The present security issues surround the loss of personal information through the theft of the cell phone. The authors present the proposed biometrics mechanism in order to make more secure the mobile payment and also to provide security at the wireless transmission level. In [22] the authors present a new way of generating behavioral (not biometric) fingerprints from the cellphone usage data. In particular, they explore if the generated behavioral fingerprints are memorable enough to be remembered by end users. They built a system, called HuMan that generates fingerprints from cellphone data. Android is one of the most popular and fully customizable open source mobile platforms that come with a complete software stack. One of the main reasons behind the rapid growth in adoption of smartphones is their capability to facilitate users with third-part applications. However, this rapid growth in smartphone usage and the ability to install third-part applications has given rise to several security concerns.

3. The Proposed Novel Approach

The fingerprinting is the basis of presented approach. In the market there are several sensor typologies:

- optical – the fingerprint is detected using the reflection law, in order to have a good contrast image;
- capacitive – a series of silicon sensors read a small part of the fingerprint and then join it in the complete image;
- ultrasonic – the sound waves strike the finger surface and based on the return signal valleys and ridges are defined;
- thermal – it uses the temperature difference between the valleys and ridges of the fingerprint.

In this approach the authors would like not use any fingerprint scanner since we have carried out a feasibility study for a future implementation. It will be possible to detect the fingerprint in any part of the screen, without the use of a specific sensor. In presented model, it is important that the fingerprint is detected directly through the screen, as detection must be almost invisible to the authorized user. Compared to other detection systems which deal with the device unlock only, a continuous control in order to check

Table 1
Device datasheet

Parameter	Value
Product name	LG Nexus 5
Wireless connectivity	Wi-Fi a/b/g/n/ac
Dimensions	$17.84 \times 69.17 \times$ 8.59 mm
Display	495 Corning Gorilla Glass 3 1080×1920 multi-touch 5 point
CPU clock frequency	2.26 GHz
Processor	Quad core Qualcomm Snapdragon 800
RAM	2 GB
Memory	32 GB integrated

user identity when each activity starts is inserted. An application for the Android platform has been developed in order to control the system. Every 500 ms a background application checks if running activities are in the authorized applications list. If an activity is not present, the system controls the user fingerprint. The list of authorized activities, is refreshed every 5 min and at every device rebooting. In the final version a variable will be included in order to count invalid fingerprint-based accesses. When the fifth failed attempt occurs, the device activates the lock-screen and delegates to Android policies the access management. The application was tested on a device whose data sheet is shown in Table 1.

3.1. Model Processing Phases

The idea of the proposed system is shown in Fig. 1. The system checks if the user is trying to access to an authorized application. If the desired application is not in the authorized applications list, the system provides a biometric control based on fingerprint recognition. In case of recognized fingerprint, the system will insert the application in the authorized applications list allowing the access. Otherwise the system will lock the screen denying the access.

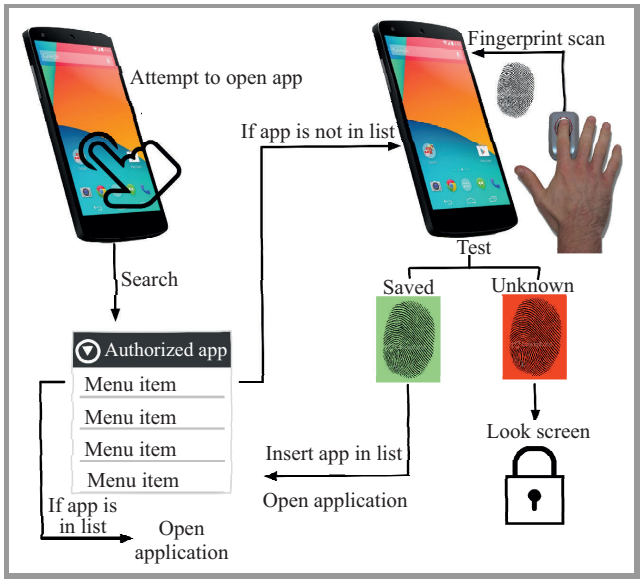


Fig. 1. The proposed system architecture.

Figure 2 describes the algorithm functioning. The number of possible access attempts is indicated by the variable *Number of attempts* (NoA), initially set to zero. The user will try to access to an application. The system controls if it is an enabled application or not. In the case of enabled application, the application will be launched. Otherwise, the system will check fingerprint to see if the access attempt has been made by the owner. If the fingerprint is recognized, the application will be included in the authorized applications list. Otherwise, the variable NoA will be incremented by one. The number of possible attempts

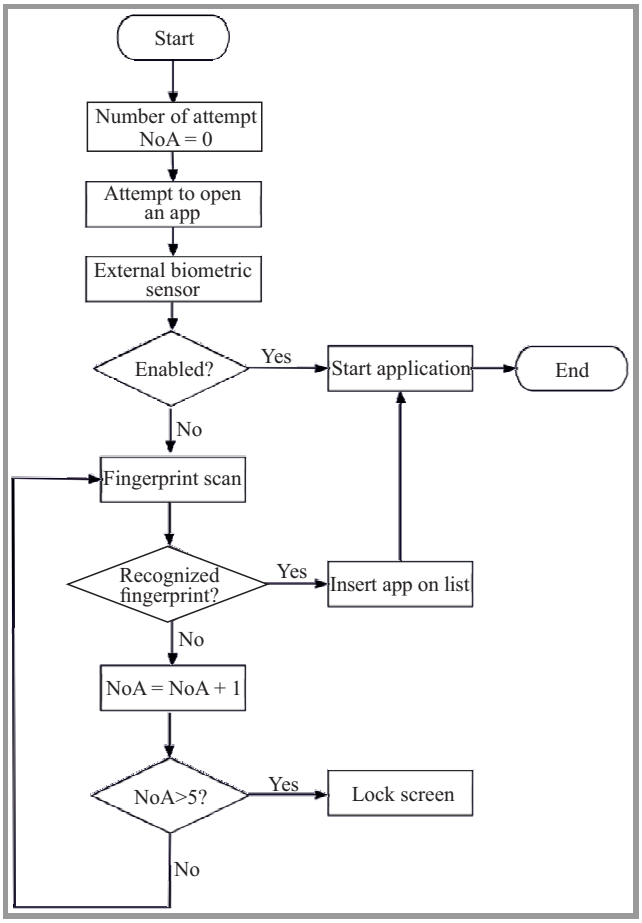


Fig. 2. Algorithm dataflow of the proposed approach.

is five. Exceeded five attempts, the system will lock the screen.

3.2. Fingerprint Authentication System

The goal of an authentication system is to compare two fingerprint images: a fingerprint captured and processed in the startup phase with the fingerprint acquired in real time. With more details, two steps, an off-line and on-line step, compose this model. In the off-line step the user's fingerprint is captured, processed and stored in the mobile device. In the online step the user gives its own fingerprint to verify the identity – the fingerprint is compared with one stored. The most used authentication systems are based on Minutiae or Singularity points.

In this work, three different authentication systems have been implemented using good quality fingerprint images. These authentication systems are characterized by different execution times and accuracy rates. Usually, authentication systems very strong in terms of accuracy rates have very high execution times and vice versa. Since the proposed biometric module is oriented to mobile devices, the final systems must be implemented in order to reduce the execution time maintaining a good accuracy level. Only one of these three systems, achieving the best compromise, will be used in the final mobile device.

First implementation: Algorithm 1

It is based on Singularity points extraction using the Poincaré indexes [23]. It is composed only by the following steps:

- directional image extraction – every element represents the local ridges orientation in the original grey-scale image;
- Poincaré indexes technique – it is computed by summing the orientation changes along a closed curve around the pixel of interest. Poincaré index, making a full counter-clockwise turn along the curve in the orientation field image, the direction angle is equal to $0°$, $\pm 180°$ or $\pm 360°$. So, according by the value of the Poincaré index (0 when orientation angle change is $0°$, $\frac{1}{2}$ when orientation angle change is $180°$, $-\frac{1}{2}$ when orientation angle change is $-180°$), the system is able to detect the singular points;
- matching technique [24] – two matching algorithms are applied: the single rotation matching and the multiple rotation matching. The single rotation matching is applied when the algorithm receives images with two singularity regions for each fingerprint and if the singularity regions are of same type and the difference of their relative distances is lower a threshold. The multiple rotation matching algorithm is applied when a fingerprint image has only a singularity region. The XOR operator is applied between the correspondent regions to obtain the similarity degree.

Second implementation: Algorithm 2

It is based on Minutiae extraction and a robust matching algorithm. It is composed by the following steps:

- binarization algorithm – this step aims to obtain a binary image, where pixels can assume a binary value;
- thinning algorithm – it aims to reduce ridge thickness to the unitary value;
- minutiae extraction algorithm – it is devoted to minutiae analysis (i.e. ending points and bifurcation points classification) and localization. As results, for each detected minutia, spatial coordinates are used to generate fingerprint template;
- alignment algorithm – it calculates roto-translation parameters if the value of Euclidean distance is lower than a threshold. The rotation parameter is based on the differences between the corresponding angles in the selected minutiae pairs. The translation parameter is based on the differences between the respective Cartesian coordinates in the selected minutiae pairs;
- matching technique [25] it is performed between the roto-translated test and template image. For each test image minutia, all template image ones are considered to calculate the differences between respective coordinates $x - y(\overline{diff}_{xy})$ and angles $\theta(\overline{diff}_{theta})$. Only when these differences are lower than two thresholds the first partial score is obtained and mapped into $[0, 1]$ range. Among all complete scores, only the greater is considered.

Third implementation: Algorithm 3

It is based on Minutiae extraction and a fast matching algorithm. It is composed only by the following steps:

- binarization algorithm – the same used for Algorithm 2;
- thinning algorithm – the same used for Algorithm 2;
- minutiae extraction algorithm – the same used for Algorithm 2;
- matching technique [26] off-line registration phase and one acquired during the authentication phase. It is based only roto-translation comparisons of Minutiae individualized.

4. Human-Machine Interaction Evaluation Techniques

Usability is defined in ISO 9241 standard, as "*the effectiveness, the efficiency and the satisfaction with which specified users achieve certain goals in determined contexts*". This standard provides a general definition applicable to digital interfaces and many other areas. In any case, an absolute definition of usability does not exist as usability is always compared to a user who needs to reach a certain goal. In the user-centered design context, usability is aimed to see how people relate with a certain product as objective as possible. The simplicity and standards compliance are essential to usability. The user's interest relates only to the product and its pure functionality. To find out if an application is usable it is necessary to know how a user can achieve a specific goal (effectiveness) in a reasonable amount of time (efficiency), finding comfortable and enjoyable this experience (satisfaction). The best way to understand it is through usability testing with users [27].

The main goal of the test is to study the behavior of users which interact with real products or prototypes [28]. Moreover it is really important to identify problems and bottlenecks of the interface, in order to be able to correct them during the design phase.

Another important point is to understand how the user moves and thinks its difficult reasons in order to address them in the design phase. The tests require that each user is observed individually, and not in group. Furthermore, the performed tasks must be coherent for each participant. These aspects are always present in all test methods and the rest will change depending on the constraints of each project. A very important step is the usability test planning [29]. This phase is focused on a number of factors on which the entire test is based: test objectives, user characteristics, tasks and questionnaire characteristics at the end of test.

Some requirements of usability test include:

- identification of all the variables involved in the interaction between user and product. Typically, they involve certain assumptions on the tested users, but also on the interface characteristics, and on what can vary and affect system performance;
- subjects recruitment – users can be divided in statistically equivalent groups;
- precise experimental hypothesis – the test is a real scientific experiment. Through the control of the involved variables the main aim is to verify a certain hypothesis;
- rigorous measurement of the experimental values – relevant data are collected for measurement and analysis of necessary variables (number of errors, number of clicks, execution time, etc.);
- statistical analysis – collected data are analysed and adjusted according to appropriate statistical techniques.

If necessary, during the test it is possible to record the session. However, the presence of a camera can embarrass the user and it is not always recommended. The test can be conducted through the think aloud technique [30], which asks users to verbalize aloud their thoughts, comments and emotions during the test. The think aloud method shows the differences between the designer and the user mental model. The main goal is to bring closer these two models as much as possible. In other cases it is possible to use the eye-tracking [31], a hardware and software technology that allows to track the user's eye movements while looking at the interface. The eye tracking is very useful when it is necessary to get very accurate and quantitatively significant data, for example to analyse the key pages of the application, to make comparative studies of different versions, to see the visual impact of the display.
The usability test on mobile touch devices must also take into account other technical constraints:

- sound – users may not feel it or, on the contrary, may have to disable it in order to avoid disturbing people around them;
- light conditions – mobility user might want to use the interface in non-optimal lighting conditions. So, it is very important the contrast between the background and text elements in the foreground;
- connection – it is necessary to optimize the loading time. For example, it is possible to load the main info immediately or define information architecture for this purpose;
- screen size: it is possible to optimize the interface in order to avoid unnecessary vertical or horizontal scrolling;
- touch: clickable elements must be sufficiently spaced.

4.1. Human-Machine Interaction Evaluation Test-bed

In order to validate presented approach a usability test has been implemented. The usability test involved 100 users for a qualitative and a quantitative test. With more details, user satisfaction and the percentage of tasks successfully completed (success rate) have been measured. After an initial briefing where the participants to the test goals have been introduced, each user was escorted to a separate room in order to feel at ease and concentrate on the goals of the test. The test does not provide audio or video recordings, it does not use the think aloud or the eye tracking methods. In order to collect feedbacks from users it has been prepared an analysis grid of critical situations accompanied by a short final questionnaire to gather tips. The Android application, installed on the mobile device, has been implemented in such a way to track user usage.
First of all, not having a device with a fingerprint detector, images acquired with external equipment have been used. With more details, to quantify the user satisfaction, it has been optimized the touches number on the various buttons and the number of applications starts. Figure 3 shows the user satisfaction after interacting with three different biometric recognition algorithms. The results show that the Algorithm 3 has received the greater number of positive feedback in order to execution time and accuracy rate.

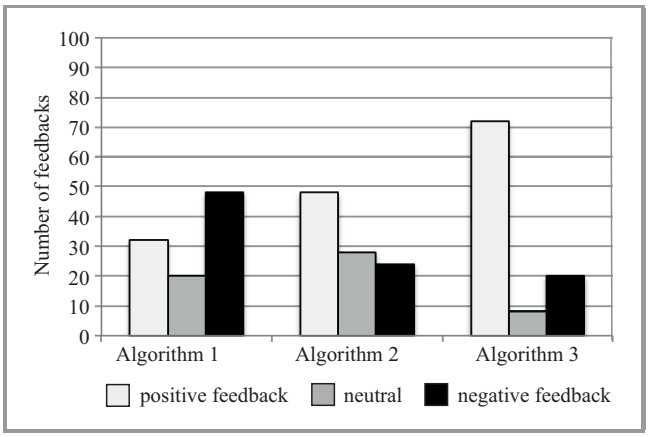


Fig. 3. User satisfaction feedbacks using the different implementation of the biometric recognition algorithm.

One of the most important Algorithm 3 phases is related to the minutiae identification and extraction. First of all, the thinning algorithm has been applied in order to obtain fingerprint ridges with size of 1 pixel. After, for the entire image, all 3×3 submatrices have been analyzed to calculate the number of black pixels. In every submatrix with a central black pixel, the following cases can be obtained:

– 1 black pixel – it is an isolated point;

– 2 black pixels – it is a minutia, said end-point;

– 4 black pixels – it is a minutia, said bifurcation.

In the proposed system, the minutia characteristics as position (spatial coordinates in Cartesian axes) and type have

Table 2
LG Nexus 5 processing times

No.	Binarization [ms]	Thinning [ms]	Minutiae extraction and post-processing [ms]	Matching algorithm [ms]	Total [ms]
1	66	1033	1474	87	2660
2	80	1282	1579	95	3036
3	46	1008	1474	85	2613
4	70	1227	1609	104	3010
5	73	1124	1506	101	2804

been considered. In addition, to decrease the number of false minutiae due to the noise presence, some choices have been made:

– all end-points and bifurcations located in the image edge are discarded;

– all end-points and bifurcations too close together are discarded.

The implemented fingerprint authentication system on the LG Nexus 5 has given the following experimental results in terms of minutia extraction (Fig. 4), execution time and accuracy. Table 2 shows the obtained processing time using the Algorithm 3 implementation on the Android device. The five rows correspond to tests carried out on five different fingerprints. The average time measured was 3 s. This is a tolerable value considering what expressed by users. Experimental results show good performance about the proposed system. Figure 5 shows tips provided by user regarding the Android application. Most of the users which participated at the usability test would like a biometric recognition speed improvement. This

Fig. 4. The proposed fingerprint authentication systems implemented on the LG Nexus 5: (a) the original fingerprint image, (b) the binarized fingerprint image, (c) the thinning fingerprint image, (d) detected minutiae, (e) the minutiae (end points and bifurcations) extracted after checking its distance.

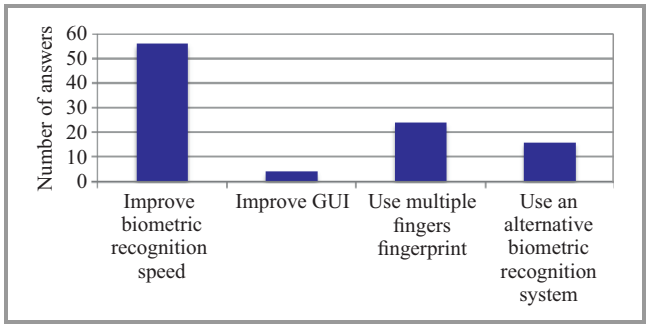


Fig. 5. Tips provided by users on the biometric application.

speed will be significantly improved when the biometric recognition system will be integrated directly into the mobile device.

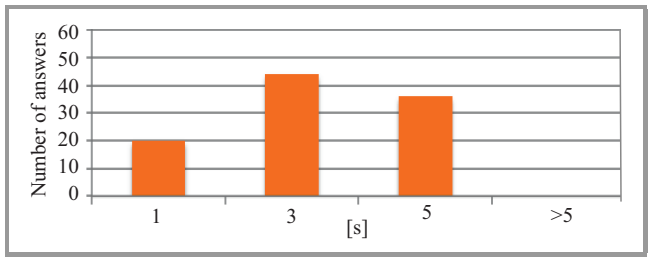


Fig. 6. Answers provided by users on the tolerable biometric recognition speed.

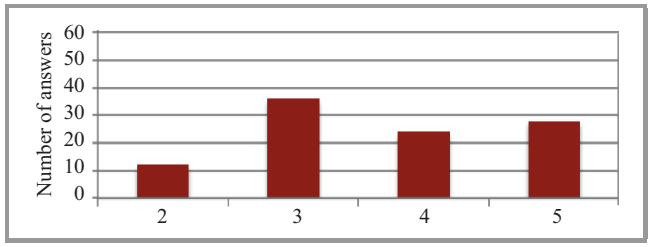


Fig. 7. Answers provided by users on the desired fingers acquisition number for biometric recognition.

The user's tolerance level about the biometric recognition speed is shown in Fig. 6. Users tolerate a biometric recognition speed ranging between 3 and 5 s. Figure 7 shows the answers provided by users regarding the desired fingers number for biometric recognition. It is clear that users want to use fingerprints from multiple fingers. Figure 8 shows the answers provided by users regarding to an alternative biometric recognition system. Among the various proposed

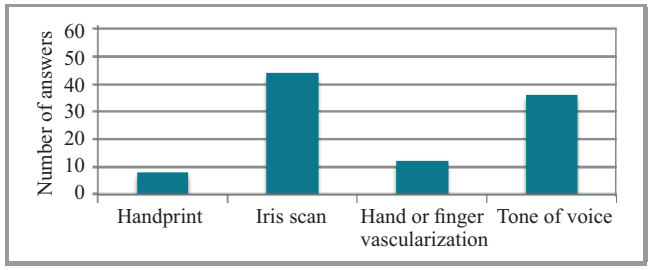


Fig. 8. Answers provided by users on an alternative mobile biometric recognition system.

systems users would be more willing to use an iris scan system or a tone of voice recognition system.
Finally the Success Rate (SR), related to tasks to be performed by each user, has been evaluated using the following equation [32]:

$$SR = \frac{Successful\_trials + (Partially\_Successful \cdot 0.5)}{Total\_trials} \quad (1)$$

Two parameters are also considered. The Precision (also known as positive predictive value) is the fraction of retrieved instances that are relevant, and the Recall (also known as sensitivity) is the fraction of relevant instances that are retrieved. Precision and Recall [33] are then defined through the Eqs. 2 and 3, respectively:

$$Precision = \frac{TP}{TP+FP}, \quad (2)$$

$$Recall = \frac{TP}{TP+FN}, \quad (3)$$

where TP is the True Positive value, TN is the True Negative value, FP is the False Positive value, and FN is the False Negative value. Specifically, the instance is negative and it is predicted negative in TN, the instance is positive and it is predicted positive in TP, the instance is positive but it is predicted negative in FN, and, finally, the instance is negative but it is predicted positive in FP.

Table 3
Hit and failure percentages

Task	Success [%]	Partial success [%]	Failure [%]
1	92	8	0
2	94	6	0

As shown in Table 3, the usability test has been carried out considering two specific tasks: the search of the application to launch in the list of enabled applications (Task 1) and the fingerprint control (Task 2). Moreover, the percentages of success and failure are also shown in Table 3. Using Eq. 1, the success rate of both tasks has been calculated as:

$$SR = \frac{172 + (28 \cdot 0.5)}{200} = 93\% \quad (4)$$

Then the Precision and Recall parameters, always considering 100 users, have been calculated. The measured occurrences of TP, FP, TN and FN are shown in Table 4. Moreover, Precision and Recall rates have been calculated for both tasks, using Eqs. 2 and 3 and the results are listed in Table 5.

Table 4
Authentication system: Precision and Recall

Parameter	Task 1	Task 2
TP	88	84
TN	0	4
FP	4	8
FN	8	4

Table 5
Precision and Recall of Task 1 and Task 2

Parameter	Task 1 [%]	Task 2 [%]
Precision	95.6	91.3
Recall	91.7	95.4

A statistical analysis has been also carried out through the MedCalc software [34] suite. This analysis focused on the inter-rater reliability (or even "agreement between judges") that measures the degree to which the ratings of two or more judges are consistent beyond the case. In the first analysis the Intraclass Correlation Coefficient (ICC) [35], [36], a measure of the reliability of measurements or ratings, has been calculated. For the purpose of assessing inter-rater reliability and the ICC, two or preferably more raters rate a number of study subjects. In this case different users rate the three algorithms. It is necessary to made a distinction between two study models: (1) each algorithm is rated by a different and random selection of a pool of raters/users, and (2) each algorithm is rated by the same raters/users. In the first model, the ICC is always a measure for "absolute agreement"; in the second model a choice can be made between two types: "consistency" when systematic differences between raters are irrelevant, and "absolute agreement", when systematic differences are relevant.

Table 6
Intraclass Correlation Coefficient

	Intraclass Correlation	95% confidence interval
Single measures	0.6037	0.2653 to 0.9841
Average measures	0.6037	0.2653 to 0.9841

In the presented analysis, the authors considered this last case and the results are shown in Table 6. In detail, the "Intraclass Correlation" represents the degree of absolute agreement among measurements, the "Single measures" estimates the reliability of single ratings (an index for the reliability of the ratings for one, typical, single rater) and the "Average measures" estimates the reliability of averages of k ratings (an index for the reliability of different raters averaged together, always higher than the Single measures ICC).

5. Conclusions

In new generation mobile devices, biometrics can be a safe approach for user identity and authentication management. However, in this context, a biometric authentication system must have an authentication capacity with a high level of security. Moreover, the biometric approaches are involved into the tasks scheduling of the operating system that can causes latency and then the user satisfaction can

be compromised. So, some real-time operations concerning human-machine interactions can slow down due to biometric authentication process. In this paper the feasibility of a trusted biometric authentication system has been evaluated. A deep analysis has been performed in order to evaluate users reactions towards the delay times for acquisition, processing and verification of fingerprints. The obtained results provide a clear guidance on the users' satisfaction about used algorithms and on the tolerable speed for identification. This information can be the main starting point for developers in order to find the optimum trade-off for future implementations.

References

[1] C. Militello, V. Conti, S. Vitabile, and F. Sorbello, "Embedded access points for trusted data and resources access in HPC systems", *The J. of Supercomput.*, vol. 55, no. 1, pp. 4–27, 2011.

[2] S. Vitabile, V. Conti, M. Collotta, G. Scatà, S. Andolina, A. Gentile, F. Sorbello, "A real-time network architecture for biometric data delivery in Ambient Intelligence", *J. Ambient Intelligence and Humanized Computing*, vol. 4, no. 3, pp. 303–321, 2013.

[3] C. Militello, V. Conti, S. Vitabile, and F. Sorbello, "An Embedded Iris Recognizer for Portable and Mobile Devices", *International Journal of Computer Systems Science & Engineering*, vol. 25, no. 2, pp. 119–131, 2010.

[4] V. Conti, C. Militello, F. Sorbello, and S. Vitabile, "A frequency-based approach for features fusion in fingerprint and iris multimodal biometric identification systems", *IEEE Trans. Syst., Man, and Cybernet. Part C: Applications & Reviews*, vol. 40, no. 4, pp. 384–395, 2010.

[5] S. Vitabile, V. Conti, C. Militello, and F. Sorbello, "An extended JADE-S based framework for developing secure multi-agent systems", *Comp. Stand. Interfsace J.*, vol. 31, no. 5, pp. 913–930, 2009.

[6] I. Rossameeroj and Y. Tanahashi, "Various approaches in analyzing android applications with its permission-based security models", in *Proc. IEEE Int. Conf. Electro/Inform. Technol. EIT 2011*, Mankato, MN, USA, 2011, pp. 1–6, 2011.

[7] B. J. Berger, M. Bunke, and K. Sohr, "An Android security case study with bauhaus", in *Proc. 18th Work. Conf. Reverse Engin. WCRE 2011*, Lero, Limerick, Ireland, 2011, pp. 179–183.

[8] S. Khan, M. Nauman, A. T. Othman, and S. Musa, "How secure is your smartphone: an analysis of smartphone security mechanisms", in *Int. Conf. Cyber Secur., Cyber Warfare and Digit. Forensic CyberSec 2012*, Kuala Lumpur, Malaysia, 2012, pp. 76–81.

[9] K. Il Shin, J. S. Park, J. Y. Lee, and J. H. Park, "Design and implementation of improved authentication system for Android smartphone users", in *Proc. 26th Int. Conf. Adv. Inform. Netw. Appl. Worksh. WAINA 2012*, Fukuoka, Japan, 2012, pp. 704–707.

[10] M. A. Ferrer, A. Morales, C. M. Travieso, and J. B. Alonso, "Low cost multimodal biometric identification system based on hand geometry, palm and finger print texture", in *Proc. 41st Ann. IEEE Int. Carnahan Conf. Secur. Technol.*, Ottawa, ON, Canada, 2007, pp. 52–58.

[11] B. Saropourian, "A new approach of finger-print recognition based on neural network", in *Proc. 2nd IEEE Int. Conf. Comp. Sci. Inform. Technol. ICCSIT 2009*, Beijing, China, 2009, pp. 158–161.

[12] W. Shin, S. Kiyomoto, K. Fukushima, and T. Tanaka, "Towards formal analysis of the permission-based, security model for Android", in *Proc. 5th Int. Conf. Wirel. Mob. Commun. ICWMC'09*, Cannes, France, 2009, pp. 87–92.

[13] Y. Tong, F. W. Wheeler, and X. Liu, "Improving biometric identification through quality-based face and fingerprint biometric fusion", in *Proc. IEEE Comp. Soc. Conf. Comp. Vision and Pattern Recog. Worksh. CVPRW 2010*, San Francisco, CA, USA, 2010, pp. 53–60.

[14] B. Ashwini, J. S. Digambarrao, and S. P. Patil, "Performance analysis of finger print sensors", in *Proc. 2nd Int. Conf. Mechan. Electron. Engin. ICMEE 2010*, Kyoto, Japan, 2010, pp. 169–174.

[15] P. Shi, J. Tian, Q. Su, and X. Yang, "A novel fingerprint matching algorithm based on minutiae and global statistical features", in *Proc. 1st IEEE Int. Conf Biometrics: Theory, Appl. and Syst.*, Washington, USA, 2007, pp. 1–6.

[16] M. Zsolt and V. Kovacs, "A fingerprint verification system based on triangular matching and dynamic time warping", *IEEE Trans. Pattern Anal. and Machine Intell.*, vol. 22, no. 11, pp. 1266–1276, 2000.

[17] V. Bonato, R. F. Molz, J. C. Furtado, M. F. Ferraao, and F. G. Moraes, "Propose of a hardware implementation for fingerprint systems", in *Field Programmable Logic and Application*, *LNCS*, vol. 2778, pp. 1158–1161, Springer, 2003.

[18] P. Schaumont and I. Verbauwhede, "ThumbPod puts security under your thumb", *Xilinx Xcell J.*, Winter 2004.

[19] P. Ambalakat, "Security of biometric authentication systems", in *Proc. 21st Computer Science Seminar*, Hartfort, USA, 2005.

[20] D. Gentles and S. Sankaranarayanan, "Biometric secured mobile voting", in *Proc. 2nd Asian Himalayas Int. Conf. Internet AH-ICI 2011*, Kathmandu, Nepal, 2011, pp. 1–6.

[21] M. Belkhede, V. Gulhane, and P. Bajaj, "Biometric mechanism for enhanced security of online transaction on Android system: A design approach", in *Proc. 14th Int. Conf. Adv. Commun. Technol. ICACT 2012*, PyeongChang, South Korea, 2012, pp. 1193–1197.

[22] P. Gupta *et al.*, "HuMan: Creating memorable fingerprints of mobile users", in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Worksh. (Percom Workshops)*, Lugano, Switzerland, 2012, pp. 479–482.

[23] H. Zhang, Y. Yin, and G. Ren, "An improved method for singularity detection of fingerprint images", in *Book Advances in Biometric Person Authentication*, *LNCS*, vol. 3338, pp. 516–524, Springer, 2004.

[24] V. Conti, C. Militello, S. Vitabile, and F. Sorbello, "Introducing pseudo-singularity points for efficient fingerprints classification and recognition", in *Proc. 4th IEEE Int. Conf. Complex, Intell. Softw. Intens. Syst. CISIS 2010*, Krakow, Poland, 2010, pp. 368–375.

[25] V. Conti, G. Vitello, F. Sorbello, and S. Vitabile, "An advanced technique for user identification using partial fingerprint", in *Proc. 7th Int. IEEE Conf. Complex, Intell. Softw. Intens. Syst. CISIS 2013*, Taichung, Taiwan, 2013, pp. 236–242.

[26] V. Conti, S. Vitabile, G. Vitello, and F. Sorbello, "An embedded biometric sensor for ubiquitous authentication", in *Proc. AEIT Ann. IEEE Conf.*, Mondello, Italy, 2013, pp. 1–6.

[27] G. Chao, "Human-computer interaction, the usability test methods and design principles in the human-computer interface design", in *Proc. Int. Conf. Comp. Sci. Inform. Technol. ICCSIT 2009*, Beijing, China, 2009, pp. 283–285.

[28] M. Lv, W. Hou, and C. Zhao, "Research of usability test mode based on the implicit user behavior lib", in *Proc. 9th Int. Conf. Comp.-Aided Indust. Des. Concept. Des. CAID/CD 2008*, Kunming, China, 2008, pp. 157–161.

[29] W. P. Brinkman, R. Haakma, and D. G. Bouwhuis, "Component-specific usability testing", *IEEE Trans. Syst., Man and Cybernet., Part A: Systems and Humans*, vol. 38, no. 5, pp. 1143–1155, 2008.

[30] L. Cooke, "Assessing concurrent think-aloud protocol as a usability test method: A technical communication approach", *IEEE Trans. Profess. Commun.*, vol. 53, no. 3, pp. 202–215, 2010.

[31] H. Fengpei, "The Studies of Eye Tracking and Usability Test", in *Proc. 7th Int. Conf. Comp.-Aided Indust. Des. Concept. Des. CAID/CD 2006)*, Hangzhou, China, 2006, pp. 1–5.

[32] T. Tullis, B. Thomas, and W. Albert, *Measuring the User Experience: Collecting, Analyzing, and Presenting Usability Metrics*. Morgan Kaufmann, 2010.

[33] D. L. Olson and D. Delen, *Advanced Data Mining Techniques*, 1st ed. Springer, 2008.

[34] MedCalc – User-friendly statistical software [Online]. Available: http://www.medcalc.org/index.php

[35] P. E. Shrout and J. L. Fleiss, "Intraclass correlations: uses in assessing rater reliability", *Psycholog. Bull.*, vol. 86, pp. 420–428, 1979.

[36] K. O. McGraw and S. P. Wong, "Forming inferences about some intraclass correlation coefficients", *Psycholog. Meth.*, vol. 1, pp. 30–46, 1996.

Vincenzo Conti is an Assistant Professor with the Faculty of Engineering and Architecture at the Kore University of Enna, Italy. He received his Laurea cum Laude degree and his Ph.D. in Computer Engineering from the University of Palermo in 2000 and 2005, respectively. His research interests include biometric recognition systems, programmable architectures, bio-inspired processing system, and user ownership in multi-agent systems. He has chaired and participated at several national and international conferences, coauthoring over 50 scientific publications, journals and conferences. Moreover, he has participated to several research projects funded by industries and research institutes in his research areas. Currently, he collaborates too with the Department of Chemical Engineering, Management, Mechanics and Computer Science (DICGIM) of the University of Palermo and with Council National of Researches (CNR) of Cefalú (Palermo).

E-mail: vincenzo.conti@unikore.it
Faculty of Engineering and Architecture
Kore University of Enna
Cittadella Universitaria
94100 Enna, Italy

Mario Collotta is an Assistant Professor with tenure in the Faculty of Engineering and Architecture at the Kore University of Enna, Italy, and since 2011 he is scientific responsible and director of Telematics Engineering Laboratory. His research activity is mainly focused on the study of real-time networks and systems. His interests concern the realization of strategies and innovative algorithms in order to ensure a flexible management of resources (band/CPU or resource allocation, battery consumption, etc,) in real-time systems and networks. The flexibility refers to the ability of the system to dynamically adapt to changes in its operating conditions, without reconfiguration need. He is a member of IEEE and has published 2 book chapters, and over 40 refereed international journals and conference papers.

E-mail: mario.collotta@unikore.it
Faculty of Engineering and Architecture
Kore University of Enna
Cittadella Universitaria
94100 Enna, Italy

Giovanni Pau is a Ph.D. student at the Kore University of Enna. He received his Bachelor degree in Telematic Engineering from Catania University in 2008 discussing a thesis entitled "Study and development of an algorithm for the assignment of cardinality in low power wireless networks" and then in 2010, his Master degree summa cum laude in Telematic Engineering from the Kore University of Enna discussing a thesis entitled "A dynamic control approach to manage real-time traffic light timing through a wireless sensor network". His research interest includes wireless sensor networks, soft computing techniques and real-time systems. In each of these research fields, he has produced several publications in international conferences and journals.

E-mail: giovanni.pau@unikore.it
Faculty of Engineering and Architecture
Kore University of Enna
Cittadella Universitaria
94100 Enna, Italy

Salvatore Vitabile received the Laurea degree in Electronic Engineering and the doctoral degree in Computer Science from the University of Palermo, Italy, in 1994 and 1999, respectively. He is currently an assistant professor with the Department of Biopathology, Medical and Forensic Biotechnologies, University of Palermo, Italy. In 2007, he was a visiting professor in the Department of Radiology, Ohio State University, Columbus, USA. His research interests include computational intelligence, biometric authentication systems, architecture design and prototyping, real-time driver assistance systems, multi-agent system security, and medical data processing and analysis. He has chaired, organized, and served as member of the organizing committee of several international conferences and workshops. He is also the editor in chief of the International Journal of Adaptive and Innovative Systems, Inderscience Publishers, and a member of the board of directors of SIREN (Italian Society of Neural Networks) .

E-mail: salvatore.vitabile@unipa.it
Department of Biopathology and Medical
and Forensic Biotechnologies
University of Palermo
Via del Vespro 129
90127 Palermo, Italy

Paper

Bayesian Network Based Fault Tolerance in Distributed Sensor Networks

B. Bhajantri Lokesh[1] and N. Nalini[2]

[1] *Department of Information Science and Engineering, Basaveshwar Engineering College, Karnataka, India*
[2] *Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology, Karnataka, India*

Abstract—A Distributed Sensor Network (DSN) consists of a set of sensors that are interconnected by a communication network. DSN is capable of acquiring and processing signals, communicating, and performing simple computational tasks. Such sensors can detect and collect data concerning any sign of node failure, earthquakes, floods and even a terrorist attack. Energy efficiency and fault-tolerance network control are the most important issues in the development of DSNs. In this work, two methods of fault tolerance are proposed: fault detection and recovery to achieve fault tolerance using Bayesian Networks (BNs). Bayesian Network is used to aid reasoning and decision making under uncertainty. The main objective of this work is to provide fault tolerance mechanism which is energy efficient and responsive to network using BNs. It is also used to detect energy depletion of node, link failure between nodes, and packet error in DSN. The proposed model is used to detect faults at node, sink and network level faults (link failure and packet error). The proposed fault recovery model is used to achieve fault tolerance by adjusting the network of the randomly deployed sensor nodes based on of its probabilities. Finally, the performance parameters for the proposed scheme are evaluated.

Keywords—Bayesian network, distributed sensor networks, fault detection, fault tolerance, fault recovery, network control, routing.

1. Introduction

Distributed Sensor Network (DSN) is a collection of sensor nodes organized in a cooperative network, which are densely deployed in hostile and unattended environment with capabilities of sensing, wireless communication, and computations. The most important characteristics of DSN are:

- sensor nodes are prone to maximum failures,
- sensor nodes make use of the broadcast communication pattern and have severe bandwidth restraint,
- sensor nodes have limited amount of resources [1].

Sensor nodes may fail by impact of deployment such as fire or extreme heat, animal or vehicular accidents, and malicious activity. These failures may occur upon deployment or over time after, extensive operation may drain power or external factors may physically damage their part. Additionally, hazards may change devices positions over time, possibly disconnecting the network. Any of these initial deployment errors, sensor failures or change in sensor positions cause the network to be disconnected or malfunctioning, and need to deploy additional sensors to fix the network. Fault occurrence in a DSN may exist at hardware, software, network communication, node levels and application layer [2].

In this work, BN is used for fault tolerance in DSN and to represent conditional independencies between a set of random variables (nodes). The network representing different variables (nodes) have edges that constitutes relationship among random variables that are often casual. BN consists of a set of variables and directed edges between variables (nodes), and each variable has finite set of mutually exclusive states, together with the edges forms a directed acyclic graph. The acyclic network state means there must not be any feedback link or loop.

Over the last decade, the BN has become a popular representation for encoding uncertain knowledge in expert systems [3]. More recently, researchers have developed methods for learning BNs from data. The techniques that have been developed are new and still evolving but they have been shown to be remarkably effective for some data analysis problems. There are numerous representations available for data analysis, including rule bases, decision trees, and artificial neural networks. There are also many techniques for data analysis such as density estimation, classification, regression, fault tolerance and clustering [4].

2. Related Works

The work presented in [5] depicts a distributed fault tolerant topology control in static and mobile wireless sensor network (WSN). The distributed algorithm for assigning minimum possible power to all the nodes in the WSN, such that the network is K-connected is proposed. The paper given in [6] presents a distributed topology control in WSN with asymmetric links. It considers the problem of topology control in a heterogeneous wireless network devices with different maximum transmission ranges. The research given in [7] presents a Bayesian decision model for intelligent routing in sensor networks. A new efficient energy-aware routing algorithm is proposed based on learning patterns that minimizes the main constraints imposed by this kind of networks. The probabilistic decision model both considered the estimation of the available energy at

the neighboring nodes and the importance of the messages to make intelligent decisions. The paper [8] presents a survey on fault management in WSNs. The fault management process is divided into three phases such as fault detection, diagnosis and recovery and also summarizes the existing management architectures, which are adopted to support fault management in WSNs.

The work given in [9] addresses fault-tolerant topology control in a heterogeneous WSN consisting of several resource rich super nodes, used for data relaying, and a large number of energy constrained wireless sensor nodes. It introduces the K-degree anycast topology control (K-ATC) problem. The paper [10] presents a distributed Bayesian algorithm for fault-tolerant event region detection in WSN. The proposed solution in the form of Bayesian fault-recognition algorithms, exploits the notion that measurement errors due to faulty equipment are likely to be uncorrelated, while environmental conditions are spatially correlated. It presented two Bayesian algorithms, the randomized decision and threshold decision schemes, and derived analytical expressions for their performance.

Bayesian fusion algorithm for inferring trust in WSNs is presented in [11]. This paper introduces a new fusion algorithm to combine more than one trust component (data and communication) to infer the overall trust between nodes. Simulation results demonstrate that a node is highly trustworthy provided that both trust components simultaneously confirm its trustworthiness and conversely, a node is highly untrustworthy if its untrustworthiness is asserted by both components. The some of the related works are given in [12]–[17].

The rest of the paper is organized as follows. A proposed work for fault tolerance approach to network control is discussed in Section 3. Simulation and results analysis are presented in Section 4 and Section 5 finally concludes the article.

3. Proposed Work

Earlier works do not consider the zones or regions of network construction in DSN. The size of the network becomes complex and divided into number of networks. They are compared against the different networks in sensor network environment and also prolonging sensors operable lifetime is a main design challenge. This work considers the problem of network control in heterogeneous wireless devices with different maximum transmission ranges in the network. Objectives of the proposed scheme are as follows:

– formation of BN as a mesh network in DSN,

– construct the zones/regions using BN as the network becomes complex,

– placing of Control Manager Node (CMN) in each zone which acts as sink node for monitoring the network,

– achieving fault tolerance by using BNs in two phases: fault detection and fault recovery for transmission of data between source nodes and sink node,

– to achieve optimization of routing as well as energy of all nodes in the DSN.

3.1. System Model

Failures are inevitable in DSNs due to inhospitable environment and unattended deployment. Therefore, it is necessary that network failures are detected in advance and appropriate measures are taken to sustain network operation. The work presents an approach to achieve fault tolerance in two phases:

- fault detection – the fault detection phase is used finds the faulty nodes and the type of faults in the DSN environment based on their probabilities,
- fault recovery re-initializes the network to establish path between sources and sink node.

These two methods are based on the probabilities using BNs to achieve fault tolerance in the DSN.

The proposed system model is composed of distributed sensor nodes with diversified sensing competence and sink node. Group of sensor nodes can be constructed in the form mesh network using BNs in DSN environment. A sensor node V is connected to the BN, G = (V, E), where V set of nodes or vertices in the network and E is the set of edges in the network. While the data is traveling on the BN, it is automatically configured to reach the destination by taking the shortest route which means that least number of hops. Data travels by hopping from one node to another to reaches the destination node in a DSN as shown in Fig. 1.

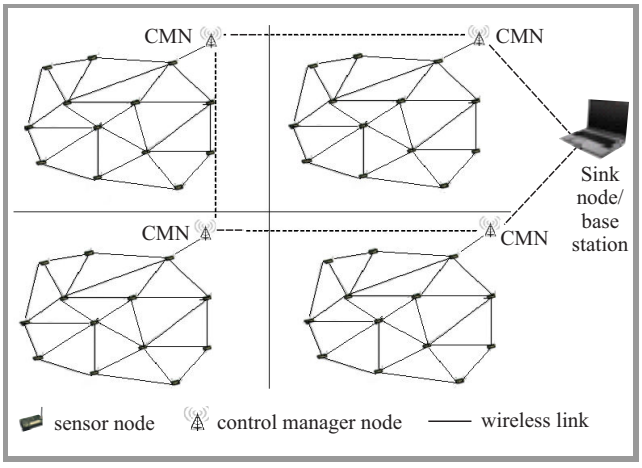


Fig. 1. System architecture.

Nodes sense the data periodically and send it to the sink node with multi hop communication. It is assumed that all nodes (sensor and sink nodes) in the network are static

and have initial energy. All the sensor nodes are equipped with Global Positioning System (GPS), processor and transceiver for the communication able to set the transmission power level. It is assumed that during deployment or construction of network phase each node has full initial energy. All the sensor nodes are equipped with message updating function such as: node_id, residual energy, threshold level energy, number of nodes connected, number of faulty nodes, and connection status in the network. This function is used to calculate the probabilities of each node by using BNs.

As the number of nodes increase, the network becomes complex. Hence the network is divided into number of zones or square regions. Each zone has BN in the form of mesh network for reducing complexities in the environment.

This research using no cluster head mechanism and most of the works are on the basis of cluster heads. Because each round cluster head changes in the network as its takes more end to end delay. The data is transmitted from nearest nodes or distance from different zones and each region employs a network CMN on behalf of sink node. CMN is responsible for monitoring and detecting failure in its region because base station or sink node is far away from the regions. It is also able to directly communicate with other CMN for fault detection.

The fault model is done at two levels using BNs as follows. A node or sink level is used when the nodes probability is less than the threshold level probability, which is based on the residual energy, bandwidth and link efficiency. Otherwise a network level is used as a link failure between nodes and packet error.

3.2. Construction of Bayesian Networks

Figure 2 shows the BN for proposed scheme in which the nodes represent the variables of BN and arcs indicate probabilistic dependencies between nodes. Every node calculates

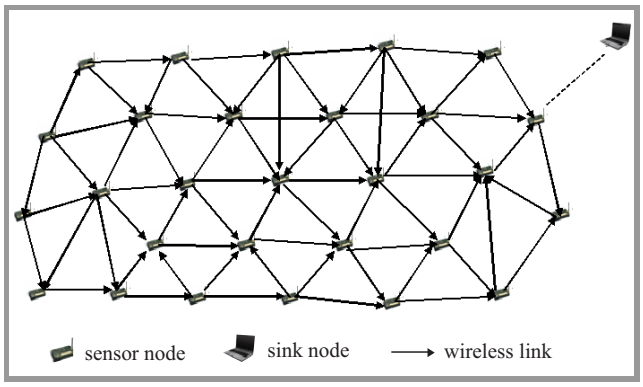


Fig. 2. Bayesian Network for proposed scheme.

the conditional probabilities at each node. Root nodes do not have any parents and its uses the prior probability $P(S_i)$. The ordering guarantees that the BN will have no cycles. The construction of BN algorithm is given by following procedure.

Step 1. Choose a set of variables (nodes) that describes the application domain.

Step 2. Choose an ordering of variables (nodes), i.e., $S_1 \ldots S_N$.

Step 3. Start with the empty network and add variables (nodes) to the network in DSN environment.

For i = 1 to N

Add S_i to network

Select parents from $S_1 \ldots S_N$ such as

$P(S_i \mid \text{parents}(S_i)) = P(S_i \mid S_i \ldots S_{i-1})$

Next i

This choice of parents guarantees the global semantics.

$P(S_1 \ldots S_N) =$

$= \prod_{i=1}^{N} P(S_i \mid S_i \ldots S_{i-1})$ (by chain rule)

$= P(S_1)\, P(S_2 \mid S_1) \ldots P(S_N \mid S_1 \ldots S_{N-1})$

$= \prod_{i=1}^{N} P(S_i \mid \text{parents}(S_i))$ (by construction).

Step 4. Draw an arc from the each variable (node) in parents (S_i) to S_i.

This scheme may be expressed as the product of the prior probabilities of all the root nodes and the conditional probabilities of all the other nodes in the network. The conditional probabilities are important for building BNs. But BNs are also built to facilitate the calculation of conditional probabilities, namely the conditional probabilities for variables (nodes) of interest given the data (evidence). Each variable (nodes) S_1 with parents $S_2 \ldots S_N$ in a BN has an attached conditional probability table $P(S_1 \mid S_2 \ldots S_N)$.

3.3. Inferences or Probability Tables

The given inferences are used in the process of deriving logical conclusion from premises known or assumed to be true. Here BN is used to determine the probabilities of particular types of events. Inference is used to compute the conditional probability for variables with given information (evidence) concerning other nodes or variables. The evidence is available on ancestors of the variables or interests nodes. The evidence is available on a descendant of the variable(s) or nodes of interest to perform inference against the direction of the edges. The proposed Bayes' theorem is given by [18]:

$$P(S_2 \mid S_1) = \big(P(S_1 \mid S_2) P(S_2)\big) / P(S_1). \tag{1}$$

Let d_i be the distance between nodes in the network. It can be computed by using Euclidian Distance Formula (EDF) given by Eq. (2) [19]:

$$d_i = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}. \tag{2}$$

Link efficiency can be computed as follows. Let C_i be capacity of a discrete-time discrete-valued channel, B be the

bit rate (Hz) of a channel, E_T be the total energy consumed for transmission of a bit in link i, SNR be the signal-to-noise ratio [20]. Capacity of channel i is:

$$C_i = B \log_2(1 + SNR). \tag{3}$$

Assume E_N stands for energy consumption for the transmission of the packets. E_N can be computed by

$$E_N = S_E \cdot P_i/\text{bits} + T_E \cdot P_i/\text{bits}, \tag{4}$$

where S_E – energy required for sensing data or packets, T_E – energy required for transmission of data or packets, P_i – size of packets in terms of bits.

Let E would be the energy consumed for the transmission of a bit per distance d_i. The energy of node E is [20].

$$E = E_N d_i. \tag{5}$$

Assume L_{eff} is the link efficiency for the nodes in the network [21].

$$L_{eff} = \frac{C_i}{E}. \tag{6}$$

Let R_E be the residual energy of each node:

$$R_E = I_E - E_i, \tag{7}$$

where I_E – initial energy of node, E_N – energy consumption.

Assume E_T as the total energy consumption of the path for optimization of routing over the nodes. The total energy required by nodes to sink node over the path is

$$E_T = S_i \cdot C_i \cdot 0.05\ [\text{nJ}], \tag{8}$$

where S_i – number of sensor nodes, C_i – number of Control Manager Node (CMN).

Based on above equations the inferences for the proposed work as given in Tables 1–3 was derived.

Table 1
Inferences

Energy	Distance	Bandwidth	Result
Max.	High	Min.	High
Max.	Fair		Fair
Min.	High		Min.
Fair			High
Max.	Min.	Fair	Fair
Max.		Max.	Min.

Table 2
Distance vs. bandwidth

	Low	Fair	High	Result 1
Min.	0.55	0.80	0.96	2.31
Fair	0.52	0.72	0.85	2.09
Max.	0.44	0.63	0.71	1.78
Result 2	1.51	2.15	2.52	

Table 3
Energy vs. channel capacity

	Low	Fair	High
Min.	0.40	0.56	0.70
Fair	0.55	0.74	0.85
Max.	0.60	0.78	0.97

3.4. Fault Management System

The proposed fault management system consists of two main phases such as: fault detection and recovery.

The fault detection is the beginning phase of the DSN, where faults and failures in the network are properly identified either by using node, sink or CMN. In this work, fault detection by two mechanisms such as self detection (passive detection) and active detection is proposed.

In self detection, sensor nodes are required to periodically monitor their probabilities of the nodes which are based on: residual energy, bandwidth and link efficiency, and then identify the potential failure. This scheme considers the energy depletion as a main cause of nodes sudden death. A node is termed as failing when its probability drops below the threshold level. Detection of decrease in the probabilities of a node by a node itself is called self detection method and is shown in Fig. 3. The probabilities of each node in the network are calculated by using probabilities or inference tables.

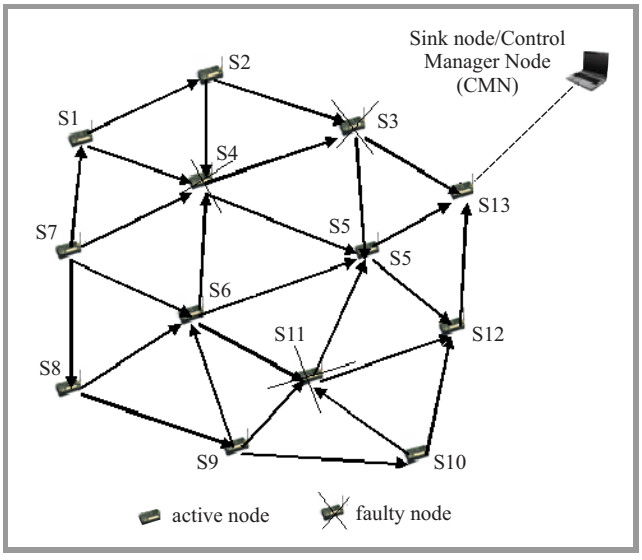


Fig. 3. Self detection method.

In active detection, network control manager node or base station/sink node are continuously monitoring the status of each node in the network. The sink node maintains the update message function. It consists of node ID, energy, bandwidth and link efficiency. Based on the update message function, sink node calculates the probabilities of each node. If sink node do not receive any data from a node for defined time period, then sink node considers that node

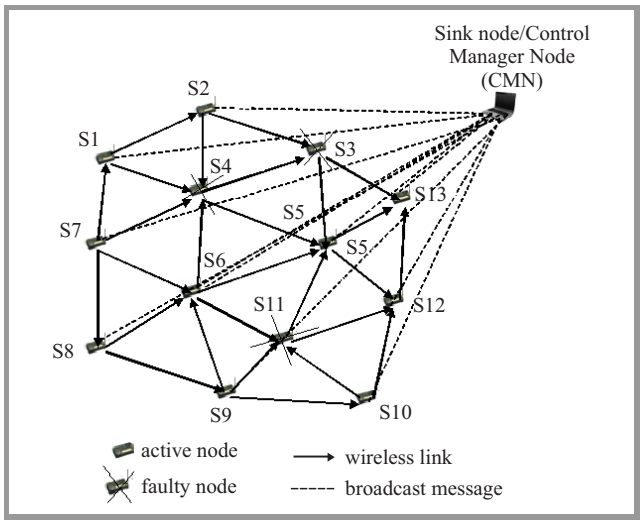


Fig. 4. Active detection method.

as a faulty with low probability in the network and reconstruct the network with node probabilities. Also if any node is below threshold level probabilities, it is assumed to be faulty node in the network, sink node or control manager node broadcast the message or beacon packet to all its nodes in the network and reconstruct the network with active nodes. The beacon packet consists of probabilities of each node. So, this detection is called as active detection as shown in Fig. 4.

Fault recovery is the phase where the sensor network is restructured or reconfigured in such way that failure or faulty nodes to not impact further on network performance. Faulty recovery process is carried out as follows:

- Nodes probability less than threshold – once fault is detected in the network, the nodes with low probability are sent to sleep mode;
- Link Failure – in case of link failure in network, the next nearest node with probability greater than threshold level is selected for forwarding the packets or route the data;
- Packet Error – in case of packet error, the timestamp field is checked. If it is non zero then there is no packet error. Otherwise error has occurred and the packet has to be retransmitted to the desired node through alternate path.

3.5. Routing

Each node in the network senses and forwards the data to sink node. The operations of self detection method for routing over the networks using BN is:

– each node has probability tables in the network,

– each source sensor node checks the probabilities of its neighboring node,

– it always selects the highest probabilities of its neighboring node for forwarding the data,

– it selects another path for transmission if any node is fault in the path or its neighboring node is fault due to some reasons,

– the optimal path for transmission from sources to sink node is based on the highest probabilities,

– sink node takes the action upon receiving the information.

The procedure of active detection method for routing over the networks using BN is as follows:

– network control manager node or base station/sink node are continuously monitoring the status of each node information in the network,

– the sink node maintains the update message function or probability tables,

– in each round sink node or CMN continuously monitors the each nodes probabilities in each region or network,

– if sink node do not receive any data every for some period of time, then sink node considers the node as a faulty and reconstruct the network,

– otherwise, sink broadcast the beacon packet to all its nodes in the network, to detects the faults,

– to reconstruct the network,

– the source node forward the data with highest probabilities of nodes in the network.

The algorithm for proposed scheme is as given below:

Step 1. Deploy S_N number of nodes in DSN as randomly,

Step 2. Find the probability of each node by considering the parameters such as: Energy (E_N), Bandwidth (b), link efficiency (L_{eff}),

- Find the prior probability for parent node,
- Find the joint probability for parent node and child node by using: $P(S_1, S_2 \ldots S_N) = = \prod_{i=1}^{N} P(S_i \mid \text{parents}(S_i))$
- Find the conditional probability for each node: $P(S_1 \mid S_2, S_3, S_4 \ldots S_N) = (P(S_1 \mid S_2, S_3, S_4 \ldots S_N) \times \times P(S_2, S_3, S_4 \ldots S_N)) / P(S_1)$

Step 3. Find the path for each node:

```
For (i = 0; i < N; i++)
{
  if (Probability_Node(Prob_S_N)>=Neighbor_Node)
  {Select highest probability of node for forward
  the data} //Optimization of routing
  Else
  {Select next node with highest probabilities
  in the network}
}
```

Select the highest probability node among these neighboring nodes and make it as next source node and continue this process until it reaches the sink node. This algorithm avoids the cycle formation and find optimal path. After finding optimal path transmit the packets to sink node. Once packets are sent probability of each node is compared with the threshold level probability Th_b. If it is less than Th_b, then the node will be indicated as a dead. Recover the network topology and then consider next optimal path to transmit the packets.

3.6. Fault Tolerance in Network

When node S_1 wants to send packets to S_2 first it will measure the probability of nodes that are in the path between S_1 and sink node. If the probability of nodes in path between S_1 and S_2 are greater than the threshold level probability then packets are forwarded from node S_1 to S_2. If any of the node's probability level is below threshold then it is sent to sleep mode and reconstruct the network. So, this is used to achieve fault tolerance in the network.
Link failure between nodes is detected as follows. If node S_N does not receive packets from its nearest neighbors, whose probability level is less than threshold within predetermined time interval then it assumes that link from those nodes to node S_N are failed. Packet error rate can be used to monitor the network health and help debug potential problems. If errors do occur a pattern can be identified. This can help isolate and solve problems before the system fails. Packet errors are node specific i.e., nodes only check their own packets and ignore all other. In case of error, the timestamp field in message is checked. If it is zero then it cause to reconstruct the network.

Theorem 1. Suppose N = (V, E) is a Bayesian Network. Algorithm has time complexity for fault tolerance as $O(\log_n)$ for routing in DSN.

Proof. Let N = (V, E) is a BN with Directed Acyclic Graph (DAG) having set of vertices or nodes V = $(v_1, v_2, \ldots v_n)$ and set of edges E = $(e_1, e_2 \ldots e_n)$. To associate with G and a given integer K >= 2 (number of neighboring nodes) is in the network. Phase one involves a simple construction of BN is given in Section 3.2. Phase two is a detection of faults in the network over an environment. The proposed work involves two phases such as self and active detection methods. The computation of fault tolerance is done by selecting S_1 as a source node, and then calculating probability for its neighbor nodes in presence of faulty nodes in the network. Next an optimization of routing in presence of faulty nodes, if presence of probability of node greater than threshold level is needed. Then calculate the probability of nodes (i.e. nodes or sink node/CMN) in each round is processed. Therefore, time complexity of fault tolerance is $O(\log_N)$ for optimization of routing in DSN.

3.7. Functioning Scheme

This section describes the algorithm for fault detection and recovery using BNs to find the optimal path for transmitting the packets. This work finds the joint and conditional neighbor nodes probabilities of selected source node. A prior probability is used in distinguishing the ways in which values for probabilities can be obtained. In particular, an "a prior probability" is derived purely by deductive reasoning. The joint probability distribution of the network is the joint probability of all variables or nodes in the network. Using the chain rule, this may be expressed as the product of the prior probabilities of all the root nodes and the conditional probabilities of all the network.

Algorithm for Fault Detection and Recovery

Nomenclature: {$S_N = S_1, S_2, S_3, \ldots S_N$, Prob_$S_N$ = Probability of sensor nodes, Th_b = Threshold level probability, L_{eff} = Link efficiency, $Th_{L_{eff}}$ = Threshold level link efficiency}.

Step 1. Node failure/Sink node failure
if (Prob_S_N < Th_b)
{
Send node to sleep mode and disconnect the links of that node.
- Reconstruct the network with Prob_S_N >= Th_b, (i.e., for considering each node should be higher than threshold level probability Th_b in the network).
- Select next highest probability of node in the network for routing.
- Repeat Step 1 // Fault recovery

}
Else
{
Transfer packet to next node over the network
} Repeat Step 1

Step 2. Link or Path failure
if (Prob_S_N < Th_b !! L_{eff} <= ThL_{eff})
{
Path or link failure
Select new neighbor node with highest probability
}
Else
{
Continue with the same node.
}

Step 3. Packet transmission failure
if (time stamp == 0)
{
Re-transmit the packet over the network
}

4. Simulation

The authors conducted simulation in various network scenarios of the proposed scheme by using C programming language. Simulations are carried out extensively with random number for 100 iterations. This section presents

the simulation model, procedure, performance parameters, and results.

4.1. Simulation Model

The simulation model consists of S_N number of nodes deployed in a distributed environment and connected as in BN. The performance parameters such as probability of fault tolerance, time complexity, energy optimization, network lifetime and fault detection ratio (FDR) is measured.

4.2. Simulation Procedure

To illustrate simulation results, the following variables have been considered: number of sensor nodes $S_N = 500$, energy of each nodes $E_N = 2$ J, number of sink nodes $N_s = 1$, number of control manager nodes CMN = 4, size of the network = $5000 \cdot 5000$ m, transmission range R_c = 100 m, energy required for sensing of data in each node $E_S = 50$ nJ/bit, energy required for transmission of data $E_T = 50$ nJ/bit, size_packets P = 64, 128, 512, 1024 bits and so on, threshold level probability $TH_b = 0.05\%$, and transmission of data = bits/s.

Begin

- Deploy the number of nodes randomly as in DSN environment.
- Divide the network into number of regions.
- Construct the BN in each region.
- Find the fault node on the basis of threshold level probability of each node.
- Find the link failures (node failure).
- Find the packet error (node error).
- Apply the proposed scheme to control network in DSN.
- Compute the performance parameters.
- Generate graphs.

End

4.3. Performance parameters

The following performance parameters were used in proposed scheme:

- probability of fault tolerance – it measures the ability of system to continue to operate properly in the event of failure in DSN environment;
- time complexity for fault tolerance – it is defined as the number nodes increases as the percentage of time complexity is increases for the fault tolerance in the network;
- network lifetime – as the probability of fault tolerance increases the network lifetime of DSN increases. The network lifetime is measured in terms of percentage;
- energy optimization – it is defined as the increase the probability of fault tolerance as the increase the optimization of energy of nodes in the network;
- Fault Detection Ratio – it is defined as the number of nodes increases the probability of fault detection ratio increases in the network.

4.4. Results and Discussions

Figure 5 shows that as the probability of Fault Detection Ratio (FDR) increases in the network, the probability of fault tolerance of the network decreases. The probability of FDR as 10%, and 20% for the total number of nodes ranging from 100 to 500 was considered. As the probability of FDR increases i.e., from 10% to 20% for 100 nodes, the probability of fault tolerance decreases with the number of neighboring nodes (K >= 2) on the network. The probability of fault tolerance of the proposed BN is more than the other network in the environment.

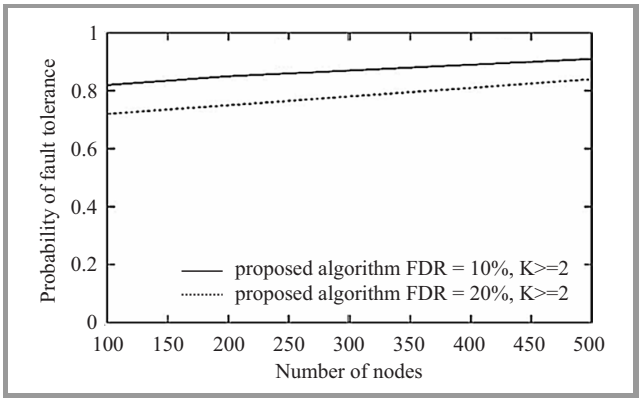


Fig. 5. Probability of fault tolerance vs. number of nodes.

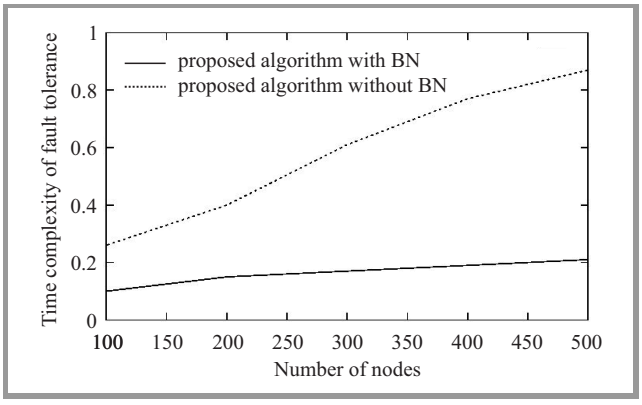


Fig. 6. Time complexity of fault tolerance vs. number of nodes.

Figure 6 depicts the time complexity for fault tolerance with given number of nodes in DSN. As the number of nodes increases, fault tolerance complexity increases. With proposed BN, time complexity of fault tolerance of DSN will be less than the case without BN. This work, we have considered that time complexity proposed method for fault tolerance of DSN is $O(\log_N)$. The proposed BN is more

efficient other than the network. Because, fault detection can be achieved by two mechanisms: self (passive) and active detections are considered in this scheme.

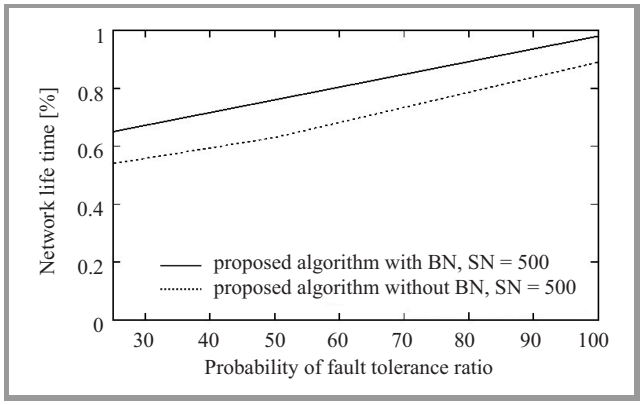


Fig. 7. Network lifetime vs. probability of fault tolerance.

Network lifetime with nodes given number is shown in Fig. 7. As the number of probability of fault tolerance of the network increases with given number of nodes ($S_N = 500$), the increase in the network lifetime of the DSN environment. The proposed algorithm (BN) is used to achieve better network lifetime with 98%.

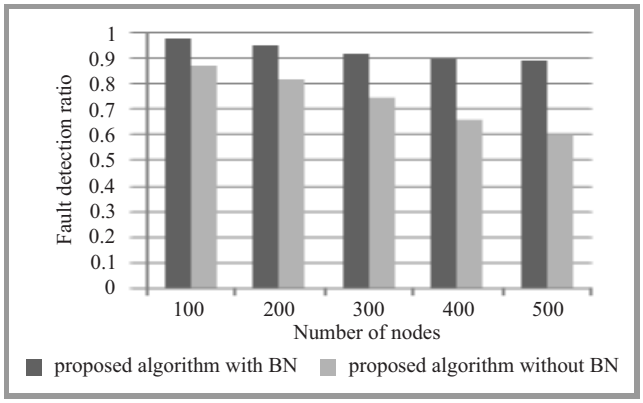


Fig. 8. Probability of FDR vs. number of nodes.

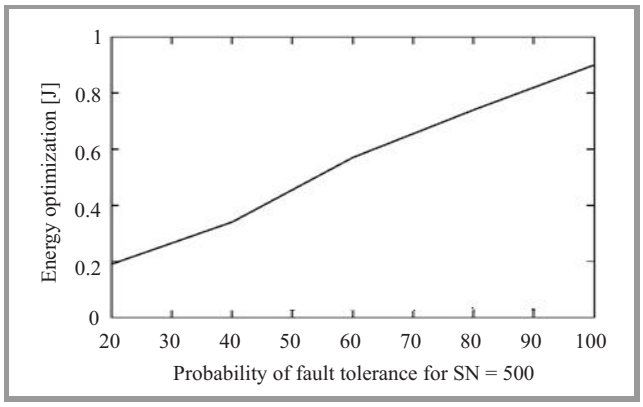


Fig. 9. Energy optimization vs. probability of fault tolerance.

Figure 8 shows probability of fault detection ratio (FDR) with given number of nodes. As the number of nodes increases, the probability of FDR decrease. The proposed method detects the fault detection in the network will be more in the network. Because proposed algorithm, works on the basis of proposed detection methods. As the size of the network increases, gradually probability of FDR decreases in the DSN. The size of the network is small, so probability of FDR is more. Otherwise probability of FDR is gradually decreases.

Figure 9 presents the energy optimization for varying number of fault tolerance among nodes. As the number of percentage of fault tolerance increases, optimization of energy of each node increases in the distributed sensor environment.

5. Conclusions

The proposed BN based fault tolerance mechanism is energy-efficient and responsive to network in DSN environment. It includes faults at node/sink, level and network level. The proposed system detects energy depletion of a node, link failure between nodes and packet error using their probabilities of nodes in the network.

Simulation results show that proposed system is more efficient than the other network. The proposed system continues to operate properly in the event of failure in DSN using BNs.

References

[1] S. S. Iyengar, T. Ankit, and R. R. Brooks, "An overview", in *Distributed Sensors Network*", S. S. Iyengar and R. R. Brooks, Eds. Chapman & Hall/CRC, 2004.

[2] B. B. Lokesh and N. Nalini, "Energy aware based fault tolerance approach for topology control in distributed sensor networks", *Int. J. High Speed Netw.*, vol. 18, no. 3, pp. 197–210, 2012.

[3] I. Ben-Gal, "Bayesian networks", in *Encyclopedia of Statistics in Quality and Reliability*, F. Ruggeri, R. Kenett, and F. Faltin, Eds. Wiley, 2007.

[4] R. E. Neapolitan, *Learning Bayesian Networks* [Online]. Available: http://www.cs.technion.ac.il/~dang/books/Learning%20Bayesian%20Networks

[5] I. Saha, L. K. Sambasivan, R. K. Patro, and S. K. Ghosh, "Distributed fault-tolerant topology control in static and mobile wireless sensor networks", in *Proc. 2nd Int. Conf. Commun. Syst. Softw. Middlew. COMSWARE 2007*, Bangalore, India, 2007, pp. 1–8.

[6] J. Liu and L. Baochun, "Distributed topology control in wireless sensor networks with asymmetric links", in *Proc. IEEE Global Telecommun. Conf. GLOBECOM 2003*, San Francisco, CA, USA, 2003, vol. 3, pp. 1257–1262.

[7] R. Arroyo-Valles, A. G. Marques, J. J. Vinagre-Diaz, and J. Cid-Sueiro, "A Bayesian decision model for intelligent routing in sensor networks", in *Proc. 3rd Int. Symp. Wirel. Commun. Syst. ISWCS 2006*, Valencia, Spain, 2006, pp. 103–107.

[8] P. Lilia and H. Qi, "A survey of fault management in wireless sensor networks", *J. Netw. Syst. Managem.*, vol. 15, no. 2, pp. 171–190, 2007.

[9] C. Mihaela, Y. Shuhui, and W. Jie, "Fault-tolerant topology control for heterogeneous wireless sensor networks", in *Proc. IEEE 4th Int. Conf. Mob. Adhoc and Sensor Sys. MASS 2007*, Pisa, Italy, 2007, pp. 1–9.

[10] K. Bhaskar and I. Sitharama, "Distributed Bayesian algorithms for fault-tolerant event region detection in wireless sensor networks", *IEEE Trans. Comp*., vol. 53, no. 3, pp. 241–250, 2004.

[11] M. Mohammad, C. Subhash, and A. Rami, "Bayesian fusion algorithm for inferring trust in wireless sensor networks", *J. of Netw.*, vol. 5, no. 7, pp. 815–822, 2010.

[12] C. Mihaela, Y. Shuhui, and W. Jie, "Algorithms for fault-tolerant topology control for heterogeneous wireless sensor networks", *IEEE Trans. Parall. Distrib. Syst.*, vol. 19, no. 4, pp. 545–558, 2008.

[13] N. Ababneh, A. Viglas, H. Labiod, and N. Boukhatem, "ECTC: Energy efficient topology control algorithm for wireless sensor networks", in *Proc. 10th IEEE Int. Symp. World of Wirel., Mob. Multim. Netw. & Workshops WOWMOM 2009*, Kos Island, Greece, 2009.

[14] A. Abolfazl, D. Arash, K. Ahmad, and B. Neda, "Fault detection and recovery in wireless sensor network using clustering", *Int. J. Wirel. & Mob. Netw*., vol. 3, no. 1, pp. 130–138, 2011.

[15] H. Xiaofeng, C. Xiang, L. L. Errol, and S. Chien-Chung, Fault-tolerant relay node placement in heterogeneous wireless sensor networks", *IEEE Trans. Mob. Comput.*, vol. 9, no. 5, pp. 643–656, 2010.

[16] J. L. Bredin, E. D. Demaine, M. T. Hajiaghayi, and D. Rus, "Deploying sensor networks with guaranteed fault tolerance", *IEEE/ACM Trans. Netw.*, vol. 18, no. 1, pp. 216–228, 2010.

[17] R. H. Abedi, S. Ghani, and S. Haider, "Selection of cluster heads in wireless sensor networks using bayesian network", in *Proc. Int. Conf. Comp., Electr. Sys. Sci., and Engin. ICCESSE 2010*, Venice, Italy, 2010.

[18] S. Nishant and S. Upinderpal, "A location based approach to prevent wormhole attack in wireless sensor networks", *Int. J. Adv. Res. Comp. Sci. Softw. Engin*., vol. 4, no. 1, pp. 840–845, 2014.

[19] H. Taub and D. L. Schilling, *Principles of Communication Systems*. Columbus, OH, USA: McGraw-Hill, 1986.

[20] G. Miao, N. Himayat, abd G. Y. Li, "Energy efficient link adaptation in frequency-selective channels", *IEEE Trans. Commun.*, vol. 58, no. 2, pp. 545–554, 2010.

B. Bhajantri Lokesh received his M.Tech. degree in Computer Science and Engineering (CSE) from Basaveshwar Engineering College, Bagalkot, India, in 2005. He is working as a Assistant Professor in the Department of Information Science and Engineering, Basaveshwar Engineering College, Bagalkot, India. Currently he is pursuing Ph.D. in CSE, Visvesvaraya Technological University (VTU), Belgaum, Karnataka, India. He has experience of around 10 years in teaching and research. His areas of interest include Distributed Sensor Networks, e-Commerce, u-Commerce, mobile computing and communications, networking protocols, genetic algorithms, applications of agents and real time systems. He has published one book chapter in Handbook of Research on Telecommunications Planning and Management for Business, 8 referred international conferences papers and 7 referred international journals. He is a reviewer of some journals and conferences. He is a member of Board of Studies (BOS) in the Department of Information Science and Engineering, Basaveshwar Engineering College, Bagalkot, Karnataka, India. He is a member of International Association of Computer Science and Information Technology (IACSIT).

E-mail: lokeshcse@yahoo.co.in
Department of Information Science and Engineering
Basaveshwar Engineering College
Bagalkot, India

N. Nalini received her Ph.D. from Visvesvaraya Technological University (VTU), Belgaum, Karnataka, India. She is currently working as Professor and Head of Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology (NMIT), Bangalore, Karnataka, India. She has experience of around 22 years in teaching and research. She is involved in research of wireless and Distributed Sensor Networks, cloud computing, Cryptography & Network Security, Genetic Algorithms, and Heuristic Algorithms in Secure Networks. She is an associate editor of Research Journal of Information Technology, Maxwell Scientific Organization. She has many given invited lectures and has conducted several seminars and conferences. She has published 30 in journals and about 50 conferences papers. She is a reviewer of many journals and conferences.

E-mail: nalinaniranjan@hotmail.com
Department of Computer Science and Engineering
Nitte Meenakshi Institute of Technology (NMIT)
Bangalore, Karnataka, India

Paper

Partner Selection Using Reputation Information in *n*-player Cooperative Games

Pedro Mariano and Luís Correia

Departamento de Informatica, Faculdade de Ciencias da Universidade de Lisboa, Lisboa, Portugal

Abstract—To study cooperation evolution in populations, it is common to use games to model the individuals interactions. When these games are *n*-player it might be difficult to assign defection responsibility to any particular individual. In this paper the authors present an agent based model where each agent maintains reputation information of other agents. This information is used for partner selection before each game. Any agent collects information from the successive games it plays and updates a private reputation estimate of its candidate partners. This approach is integrated with an approach of variable sized population where agents are born, interact, reproduce and die, thus presenting a possibility of extinction. The results now obtained, for cooperation evolution in a population, show an improvement over previous models where partner selection did not use any reputation information. Populations are able to survive longer by selecting partners taking merely into account an estimate of others' reputations.

Keywords—evolution of cooperation, multi-agent systems, n-player games, partner selection, reputation.

1. Introduction

Modeling of cooperation evolution in populations has frequently used games with cooperative and coordination dilemmas [1], [2]. However real cases frequently do not match model predictions and therefore research tried to explain these results [3]–[9]. A common denominator in the majority of these works is either infinite population or finite but constant size population. Taking into account that these features are unrealistic, a recent line of research [10] has developed a model where populations may fluctuate, and therefore, in extreme cases, may extinguish, which in nature may happen as internal or external influences consequence. In this model the choice of partners is made in groups and does not take into account individual cooperation assessment.

In *n*-player games used in cooperation models a player usually does not have any information about other players. However it is known that the ability to select partners based on previous interactions knowledge can explain the prevalence of cooperation in many cooperative dilemmas [8]. An approach in which an agent estimates reputation of others from previous interactions [11] has revealed to be efficient towards an extended survival of populations [12].

In this work the authors investigate a combined approach where a population whose individuals can be born, reproduce and die, interact through a *n*-player game where each agent maintains an estimate other individuals reputation based on its own previous interactions. The model is general enough to encompass any scenario modeled by a *n*-player game.

2. Related Work

The replicator equation or the Moran process [13] are the most common models to study cooperation. There are a set of assumptions behind the replicator equation [14]. One assumes a considerably large or infinite population. Another assumes a well mixed-population such that everybody plays with everybody else. A similar approach is randomly pairing players. These are unrealistic assumptions and have led to alternative proposals. Among them are structured populations where players are placed in the nodes of some graph and interactions are restricted to links between nodes [15], [16]. In structured populations, agents have the possibility of selecting their partners [5]. Other approaches include finite but constant size population whose dynamics are modeled by a Moran process. Despite not allowing varying population size, they have been used to model scenarios that may cause extinctions such as climate change [17].

In models that allow variable population size most use Agent Based Models (ABM) [18], or are artificial ecosystems [19], [20]. ABM address the difficulties of creating a formal model of a complex system [21]. There are ABMs that analyze the extinctions possibility but they do that in specific contexts such as modeling population growth of endangered species [22], tree mortality [23], impact of logging activities in bird species [24].

McLane *et al.* provide in [25] a review of ABM used in the literature of ecology to address the issues of managing ecosystems. They presented a set of behaviors that individuals can choose in their life cycle: habitat selection, foraging, reproduction, and dispersal. In the papers that they reviewed, some used all the behaviors in the set while others used just one. Such behaviors could constitute the set of actions of some generic game played by animals. Moreover we can roughly divide them in two sets, one where an animal obtains energy (foraging) and a second where an animal spends energy, e.g., habitat selection, reproduction, and dispersal.

Some of these models are characterized by using specific differential equations or operate at higher level than the individual. Often they are specific to their case study and their methods are not directly transferable to another scenario. The Energy Based Evolutionary Algorithm (EnBEA) model [10] with variable population size came up as a solution that can be applied to any scenario modeled by a game. In that model agents are born, they interact with each other, reproduce and die. When that model is applied to a set of cooperative and coordination dilemmas, extinction may occur.

Partner selection is one of the possible explanations for the prevalence of cooperation [26], [27]. This characteristic is also combined with the possibility of refusing an interaction. The selection mechanism is usually dependent on the game: in Prisoner's Dilemma (PD) it depends on the partner defecting or not [8], in trading networks it depends on the trading offer [28]. However, there has been little concern to generalize the mechanism to be applied to any game, which is a problem that this work tackles.

In presented approach a player obtains a reputation representation of other players from results of games he played with them. Reputation is then used by a focal player to choose partners whenever needed. If a player chooses partners with higher reputation he should benefit his outcome in the game. Similar approaches have been followed to study evolution of cooperation [29], [30], sometimes combined with other features such as punishment [31] that favor emergence of cooperation.

Previous work [32] has investigated partner choice based on binary reputation of players, in the PD game. However, a binary reputation is too coarse and does not allow a gradation of reputation. This gradation seems to better correspond to real situations where a binary classification is seldom realistic.

When players assess their peers, this information may be shared with others. This is used in artificial markets where sellers and buyers rate each other [33], [34]. Sabater and Sierra [35] review some models of computational reputation management. They present models where reputation is built from direct interactions or from information given by others. These, as well as other works on player reputation [36], [37] require perfect identification of players.

Kreps and Wilson [38] study the effect of imperfect information about players payoffs in building a reputation about opponents strategies. This is applied to firms competing for a market, in a scenario with a dominant firm and others that, one at a time, may challenge the dominance. Brandts and colleagues [39] made a similar study in loan decision making.

However all these cases use two player games. In [40] a Public Good Provision (PGP) game of three players is used with reputation. A focal player gets perfect knowledge of his neighbors actions in a network of contacts and, for each round, he can choose two partners based on their reputation. The measure of reputation is the number of cooperative actions a player has performed. A similar measure is also used in [41] in a 5-player PGP, also with perfect reputation information.

In the case we are addressing a player does not obtain direct information about individual actions of his partners. We consider that a player only obtains information from his own payoff. This means that he cannot directly identify partners that have not cooperated, nor obtain some kind of signal from them. This is a situation that often occurs in human interaction. In a group of people sometimes is not possible to pinpoint who shirked from contributing. We find that for instance in a n-player snow-drift type game. Suppose a bus that has to be pushed by several individuals. No one knows exactly if a specific individual is cooperating. One can only assess the global outcome in the form of the progress of the bus.

The work in [12] has seemingly been the first to deal with imperfect reputation information in n-player games. This happens for instance in a PGP game when only the player's own payoff is known without access to the individual actions of the players. In such a case, the only situation with perfect information is when all players cooperate. Otherwise each player has an uncertainty about the other $n-1$ players' actions. One or more of them may have defected. That work takes two ways to solve the problem from the point of view of the focal player. One is to have the player using imperfect reputation knowledge to choose his successive partnerships, and the other is to have him gathering individual reputation information from the result of a PGP type game. A private reputation model is used. A player associates to each potential partner a single value that measures his utility. This value is updated from direct interactions with partners, considering all partners in a game as equally responsible for the outcome. The authors classification system is independent of the game being played, which contrasts with others [31] that are game specific.

3. Dynamic Population Model

In this section a formal description of EnBEA is given. It is a population model where agents are born, interact, reproduce and die. Agent interaction is mediated by some game. Interaction is essential because agents acquire or lose energy when playing games and energy is necessary to reproduce. Agents can die because of old age, starvation (lack of energy) and overcrowding.

The games are used as an energy transfer process. This means a redefinition of the payoff function. A game G is a tuple (N,A,E) where N is a set of n players, $A = \{A_1,\ldots,A_n\}$ and each A_i a set of actions for player i, and $E = \{e_1,\ldots,e_n\}$ is a set of energy functions, with $e_i : A_1 \times \ldots \times A_n \to \mathbb{R}$ being the energy obtained by player i given the actions of the n players.

An agent α is characterized by a strategy s which he uses to play game G, an energy level e and an age. We thus have $\alpha = (s,e,a)$. In each iteration t of EnBEA a population of agents, $\mathscr{P} = \{\alpha_1,\ldots\}$ is updated through three phases:

- **play** – in this phase all agents play the game and update their energy. Partners can be randomly selected or agents can choose them;
- **reproduction** – in this phase the agents whose energy is above some threshold produce one offspring by cloning and mutation, and their energy is decremented by some value;
- **death** – in this phase the entire population goes through death events that depend on population size, on agent's age and agent's energy. Age of surviving agents is incremented by one.

In the play phase, the game is used as energy transfer. Regarding the relation between the payoff function and the energy function, the authors have extended the approach followed in [42] and considered the case where the obtained energy is scaled and translated to the interval $[-1,1]$:

$$e \leftarrow e + \frac{\pi}{\max(\overline{\pi}, |\underline{\pi}|)}, \tag{1}$$

where π represents the payoff obtained by an agent, and $\overline{\pi}$ and $\underline{\pi}$ are the highest and lowest payoffs obtainable in game G.
Scaling allows to compare the evolutionary dynamics of games with different payoff functions, e.g. comparing the number of offspring per iteration or the number of iterations until an extinction occurred. We could remove scaling, if we made energy range equal to payoff range.
With Eq. (1) the possibility of an agent dying through starvation is introduced when the energy drops below zero, thus augmenting the risk of extinction. Instead of zero, we could have used another energy threshold in the decision to remove agents, which would only amount to one more parameter in the model. This case is more realistic as the payoff value reflects gains and costs of an agent. Consider for instance, the costs of providing in the PGP game or of being exploited in the PD game.
When an agent's energy reaches the reproduction threshold e_g, it is decremented by this value, and a new offspring is inserted in the population. Moreover, we have to deal with the possibility of an agent's energy dropping below zero. Similarly to [8] an agent is removed when its energy drops below zero. The energy of newborns could be zero, but this puts pressure on the first played games to obtain positive energy, otherwise infancy mortality may be high. Instead we opt for providing each newborn with e_B units of energy. Therefore, the dynamics of an agent's energy depends on two parameters, namely e_R and e_B.
In order to avoid exponential growth, in each iteration of the algorithm all agents go through death events. The two events are considered: one depends on population size and a second that depends on agent's age. The probability of an agent dying due to overcrowding is:

$$P(\text{death population size}) = \frac{1}{1+e^{6\frac{K-|\mathscr{P}|}{K}}}, \tag{2}$$

where $|\mathscr{P}|$ is the current population size and K is a parameter called carrying capacity. This probability is a sigmoid function. The exponent was chosen because the logistic curve outside the interval $[-6,6]$ is approximately either zero or one. In the event of the entire population doubling size, it will not go from a zero probability of dying to certain extinction. This assumes that each agent has at most one offspring per simulation iteration.
The probability of an agent dying because of old age is:

$$P(\text{death agent's age}) = \frac{1}{1+e^{\frac{L-a}{V}}}, \tag{3}$$

where L is agents' life expectancy and V controls the variance in the age at which agents die through old age.

4. Reputation Model

The reputation model is based on partner selection starting from a random partner selection model that served as base. First the main features of the random model are described and then the reputation mechanism is presented.

4.1. Random Partner Selection

Whenever a focal player needs to play a game, he selects one of the combinations of partners stored in vector **c**. Each combination has a probability of being selected. This probability is stored in vector **p**. The length of these vectors is represented by pool size parameter l. In this model, when a focal player selects his game partners, they cannot refuse playing.
After a player has played the game with partner combination c_k, he compares the utility obtained u with utility threshold u_T. If the utility is higher or equal than the threshold, no changes occur. If the utility is lower than the threshold, the corresponding probability is decreased by factor δ, and the combination is replaced. The following equation represents the probability update policy for the used combination k:

$$p_k^{t+1} = \begin{cases} \delta p_k^t & \text{if} \quad u < u_T \\ p_k^t & \text{if} \quad u \geq u_T \end{cases}. \tag{4}$$

The probabilities of other combinations are updated as follows (to maintain unit sum):

$$p_i^{t+1} = \begin{cases} p_i^t + \dfrac{(1-\delta)p_k^t}{l-1} & \text{if} \quad u < u_T \\ p_i^t & \text{if} \quad u \geq u_T \end{cases}. \tag{5}$$

The used combination is replaced by a new one if the utility is lower than u_T:

$$c_k^{t+1} = \begin{cases} \text{rnd}(\mathscr{C}) & \text{if} \quad u < u_T \\ c_k^t & \text{if} \quad u \geq u_T \end{cases}. \tag{6}$$

If a new combination is to be added, it is previously checked against the ones in the combination vector. If it is identical to any of those, a new one is drawn until it is unique.

The overall behavior of this model is that good combinations remain in the probability vector because they are not replaced and absorb the probabilities of bad combinations.

4.2. Partner Selection with Reputation

In the new model, reputation is used only when a new combination must be drawn in order to replace a combination deemed unacceptable. To represent reputation, a focal player assigns a weight to each possible partner. These weights are stored in vector $\mathbf{w}$. When a new combination is drawn, the probability of partner i being selected is proportional to his weight:

$$P(X = i) = \frac{w_i}{\sum_j w_j} . \tag{7}$$

Therefore a weight represents the desire to choose the corresponding player as a partner. It can be considered as his reputation. Higher values mean a partner has a higher reputation and thus should be chosen more often.

We consider that the n-player game does not allow the focal player to identify the partner that has done a particular action. In light of Eq. (7), the model assumes that a player can correctly identify the partners in a combination.

Weights are updated after knowing the result of playing a game with selected combination c_k according to:

$$w_j^{t+1} = w_j^t(1 - p_k^t) + (u - \underline{u})p_k^t , \tag{8}$$

where $j \in c_k$ and $\underline{u}$ is the lowest utility obtainable by the player.

The initial value of the weight vector may depend on the game. An optimistic approach is to define every initial weight to be the utility obtained by a player using a strategy belonging to a Pareto Optimum profile. This is tantamount to consider that all players are cooperative until shown otherwise.

Weight domain is the domain of the utility, but translated by $\underline{u}$ in order to always have positive weights even when the game has negative values. The dynamics of Eq. (8) could be interpreted as assigning to any partner the utility the focal player obtained while playing with him, discounted by probability p_k associated to the combination c_k where the partner is.

Algorithm 1 shows the details the partner selection based on reputation. The parameters of the algorithm are the strategy s used by the player, his set of candidate partners $\mathscr{N}$, the game he is going to play, $\mathscr{G}$, and the parameters of the partner selection model: pool size l, probability update factor δ, utility threshold u_T, and d that is a boolean indicating whether combinations in the vector are all distinct or repetitions are allowed.

Figure 1 lists the parameters of the model and sketches the player architecture.

Algorithm 1. Partner selection with reputation model algorithm

Require: s, $\mathscr{N}$, $\mathscr{G}$, l, δ, u_T, d
  $w^0 \leftarrow f(\mathscr{G})$
  $\mathbf{p}^1 \leftarrow \{p_i^1 : p_i^1 = 1/l \wedge 1 \leq i \leq l\}$
  $\mathbf{c}^1 \leftarrow \{c_i^1 : c_i^1 = \text{rnd}(\mathscr{C}) \wedge 1 \leq i \leq l\}$
  $\mathbf{w}^1 \leftarrow \{w_\alpha^1 : w_\alpha^1 = w^0 \wedge \alpha \in \mathscr{N}\}$
  for $t = 1$ **to** N_I **do**
    select combination of partners from $\mathbf{c}^t$ using $\mathbf{p}^t$
    play game $\mathscr{G}$ and obtain u
    compute $\mathbf{p}^{t+1}$ using Eqs. (4) and (5) with δ, u_T and u
    compute $\mathbf{c}^{t+1}$ using Eq. (6) with $\mathbf{w}^t$, u_T, u and d
    compute $\mathbf{w}^{t+1}$ using Eq. (8)
  end for

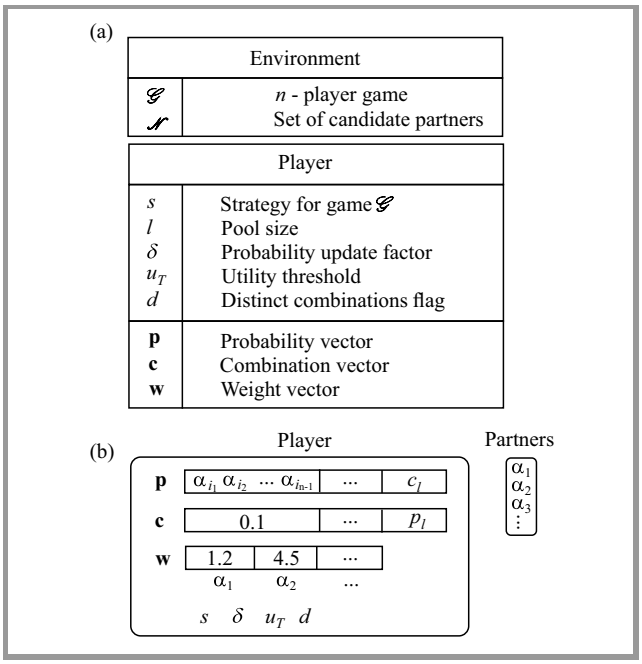


Fig. 1. Player description: (a) the parameters that effect the player, (b) the player architecture.

5. Experimental Analysis

In this section a simulation experiments are described that were conducted to show the capability to support cooperation of the composed model of dynamic populations and reputation based partner selection. The authors selected Public Good Provision (PGP) game, a n-player game to test the model. In this game each iteration involves n players and it does only provide an overall payoff, without identification of whether each player cooperated or defected. This poses the most demanding scenario for an individual reputation maintenance mechanism and that is the reason why such a game was chosen. Besides a description of PGP, this section also identifies the parameter values used for the dynamic population model and the parameter values of the partner selection model using individual reputation.

5.1. Public Good Provision

The authors have performed simulations using the PGP game [43], [44]. This game is commonly studied to anal-

yze cooperative dilemmas. It is considered a generalization of PD to n players. In the PGP game, a player that contributes to the good, incurs a cost c. The good is worth g for each player. The good value was fixed to $g = 1$ and varied the other game parameters n and c. To handle PGP we need to add a single gene, the probability to provide p_p to the agent's chromosome. The mutation operator adds to p_p a random value from a Gaussian distribution with mean zero and standard deviation 0.1. The resulting value is truncated to remain in interval $[0,1]$.
In this game, we have varied the number of players in the game, and the provision cost. Table 1 summarizes the parameters tested in the simulations.

Table 1
Game specific parameters used in the experiments

Parameters used in PGP		
n	Number players	$\{3,4,5,\ldots,8\}$
c	Provision cost	$\{0.1, 0.2, \ldots, 0.9\}$
p_c	Provision probability	1
$\lvert\mathscr{P}_0\rvert$	Size of initial population	10

5.2. Partner Selection Parameters

The two scenarios have been considered: one with Normal Partner Selection (NPS) – and a second with Reputation based Partner Selection (RPS). The partner selection model adds to the agent's chromosome three more genes. One for the vector size, l, one for payoff threshold π_T and a third for the probability update factor, δ. Whenever the mutation operator is applied to any of these genes, the first gene is perturbed by a discrete Gaussian distribution with mean zero and standard deviation one, while the second and third genes are perturbed by a Gaussian distribution with mean zero and deviation 0.1. In any case, the resulting value is truncated to a valid value. In these simulations, the values of these genes in the initial population were the following: $l = 4$, $\delta = 0.5$ and $\pi_T = 0.5$.

5.3. EnBEA Parameters

In the experiments that were performed a panmictic population was used. Although unrealistic, given that we used a carrying capacity, K, of 100, it is reasonable to assume that all agents can potentially interact with each other. When agents are capable of choosing with whom they will play, networks of agents can be formed. The initial population size was 10.
In this work we are interested in analysing different versions of the games we have used and to measure the occurrence of extinctions. With reproduction energy, e_R, set to 50, an agent that obtains per game the highest payoff, reproduces in less than 50 iterations. Since life expectancy, L, is set to 150, such agent can produce on average three offspring during its lifetime. Offspring were subject to a single-gene mutation with 10% probability. This is an evolutionary model with clonal reproduction subject to mutation.

Table 2
Common parameters used in all scenarios

K	Carrying capacity	100
e_R	Reproduction energy	50
	Energy birth	10
L	Old age	150
	Mutation probability	10%
	Number of iterations	10000
	Number or runs	30

The number of iterations was set to 100000, three orders of magnitude higher than an agent's average lifetime, in order to have a duration enough to observe an extinction or not. In order to obtain statistical results, we performed thirty runs for each parameter combination. Table 2 shows the values of these parameters.

6. Results

For each simulation run we recorded the number of iterations it lasted[1]. This measure is sufficient to assess the impact of weighted partner selection on players survivability. The authors assume that if a simulation reaches the maximum number of iterations (10000) players have successfully gained a foothold in the population.

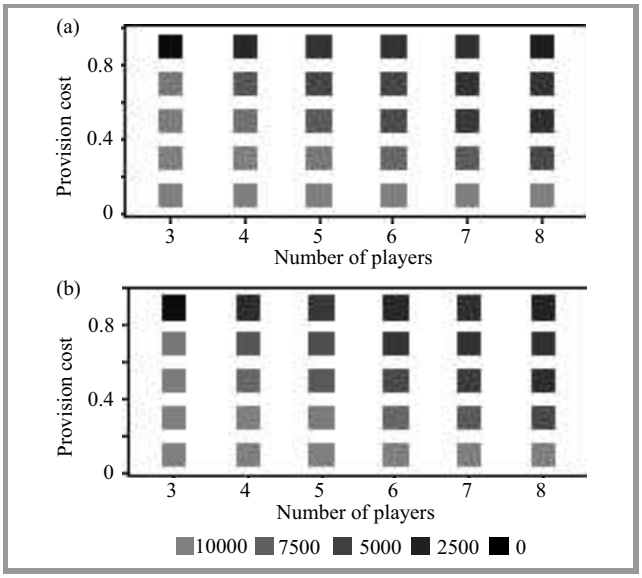


Fig. 2. Average number of iterations in: (a) RPS and (b) NPS scenarios. The lighter is the point, the longer is the corresponding set of simulations.

Figure 2 shows the average number of iterations in both scenarios. Although the fact that parameter values of the partner selection model were set to proper values there are still extinctions compared to previous work [10]. They are more frequent when the game has a higher number of players and higher provision cost. A higher number of players

[1]The simulation was implemented in Mercury, a declarative language, and is available at https://github.com/plsm/EBEA/releases/tag/v2.0.

means a single defector does not impair the payoff of all the other cooperators. It also means that he was more chances of being selected when a new combination is drawn. A high provision cost is beneficial for defectors as there is a higher payoff difference between defectors and cooperators. We also observed simulations where no extinction occurred, namely with low provision cost.

To better analyze the impact of partner selection with reputation, Fig. 3 shows the average number of iterations ratio between RPS and Normal Partner Selection (NPS) scenarios for all parameter combinations of the tested games. In thirteen parameter combinations (triangles pointing upward) the ratio is higher than one, meaning RPS simulations last longer than NPS simulations, while in seven conditions (triangles pointing downward) the ratio is lower than one, meaning NPS simulations last longer.

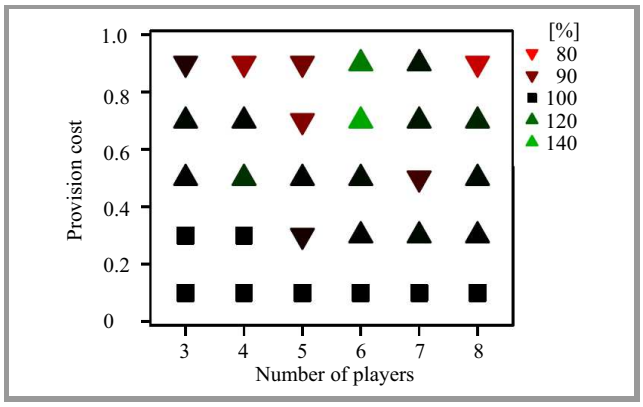


Fig. 3. Average number of iterations ratio between RPS and NPS scenarios: the lighter the point, the longer is the corresponding set of RPS simulations.

The authors have applied a Kolmogorow-Smirnov statistical test between two sets of number of iterations, one for each scenario. The results show that only in one parameter combination ($n = 6 \wedge c = 0.7$) the two sets are from different distributions. In this parameter combination reputation increased the number of iterations. Although there are more parameter combinations with a ratio higher than one, the impact of reputation is not statistical significant (p-value less than 0.1).

Compared to previous work [10], the results reported in this paper are better because agents do not need to evolve the capability to select partners.

7. Conclusions

It is known that simulations with partner selection last longer than simulations with random partners. The improvement is noticeable in PGP although population dynamics are sensitive to initial conditions. If agents in the initial population cannot gain any energy because they are pure exploiters, the population is condemned from the start. However, previous models chose partner groups and not individual partners [10] to create a team of n-players. Also, in that work, the parameter values of the partner selection model of agents in the initial population was set to random selection. Therefore, agents had to evolve the capability of selecting partners. This requires a combination of mutations in the genes that encode partner selection. However, mutation may introduce a defector that exploits existing cooperators thus leading the population to extinction. Here we used as control a model where the initial population starts with the right combination of partner selection parameter values. This means that these results are better than in [10] and this constitutes a more demanding challenge to the new model that uses partner selection based on individual reputation.

In n-player cooperation it is not always possible to identify individual behaviors. This causes an indetermination in case some player fails to cooperate. However even in such a stringent situation it may possible for a focal player to gather information about other players' strategies, by gradually forming their reputations. To model this problem a PGP type game is considered: when all players cooperate the payoff is one, otherwise it is zero. Reputation for each game partner is obtained from the payoff obtained in successive games where he participates. This results in a pessimistic approach with all players from a group of $n-1$ being penalized in case at least one of them defects. When the focal player needs to choose a new partner combination, the probability of choosing a player as partner is proportional to his reputation.

The reputation model is therefore characterized by a weight update policy that does not add any new parameter to the previous partner selection model. It only depends on the payoff obtained by the player, the partner weight, and the probability of selecting the combination where the partner is. This greatly reduces the complexity of the model. The results showed that the reputation model improved the payoff obtained by the focal player. Even when there are not enough acceptable players, the reputation model favored the best $n-1$ partners. As for the parameters of the partner selection algorithm, the best results were observed when the probability update factor was higher and when repetitions were allowed in the combination vector. When all combinations had to be distinct, there could be some bad partner combinations in a larger combination vector.

Results show that this reputation information, for slight it might be, enables higher payoffs for the focal player. Payoff differences between experiments using the reputation model and control experiments decrease with increasing number of partners n. This is consistent with an increased difficulty in assigning responsibility of defection to individual partners. In spite of the more stringent control experiment (with pre-evolved initial parameter values) the reputation model produced slightly better results in terms of number of iterations. Notice that the initial parameter values were chosen based on results of the choice of groups of partners. The reputation model may prove to have even better results with other set of initial values. This is an aspect to investigate further.

In future work, we will also investigate what type of network connections arise with partner selection, how stable a population is, and additional features that delay or avoid extinctions. There are many societal problems such as resource management [45] that can be better analyzed with EnBEA. This can be implemented if a fourth step in EnBEA that given agents' actions is introduced, current game parameters and common parameters such as carrying capacity, returns the set of parameters to be used in the following iteration of EnBEA. One can investigate how agents could be organized, what norms they should follow, which institutions should exist in order to avoid a collapse in the resource base. High game payoffs or carrying capacity values can be interpreted as a stable resource. Lower values can be interpreted as a polluted or depleted resource.

In terms of the reputation model, future work will focus on experimenting different reputation assignments and on other partner selection procedures. The number n of players in a game should influence the modifications to the current reputation. With higher n the modification of an individual reputation should be lower than with smaller n given that the uncertainty about individual responsibility in a negative result is higher. Partner selection taking into account reputation values can me made more or less greedy and this may have significant influence in the results.

Acknowledgements

This work was partially supported by FCT, Portugal (PEst-OE/EEI/UI0434/2011).

References

[1] H. Gintis, *Game Theory Evolving – A problem-centered introduction to modeling strategic interaction*, 1st ed. Princeton University Press, 2000.

[2] C. Camerer, *Behavioral Game Theory*. Princeton University Press, 2003.

[3] D. G. Rand, C. E. Tarnita, H. Ohtsuki, and M. A. Nowak, "Evolution of fairness in the one-shot anonymous ultimatum game", *Proc. Nat. Academy of Sciences*, vol. 110, no. 7, pp. 2581–2586, 2013.

[4] D. G. Rand and M. A. Nowak, "Evolutionary dynamics in finite populations can explain the full range of cooperative behaviors observed in the centipede game", *J. Theoretical Biology*, vol. 300, pp. 212 – 221, 2012.

[5] F. C. Santos, J. M. Pacheco, and T. Lenaerts, "Cooperation prevails when individuals adjust their social ties", *PLoS Comput. Biol.*, vol. 2, no. 10:e140, 2006.

[6] J. M. Pacheco, A. Traulsen, and M. A. Nowak, "Active linking in evolutionary games", *J. Theoretical Biology*, vol. 243, pp. 437–443, 2006.

[7] D. K. Levine and W. Pesendorfer, "The evolution of cooperation through imitation", *Games and Econ. Behav.*, vol. 58, no. 2, pp. 293–315, 2007.

[8] C. A. Aktipis, "Know when to walk away: contingent movement and the evolution of cooperation", *J. Theoretical Biology*, vol. 231, no. 2, pp. 249–260, 2004.

[9] S. S. Izquierdo, L. R. Izquierdo, and F. Vega-Redondo, "The option to leave: Conditional dissociation in the evolution of cooperation", *J. Theoretical Biology*, vol. 267, no. 1, pp. 76–84, 2010.

[10] P. Mariano and L. Correia, "Partner selection delays extinction in cooperative and coordination dilemmas", *Multi-Agent-Based Simul.* (to appear).

[11] R. Axelrod, *The Evolution of Cooperation*. New York: Basic Books, 1984.

[12] P. Mariano and L. Correia, "A private reputation mechanism for *n*-player games", in *Advances in Artificial Intelligence – IBERAMIA 2012*, J. Pavên, N. D. Duque, and R. Fuentes, Eds. Springer, 2012, pp. 432–441.

[13] M. Nowak, *Evolutionary Dynamics: Exploring the Equations of Life*. Belknap Press of Harvard University Press, 2006.

[14] C. P. Roca, J. A. Cuesta, and A. Sánchez, "Effect of spatial structure on the evolution of cooperation", *Phys. Rev. E*, vol. 80, no. 046106, 2009.

[15] G. Szabó and C. Hauert, "Phase transitions and volunteering in spatial public goods games", *Phys. Rev. Lett.*, vol. 89, no. 118101, 2002.

[16] M. Nowak, S. Bonhoeffer, and R. May, "Spatial games and the maintenance of cooperation", *Proc. Nat. Academy of Sciences*, vol. 91, pp. 4877–4881, 1994.

[17] F. C. Santos, V. V. Vasconcelos, M. D. Santos, P. Neves, and J. M. Pacheco, "Evolutionary dynamics of climate change under collective-risk dilemmas", *Mathem. Models Methods in Appl. Sci.*, vol. 22, no. 1 1140004-1–1140004-17, 2012.

[18] V. Grimm *et al.*, "A standard protocol for describing individual-based and agent-based models", *Ecolog. Modell.*, vol. 198, no. 1–2, pp. 115–126, 2006.

[19] R. E. Lenski, C. Ofria, R. T. Pennock, and C. Adami, "The evolutionary origin of complex features", *Nature*, vol. 423, no. 6936, pp. 139–144, 2003.

[20] T. S. Ray, "Evolving complexity", *Artif. Life and Robot.*, vol. 1, no. 1, pp. 21–26, 1997.

[21] S. Forrest and T. Jones, "Modeling complex adaptive systems with echo", in *Complex Systems: Mechanism of Adaptation*, R. J. Stonier and X. H. Yu, Eds. IOS Press, 1994, pp. 3–21.

[22] S. R. Beissinger and M. I. Westphal, "On the use of demographic models of population viability in endangered species management", *The J. Wildlife Manag.*, vol. 62, no. 3, pp. 821–841, 1998.

[23] C. Manusch, H. Bugmann, C. Heiri, and A. Wolf, "Tree mortality in dynamic vegetation models – a key feature for accurately simulating forest properties", *Ecolog. Modell.*, vol. 243, pp. 101–111, 2012.

[24] V. T. Thinh, P. F. Doherty Jr., and K. P. Huyvaert, "Effects of different logging schemes on bird communities in tropical forests: A simulation study", *Ecolog. Modell.*, vol. 243, pp. 95–100, 2012.

[25] A. J. McLane, C. Semeniuk, G. J. McDermid, and D. J. Marceau, "The role of agent-based models in wildlife ecology and management", *Ecolog. Modell.*, vol. 222, no. 8, pp. 1544–1556, 2011.

[26] J. Orbell and R. Dawes, "Social welfare, cooperators' advantage, and the option of not playing the game", *Amer. Sociolog. Rev.*, vol. 58, no. 6, pp. 787–800, 1993.

[27] E. A. Stanley, D. Ashlock, and M. D. Smucker, "Iterated prisioner's dilemma with choice and refusal of partners: Evolutionary results", in *Advances in Artificial Life*, F. Morán, A. Moreno, J. J. Merelo, and P. Chacón, Eds., *LNCS*, vol. 929, pp. 490–502. Springer, 1995.

[28] L. Tesfatsion, "How economists can get alife", in *The Economy as an Evolving Complex System II*, W. B. Arthur, S. N. Durlauf, and D. A. Lane, Eds., *SFI Studies in the Sciences of Complexity*, vol. XXVII, pp. 533–564. Addison-Wesley, 1997.

[29] M. Milinski, D. Semmann, and H.-J. Krambeck, "Reputation helps solve the 'tragedy of the commons'", *Nature*, vol. 415, pp. 424–426, 2002.

[30] M. A. Nowak and K. Sigmund, "Evolution of indirect reciprocity", *Nature*, vol. 437, pp. 1291–1298, 2005.

[31] H. Brandt, C. Hauert, and K. Sigmund, "Punishment and reputation in spatial public goods games", *Proc. R. Soc. Lond. B*, vol. 270, no. 1519, pp. 1099–1104, 2003.

[32] H. Ohtsuki and Y. Iwasa, "Global analyses of evolutionary dynamics and exhaustive search for social norms that maintain cooperation by reputation", *J. Theoretical Biology*, vol. 244, pp. 518–531, 2007.

[33] C. Dellarocas, "Goodwill hunting: An economically efficient online feedback mechanism in environments with variable product quality", in *5th Worksh. Deception, Fraud and Trust in Agent Societies*, R. Falcone and L. Korba, Eds., Bologna, Italy, 2002, pp. 26–40.

[34] C. Dellarocas, "The digitization of word-of-mouth: Promise and challenges of online reputation systems", *Manag. Science*, vol. 49, no. 10, pp. 1407–1424, 2003.

[35] J. Sabater and C. Sierra, "Review on computational trust and reputation models", *Artif. Intell. Rev.*, vol. 24, no. 1, pp. 33–60, 2005.

[36] M. A. Nowak and K. Sigmund, "Evolution of indirect reciprocity by image scoring", *Nature*, vol. 393, pp. 573–577, 1998.

[37] M. A. Janssen, "Evolution of cooperation in a one-shot prisoner's dilemma based on recognition of trustworthy and untrustworthy agents", *J. Econ. Behav. & Organiz.*, vol. 65, pp. 458–471, 2008.

[38] D. M. Kreps and R. Wilson, "Reputation and imperfect information", *J. Econ. Theory*, vol. 27, pp. 253–279, 1982.

[39] J. Brandts and N. Figueras, "An exploration of reputation formation in experimental games", *J. Econom. Behav. & Organiz.*, vol. 50, pp. 89–115, 2003.

[40] T. Wu, F. Fu, and L. Wang, "Partner selections in public goods games with constant group size", *Phys. Rev. E*, 2009.

[41] C. McIntosh, E. Sadoulet, S. Buck, and T. Rosada, "Reputation in a public goods game: Taking the design of credit bureaus to the lab", *J. Econ. Behav. & Organiz.*, vol. 95, pp. 270–285, 2013.

[42] P. Mariano and L. Correia, "Population dynamics of centipede game using an energy based evolutionary algorithm", in *Advances in Artificial Life, ECAL 2013*, P. Liò, O. Miglino, G. Nicosia, S. Nolfi, and M. Pavone, Eds. MIT Press, 2013.

[43] R. Boyd, H. Gintis, S. Bowles, and P. J. Richerson, "The evolution of altruistic punishment", *Proc. Nat. Acad. Sci.*, vol. 100, no. 6, pp. 3531–3535, 2003.

[44] C. Hauert, S. De Monte, J. Hofbauer, and K. Sigmund, "Volunteering as red queen mechanism for cooperation in public goods games", *Science*, vol. 296, pp. 1129–1132, 2002.

[45] P. R. Ehrlich and A. H. Ehrlich, "Can a collapse of global civilization be avoided?" *Proc. Royal Soc. B: Biological Sci.*, vol. 280, no. 1754, 2013.

Pedro Mariano has a 5 year degree in Informatics Engineering obtained in 1997 at Faculty of Science and Technology of the New University of Lisbon (FCT/UNL). He obtained the M.Sc. degree in FCT/UNL at 2000 and a Ph.D. degree at Faculty of Sciences of the University of Lisbon (FC/UL) at 2006. From 2004 to 2011 he was a practising assistant and assistant in Department of Electronics, Telecommunications and Informatics of the University of Aveiro where he has taught courses on operating systems, artificial intelligence, programming, automata theory, databases and distributed systems. Currently he is an assistant at the Department of Informatics of FC/UL. He has been member of program committees of conferences in the area of artificial intelligence and part of organizing committees of conferences and Portuguese programming contents. His research interests are focused in the evolution of cooperation using the Give-Take game and in developing agents capable of playing multi-player games such as Diplomacy.
E-mail: Plmariano@ciencias.ulisboa.pt
Departamento de Informática
Faculdade de Ciências
Universidade de Lisboa
Campo Grande
1749-016 Lisboa, Portugal

Luís M. P. Correia is an Associate Professor with habilitation at the Department of Informatics of the Faculty of Sciences of University of Lisbon (DI-FCUL) in Portugal. From 2004 he has lead the Laboratory of Agent Modeling (LabMAg) research center. Currently he is head of department at DI-FCUL. His research interests are in the area of artificial life, autonomous robots and self-organization in multi-agent systems. Besides lecturing in the three cycles of informatics he has also appointments at the post-graduations in cognitive science and in complexity sciences.
E-mail: Lmcorreia@ciencias.ulisboa.pt
Departamento de Informática
Faculdade de Ciências
Universidade de Lisboa
Campo Grande
1749-016 Lisboa, Portugal

Paper

An Agent-Based Collaborative Platform for the Optimized Trading of Renewable Energy within a Community

Luca Tasquier and Rocco Aversa

Dipartimento di Ingegneria Industriale e dell'Informazione, Second University of Naples, Aversa, Italy

Abstract—Cities are increasingly recognized for their ability to play a catalytic role in addressing climate and energy challenges using technologically innovative approaches. Since energy used in urban areas accounts for about 40% of total EU energy consumption, a change of direction towards renewable energy is necessary in order to alleviate the usage of carbonized electricity and also to save money. A combination of IT and telecommunication technologies is necessary to enable the energy and resources saving. ICT based solutions can be used to enable energy and money saving not only for a single building, but for the whole community of a neighborhood. In this paper a model for the energy cost minimization of a neighborhood together with an agent-based interaction model that reproduces the proposed formal representation is presented. Furthermore the authors present a prototype implementation of this model and first experimental tests.

Keywords—collective intelligence, energy cost minimization, multi-agent systems, Smart Cities.

1. Introduction

The Internet of Things (IoT) paradigm is rapidly gaining ground in the scenario of modern wireless telecommunications. The basic idea of this concept is the pervasive presence around us of a variety of things or objects – such as Radio-Frequency IDentification (RFID) tags, sensors, actuators, mobile phone – which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals [1]. As application of IoT, Smart Cities mainly focus on applying the next-generation information technology to all walks of life, embedding sensors and equipment to hospitals, power grids, railways, bridges, tunnels, roads, buildings, water systems, dams, oil and gas pipelines and other objects in every corner of the world [2].

The issues related to the climate challenge make Smart Cities even more attractive. Nowadays a change of direction towards renewable energy is necessary in order to alleviate the usage of carbonized electricity and also to save money. One of the renewable energy options is solar electricity, which could be deployed decentralized in urban areas. In Europe, 21.9 GW of photovoltaic systems were connected to the grid in 2011, compared to 13.4 GW in 2010, which is in line with the average of 40% increase during the past 15 years. Under this aspect, ICT based solutions can be used to enable energy and money saving not only for a single building, but for the whole community of a neighborhood. First of all, a formal representation of the problem is needed in order to study the feasibility of a possible solution and to map it on hardware and software structures. This introduces a model for the minimization of energy costs that leads to benefits not only to the single household, but to the entire community of a neighborhood. Each house is represented by an agent acting on its behalf in order to implement the developed model and to automate the optimization operations by using and exchanging the energy within the community according to the house own requirements and capabilities.

The presented work has been conceived within the research activities of CoSSMic project. CoSSMic (Collaborating Smart Solar-powered Micro-grids. FP7 – SMARTCITIES, 2013) is an ICT European project that aims at fostering a higher rate for self-consumption (50%) of decentralized renewable energy production by innovative autonomic systems for the management and control of power micro-grids on users' behalf [16]. Home Area Network (HAN) is formed by all electrical devices of the home connected to the network. In each house there is an agent gateway. Agents are used to manage the HAN with the aim of optimizing self-consumption rates using renewable energy sources. Micro-grids, embedded with renewable energy production, storage capacity and consumption, are combined with an intelligent ICT platform.

The paper is structured as follows. Section 2 reviews some related works, while in Section 3 a formal modeling of the cost minimization problem is presented, as well as an agent interaction model that maps the proposed solution. A prototypal implementation of the agent model and experimental results are described in Section 4. Finally conclusions are drawn in Section 5.

2. Related Work

The scientific community investigates different priorities in the field of smart grids. Some examples are market deregulation, ICT architecture, IT security and data protection, energy efficiency, integration of renewable energies, supply security, grid bottlenecks, grid expansion, decentralized energy production, smart meteorology, storage

devices and load flexibilization. Much effort has been spent on the investigation in the field of agents' technology. In [7] the authors describe why they believe that artificial intelligence, and particularly, the fields of autonomous agents and multi-agent systems are essential for delivering the smart grid as it is envisioned. In [8] a multi-agent system architecture simulates and analyses competitive electricity markets combining bilateral trading with power exchange mechanisms. Several heterogeneous and autonomous intelligent agents representing the different independent entities in electricity markets are used and a detailed description of a promising algorithm for decision support is presented and used to improve agents bidding process and counter-proposals definition. Agents are endowed with historical information about the market including past strategies of other players, and have strategic behavior to face the market. In [9] authors consider how consumers might relate to future smart energy grids, and how exploiting software agents to help users in engaging with complex energy infrastructures. Paper [10] presents the architecture of an agent-based platform for power generating and power consuming companies in contract electricity market. An intelligent agent, by using fuzzy logic modification of genetic algorithm in order to accomplish strategy optimization, implements the negotiation process by selecting a strategy using learning algorithms. In [11] another negotiation algorithm using game theory is proposed, where agents act on behalf of end users, thus implying the necessity of being aware of multiple aspects connected to the distribution of electricity related to outside world variables like weather, stock market trends, location of the users etc. In [12] authors define a methodology for predicting the usage of home appliances. An agent based prediction algorithm captures the everyday habits by exploiting their periodic features. In addition, the algorithm uses an episode generation hidden Markov model (EGH) to model the interdependency among appliances. In [13] and [15] an agent-based approach to manage negotiation among the different parties is presented. The goal is to propose adaptive negotiation strategies for energy trading in a deregulated market. In particular, strategies derived from game theory are used, in order to optimize energy production and supply costs by means of negotiation and adaptation. Negotiation strategies in a multi-agent environment are also used in [14] where agents collaborate to assist human activities in safety critical scenarios. In [17], [19], [20] agents' technology is used for the negotiation and brokering of computational resources in cloud markets.

3. Energy Model

In the context of Smart Cities it is possible to model and analyze the energy profile of a house within a neighborhood so that it is possible to identify the best strategies to minimize the energy cost of the single house and of the overall neighborhood. Some notations useful for the discussion are introduced in Table 1. The proposed model is discrete-time, with sampling period T.

Table 1
Energy model parameters

Parameter	Description	Constraints
T	Sampling period	$T \geq 0$
c_a	Auto-consumed energy unit cost	$c_a \geq 0$
c_p	Provider's energy unit cost	$c_p \geq 0$
c_n	Neighbor's energy unit cost	$c_n \geq 0$
f_a	Auto-consumed energy selling indicator	$0 \leq f_a \leq 1$
f_p	Provider's energy selling indicator	$0 \leq f_p \leq 1$
f_n	Neighbor's energy selling indicator	$0 \leq f_n \leq 1$
e_r	Required energy	$e_r \geq 0$
e_{ra}	Auto-consumed required energy	$e_{ra} \geq 0$
e_{rp}	Required energy acquired from provider	$e_{rp} \geq 0$
e_{rn}	Required energy acquired from neighbor	$e_{rn} \geq 0$
e_p	Produced energy	$e_p \geq 0$
C	House total energy cost	
C_a	Auto-consumed energy cost	
C_p	Energy cost acquired from provider	
C_n	Energy cost acquired from neighbor	

3.1. House Cost Minimization

In principle it is possible to define the house required energy e_r as the sum of three contributions: the part of the required energy that is auto-consumed from the produced one, the part of the required energy acquired from a neighbor and the part of the required energy acquired from the energy provider:

$$e_r(kT) = e_{ra}(kT) + e_{rn}(kT) + e_{rp}(kT), \forall k \in \mathbb{Z}. \quad (1)$$

The auto-consumed energy cost C_a can be defined as:

$$C_a(kT) = c_a e_{ra}(kT), \forall k \in \mathbb{Z}, \quad (2)$$

where c_a can be decomposed in a constant part and a part that takes into account costs and fees for the energy consumption (f_a):

$$c_a = c + c f_a. \quad (3)$$

Thus C_a becomes:

$$C_a(kT) = c e_{ra}(kT) + c f_a e_{ra}(kT). \quad (4)$$

$$C(kT) = c\Big[\underbrace{\big(e_{ra}(kT)+e_{rn}(kT)+e_{rp}(kT)\big)}_{e_r(kT)} + \underbrace{\big(f_n e_{rn}(kT)+f_p e_{rp}(kT)\big)}_{F(kT)}\Big] \geq 0, \quad \forall k \in \mathbb{Z}$$

Fig. 1. House total cost.

In the same way it is possible to evaluate the energy cost acquired from a neighbor (C_n) and the energy cost acquired from provider (C_p):

$$\begin{cases} C_n(kT) = c_n e_{rn}(kT) \\ c_n = c + cf_n \end{cases} \rightarrow C_n(kT) = ce_{rn}(kT) + cf_n e_{rn}(kT)\ , \forall k \in \mathbb{Z}$$

$$\begin{cases} C_p(kT) = c_p e_{rp}(kT) \\ c_p = c + cf_p \end{cases} \rightarrow C_p(kT) = ce_{rp}(kT) + cf_p e_{rp}(kT)\ , \forall k \in \mathbb{Z} \tag{5}$$

The house total energy cost C is the sum of the contribution calculated in Eqs. (4) and (5):

$$C(kT) = C_a(kT) + C_n(kT) + C_p(kT)\,. \tag{6}$$

By expanding the Eq. (6) we obtain:

$$\begin{aligned} C(kT) &= c_a e_{ra}(kT) + c_n e_{rn}(kT) + c_p e_{rp}(kT) = \\ &= ce_{ra}(kT) + cf_a e_{ra}(kT) + ce_{rn}(kT) + cf_n e_{rn}(kT) + \\ &\quad + ce_{rp}(kT) + cf_p e_{rp}(kT) = \\ &= c\big[(e_{ra}(kT) + e_{rn}(kT) + e_{rp}(kT)) + \\ &\quad + (f_a e_{ra}(kT) + f_n e_{rn}(kT) + f_p)\big], \quad \forall k \in \mathbb{Z} \end{aligned} \tag{7}$$

Assuming that for the auto-consumed energy fees are nullable, $f_a = 0$ could be considered. The equation becomes as shown in Fig. 1.

Derived from the equation, the house total energy cost depends on the required energy and on a part that takes into account the fees for purchasing energy from neighbor and provider, weighed by a scale factor on the amount of required energy F. Since C is a non-negative value, to minimize the house energy cost is equivalent to tend C to zero. Given the fact that the naive solution $e_r = 0$ is a non-feasible solution (the authors are supposing that the house needs energy to power its devices), it is possible to analyze two situations:

1. The house produces more energy than it requires, $e_p \geq e_r$. In this case the best strategy is to tend F to zero, that translates in tending e_{rn} and e_{rp} to zero:

$$\begin{aligned} \min\big\{C(kT)\big\} &= \lim_{e_{rn}(kT)\to 0} \lim_{e_{rp}(kT)\to 0} C(kT) = \\ &= c\,(e_{ra}(kT) + 0 + 0)\,. \end{aligned} \tag{8}$$

   The Eq. (8) means that the best efficiency in terms of house's consumption cost is when $\boldsymbol{e_r = e_{ra}}$, i.e., the best strategy is to auto-consume the produced energy.

2. The house requires more energy than it produces (or it is unable to produce energy), $e_p \leq e_r$. In this case the house has to acquire the required energy (or part of this) from two of the possible energy sellers, i.e., the neighborhood and the energy provider. Usually energy providers introduce significant fees and ancillary costs. Thus it is possible to assume that

$$f_p \gg f_n\,. \tag{9}$$

   In order to minimize C to minimize e_{rp} would be necessary:

$$\begin{aligned} \min\{C(kT)\} &= \lim_{e_{rp}(kT)\to 0} C(kT) = \\ &= c\,[(e_{ra}(kT) + e_{rn}(kT) + 0) + f_n e_{rn}(kT)]\,. \end{aligned} \tag{10}$$

By unifying the results reached in cases 1 and 2 it is evident that the best strategy to minimize the house energy cost is to auto-consume the produced energy and to acquire the remaining requested part from the neighborhood, thus minimizing the exchange with the energy provider.

3.2. Neighborhood Cost Minimization

The neighborhood is composed by several buildings, that can be handled as houses in presented model. In general a neighborhood is composed by NH houses that can consume and/or produce energy.

Define C_{NH} as neighborhood's total energy cost, that is:

$$C_{NH}(kT) = f\,[S_i\,(kT)]\,, \forall i \in NH, \quad \forall k \in \mathbb{Z}, \tag{11}$$

where S_i is the energy state of each house.

From Eq. (11) it is possible to understand that in order to find the best energy exchange in the neighborhood's that leads to a minimization of C_{NH} the neighborhood should know the energy state of the houses at any time. This requirement implies a number of technological issues:

- **Needing of a centralized controller**. In order to evaluate the best energy exchange a global vision of the neighborhood's energy state is needed. Thus there is the necessity of a centralized controller that collects data about S_i and manages energy exchanges among the houses, having scalability and efficiency losses;

- **Real-time constraints**. Time instant t depends on the sample time of the sensors that gather data within the houses and on the processing capacity of the controller. The efficiency of the minimization algorithm is bound to the performances of the used technologies;

- **Communication overhead**. Even when the houses don't need an energy exchange, they must communicate to the controller their state, thus increasing traffic on the neighborhood's network and leading the controller to become a bottleneck.

C_{NH} can be described as the sum of contribution coming from each house:

$$C_{NH}(kT) = \sum_{i=1}^{NH} C_i(kT),\ \forall i \in NH,\ \forall k \in \mathbb{Z}. \tag{12}$$

Thus it is possible to define:

$$\min\left\{C_{NH}(kT)\right\} = \min\left\{\sum_{i=1}^{NH} C_i(kT)\right\},\ \forall i \in NH,\ \forall k \in \mathbb{Z}. \tag{13}$$

In order to minimize the neighborhood's total energy cost it is possible to lighten model's requirements. Assume that each S_i is independent of any S_j:

$$S_i(kT) \perp\!\!\!\perp S_j(kT),\ \forall k \in \mathbb{Z},\ \forall i \in NH,\ j \neq i. \tag{14}$$

Equation (14) means that every house can look only at itself in order to minimize the energy cost, by acting autonomously without a centralized orchestrator. Due to the unfeasibility of a centralized solution and by taking a cue from the assumption of energy status independence, the minimization of the neighborhood's total energy cost can be processed as the minimization of the each house local energy cost:

$$\min\left\{C_{NH}(kT)\right\} = \sum_{i=1}^{NH} \min\left\{C_i(kT)\right\},\ \forall i \in NH,\ \forall k \in \mathbb{Z}. \tag{15}$$

By combining Eqs. (12) and (15), we obtain:

$$\min\left\{C_{NH}(kT)\right\} = \sum_{i=1}^{NH} \min\{C_i(kT)\} =$$

$$= \sum_{i=1}^{NH} \begin{Bmatrix} \lim_{e_{rn_i}(kT)\to 0} \lim_{e_{rp_i}(kT)\to 0} C_i(kT),\ \text{if } e_{p_i}(kT) \geq e_{r_i}(kT) \\ \lim_{e_{rp_i}(kT)\to 0} C_i(kT),\ \text{if } e_{p_i}(kT) < e_{r_i}(kT) \end{Bmatrix} =$$

$$= \sum_{i=1}^{NH} \begin{Bmatrix} ce_{ra_i}(kT),\ \text{if } e_{p_i}(kT) \geq e_{r_i}(kT) \\ c[(e_{ra_i}(kT) + e_{rn_i}(kT)) + f_{n_i} e_{rn_i}(kT)],\ \text{if } e_{p_i}(kT) < e_{r_i}(kT) \end{Bmatrix},$$

$$\forall i \in NH,\ \forall k \in \mathbb{Z}. \tag{16}$$

This approach brings an optimization of energy costs by using a selfishly behavior of each house, where the collaboration and communication among the houses is limited to the energy demand in case of its unavailability to auto-consume. This solution is completely distributed and doesn't need a centralized management and coordination, being highly scalable and efficient.

3.3. Energy Characterization

In order to characterize the house behavior, it is necessary to identify the constraints that the home must comply with, in energy state $S(t)$ terms. First of all, it is assumed that each house has an accumulator to store the produced energy to use or to sell if needed. Notations are introduced in Table 2.

Table 2
Energy characterization parameters

Parameter	Description
$P_p(t)$	Power produced by photovoltaic system (PV system)
$A_c(t)$	Current consumed by the load
V	House supply voltage
$P_{acc-max}$	Maximum power supplied by the accumulator
$E_{acc}(t)$	Energy stored in the accumulator in time t

The consumed power $P_c(t)$ is:

$$P_c(t) = A_c(t)V, \tag{17}$$

while $S(t)$ is defined as:

$$S(t) = P_c(t) - P_p(t). \tag{18}$$

Due to Eqs. (17) and (18), it is possible to understand that the condition for the auto-consumption is:

$$\int_{t_0}^{t_0+\Delta t} S(t)dt - E_{acc}(t_0) \leq 0. \tag{19}$$

Since the accumulator are characterized by a maximum amount of power that it is able to provide ($P_{acc-max}$), the condition for the auto-consumption becomes:

$$\begin{cases} \int_{t_0}^{t_0+\Delta t} S(t)dt \leq E_{acc}(t_0) \\ S_{max} \leq P_{acc-max} \end{cases}. \tag{20}$$

Due to the fact that the accumulator is modeled as a capacitor, the maximum amount storable energy is:

$$E_{acc-max} = \frac{1}{2} C_{acc} V^2. \tag{21}$$

Thus:

$$E_{acc}(t) \leq \frac{1}{2} C_{acc} V^2. \tag{22}$$

Let us suppose that the production profile of the PV system and the consumption profile of the load can be predicted. This translates in estimates a-priori $P_p(t)$ and $A_c(t)$:

$$\int_{t_0}^{t_0+\Delta t} S_{est}(t)dt = \int_{t_0}^{t_0+\Delta t} P_{\text{c est}}(t)dt - \int_{t_0}^{t_0+\Delta t} P_{\text{p est}}(t)dt =$$

$$= V \int_{t_0}^{t_0+\Delta t} A_{\text{c est}}(t)dt - \int_{t_0}^{t_0+\Delta t} P_{\text{p est}}(t)dt. \tag{23}$$

$$E_{acc}(t_0-\Delta t)=E_{acc}(t_0-\Delta t)+E_{surplus}[t_0-\Delta t;t_0]-E_{sold}[t_0-\Delta t;t_0]$$

$$E_{exc}[t_0;t_0+\Delta t]=E_{acc}(t_0-\Delta t)+\int_{t_0}^{t_0+\Delta t}P_{\text{p est}}(t)dt-V\int_{t_0}^{t_0+\Delta t}A_{\text{c est}}(t)dt$$

$$E_{\text{to-sell}}[t_0-\Delta t;t_0]=\begin{cases}E_{\text{exc}}[t_0;t_0+\Delta t],\text{if } E_{exc}[t_0;t_0+\Delta t]>0\\0,\text{otherwise}\end{cases}$$

$$E_{\text{to-buy}}[t_0-\Delta t;t_0]=\begin{cases}\left|E_{\text{exc}}[t_0;t_0+\Delta t]\right|,\text{if } E_{\text{exc}}[t_0;t_0+\Delta t]<0\\0,\text{otherwise}\end{cases}$$

Fig. 2. Prediction algorithm.

The authors assume that only energy stored in $t_0-\Delta t$ is available so to plan the necessary actions to undertake in $t_0<t<t_0+\Delta t$. By predicting $P_p(t)$ and $A_c(t)$ it is possible to forecast the amount of exceeding energy:

$$E_{exc}[t_0;t_0+\Delta t]=E_{acc}(t_0-\Delta t)+\\+\int_{t_0}^{t_0+\Delta t}P_{\text{p est}}(t)dt-V\int_{t_0}^{t_0+\Delta t}A_{\text{c est}}(t)dt \tag{24}$$

By forecasting the amount of exceeding energy, it can be evaluated if there is energy to sell or buy:

$$E_{exc}[t_0;t_0+\Delta t]=\begin{cases}E_{\text{to-sell}}[t_0-\Delta t;t_0],\ \text{if } E_{exc}[t_0;t_0+\Delta t]\geq 0\\E_{\text{to-buy}}[t_0-\Delta t;t_0],\ \text{if } E_{exc}[t_0;t_0+\Delta t]<0\end{cases}. \tag{25}$$

Since the load optimization operations and the prediction starts in $t_0-\Delta t$, and the forecasting is valid for the period between t_0 and $t_0+\Delta t$, **the time limit for publishing the proposal and the energy requests and for closing the evaluations is Δt**.

By taking a cue from the described relations, the steps that the houses should do each timespan Δt are described by the algorithm in Fig. 2. The authors suppose that is possible to get information about the energy stored by the accumulator at any instant. This value is not the real amount of energy available to be auto-consumed because there is the possibility that the house decided the selling part of energy to a neighbor in the previous timespan. If $E_{to-sell}[t_0-\Delta t;t_0]$ is greater than zero, the house publishes a proposal to sell energy that is valid until t_0. By the contrary, if $E_{to-buy}[t_0-\Delta t;t_0]$ is greater than zero, the house publishes a energy request in order to buy the future consumed energy from someone in the neighborhood. The search and the evaluation are allowed up to t_0, if the evaluation fails or there are not proposals during this period, the house buys the needed energy from the provider. Since it is possible to acquire from a neighbor more energy than the required one, it is possible to store the exceeding amount in the accumulator. This energy is taken into account by $E_{surplus}[t_0-\Delta t;t_0]$. In this way there is the possibility that also a building that has not production facilities can become a seller.

The algorithm relies on the knowledge about the power production and consumption in the future. For $P_p(t)$ it is possible to use historical data about the production of the PV panels and to rely on short-term weather forecasts. For the estimation of $A_c(t)$ it is possible to use historical series and the current scheduling of the expected loads (dishwasher, washing-machine, etc.) generated according to some optimization actions of the house's loads. Boundaries such as $P_{acc-max}$ and $E_{acc-max}$ can be used as evaluation's parameters in the proposals and in the energy requests.

The one-step prediction used in the algorithm could lead to performances that aren't the best for the single house. In fact, suppose that in $t_0-\Delta t<t<t_0$ an house decides to sell energy because it predicts that in $t_0<t<t_0+\Delta t$ it has an energy surplus. After that, if the evaluation succeeds, it predicts that in $t_0+\Delta t<t<t_0+2\Delta t$ it needs to buy energy because it doesn't have enough energy stored in order to satisfy the load in this timespan and it is forced to make an energy request in $t_0<t<t_0+\Delta t$. In this case it is evident that the best for the house would have been not to sell the energy so to have enough energy stored to auto-consume also in $t_0+\Delta t<t<t_0+2\Delta t$. Even if it seems that a multi-step prediction has better performances for the single house, the one-step prediction has a lower computational complexity which corresponds to a higher reactivity in the application of the algorithm, which becomes crucial by dealing with a system with strong real-time constraints. Moreover, since the algorithm is based on the usage of historical data and forecasts, a short-term prediction has more accuracy than a long-term one, that impacts positively on the prediction performances.

One way to give more robustness to the algorithm is to change the evaluation of $E_{\text{to-sell}}[t_0-\Delta t;t_0]$ and $E_{\text{to-buy}}[t_0-\Delta t;t_0]$ as follows:

$$E_{\text{to-sell}}[t_0-\Delta t;t_0]=\begin{cases}E_{\text{exc}}[t_0;t_0+\Delta t]-\varepsilon_{sell},\ \text{if } E_{exc}[t_0;t_0+\Delta t]>0\\0,\ \text{otherwise}\end{cases},$$

$$E_{\text{to-buy}}[t_0-\Delta t;t_0]=\begin{cases}\left|E_{\text{exc}}[t_0;t_0+\Delta t]\right|+\varepsilon_{buy},\ \text{if } E_{exc}[t_0;t_0+\Delta t]<0\\0,\ \text{otherwise}\end{cases}, \tag{26}$$

where ε_{sell} and ε_{buy} are parameters that take into account possible forecasting errors in selling and buying energy.

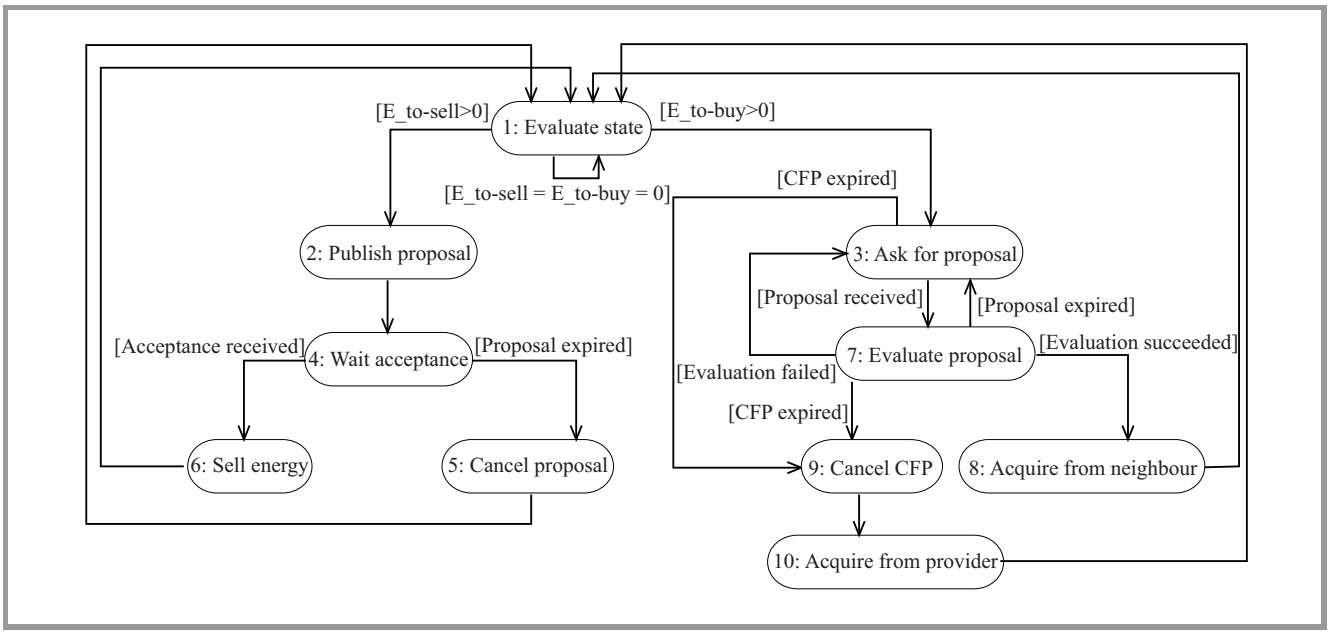


Fig. 3. Agent interaction model for energy cost minimization.

3.4. Agent Interaction Model for Cost Minimization

To implement the abovementioned strategy, the agent paradigm is used, building up an interaction model for Collective Intelligence that aims at minimizing the overall neighborhood's cost. Each house is modeled by an agent that adapts its behavior in order to maximize auto-consumption of energy and minimize the exchange with the energy provider. Thus the neighborhood is represented by a number of agents that are distributed within a "virtual" community and run autonomously in order to implement their own strategy. Since every house might have different sensors in order to retrieve information about the energy consumption/production of the devices, the connection between sensors and the agent is implemented by a RESTFul gateway that is in charge of translating the events in an agent common language and forwarding them to the agent [18]. Thanks to its reactiveness and proactiveness capabilities, the agent paradigm is able to match the described selfish behavior with on-demand collaboration in a distributed environment by using an asynchronous communication approach. The agent technology allows to easily react to environment's changes in order to reach the cost minimization goals. Moreover, the architecture is highly scalable and can easily grow and decrease with the neighborhood by simply adding and removing agents from the platform, thus exploiting the complete decoupling among the agents.

The minimization's strategy can be translated in three agent's macro-behaviors:

- **maximize auto-consumption** – whatever state the agent is in, if the agent needs energy and an energy production's event occurs, this event triggers a series of state transitions that lead it to consume the produced energy;
- **minimize energy requests to the provider** – if there is an energy request and the produced energy is not sufficient to completely satisfy the request, the agent asks for the needed energy to the neighborhood;
- **collaborative approach** – if the house has an excess of produced energy, the agent provides this energy to the neighborhood.

The agent interaction model is drawn in Fig. 3 while the description of each state is provided in Table 3.

Being consistent with the discrete-time model presented in Section 3, even if the interaction model is event-based, the full set of operations is marked by Δt. Every Δt the automata returns to its initial state, starting a new round of estimation-trading-purchasing/selling.

As it is possible to understand, Δt becomes a crucial parameter for the algorithm performances. Too small a value of Δt makes stressing the prediction algorithm and might be too short to complete the negotiation phase. Too high a value of Δt makes the energy performances of the house too bind to the accuracy of the forecasting. For these reasons, the tuning of Δt strongly impacts on the house cost minimization.

4. Prototype Implementation

As described in Section 3.4, it is possible to map the house behavior to an agent in charge of performing the operations aimed at minimizing the energy cost. The designed interaction model has been implemented by using the agent technology. Execution environment for agents and communication facilities are provided by the JADE agent platform [3], that supplies an execution environment of soft-

Table 3
Agent's state description

No.	State	Description
1	Evaluate state	In this state are performed all the operation described in Fig. 2.
2	Publish proposal	If the house produces some exceeding energy, the agent publishes a proposal in order to sell the energy to other houses in the neighborhood.
3	Ask for proposal	If the house needs energy and it has not produced one, it asks the neighborhood for energy to buy by using a Call for Proposal (CFP).
4	Wait acceptance	In this state the house waits for acceptance of a proposal published in state 2.
5	Cancel proposal	If during the waiting of a proposal acceptance notification t passes, the proposal is canceled.
6	Sell energy	If a proposal acceptance notification has been received, the agent sells the agreed energy to the buyer.
7	Evaluate proposal	If a proposal is received, the agent evaluates it in order to the buy neighbor's energy.
8	Acquire from neighbor	If a proposal evaluation succeeded, the agent buys the agreed energy from the seller.
9	Cancel CFP	If during a proposal evaluation or the waiting of proposals t passes, the CFP is canceled.
10	Acquire from provider	This is the worst state in which the agent can be. If the agent needs energy and no acceptable proposals come within Δt, the only thing that the agent can do is to acquire the needed energy from the energy supplier.

ware agents, an Agent Communication Channel (ACC) and some protocol implementation to support communication. AMS and DF provide standard services of FIPA compliant agent platforms [4]. A management system for agents and a yellow pages registry for publication and discovery of agent based services. Agents will communicate among them via standard ACL (Agent Communication Language). JADE is completely written in Java so that each agent is represented by a Java class as well as the behaviors of every agent.

The agent representing the house is called Energy Agent (EA). It is composed by a number of behaviors that implement the Finite State Machine (FSM) designed in Fig. 3. Each behavior contains the particular operations that characterize the state of the house. For example, the *Evaluate State* behavior includes the forecasting of $P_p(t)$ and $A_c(t)$ as well as the prediction algorithm described in Fig. 2, while the *Evaluate Proposal* behavior embeds the algorithms used to evaluate a given proposal against a submitted CFP.

In order take in account the temporal constraint given by Δt, it is used a *Watchdog* behavior that runs in parallel with the ones representing the state of the FSM. If Δt passes and it marks the proposal/CFP as expired by writing a particular variable in memory. Each state of the FSM controls this variable and adapts its behavior according to the read value, being compliant with the described interaction model. When the EA is in the *Evaluate State* behavior, it resets the *Watchdog* behavior in order to restart all the operations.

To ensure the scalability of the distributed platform, it has been used a bus-based approach. When an agent wants to sell some energy, it publishes the proposal on the bus and waits for an acknowledgement coming from someone in the neighborhood that is interested in buying its energy. When the proposal expires, it simply withdraws this from the bus. If someone is evaluating the proposal, it is notified about the withdrawal. On the other hand, if an agent is interested in buying some energy, it can retrieve a proposal from the bus (if any) and can evaluate it. The bus usage for the communication within the neighborhood allows also the synchronization among sellers and buyers. When a buyer asks for a proposal, the bus gives to the asker the first proposal in the queue that is not yet under the evaluation by another agent. In fact, when an agent is evaluating a proposal, it puts a lock on it in order to prevent that someone can evaluate at the same time the same proposal. If the evaluation succeeds, the seller is alerted and it starts to give the agreed energy to the buyer. If the evaluation fails,

Table 4
Agent Bus operations

Method	Description
Publish proposal	This method allows a seller to publish a new proposal to be evaluated by other agents in the neighborhood.
Ask for proposal	It is used by a buyer to retrieve the first unlocked proposal in the queue (if any). It returns a proposal and locks it in case of success, a null value otherwise.
Release proposal	This method allows a buyer to unlock a proposal that has been evaluated and refused.
Accept proposal	In order to mark a proposal as accepted, a buyer can use this method.
Receive acceptance notification	This method is used by a seller in order to ask the bus about the acceptance of a published proposal by a buyer. It returns a boolean value, true if accepted, false otherwise.
Cancel proposal	When a proposal expires, the publisher can use this method to withdraw the proposal.

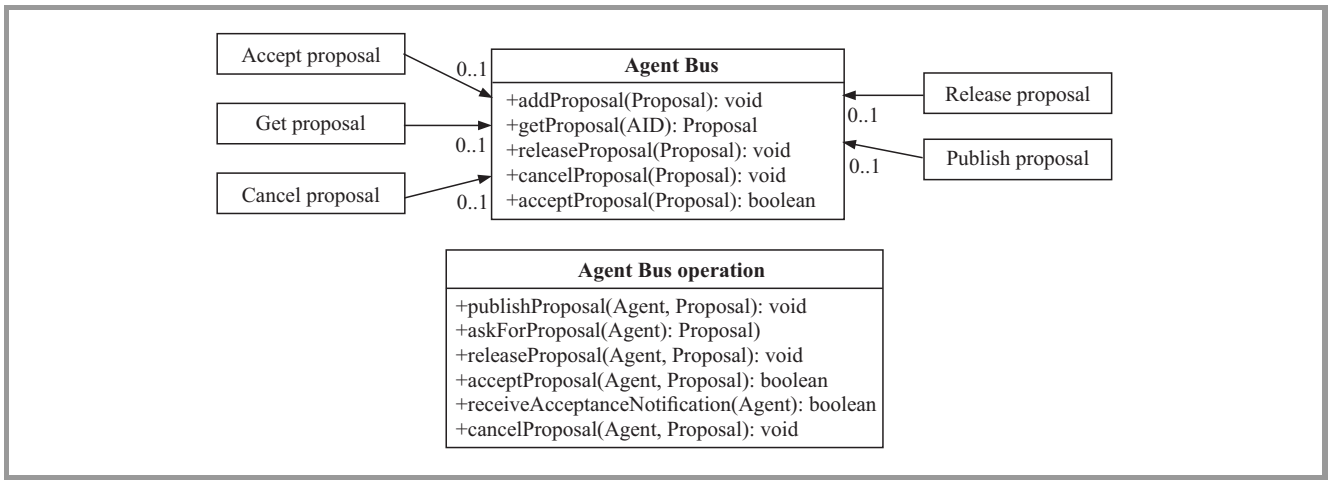


Fig. 4. Agent Bus class diagram.

the buyer unlocks the proposal so that it can be evaluated by others.

The bus can be realized by using different technologies, such as queue servers like ActiveMQ [5], RabbitMQ [6], etc. In first prototype, the bus has been implemented as an agent within the platform, called Agent Bus (AB). AB runs at boot time and provides to the EAs all the operations they need in order to perform the overmentioned operations. In particular, the methods that the bus makes available are described in Table 4.

As it is possible to understand from the AB class diagram in Fig. 4, the Agent Bus Operation exposes operations that are used by each EA and embeds the ACL messages sent and received to/from the AB in order to perform the chosen action: in other words, EAs and AB are connected by using Agent Bus Operation via messages' exchange. On the other hand, for each operation, the AB has a particular behavior that allows to receive the specific message and to act on its data structures in order to perform the requested action.

4.1. Experimental Results

In order to validate the proposed approach a synthetic workload built up by using five buildings in a neighborhood is used. We define *consumer* a building that has not energy production facilities and, in its normal behavior, it has only the possibility to consume energy. By the contrary, a *prosumer* is a building that has energy production capabilities. In presended experiments the energy profiles of three consumers and two prosumers are used and the attention is focused on a consumer, called *target*. As previously said, the predefined energy profiles for each building are used, thus zeroing the time for $P_p(t)$ and $A_c(t)$ estimations. Furthermore, it is assumed that these estimations are correct, thus not introducing errors in the prediction phase.

The experiments aim at evaluating the impact of Δt on the house performances varying the buildings in the neighborhood. The Δt is set on two consumers and two prosumers to a fixed value $\Delta t_{others} = 1000$ ms. The Δt_{target} was varied at 500, 1000, 2000 ms, gradually introducing buildings in the neighborhood.

In order to understand the performances of the prototype, the percentage of occurrences of the *Acquire from Provider* state is analyzed, that represents the less favorable state of the agent (Fig. 5). As it is possible to see, Δt_{target} strongly impacts on the number of occurrences of this state. In fact a greater value of Δt_{target} provides much time to evaluate proposal in the neighborhood before the CFP expires. However the performances are also influenced by the ratio among consumers and prosumers within the neighborhood. If there are too many consumers with respect to prosumers, the speed in evaluating the proposals becomes crucial and consequently the energy performances are closely linked to the performances of the evaluation algorithm. The introduction of a new prosumer radically changes the scenario, as reported in the chart.

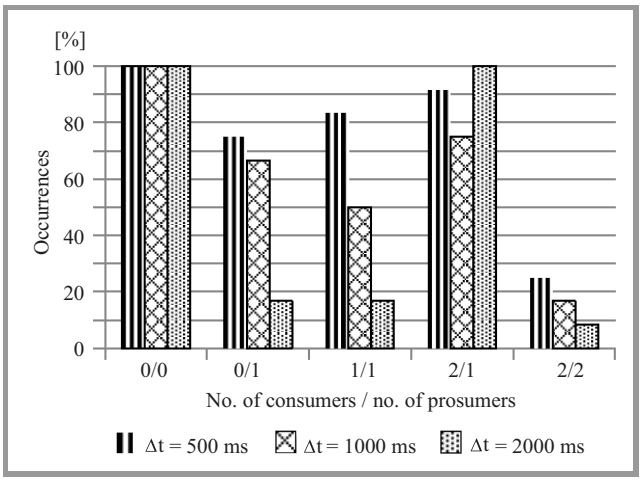


Fig. 5. Acquire from provider percentage of occurrences.

Another interesting result coming from the experiments is evincible by looking at Figs. 6 and 7. The fact that the values in these charts are not completely null denotes the

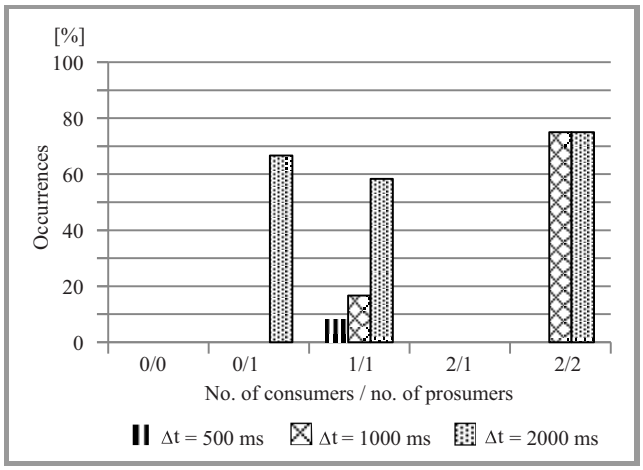


Fig. 6. Cancel proposal percentage of occurrences.

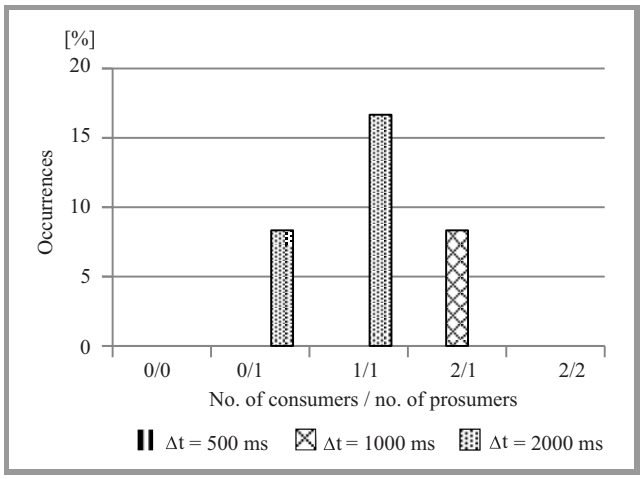


Fig. 7. Sell energy percentage of occurrences.

situation in which target bought more energy than it needed and it converts itself to a seller, publishing proposals and, in some cases, being able to sell excess energy.

5. Conclusion

In this paper authors present a model for the energy cost minimization of a neighborhood. The energy cost function of a single house at first is analyzed and modeled. After that the authors model, under houses' independence hypothesis, the neighborhood energy cost function and how to minimize it. Also a characterization of the house behavior is proposed in terms of energy production and consumption and a way to reach the cost minimization by using predictions and load estimation. On this basis, an agent-based interaction model that aims at maximize the auto-consumption of the produced energy and at buying the needed one from neighbors instead of supplier is presented. The validation of the interaction model has been performed by developing and testing a prototypal model implementation. Experimental results highlight how a correct tuning of the operations timespan has a strong impact on the performances, as well as a balanced ratio among the number of consumers and prosumers can play a crucial role on the performances of the whole neighborhood. The authors are planning other experiments aimed at evaluating the performances of the prototype by having different timespans for each building within the neighborhood. Furthermore, future works will deal with the introduction of constraints on the house devices control in order to optimize the cost function as well as the introduction of algorithms for the estimation of produced and consumed energy.

Acknowledgements

This work has been partially supported by the European Community's Seventh Framework Programme as part of the ICT CoSSMic project (FP7-ICT-608806)

References

[1] D. Giusto, A. Lera, G. Morabito, and L. Atzori, *The Internet of Things*. Springer, 2010.

[2] K. Su, J. Li, and H. Fu, "Smart city and the applications," in *Proc. Int. Conf. Elec. Commun. Contr. ICECC 2011*, Ningbo, China, 2011, IEEE, pp. 1028–1031.

[3] F. Bellifemine, A. Poggi, and G. Rimassa, "JADE–A FIPA-compliant agent framework," in *Proc. Pract. Appl. Intell. Agents Multi-Agents PAAM 1999*, London, 1999, vol. 99, no. 97–108.

[4] "FIPA" [Online]. Available: http://www.fipa.org

[5] B. Snyder, D. Bosnanac, and R. Davies, *ActiveMQ in Action*. Shelter Isl., USA: Manning, 2011.

[6] A. Videla and J. J. Williams, *RabbitMQ in Action*. Shelter Isl., USA: Manning, 2012.

[7] A. Rogers, S. D. Ramchurn, and N. R. Jennings, "Delivering the smart grid: Challenges for autonomous agents and multi-agent systems research", in *Proc. 26th AAAI Conf. Artif. Intell. AAAI-12*, Toronto, Canada, 2012, pp. 2166–2172.

[8] I. Praça, C. Ramos, Z. Vale, and M. Cordeiro, "Intelligent agents for negotiation and game-based decision support in electricity markets", *Engin. Intell. Syst. Elec. Engin. Commun*., vol. 13, no. 2, p. 147, 2005.

[9] T. A. Rodden, J. E. Fischer, N. Pantidi, K. Bachour, and S. Moran, "At home with agents: exploring attitudes towards future smart energy infrastructures", in Proc. SIGCHI Conf. Human Fact. Comput. Syst., Paris, France, 2013, pp. 1173–1182.

[10] Y. Jia-hai, Y. Shun-kun, and H. Zhao-guang, "A multi-agent trading platform for electricity contract market", in *Proc. 7th Int. Power Engin. Conf. IPEC 2005*. Singapore, 2005, pp. 1024–1029.

[11] D. Whitehead, "The El Farol bar problem revisited: Reinforcement learning in a potential game", *ESE Discussion Papers*, no. 186, Edinburgh School of Economics, 2008.

[12] N. C. Truong, L. Tran-Thanh, E. Costanza, and D. S. Ramchurn, "Activity prediction for agent-based home energy management", in *Proc. 4th Int. Worksh. Agent Technol. for Energy Syst. ATES 2013*, Saint Paul, Minnesota, USA, 2013.

[13] N. Capodieci, E. F. Alsina, and G. Cabri, "A context-aware agent-based approach for deregulated energy market", in *Proc. 21st IEEE Int. Worksh. Enabling Technol. Infrastruc. Collabor. Enterpr. WETICE 2012*, Toulouse, France, 2012, pp. 16–21.

[14] R. Aversa, B. Martino, M. Ficco, and S. Venticinque, "Simulation and support of critical activities by mobile agents in pervasive and ubiquitous scenarios," in *Proc. 10th Int. Symp. Parall. Distrib. Process. Appl. ISPA 2012*, Madrid, Spain, 2012, pp. 815–822.

[15] N. Capodieci, G. Cabri, G. A. Pagani, and M. Aiello, "Adaptive game-based agent negotiation in deregulated energy markets," in *Proc. IEEE Int. Conf. Collabor. Technol. Syst. CTS 2012*, Denver, CO, USA, 2012, pp. 300–307.

[16] A. Amato *et al*., "Software agents for collaborating smart solar-powered micro-grids", in *Smart Organizations and Smart Artifacts*, L. Caporarello, B. Di Martino, and M. Martinez, Eds. *Lecture Notes in Information Systems and Organisation*, vol. 7, pp. 125–133, Springer, 2014.

[17] S. Venticinque, L. Tasquier, and B. Di Martino, "A restfull interface for scalable agents based cloud services", *Int. J. of Ad Hoc and Ubiquitous Comput.*, vol. 16, no. 4, pp. 219–231, 2014.

[18] L. Tasquier, M. Scialdone, R. Aversa, and S. Venticinque, "Agent based negotiation of decentralized energy production", in *Intelligent Distributed Computing VIII*, D. Camacho, L. Braubach, S. Venticinque, and C. Badica, Eds. *Studies in Computational Intelligence*, vol. 570, pp. 59–67. Springer, 2015.

[19] S. Venticinque, L. Tasquier, and B. Di Martino, "Agents based cloud computing interface for resource provisioning and management", in *Proc. 6th IEEE Int. Conf.Complex, Intell. Softw. Intens. Syst. CISIS 2012*, Palermo, Italy, 2012, pp. 249–256.

[20] R. Aversa, L. Tasquier, and S. Venticinque, "Cloud agency: A guide through the clouds," *Mondo Digitale*, vol. 13, no. 49, 2014.

Luca Tasquier is Ph.D. student in Computer and Electronic Engineering at Department of Industrial and Information Engineering of the Second University of Naples. He received his Master degree in Computer Engineering in 2011. He is involved in research activities dealing with parallel and cloud computing and mobile/intelligent agents for distributed systems. He participated to research projects supported by international and national organizations.

E-mail: luca.tasquier@unina2.it
Dipartimento di Ingegneria Industriale e dell'Informazione
Second University of Naples
Via Roma, 29
81031 Aversa, Italy

Rocco Aversa graduated in Electronic Engineering at University of Naples in 1989 and received his Ph.D. in Computer Science in 1994. He is Associate Professor in Computer Science at the Department of Information Engineering of the Second University of Naples. His research interests are in the area of parallel and distributed systems. The research themes include: the use of the mobile agents paradigm in the distributed computing, the design of simulation tools for performance analysis of parallel applications running on heterogeneous computing architectures, the project and the development of innovative middleware software to enhance the grid and cloud computing platforms. He is associate editor of International Journal of Web Science (IJWSM Inderscience Publishers). Dr. Aversa participated to various research projects supported by national organizations (MURST, CNR, ASI) and by EC in collaboration with foreign academic institutions and industrial partners.

E-mail: rocco.aversa@unina2.it
Dipartimento di Ingegneria Industriale e dell'Informazione
Second University of Naples
Via Roma, 29
81031 Aversa, Italy

Paper

Data and Task Scheduling in Distributed Computing Environments

Magdalena Szmajduch

Department of Computer Science, Cracow University of Technology, Cracow, Poland

Abstract—Data-aware scheduling in today's large-scale heterogeneous environments has become a major research and engineering issue. Data Grids (DGs), Data Clouds (DCs) and Data Centers are designed for supporting the processing and analysis of massive data, which can be generated by distributed users, devices and computing centers. Data scheduling must be considered jointly with the application scheduling process. It generates a wide family of global optimization problems with the new scheduling criteria including data transmission time, data access and processing times, reliability of the data servers, security in the data processing and data access processes. In this paper, a new version of the Expected Time to Compute Matrix (ETC Matrix) model is defined for independent batch scheduling in physical network in DG and DC environments. In this model, the completion times of the computing nodes are estimated based on the standard ETC Matrix and data transmission times. The proposed model has been empirically evaluated on the static grid scheduling benchmark by using the simple genetic-based schedulers. A simple comparison of the achieved results for two basic scheduling metrics, namely makespan and average flowtime, with the results generated in the case of ignoring the data scheduling phase show the significant impact of the data processing model on the schedule execution times.

Keywords—data cloud, data grid, data processing, data scheduling, ETC Matrix.

1. Introduction

In the recent decade, we witness an explosive growth in the volume, velocity, and variety of the data available on the Internet. Pethabythes of data were created on a daily basis. The data is generated by the highly distributed users and various types sources like the mobile devices, sensors, individual archives, social networks, Internet of Things devices, enterprise, cameras, software logs, etc. Such data explosions has led to one of the most challenging research issues of the current Information and Communication Technology (ICT) era: how to effectively and optimally manage and schedule such large data for unlocking information?

Scheduling problems in the distributed computing environments are mainly defined based on the task processing CPU-related criteria, namely makespan, flowtime, resource utilization, energy consumption and many others [1]. In such cases, all data-related criteria, like the data transmission time, data access rights, data availability (replication) and security in data access issues are mostly ignored. Usually it is assumed, that transmission is very fast, data access rights are granted, due to the single domain of LANs and clusters (even if the whole infrastructure is highly distributed), so there is no need for special data access management. Obviously, the situation is very different in current large scale setting, where data sources needed for task completion can be located at different sites under different administrative domains.

Data-aware scheduling has been explored already in many research in cluster, grid and recently cloud computing [2], [3]. Most of the current efforts are focused on the data processing optimization, storage (loads of the data servers) in the data centers or scheduling of data transmission and data location [4] for efficient resource/storage utilization or energy-effective scheduling in large-scale data centers [5], [6]. A recent example is that of GridBatch [7] for large scale data-intensive problems on cloud infrastructures. However, the large amount of data to be efficiently processed remains a real research challenge, especially in the recent Big Data era. One of the key issues contributing to the massive processing efficiency is the scheduling with data transmission requirements.

In this paper, a new data-aware Expected Time to Compute Matrix (ETC Matrix) scheduling model is defined for computational grids and physical layers of the cloud systems, which takes into account new criteria such as data transmission and decoupling of data from processing [8]–[10]. The main aim of this work is to integrate the above criteria into a multi-objective optimization model in a similar way that it has been provided for computational grid scheduling with ETC Matrix [11]. However, the grid schedulers in presented model must take into account the features of both Computational Grid (CG) and Data Grid (DG) in order to achieve desired performance of grid-enabled applications [12], [13]. Therefore, in this paper a general data-aware independent batch task scheduling problem is considered.

The remainder of the paper is structured as follows. The data-aware ECT Matix model for independent batch scheduling and main scheduling criteria are defined in Section 2. The empirical results are analyzed in Section 3. The paper is summarized in Section 4.

2. Data-aware Expected Time to Compute (ETC) Matrix Model

Let's consider a simple batch scheduling problem in computational physical infrastructure (big distributed cluster, grid or physical layer of the cloud system), where the tasks

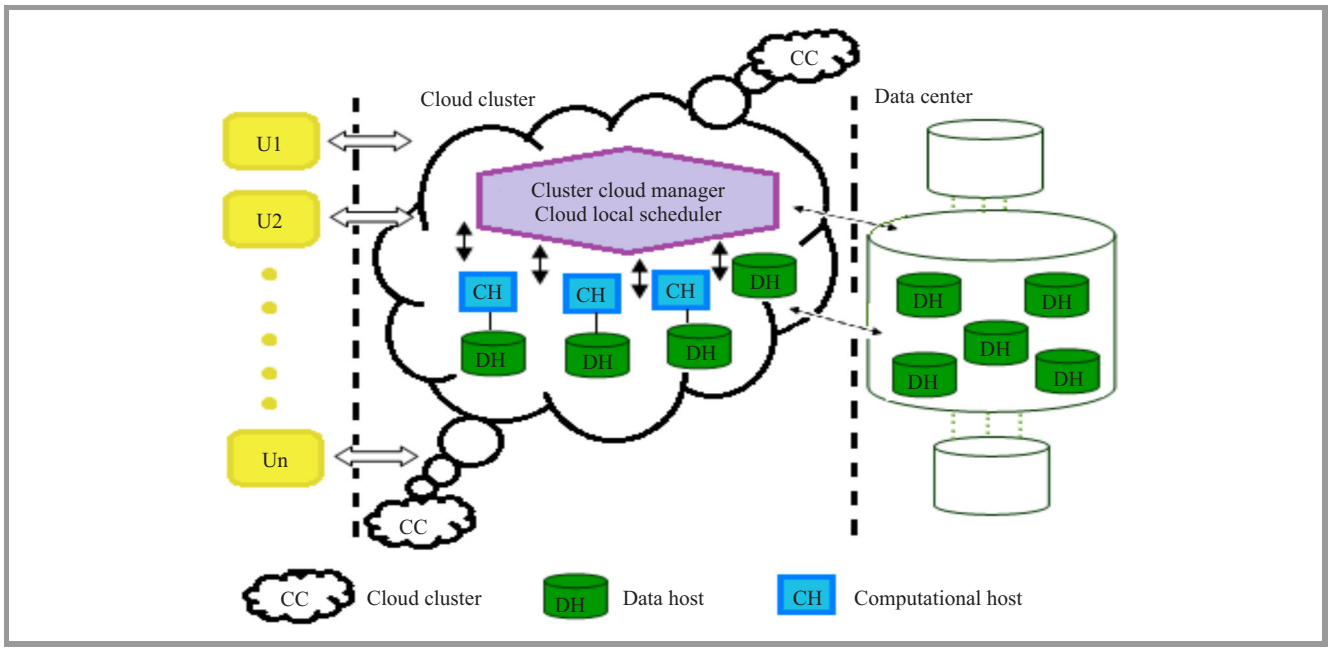


Fig. 1. Data-aware meta-task grid scheduling problem.

are processed independently and require multiple data sets from different heterogeneous data hosts. These data sets may be replicated at various locations and can be transferred to the computational grid through the networks of various capabilities. A possible variant of this scenario is presented in Fig. 1.

The components of the whole system, task and data structures in such scenario can be defined as follows:

- a batch of tasks $N = \{t_1, \ldots, t_n\}$ is defined as a meta-task structure,
- a set of computing grid nodes $M = \{m_1, \ldots, m_m\}$ available for a given batch;
- a set of data-files $F = \{f_1, \ldots, f_r\}$ needed for the batch execution,
- a set of data-hosts $D = \{dh_1, \ldots, dh_s\}$ dedicated for the data storage purposes, having the necessary data services capabilities.

The computational load of the meta-task is defined as a *tasks workload vector* $WL_{batch} = [wl_1, \ldots, wl_n]$, where wl_j is the estimated computational load of task t_j (expressed in millions of instructions (MI). Each task t_j requires for its execution the following set of data files $F_j = \{f_{(1,j)}, \ldots, f_{(r,j)}\}$ ($F_j \subseteq F_{batch}$), which is replicated and allocated at the following data servers DH_j.[1]

The computing capacity of computational servers available for a given batch is defined by a *computing capacity vector* $CC_{batch} = [cc_1, \ldots, cc_m]$, where cc_i denotes the computing capacity of the server i expressed in million instructions per second (MIPS). The estimation of the prior load of each machine from M_{batch} can be represented by a *ready times vector* $ready\_times_{(batch)} = [ready_1, \ldots, ready_m]$.

An Expected Time to Compute (ETC) matrix model [11] is used for estimation of the completion times of tasks assigned to a given computational server. Usually, the elements of the ETC matrix can be computed as the ratio of the coordinates of WL and CC vectors, namely:

$$ETC[i][j] = \frac{wl_j}{cc_i}. \tag{1}$$

The values of $ETC[j][i]$ for each pair machine m_i and task t_j in Eq. (1) depend mainly on the processing speeds of the machines, but need also express the heterogeneity of tasks and resources in the system. Therefore, in this approach the Gaussian distribution for generating the coordinates of both WL and CC vectors is used. Additionally, in data-aware scheduling, there is a need to estimate the data transfer time. For each data file $f_{cj} \in F$ ($c \in \{1, \ldots, r\}$) necessary for the execution of the task t_j, the time required to transfer this file from the data host $dh_d \in D$ to the server m_i is denoted $TT_{ij}[c][d]$ and can be calculated in the following way:

$$TT_{ij}[c][d] = RES[c][d] + \frac{Size[f_{cj}]}{B[dh_d, i]}, \tag{2}$$

where $RES[c][d]$ is a response time of the data server dh_d and is defined as a difference between the request time to dh_d and the time when the first byte of the data file f_c is received at the computational server m_i for computing the task t_j (note, that the values of i and j are fixed here). The $Size[f_c, j]$ denotes the size (in Mbits) of the data file f_c needed for execution of the task t_j, and by $B[dh_d, i]$ the

[1] DH_j is a subset of DH. Each file $f_{(p,j)} \in F_j$ ($p \in \{1, \ldots, r\}$) is replicated on the servers from DH_j. It is assumed that each data host can serve multiple data files at a time and data replication is a priori defined as a separate replication process.

bandwidth of logical link (in Mbits/time_unit) between dh_d and m_i.
$RES[c][d]$ are the elements of the Data Response Times Matrix $RES_{s\times r}$. In presented approach, the Gamma distribution [14] for generating those data response times is used. This method is widely used for estimation of the data transfer times [15]. It is similar to the Coefficient-of-Variation (CVB) [16] method used for generating the stochastic matrices with highly distributed two-dimensional random variables. It may be used also for generation ETC matrices [1]. The key parameters for this method are defined as follows:

- the cumulative estimated response times of all data servers while transferring an "average" data file, res_{ave},
- the variance in the response times of data server, $svar_{dh}$,
- the variance in the heterogeneity of data files, $rvar_f$.

The parameters res_{ave} and $svar_{dh}$ are used for estimating the response times $RES[\hat{c}][d]$ of the data servers for the file $f_{\hat{c}}$ with the "average" data server speed in the systems. The times $RES[\hat{c}][d]$ are generated by using the gamma distribution with the shape and scale parameters denoted by α_s and β_s respectively. That is:

$$RES[\hat{c}][d] = Gamma(\alpha_s, \beta_s), \tag{3}$$

where:

$$\alpha_s = \frac{1}{svar_{dh}^2}, \tag{4}$$

$$\beta_s = \frac{res_{ave}}{\alpha_s}. \tag{5}$$

The generated vector of $RES[\hat{c}][d]$ parameters ($dh_d \in D$) defines one row (indexed by $\hat{c}$) of the RES matrix. Each element of this row is then used for generating one column of the RES matrix, that is:

$$RES[c][d] = Gamma(\alpha_r, \beta_r), \tag{6}$$

where:

$$\alpha_r = \frac{1}{rvar_f^2}, \tag{7}$$

$$\beta_r = \frac{RES[\hat{c}][d]}{\alpha_r}. \tag{8}$$

and $f_c \in F$, $c \neq \hat{c}$.

The resources completion times are the main scheduling parameters in the ETC matrix model. It is denoted by $completion[j][i]$ estimated completion time for the task t_j on machine m_i. It is defined as the wall-clock time taken for the task from its submission till completion. In data-aware scheduling, it depends on computing and transmission times specified in Eqs. (1) and (2). The impact of the data transfer time on the task completion time depends on the mode, in which the data files are processed by the task. Figure 2 presents two such scenarios (see also [17]).

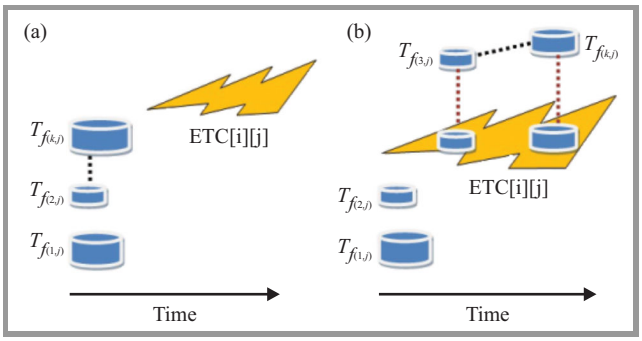


Fig. 2. Two variants of task completion times estimation assigned to the machine m_i with k data files needed for the task execution.

In the "a" scenario, data files needed for the execution of task t_j are transferred to the computational server before the calculation of all tasks assigned to this server, including task t_j. The number of simultaneous data transfers determines the bandwidth available for each transfer. The completion time of the task t_j on machine m_i in this case is defined as follows:

$$completion_a[i][j] = \max_{f_{cj}\in F; dh_d \in D} TT_{ij}[[c][d] + ETC[i][j]. \tag{9}$$

In the "b" scenario, some of the data files are transferred as in scenario "a", but the major data needed for the execution of each task assigned to the server m_i (also task t_j) is transferred during the execution of the tasks. In this case, the transfer times of the streamed data files are masked by the computation times of the tasks. The completion time of the task t_j on machine m_i in this scenario is defined in the following way:

$$completion_b[i][j] = \max_{f_{cj}\in \widehat{F}_j} TT_{ij}[c][d] + \sum_{f_{lj}\in [F\setminus \widehat{F}_j]} (TT_{ij}[l][d] + ETC[i][j]) \tag{10}$$

where $\widehat{F}_j$ denotes a set of data files which are transferred prior the execution of the task t_j and in fact all tasks assigned to this server.
In this paper the data hosts as the data storage centers are considered, which are separated from the computing resources.

2.1. Scheduling Criteria

A general data-aware batch scheduling process is realized in the following steps:

- get the information on available resources,
- get the information on pending tasks,
- get the information on data hosts where data files for tasks completion are required,

- prepare a batch of tasks and compute a schedule for that batch on available machines and data hosts,
- allocate tasks,
- monitor (failed tasks are re-scheduled).

These steps can be graphically represented as in Fig. 3.

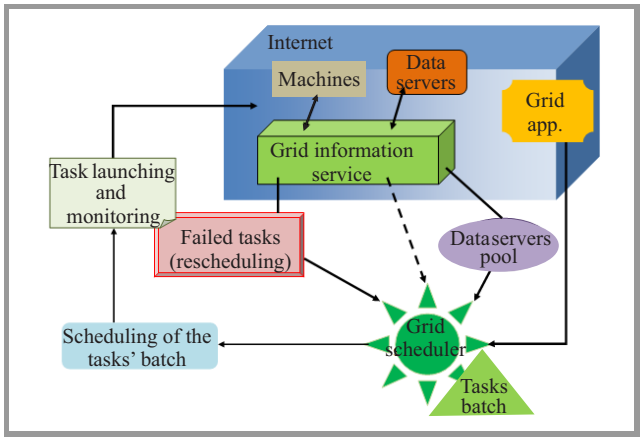


Fig. 3. Phases of the data-aware batch scheduler.

The main objectives in data-aware scheduling are similar to the objectives formulated for conventional scheduling in distributed computational systems without data files [1] and include minimization of completion time, makespan and average flowtime, namely:

- Minimizing completion time of the task batch defined in the following way:

$$completion_{batch} = \sum_{t_j \in N_{batch}; m_i \in M_{batch}} completion[i][j], \quad (11)$$

where $completion[i][j]$ is defined as in Eq. 9 or Eq. 10 depending on considered data transfer scenario;

- Minimizing makespan C_{max}:

$$C_{max} = \max_{m_i \in M_{batch}} completion[i], \quad (12)$$

where $completion[i]$ is computed as the sum of completion times of tasks assigned to machine m_i calculated by using Eq. 9 or Eq. 10;

- Minimizing average flowtime $\tilde{F}$. A flowtime for a machine m_i can be calculated as a workflow of the tasks sequence on a given machine m_i, that is to say:

$$F[i] = completion[i]. \quad (13)$$

The cumulative flowtime in the whole system is defined as the sum of $F[i]$ parameters, that is:

$$F = \sum_{i \in M} F[i]. \quad (14)$$

Finally, the scheduling objective is to minimize the average flowtime $\tilde{F}$ for one machine defined as follows:

$$\tilde{F} = \frac{F}{m}. \quad (15)$$

In the above equations the ETC matrix model is used which is very useful for the formal definition of all main scheduling criteria. The $completion[i]$ parameters are the coordinates of the completion vector $completion = [completion[1], \ldots, completion[m]]^T$. The extended list of the scheduling criteria defined in terms of completion times and by using the ETC matrix model can be found in [1].

3. Experiments

The main aim of the experiments is to illustrate the impact of the data transfer times on the completion times of the physical resources in the system. The values of makespan and average flowtime calculated by using Eqs. 12 and 15 are compared with the case of conventional scheduling, where data transfer times are ignored. In such a case it is assumed that all necessary data is stored at computational nodes and ready for use, which is unrealistic. For the analysis both data transfer scenarios specified in Section 2, namely scenario "a" and scenario "b" are considered. Therefore, the completion times in Eq. 12 are estimated by using Eq. 9 in the first scenario, and Eq. 10 in the second scenario.

The experiments were provided with simple genetic-based scheduler defined in Subsection 3.2, which has been used already as grid batch scheduler by many researchers in the domain (see [18], [19] and [20]). There are many other genetic grid and cloud schedulers that are more effective in the optimization of the makespan and flowtime criteria [1]. However, such effectiveness is not the main aim of this analysis. All those schedulers are also quite complex methods from the implementation and scaling perspectives. Therefore, a simple scheduler was used to show, how much the data transfer may delay the execution of schedules.

3.1. Data Grid Simulator

For the experiments the Sim-G-Batch simulator defined in [1] is used. The basic set of the input data for the simulator includes:

- the workload vector of tasks,
- the computing capacity vector of machines,
- the vector of prior loads of machines, and
- the ETC matrix of estimated execution times of tasks on machines.

The Sim-G-Batch simulator is highly parametrized to reflect the various realistic scheduling scenarios. In this

paper, the author limited the experiments to the static batch scheduling benchmarks. Fig. 4 presents the selected modules of Sim-G-Batch, which are active in performed experiments.

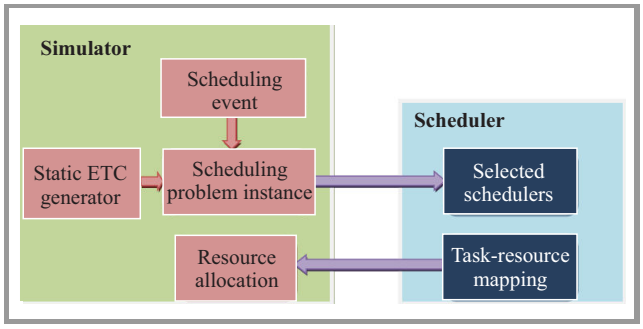


Fig. 4. Selected components of Sim-G-Batch simulator for the experiments on static benchmarks.

The benchmark for small static grid was generated by the *Static ETC Generator* module of the simulator. The instances in this benchmark are classified into 12 types of ETC matrix, according to task heterogeneity, machine heterogeneity and consistency of computing. These instances are labeled by the following parameters [1]:

$$Gauss\_xx\_yyzz.0 \tag{16}$$

where:

- *Gauss* is the Gaussian distributions used in generating the WL and CC vectors,
- xx denotes the type of consistency of ETC matrix ($\hat{c}$ – consistent, $\hat{\hat{i}}$ – inconsistent, and $\hat{s}$ – semi-consistent),
- yy indicates the heterogeneity of tasks (hi – high heterogeneity, and lo – low heterogeneity),
- zz expresses the heterogeneity of the resources (hi – high, and lo – low).

The ETC matrix is consistent if for each pair of the resources m_i and $m_{\hat{i}}$ the following condition is satisfied: if the completion time of some task t_j is shorter at resource m_i than at resource $m_{\hat{i}}$, then all tasks can be executed (and finalized) faster at m_i than at $m_{\hat{i}}$. The inconsistency of the matrix ETC means that there no consistency relation among resources. Semi-consistent ETC matrices are inconsistent matrices having a consistent sub-matrix.
The following probability distributions have been used in the experiments: $N(1000;175)$ for resources and $N(250000000;43750000)$ for tasks, where $N(\alpha,\sigma)$ denotes the Gaussian distribution with mean α and standard deviation σ. The computing cluster network is composed of 64 nodes (machines) and there are 1024 tasks submitted for scheduling. In addition, 32 data servers and 2048 data files for a given batch is assumed. The data hosts response times are generated by using the Gamma distribution according to the description in Section 2 with the following parameters $res_{ave} = 10$, and $0.1 \leq svar_{dh}$, $rvar_f \leq 0.35$. The sizes of data files and the bandwidth are generated by the uniform distributions defined for the following intervals $[2;1600]$ and $[10;100]$ respectively.

3.2. Genetic-based Scheduler

Genetic-based meta-heuristics have shown great potential to solve multi-criteria grid or cloud scheduling problems by trading-off various preferences and goals of the system users and managers [21], [22]. Simple single-population genetic schedulers can be promoted as the effective methods for solving small-scale static scheduling problems. In the experiments a simple $(\mu+\lambda)$-like evolutionary scheduler is used similar to those used for solving classical combinatorial optimization problems [23]. The general schema of this scheduler is presented in Fig. 5.
In the implementation of the scheduler two schedules' representations are used, namely direct representation and permutation-based encoding. In the direct representation, each schedule is defined as the schedule vector $x = [x_1,\ldots,x_n]^T$, where $x_i \in \{1,\ldots,m\}$ are the labels of the computational resources, to which the particular tasks labeled by $1,\ldots,n$ are assigned. In permutation-based representation, for each resource a sequence of tasks assigned to that resource is defined. The tasks in the sequence are increasingly sorted with respect to their completion times. In this representation, some additional information about the numbers of tasks assigned to each machine is required. In this work the direct representation for the encoding of the individuals in the base populations denoted by P^t and P^{t+1} in Fig. 5 is used. The permutation-based representation is necessary for the implementation of the specialized genetic operators. Based on the results of tuning process provided in [18], [20] and [21], the optimal configuration of genetic operators for considered scheduler is defined as follows:

- selection – Linear Ranking,
- crossover – Cycle Crossover,
- mutation – Rebalancing,
- replacement – Steady State.

All those genetic operators are commonly used in solving the large-scale combinatorial problems [23]. The main idea of the Cycle Crossover (CX) is identification of the cycle of alleles (positions). The existing cycles (of tasks) are kept unchanged. The remaining fragments in the parental strings are exchanged, and the resulting permutation strings are repaired if some task labels are duplicated. In rebalancing mutation, first the most overloaded machine m_i is selected. Then two tasks t_j and $t_{\hat{j}}$ are identified as follows: $t_{\hat{j}}$ is assigned to another machine $m_{\hat{i}}$,t_j is assigned to m_i and $ETC[\hat{i}][\hat{j}] \leq ETC[i][j]$. Then the assignments for tasks t_j and $t_{\hat{j}}$ are interchanged. In Steady State replacement

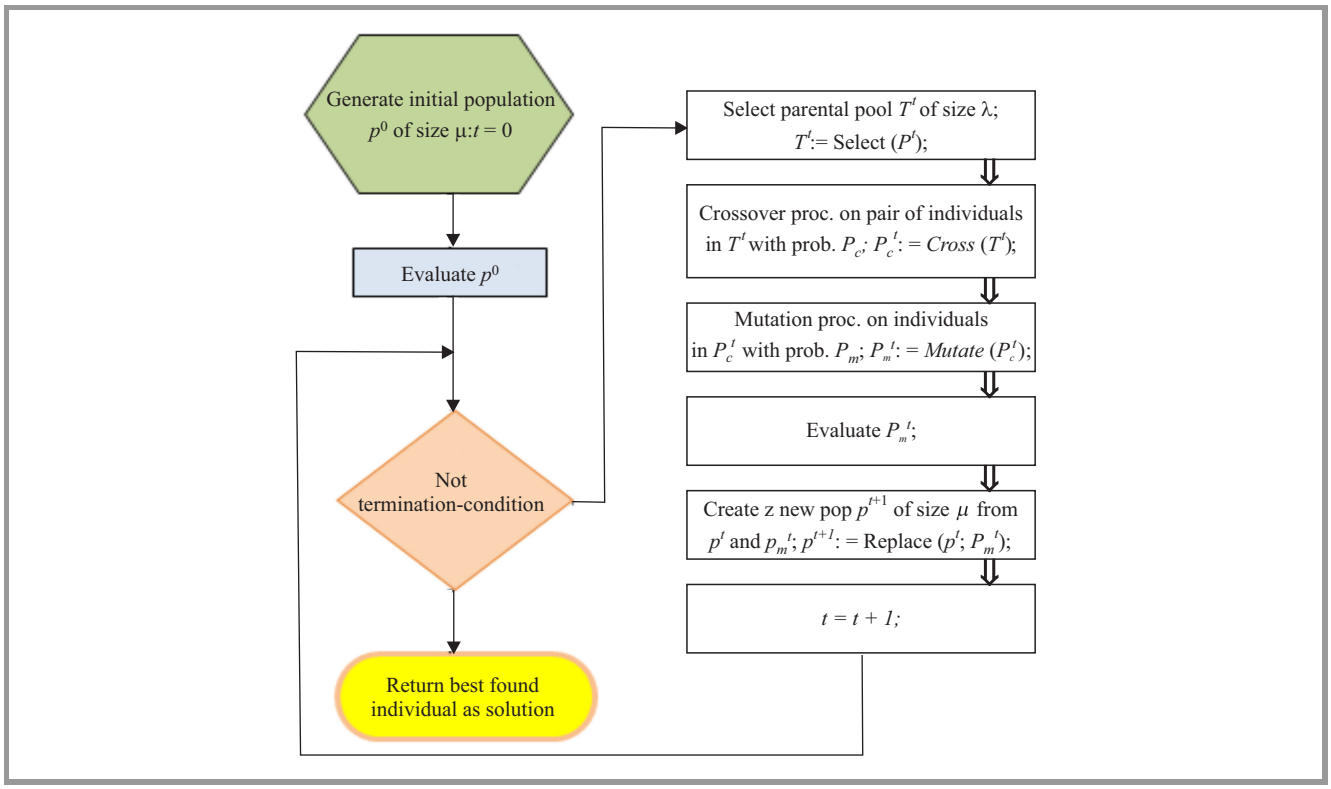


Fig. 5. General template of the GA-scheduler implementation.

method, the set of the highest quality offsprings replaces the similar set (of the same cardinality) of the solutions of the worst quality in the old base population.

Table 1
Key parameters of the GA-scheduler
(n – the number of tasks in the batch)

Parameter	Value
μ	$4 \cdot (\log_2 n - 1)$
λ	$\mu/3$
mut_prob	0.15
cross_prob	0.9
nb_of_epochs	$20 \cdot n$
max_time_to_spend	25 s

The values of the control parameters for the genetic scheduler are presented in Table 1. The number of individuals in base populations shown as P^t and P^{t+1} in Fig. 5 is denoted by μ, λ is the number of individuals in offspring populations T^t, P_c^t and P_m^t. The parameters *cross_prob*, *mut_prob* are used for the notation of of the crossover and mutation probabilities. The *nb_of_epochs* denotes the maximal number of main loop executions of the algorithm. Each loop execution is interpreted as genetic epoch. The maximal number of such epochs is defined as the main global stopping criterion for the scheduler. However, if the execution of those epochs will take much time, the algorithm is stopped after 25 s (*max_time_to_spend*).

3.2.1. Results

Tables 2 and 3 present the average values of makespan and average flowtime achieved in the scenarios "a" and "b" (see Section 2) and No data transfer case. Each experiment has been executed 30 times under the same configuration of all input parameters and data for simulator and scheduler. Both tables present the results averaged over 30 independent runs of the simulator with [$\pm s.d.$] $s.d$-standard deviation values.

Both makespan and average flowtime are expressed in arbitrary (but not concrete) time units.

In makespan optimization, scenario "b" is the case, where most of the achieved results are better than for the prior load of all data files before the task execution (scenario "a"). In the case of average flowtime optimization, the impact of the consistency of ETC matrix on the mode of the data transfer is even better illustrated. In all cases for consistent and semi-consistent matrices and for inconsistent matrices with high heterogeneity of computing resources, it is better to request just necessary data files during the computation (scenario "b"). The differences in the flowtime values in scenario "a" and scenario "b" are more significant than in the makespan case. However, in both makespan and flowtime optimizations, it is observed that the flowtime values are much higher in the case of additional data transfer times, than in the "data transfer-free" scheduling. In the case of inconsistent and semi-consistent ETC matrices, it is almost doubled.

Table 2
Makespan values in three scheduling scenarios

Instance	Scenario "a"	Scenario "b"	No data transfer
Gauss_c_hihi	10020355.256 [±801234.852]	**9621178.557 [±998911.259]**	7506387.215 [±631202.153]
Gauss_c_hilo	226250.310 [±19936.993]	**213490.536 [±19343.184]**	139974.423 [±10846.362]
Gauss_c_lohi	**459987.880 [±19323.273]**	468466.775 [±22765.627]	238839.338 [±18892.634]
Gauss_c_lolo	**6761.231 [±770.132]**	6926.864 [±240.019]	5109.783 [±258.635]
Gauss_i_hihi	6093651.564 [±702187.019]	**5866694.694 [±1191799.837]**	3069945.734 [±877534.287]
Gauss_i_hilo	146705.432 [±4451.987]	**145813.231 [±4062.978]**	75588.928 [±3184.872]
Gauss_i_lohi	198611.123 [±20873.994]	**187170.435 [±19351.412]**	109343.652 [±25636.425]
Gauss_i_lolo	5194.763 [±122.543]	**5117.546 [±138.321]**	2616.643 [±156.792]
Gauss_s_hihi	8085209.000 [±578839.375]	**7961402.628 [±663325.239]**	4254421.785 [±853673.523]
Gauss_s_hilo	186281.400 [±14746.582]	**167445.544 [±10831.231]**	99009.537 [±8763.471]
Gauss_s_lohi	**215692.530 [±64353.500]**	220844.573 [±53473.637]	126822.639 [±98723.537]
Gauss_s_lolo	6856.982 [±453.321]	**6554.654 [±643.308]**	3498.623 [±764.364]

4. Conclusions and Research Directions

In this paper the new version of ETC Matrix model for batch scheduling in the physical clusters was defined, where separate computing and data servers are located. In this model, the completion times of all tasks assigned to the computing nodes of the network have included the data transmission times. Two data transmission scenarios were considered with prior load of all files necessary for the execution of assigned tasks, and with the ad-hoc delivery of just requested (necessary) data files during the task execution. The results of the performed experiments show that omitting the data transfer phase in the scheduling process may lead to the bad estimations of the scheduling times, and more general scheduling costs.

The performed analysis in its early stage. The author plans to extend it to the virtual resources and databases and the extended cloud infrastructures, where the mobile devices (smartphones, tablets, laptops, etc.) are considered as the computational nodes of the physical cloud layer and can additionally store and generate the data. This will allow to validate proposed model in much more realistic cloud scheduling scenarios, but also will increase the complexity of the scheduling problem.

References

[1] J. Kołodziej, *Evolutionary Hierarchical Multi-Criteria Metaheuristics for Scheduling in Large-Scale Grid Systems. Studies in Computational Intelligence Serie*, vol. 419. Berlin-Heidelberg: Springer, 2012.

[2] H. Casanova, G. Obertelli, F. Berman, and R. Wolski, "The AppLeS parameter sweep template: user-level middleware for the grid", in *Proc. 2000 ACM/IEEE Conf. on Supercomputing SC 2000)*, Dallas, TX, USA, 2000.

[3] R. Buyya, M. Murshed, D. Abramson, and S. Venugopal, "Scheduling parameter sweep applications on global Grids: a deadline and budget constrained cost-time optimization algorithm", *Softw. Pract. Exper.*, vol. 35, no. 5, pp. 491–512, 2005.

[4] T. Kosar and M. Balman, "A new paradigm: Data-aware scheduling in grid computing", *Future Gener. Comp. Syst.*, vol. 25, no. 4, pp. 406–413, 2009.

[5] J. Kołodziej, S. U. Khan, and F. Xhafa, "Genetic algorithms for energy-aware scheduling in computational grids", in *Proc. 6th IEEE Int. Conf. P2P, Parallel, Grid, Cloud, and Internet Comput. 3PGCIC*, Barcelona, Spain, 2011, pp. 17–24.

[6] G. L. Valentini *et al.*, "An overview of energy efficiency techniques in cluster computing systems", *Cluster Comput.*, vol. 16, no. 1, pp. 3–15, 2011.

[7] H. Liu and D. Orban, "GridBatch: Cloud Computing for Large-Scale Data-Intensive Batch Applications", in *Proc. 8th IEEE Int. Symp. Cluster Comput. and the Grid CCGRID 2008*, Lyon, France, 2008, pp. 295–305.

[8] J. Kołodziej and F. Xhafa, "A game-theoretic and hybrid genetic meta-heuristic model for security-assured scheduling of independent jobs in computational grids", in *Proc. Int. Conf. Complex, Intell. Softw. Inten. Syst. CISIS 2010*, Krakow, Poland, 2010, pp. 93–100.

Table 3
Flowtime values in three scheduling scenarios

Instance	Scenario "a"	Scenario "b"	No data transfer
Gauss_c_hihi	1865377511.523 [±62551800.572]	**1739118543.763 [±108789000.698]**	1039888902.5391 [±87276600.974]
Gauss_c_hilo	38856381.645 [±1855790.927]	**37530920.723 [±1572700.673]**	26758471.974 [±1761150.029]
Gauss_c_lohi	45736995.532 [±1662420.635]	**44536681.673 [±4060500.216]**	33480185.582 [±4362160.982]
Gauss_c_lolo	130462.627 [±51414.523]	**1233817.453 [±56050.981]**	891295.864 [±34862.735]
Gauss_i_hihi	629477886.653 [±121534968.473]	**578364926.537 [±2075608399.845]**	349268315.516 [±147994960.873]
Gauss_i_hilo	23654208.787 [±894854.731]	**23615230.173 [±749330.642]**	12427872.618 [±680981.333]
Gauss_i_lohi	**23344908.394 [±2909746.766]**	23417596.793 [±3324080.433]	12718274.271 [±4395729.934]
Gauss_i_lolo	**826185.831 [±25385.445]**	829731.985 [±34978.732]	450123.843 [±32745.674]
Gauss_s_hihi	1048266515.861 [±103674264.922]	**994973664.431 [±90143000.322]**	522894137.524 [±107532000.119]
Gauss_s_hilo	29959243.952 [±1173072.427]	**28415261.227 [±1556320.435]**	16871684.228 [±2152640.536]
Gauss_s_lohi	22655131.553 [±4981350.195]	**21648611.228 [±6657510.587]**	14923174.777 [±7907100.555]
Gauss_s_lolo	1005375.388 [±66981.229]	**998332.695 [±67459.762]**	582565.111 [±44452.203]

[9] L. Wang and S. U. Khan, "Review of performance metrics for green data centers: a taxonomy study", *J. Supercomput.*, vol. 63, no. 3, pp. 639–656, 2013.

[10] S. Zeadally, S. U. Khan, and N. Chilamkurti, "Energy-efficient networking: past, present, and future", *J. Supercomput.*, vol. 62, no. 3, pp. 1093–1118, 2012.

[11] S. Ali, H. J. Siegel, M. Maheswaran, and D. Hensgen, "Task execution time modeling for heterogeneous computing systems", in *Proc. 9th Heterogen. Comput. Worksh. HCW 2000*, Cancun, Mexico, 2000, pp. 185–199.

[12] J. Kołodziej and F. Xhafa, "Meeting security and user behaviour requirements in grid scheduling", *Simul. Model. Pract. Theory*, vol. 19, no. 1, pp. 213–226, 2011.

[13] J. Kołodziej and F. Xhafa, "Integration of task abortion and security requirements in GA-based meta-heuristics for independent batch grid scheduling", *Comp. Mathem. Appl.*, vol. 63, no. 2, pp. 350–364, 2011.

[14] L. L. Lapin, *Probability and Statistics for Modern Engineering*, 2nd ed. Long Grove, USA: Waveland Pr. Inc., 1998.

[15] A. Deshpande, Z. G. Ives, and V. Raman, "Adaptive query processing", *Foundation and Trends in Databases*, vol. 1, no. 1, pp. 1–140, 2007.

[16] S. Ali, H. J. Siegel, M. Maheswaran, and D. Hensgen, "Representing task and machine heterogeneities for heterogeneous computing systems", *Tamkang J. Sci. Engin.*, vol. 3, no. 3, pp. 195–207, 2000.

[17] S. Venugopal and R. Buyya, "An SCP-based heuristic approach for scheduling distributed data-intensive applications on global grids", *J. Parallel Distrib. Comp.*, vol. 68, pp. 471–487, 2008.

[18] F. Xhafa, L. Barolli, and A. Durresi, "Batch mode schedulers for grid systems", *Int. J. Web and Grid Serv.*, vol. 3, no. 1, pp. 19–37, 2007.

[19] F. Pinel, J. E. Pecero, P. Bouvry, and S. U. Khan, "A two-phase heuristic for the scheduling of independent tasks on computational grids", in *Proc. of ACM/IEEE/IFIP Int. Conf. High Perform. Comput. Simul. HPCS 2011*, Istanbul, Turkey, 2011, pp. 471–477.

[20] J. Kołodziej and F. Xhafa, "Enhancing the genetic-based scheduling in computational grids by a structured hierarchical population", *Future Gener. Comp. Syst.*, vol. 27, pp. 1035–1046, 2011.

[21] F. Xhafa and A. Abraham, "Computational models and heuristic methods for grid scheduling problems", *Future Gener. Comp. Syst.*, vol. 26, pp. 608–621, 2010.

[22] J. Kołodziej and S. U. Khan, "Multi-level hierarchic genetic-based scheduling of independent jobs in dynamic heterogeneous grid environment", *Inform. Sci.*, vol. 214, pp. 1–19, 2012.

[23] Z. Michalewicz, *Genetic Algorithms + Data Structures = Evolution Programs*. Berlin: Springer, 1992.

Magdalena Szmajduch is a Ph.D. student of computer science in the Interdisciplinary Ph.D. Programme managed jointly by the Jagiellonian University in Cracow, Polish Academy of Science in Warsaw and Cracow University of Technology. She is also the assistant professor at the Department of Computer Science of Cracow University of Technology. The main topic of her interest is data processing in large scale distributed dynamic systems.
E-mail: mszmajduch@pk.edu.pl
Department of Computer Science
Cracow University of Technology
Warszawska st 24
31-155 Cracow, Poland

Paper

Statistical Analysis of Message Delay in SIP Proxy Server

Pavel Abaev[1], Rostislav Razumchik[2], and Ivan Uglov[3]

[1] *Department of Applied Informatics and Probability Theory, Peoples' Friendship University of Russia, Moscow, Russia*
[2] *Institute of Informatics Problems of RAS, Moscow, Russia*
[3] *Moscow Technical University of Radio Engineering, Electronics and Automation, Moscow, Russia*

Abstract—Single hop delay of SIP message going through SIP proxy server operating in carriers backbone network is being analyzed. Results indicate that message sojourn times inside SIP server in most cases do not exceed order of tens of milliseconds (99% of all SIP-I messages experience less than 21 ms of sojourn delay) but there were observed very large delays which can hardly be attributed to message specific processing procedures. It is observed that delays are very variable. Delay components distribution that is to identified are not exponentially distributed or nearly constant even per message type or size. The authors show that measured waiting time and minimum transit time through SIP server can be approximated by acyclic phase-type distributions but accuracy of approximation at very high values of quantiles depends on the number outliers in the data. This finding suggests that modeling of SIP server with queueing system of G|PH|c type may server as an adequate solution.

Keywords—single hop delay, SIP server, statistical analysis, waiting time.

1. Introduction

Collapses of SIP proxy servers in carrier networks as described in [1] influenced the increase of research interests of SIP overload problem. Experimental evaluation of SIP server given in [2] evidenced that its performance greatly depends of server scenario and how SIP protocol is used. A SIP server can become overloaded due to various reasons such as denial of service, flash crowds (e.g., sudden increase in the number of phone calls), unintended traffic (e.g., unnecessary multiple copies of messages due to configuration mistakes), software errors (e.g., memory leaks, infinite loops). Traditional approach – resource overprovisioning – can reduce the overload probability significantly, but such a passive action would cause low average capacity utilization and increase the capital costs. Simple rejection of calls can mitigate the overload quickly, but it would reduce the revenue and decrease user's perceived quality of service. Meanwhile SIP specifications do not provide much guidance on how to react to overload conditions and thus significant efforts have been made to address the SIP overload problem (see, e.g. [3]–[7]). The overview of current state of art in SIP overload control algorithms which aim at preventing server crashes in carrier networks can be found in [8].

According to [9], when designing a mechanism for protecting a SIP server from overload one needs to take into account many issues: how to identify and indicate load status of the server, what is the procedure which allows reduction of overload with respect to quality of service requirements. Another problem is if it requires cooperation between servers and user agents or not and in which way, how this procedure can be implemented, whether it requires changes in the protocol or not. Taking into account all of these issues within single analytical model is a challenging task. Almost surely that this approach will lead to intractable results if one considers close to real-life values of model parameters, i.e., number of servers, clients, and concurrent sessions. Nevertheless analytical results even for single components of SIP network (if one manages to obtain and validate them) are of high importance due to their versatility. Their process validation is either performed by direct comparison with measured data from real-life experiments or performed within simulation environment which allows complex assembly models from simple ones. Leaving aside all the simulation drawbacks of SIP protocol it is a valuable mean for assessing performance of SIP networks and, as stated in [10], event-driven simulation has been widely used for evaluating SIP network performance.

In order to find the root cause of overload in SIP network, different analytical models have been proposed to analyze the statistical characteristics or dynamic behavior of SIP. Analytical model (queueing network composed of six $M|M|1$ queues) for estimation of mean response time for call setup in SIP network is presented in [11]. Analogous model but with constant service time was analyzed in [12]. In [13] and [14] results of analytical modeling of SIP proxy server as $M|M|c$ queue are compared with experimental data. Problem of service times characterization motivated authors of [15] to model SIP server as $M|G|1$ queue with service time distribution with six modes. Such choice of service distribution was justified by measurements of times SIP messages spend inside SIP proxy server. More general model $M^{[X]}|G|1$ which allows two types of batch arrivals is considered in [16]. Markov-modulated queueing model is introduced in [17] to analyze the queuing mechanism of SIP server under two typical service states. Authors state that the model can be used to predict the probability of SIP retransmissions, because the theoretical retransmission probability calculated by Markov Modulated Poisson Process (MMPP) model is located within the confidence interval of the real retransmission probability obtained from nu-

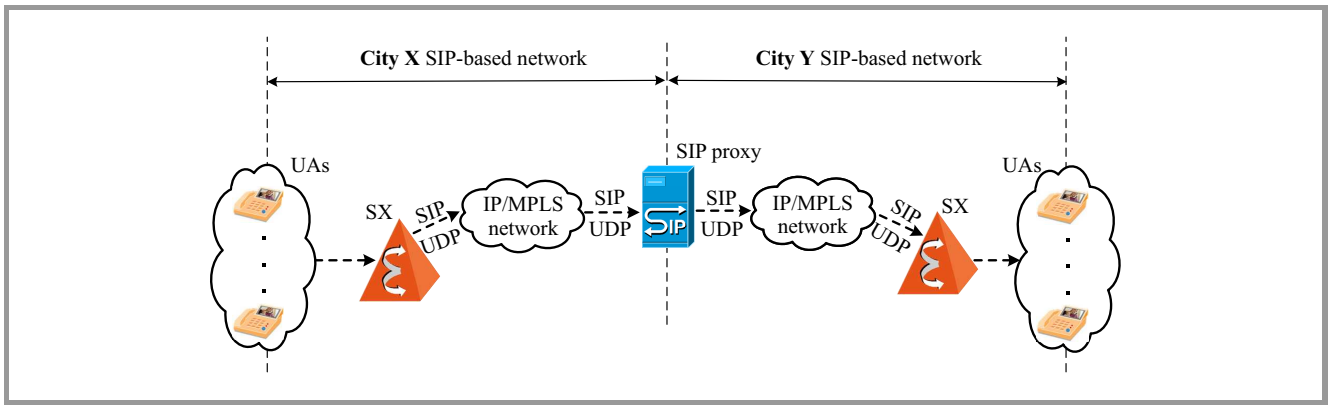


Fig. 1. Fragment of SIP based transit network under study.

merous simulation replications. Having noticed that it may be unnecessary to reject calls upon a short-term overload, authors in [10] developed a fluid model to capture the dynamic behavior of SIP retransmission mechanism of a single server with infinite buffer. A related study of a tandem server gives the guidance on how to extend the innovative approach to model an arbitrary SIP network. Fluid model for an overloaded SIP tandem server with finite buffer was developed in [18].

Both for analytical and simulation modeling it is of major importance to know the characteristics of processes that govern the incoming flow(s) and service of messages: the more close these processes resemble real-life behavior of entities of SIP network the more accurate model is. Although there are some results suggesting different SIP traffic models and service time distributions for messages entering SIP servers, amount of existing results is not enough to elaborate unified point of view. This paper contributes to the understanding of statistical properties of message service process in SIP servers, operating in carrier's backbone network. The SIP traffic circulating between two geographical regions through SIP proxy server is captured just before it enters server and right after it leaves server. Then it is analyzed following methodology proposed by authors of [19] for analysis of single-hop packet delay through operational router in Spring IP backbone network. During analysis there were observed packet processing and queueing delays and no transmission delays at output link (due to high speed of the interface). Additionally there were detected very large message delays that we were unable to explain. Having no information on how messages of different types are processes inside SIP server under consideration, assumption was made that one can model SIP server as single node queue with c processor serving messages according to some phase-type distribution (PH distribution) i.e. $\cdot|PH|c$ queue. Here "$\cdot$" means that any analytical model can be used for input flow or queueing system may be fed with SIP trace instead. Phase-type distribution is expected to embrace possible complex processing that may take place inside SIP server. One of the results is that waiting time of a SIP-I message in the queue is not exponentially distributed. The authors managed to fit measured waiting time in PH distribution using EM algorithm and ProFiDo tool (see [20]) though the fitting is not absolutely accurate at high values of quantiles (greater than 99.9%). From this experimental observation it follows that service time distribution is also of phase-type (with the same number of phases) due to the fact that waiting time in single queue systems of type $G|PH|c$ is of phase-type (see, e.g. [21]). Given experimental conditions, it is suggested that service time of message of given type equals roughly minimum time which message of such type spends in SIP server. Results of service time distribution fitting show that it can be modeled at acceptable level of accuracy with phase-type distribution.

The paper is organized as follows. In the Section 2 a description of traffic collection procedure and some insight into the traffic nature is given. Then in Section 3 delay measurements with step by step analysis of elements which contribute to single hop delay are presented. Conclusion contains short overview of obtained results and plans for further research are shown in Section 4.

2. Traffic Collection and Data Description

We consider the same fragment of telecommunication operator network depicted in Fig. 1 as in paper [22]. Traffic aggregation happens on regional access network using Signalling System No. 7 (SS7). As the caller and callee are located in different regions, the traffic goes through the two transit regional nodes – softswitches of the fourth class. Signalling exchange between them is organized by means of the SIP-I protocol. On the traffic route between softswitches SIP proxy server is set for the purpose of logical separation of regional networks.

All the SIP-I traces were captured on SIP proxy server's network interfaces during one week (7 consecutive days, starting from Wednesday, 24 hours per day) by means of span session created on one L2/L3 switch (see Fig. 2). All the transaction were stateful, underlying transport protocol was UDP. In order to capture traffic going in and out of SIP server, passive traffic monitoring system was implemented

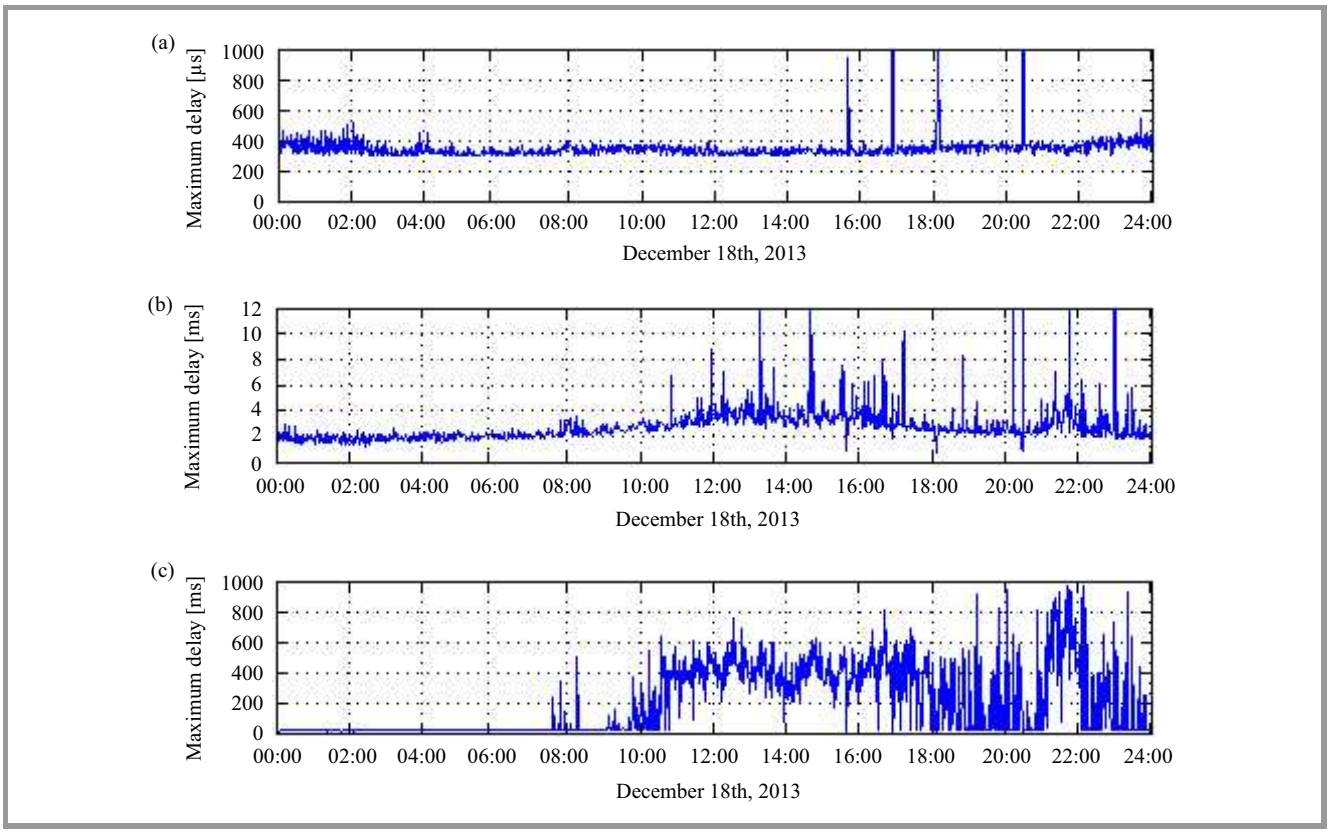


Fig. 2. Minimum (in μs), average and maximum delay (in ms) per minute during workday (24 hours).

which utilized traffic mirroring on nearest to SIP server L3 switches (see Fig. 3 and [23]).

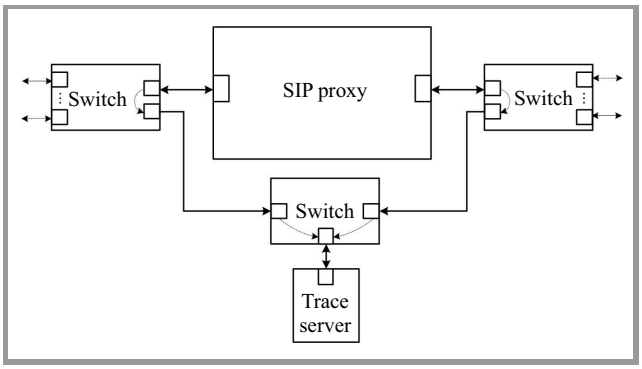


Fig. 3. Layout of monitoring circuit.

The load on the switches during the experiment did not exceed 30–40% of maximum rated capacity, thus providing no significant effect on measurements. The analysis of the flow volume of SIP-I traffic through SIP server has shown that for data capturing it is possible to use standard network interface cards installed on the data collection server. During experiment all types of SIP-I messages, passing through the SIP server for 7 consecutive days were captured.

The problem of time synchronization was solved without special tools – one trace server captured traffic from both SIP server interfaces. Since data volume flowing through SIP server during the measurement period achieved more than 100 gigabytes it was necessary to organize the automatic data backup. It was done using standard Linux operating system tools. The data collection procedure was organized in the same manner as described in [19]. Using Linux utility (tcpdump) libpcap data recording was performed. All information contained in each data packet was recorded.

In order to obtain delay we computed difference between timestamps at the input and output of monitored links. During measurement period no configuration changes, reinstallation of software or replacement of SIP server equipment parts were made. After data collection process had been finished data pre-filtering procedure was carried out. Data arrival, departure stamps and size of each SIP-I message were extracted. One of the major problems encountered in data analysis was unique identification of SIP message after its passage through the SIP server. Unfortunately, the methods of identification by the hash sum based on cyclic redundancy check algorithm (as it is done in [19]), which are widely used to identify the packet after its passage through L2/L3 device, in this case do not work: SIP server changes headers of SIP-I messages.

To solve this problem SIP-I messages are identified using fields which are not subject to change inside SIP server, e.g., session ID, number of messages in transaction, the type of message. By comparing such fields message filtering including deletion of duplicate messages was performed. Technically identification was performed using two

tables. The first contained data of SIP-I messages recorded on one interface, the second – on another interface. Each table line values were message fields and arrival timestamps (up to 1 μs). To map messages in the first and the second table the first table was sequentially scanned and checked for matching entries in the second table. As message capturing had been started at both interfaces at the same time it was assumed that the processed message by SIP server would appear at another interface with the serial number value not far from number under which it was registered at the first interface. Thus the search for SIP-I message with given serial number started in the second table from message with the same serial number. The depth of the search had been changed dynamically (depending on the number of messages per time unit) and took at least 20 s before and after the time of messages registration with the serial number from the second table.

Additional difficulty is that SIP-I messages generate additional flows of retransmissions and thus SIP server may resend the same SIP-I message when the corresponding timer fires out. Having matched SIP-I messages we have noticed the following. The organization of the monitoring circuit (see Fig. 3) implies that there are 4 serialization delays that contribute to measured delays and no forwarding/backplane delays in L2/L3 switches because traffic is simply mirrored between interfaces. But in the collected data we have observed delay values much lower than 50 μs. In fact delay values a little higher than 50 μs were present as well and such speed of SIP-I message processing seemed improbable. We found that the border line for delays with improbable values is 300 μs. The percentage of values in measured data below 300 μs is only 0.0006721%. We were unable to explain them and thus excluded them from the data and further analysis. Such delays might have occurred due to errors in identification algorithm or due to incorrect retransmission of SIP-I messages by SIP server.

Notice that SIP-I messages may have size more than 1500 bytes and thus have to fragmented before being processed. Analysis of this issue showed that percentage of fragmented messages in the data does not exceed 0.04%. Only for INVITE messages it is around 2% which is due to the presence of encapsulated big-sized IAM SS7 messages. These message were left out of further analysis as well.

3. Delay Analysis

In this section key observations of measurements of the sojourn (delay) time of SIP-I messages in SIP server are presented. We plot the empirical probability density function of the measured SIP server delay and quantify step-by-step its contributing factors. The outcome of this analysis is the proposal of analytical models for different ingredients of the delay.

3.1. General Observations

Figure 2 shows the minimum, average and maximum values of SIP server delay observed each one minute interval during 24 hours of December 18th 2013. The simplest statistical analysis showed that each day there appear critical outliers (single abnormal high delay values). For example, on the 18th of December 2013 one could observe delay values of 3.231 s, 5.952 s, 6.571 s, 12.102 s for 183 message; on the 19th of December 2013 delay values 35.702 s., 15.213 s, 12.642 s and 10.519 s of 183 message and delay values 6.501 s, 4.499 s of BYE message passing through SIP server were registered. One can see such outliers in Fig. 2. Analysis of two-week data showed that such delays appear more often during workdays than during weekends but total number of outliers per day does not usually exceed 10-30. Identification of exact reasons why it happens, i.e., errors in forwarding algorithms, switching of CPU to some other intensive task, output blocking, memory locks, poor scheduling did not give any results and in further analysis such values were excluded from the data.

Aside from outliers minimum delay is quite stable throughout all the day. The minimum delay corresponds to the minimum amount of time SIP-I message needs to go through SIP server. It is tightly bounded and bounds depend on the time of the day. This suggests that there is at least one packet that experiences no queuing in each one minute interval. The average delay varies more irregularly and is directly related to SIP server utilization. It increases from early morning as call rate increases and drops down in the evening. Maximum delays are much larger and more variable than the average delays. In the middle of the day maximum delay remains above 240 ms and in the evening shows regular spikes of hundreds of milliseconds reaching up 931 ms. Delays during the weekend are much more stable. The average delay is almost uniformly bounded by 4 ms, maximum observed delay is 792 ms.

3.2. Step-by-step Analysis

In Fig. 4 one can see empirical probability density function of SIP-I message delay, measured within monitoring

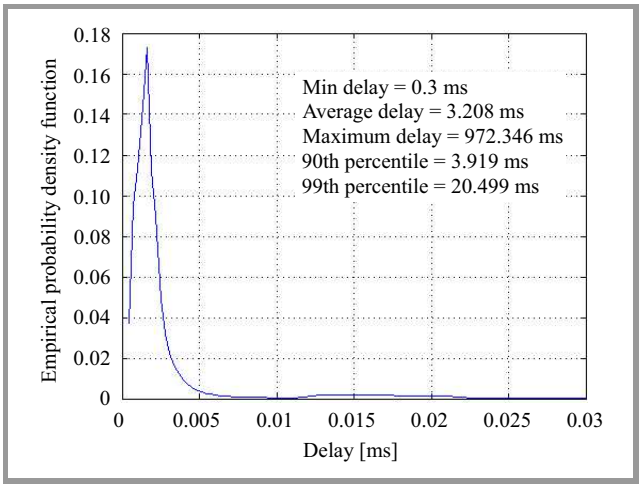


Fig. 4. Empirical probability density function of SIP-I messages measured delay (this delay includes delay in SIP server and other processing delays in switches and network interfaces).

circuit. Average delay value is around 3 ms, whereas 99% of all SIP-I messages experience delay of less that 21 ms and maximum observed delay is almost 1 s. There is only one distinct peak at the beginning of density function and one small but wide peak in the middle. We now try to conjecture what is this small peak related to. In Fig. 5 relative frequency distribution of SIP-I message sizes

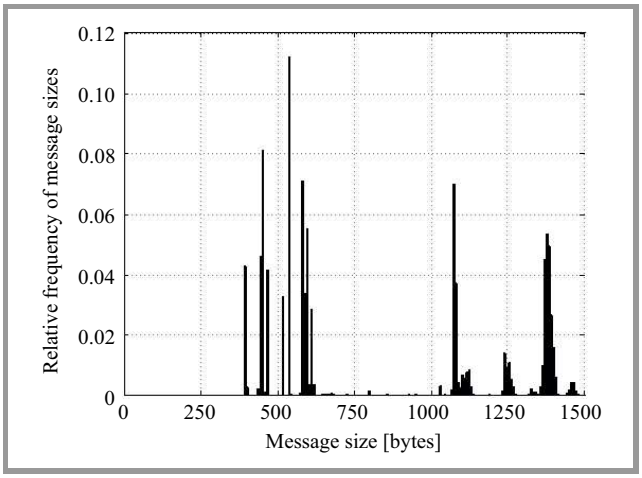


Fig. 5. Relative frequency distribution of SIP-I message sizes.

is plotted. This distribution has many peaks but one can clearly distinguish two groups of message sizes: 375–675 bytes and 1000–1500 bytes (more than 99.5% of SIP-I messages fall in these groups). Now we group SIP-I messages in these two groups and separately plot the empirical density function of the delay experienced by SIP-I messages in the given group (see Fig. 6). One can see that

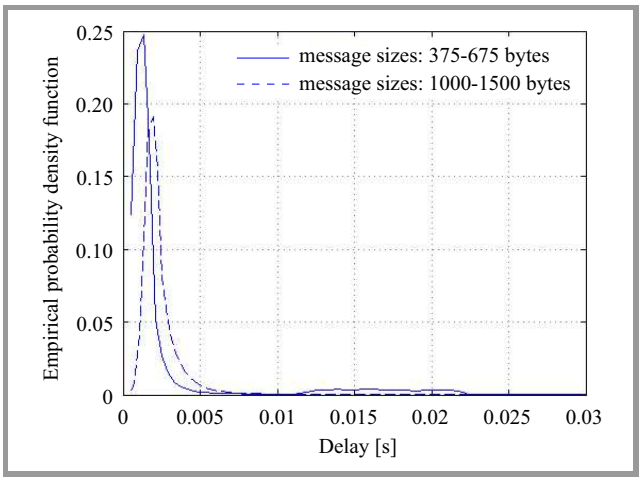


Fig. 6. Empirical probability density function of delay given that size of SIP-I message is from one of two groups: 375–675 bytes and 1000–1500 bytes.

small wide peak is present again for SIP-I messages of size 375–675 bytes but is absent for SIP-I messages of size 1000–1500 bytes. This suggests that the delay peak is related to message type but not size (as it is shown to be in IP backbone router, see [19]) and one should look for corresponding message types only among those messages which have size 375–675 bytes. Thus from this group there were selected those message types which suffer delay more than 10 ms and surprisingly the most frequent message type was 200 OK of size 391–399 bytes. Greater sizes of 200 OK messages do also occur in the whole data set but their delays remain lower. In Fig. 7 one can see empirical probability density function of 200 OK message (size 391–399 bytes) and all other SIP-I messages. It is clear now that small wide peak in Fig. 4 is related to 200 OK message of specified size.

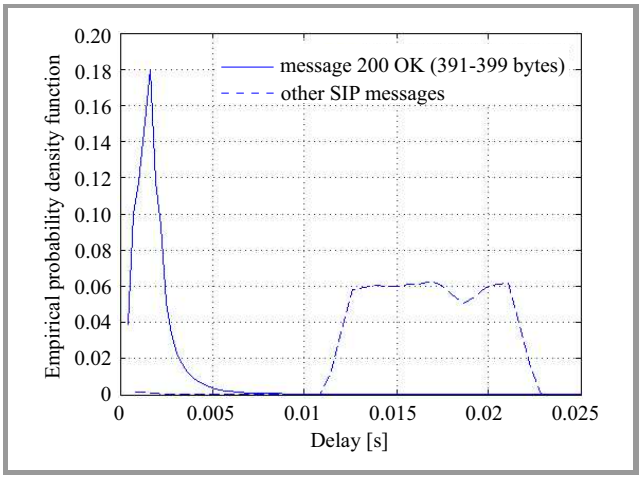


Fig. 7. Empirical probability density functions of delay of 200 OK message (size 391–399 bytes) and other SIP-I messages.

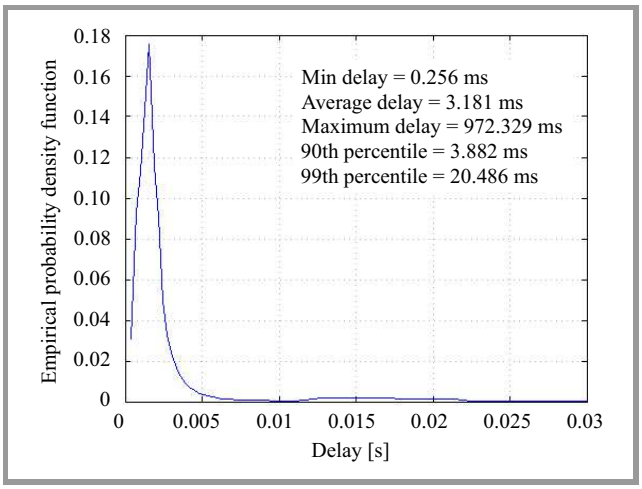


Fig. 8. Empirical probability density function of SIP-I messages transit time through SIP server.

Now we proceed to identify and quantify the factors that contribute the same amount of delay for messages of the same size. The main cause is serialization delay. Serialization delay is proportional to packet size divided by the speed of the output link. All link rates in the monitoring circuit are 1 Gb/s. Although serialization delay of the maximum Ethernet packet size (1500 bytes) is 12 μs we have to take it into account because there are 4 serialization delays.

We refer to the difference between measured delay and all serialization delays as SIP server transit time. The empirical probability density function of transit time is plotted in Fig. 8.

As expected small wide peak in the distribution is still present and high peak is almost not affected. When SIP-I message arriver at SIP server it has to go through network stack and some common and message-specific processing at application level and then again though network stack (see example, e.g. in [15]). This operation takes some time which, when SIP server is under-loaded, indicates minimum transit time experienced by messages (depending either on their size or type or both). We plot the minimum value of the SIP server transit time for each SIP-I message type in Fig. 9.

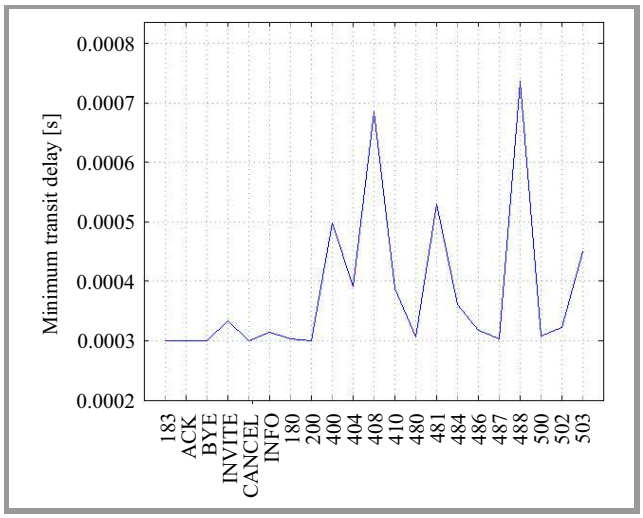


Fig. 9. Minimum transit delay per message type.

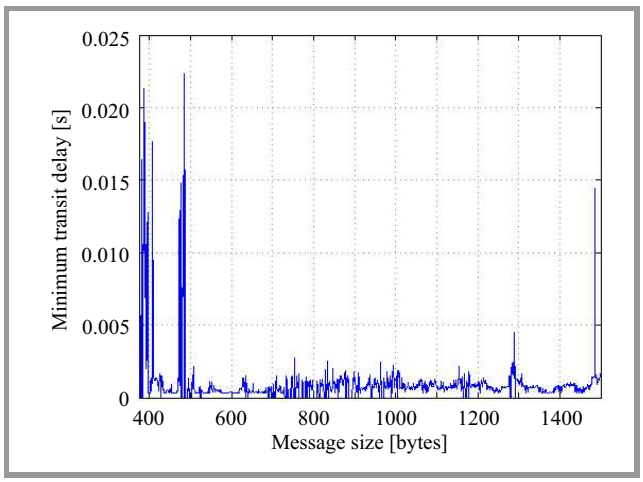


Fig. 10. Minimum transit delay per message size.

One can see that minimum transit time per message type is very low and does not give real picture of minimum delay because each type of message may have very different sizes, carry different information in headers and thus delay should vary significantly. Here it is appropriate to calculate delay characteristics of each type of SIP-I messages. There are a total of 21 type of messages in the data. Basic statistical characteristics per each message type are given in Table 1. It is worth noticing that for 200 OK message average delay differs much from the delay observed in Fig. 7 which is due to the fact that 200 OK messages of other sizes are processes most of the times much faster. In Fig. 10 the minimum transit delay per each unique packet size is plotted.

Table 1
Transit delay (in seconds) per type of SIP message

Message type	Average	Standard deviation
ACK	0.001541	0.001864
BYE	0.001445	0.002541
INVITE	0.002414	0.001977
CANCEL	0.001447	0.001680
INFO	0.008975	0.009001
180	0.002334	0.001870
183	0.004427	0.026801
200	0.005735	0.008445
400	0.001201	0.000388
404	0.001742	0.001696
408	0.003677	0.005602
410	0.001706	0.001829
480	0.001728	0.001754
481	0.001291	0.000914
484	0.001492	0.001420
486	0.001694	0.001681
487	0.001665	0.001612
488	0.001771	0.001671
500	0.001656	0.001656
502	0.001609	0.001575
503	0.001622	0.001688

It can be seen that no simple relationship between two metrics exist. Based on thorough analysis of SIP-I traces we are inclined to consider this minimum transit delay as SIP-I message pure service time. Its empirical probability density is depicted in Fig. 11. Possible explanation of such unstable minimum delays may be the fact that, according to [24], header fields of each new request may have any additional overheads, optional header fields specific to the method and their processing may introduce additional delay. Now if one subtracts this minimum from transit delay for each message in the data, one obtains amount of time each message has to wait inside SIP server. The new empirical probability density function is presented in Fig. 12.

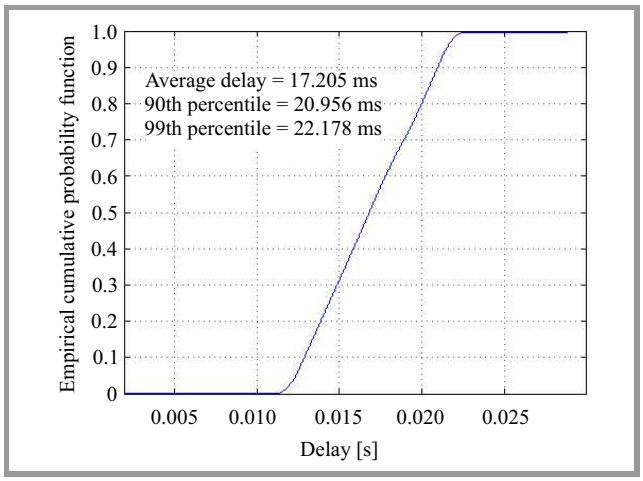


Fig. 11. Empirical cumulative distribution function of the minimum transit delay (service time).

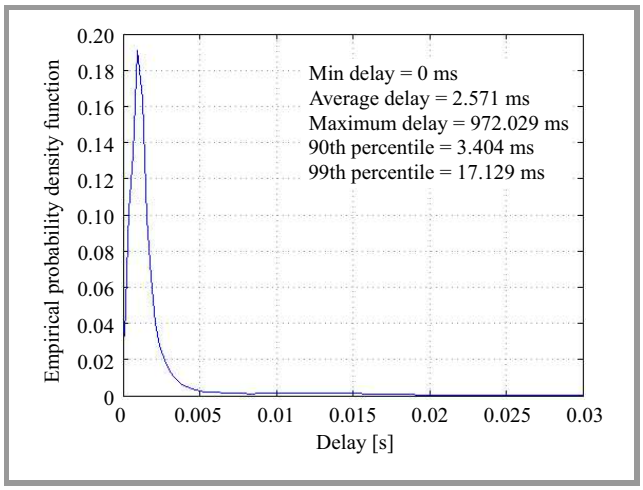


Fig. 12. Probability density of the waiting time in SIP server.

Small peak in the middle related to 200 OK message of 391–399 bytes sizes has disappeared. The distribution is characterized by average low delays, most of the messages exhibit delays close to average (90th percentile is around 3 ms), whereas maximum delay remain high (almost reaches 1 s). In Fig. 13 cumulative distribution function of the waiting time in SIP server is presented. A key observation is that the tail of the delay distribution is long accounting for the presence of high delays. However link utilization when large delays were observed was not very high and therefore long delays must not be due to queueing at the output link. The percentage of messages for which waiting time exceeds 17 ms (99th percentile of all delays) is only 2.1%. We were unable to find possible explanations for such high values. It is not that only one or two types of messages exhibit such long delays. For almost each message type there are packets with high delay values. Once these values have been removed from the data set, we found that statistics of the distribution have changed (average delay decreased to 1.7 ms, 90th percentile decreased to 2.9 ms, 99th percentile dropped to 13 ms). These outliers could be attributed to issues common for routers (e.g. memory locks, poor scheduling etc., see [19]) or SIP-I protocol specific issues but these conjectures were not checked.

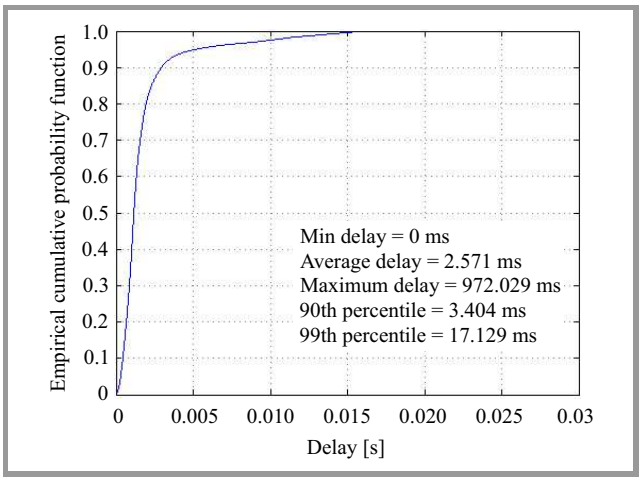


Fig. 13. Empirical cumulative distribution function of the waiting time.

Analysis of the data showed that the distribution of the waiting time is not exponential (squared coefficient of variation equals 26.83). From this it follows that possible queueing model with single (or several but identical) server and exponential service times are not adequate for the considered case. Following the assumption concerning SIP server model stated in Section 1, we tried to fit message waiting times in PH distribution using EM algorithm implemented in [20]. Quantiles of the waiting time estimated from data and of simulated fitted acyclic PH with 15 states are shown in Fig. 14. The simulation was performed using KPC-Toolbox (see [25]).

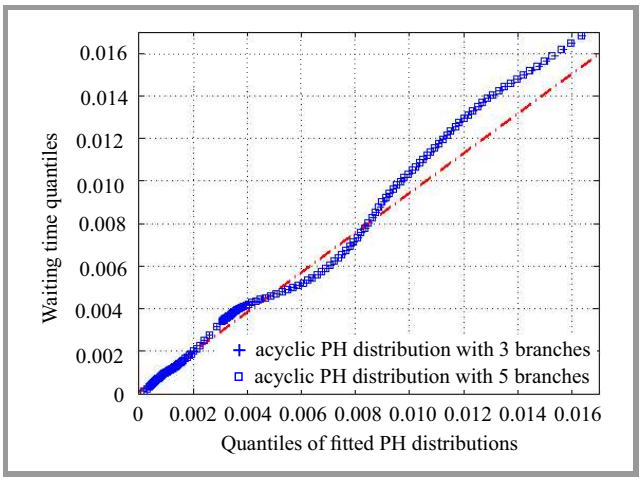


Fig. 14. Q-Q plot of the waiting time and simulated data, using fitted continuous acyclic PH distribution with 15 phases.

The fact that waiting time can be approximated by PH distribution, suggests that in the queueing model of SIP server $\cdot|PH|c$ number of processors is $c = 1$ (see e.g. [21]) with

PH distribution of service times with the same number of phases. In Fig. 15 one can see quantile-quantile plot of the minimum transit delay and simulated data, using fitted continuous acyclic PH distribution with 15 phases.

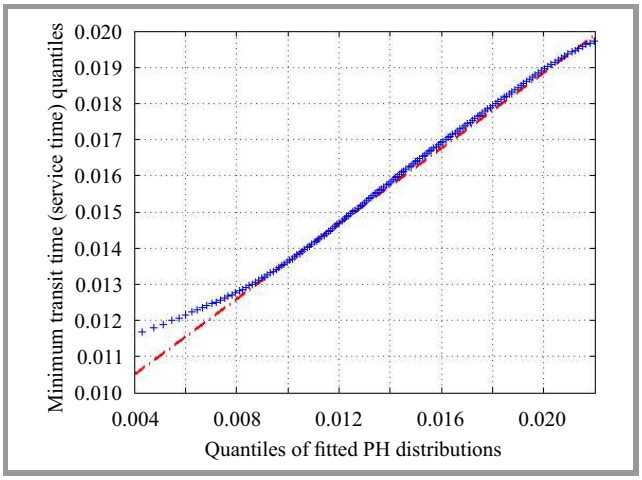


Fig. 15. Q-Q plot of the minimum transit time (service time) and simulated data, using fitted continuous acyclic PH distribution with 15 phases.

With respect to the waiting time one may observe many outliers at high quantiles (note that 99% of all waiting times is below 3.4 ms) and fitting is not absolutely accurate. This may be due to the fact that 2.1% of SIP-I messages suffer extremely high delays and number of such values within the fitted data is not enough for accurate estimation of PH parameters. The same observation is true for minimum transit time (service time) fitting but at low values of quantiles.

4. Conclusion

Paper presents analysis of single-hop delay of SIP-I message going through SIP proxy server operating in carrier's backbone network. According to our results 99% of all SIP-I messages experience less than 21 ms of sojourn delay. We have observer a small number of messages (2.1% of the data volume) which suffer from significantly larger delays and we were unable to find the reason for that. Analysis of the waiting time (queueing delay) and minimum transit time through SIP server revealed that both can be approximated by acyclic continuous phase-type distributions. But due to outliers fitting is not so accurate and thus requires additional validation by virtue of analytical models (e.g. $MMPP|PH|c$ queue).

References

[1] B. Materna, "Threat mitigation for VoIP", in *Proc. 3rd Ann. VoIP Secur. Worksh.*, Berlin, Germany, 2006.

[2] E. Nahum, J. Tracey, and C. Wright, "Evaluating SIP server performance", in *Proc. Int. Conf. Measur. Model. Comp. Syst. ACM SIGMETRICS 2007*, San Diego, CA, USA, 2007, pp. 349–350.

[3] M. Ohta, "Overload protection in a SIP signaling network", in *Proc. Int. Conf. Internet Surveill. Protect. ICISP'06*, Cote d'Azur, France, 2006.

[4] R. Garroppo, S. Giordano, S. Spagna, and S. Niccolini, "Queueing strategies for local overload control in SIP server", in *Proc. IEEE Global Commun. Conf. GLOBECOM 2009*, Honolulu, HI, USA, 2009.

[5] A. Abdelal and W. Matragi, "Signal-based overload control for SIP servers", in *Proc. 7th Ann. IEEE Consumer Commun. Netw. Conf. IEEE CCNC 2010*, Las Vegas, NV, USA, 2010, pp. 1–7.

[6] V. Hilt and I. Widjaja, "Controlling Overload in networks of SIP servers", in *Proc. 16th IEEE Int. Conf. Netw. Protoc. ICNP 2008*, Orlando, FL, USA, 2008, pp. 83–93.

[7] E. Noel and C. R. Johnson, "Novel overload controls for SIP networks", in *Proc. 21st Int. Teletraff. Congr. ITC 21*, Paris, France, 2009.

[8] Y. Hong, C. Huang, and J. Yan, "A comparative study of SIP overload control algorithms", in *Network and Traffic Engineering in Emerging Distributed Computing Applications*, J. Abawajy, M. Pathan, M. Rahman, A. K. Pathan, and M. M. Deris, Eds. IGI Global, 2012, pp. 1–20.

[9] D. Sisalem, "SIP overload control: Where are we today?", in *Trustworthy Internet*, L. Salgarelli, G. Bianchi, and N. Blefari-Melazzi, Eds. Springer, 2011, pp. 273–287.

[10] Hong Y., C. Huang, and J. Yan, "Modelling chaotic behaviour of SIP retransmission mechanism", *Int. J. Paral. Emerg. Distrib. Syst.*, no. 2, pp. 95–122, 2013.

[11] V. Gurbani, L. Jagadeesan, and V. Mendirittam, "Characterizing session initiation protocol (SIP) network performance and reliability", in *Proc. 2nd Int. Service Availabil. Symp. ISAS 2005*, Berlin, Germany, 2005, pp. 196–211.

[12] S. Subramanian and R. Dutta, "Comparative study of M/M/1 and M/D/1 models of a SIP proxy server", in *Proc. Australasian Telecommun. Netw. Appl. Conf. ATNAC 2008*, Adelaide, Australia, 2008, pp. 397–402.

[13] S. Subramanian and R. Dutta, " Measurements and analysis of M/M/1 and M/M/c queueing models of the SIP proxy server", in *Proc. 18th Int. Conf. Comp. Commun. Netw. ICCCN 2009*, San Francisco, CA USA, 2009.

[14] S. Subramanian and R. Dutta, "Performance and scalability of M/M/c based queueing model of the SIP proxy server – a practical approach", in *Proc. Australasian Telecommun. Netw. Appl. Conf. ATNAC 2009*, Canberra, Australia, 2009.

[15] R. Krishnamurthy and G. Rouskas, "Evaluation of SIP proxy server performance: Packet-level measurements and queuing model", in *Proc. Int. Conf. Commun. IEEE ICC'03*, Budapest, Hungary, 2013, pp. 2326–2330.

[16] Y. Gaidamaka, A. Pechinkin, R. Razumchik, K. Samouylov, and R. Sopin, "Analysis of M|G|1|R queue with batch arrivals and two hysteretic overload control policies", *Int. J. Appl. Mathem. Comp. Sci.*, vol. 24, no. 3, pp. 519–534, 2014.

[17] Y. Hong, C. Huang, and J. Yan, "Analysis of SIP retransmission probability using a Markov-Modulated poisson process model", in *Proc. IEEE/IFIP Netw. Oper. Manag. Symp. NOMS 2010*, Osaka, Japan, 2010, pp. 179–186.

[18] Y. Hong, C. Huang, and J. Yan, "Modeling and simulation of SIP tandem server with finite buffer", *ACM Trans. Model. Comp. Simul.*, vol. 21, no. 2, 2011.

[19] C. Diot, C. Fraleigh, S. Moon, K. Papagiannaki, and P. Thiran, "Measurement and analysis of single-hop delay on an IP backbone network", *IEEE J. Selec. Areas Commun.*, vol. 21, no. 6, pp. 908–921, 2003.

[20] F. Bause, P. Buchholz, and J. Kriege, "ProFiDo – the process fitting toolkit Dortmund", in *Proc. 7th Int. Conf. Quantit. Eval. Syst. QEST 2010*, Williamsburg, VA, USA, 2010.

[21] S. Asmussen and J. Moller, "Calculation of the steady state waiting time distribution in GI/PH/c and MAP/PH/c queues", *Queueing Systems: Theory and Appl.*, vol. 37. pp. 9–29, 2001.

[22] P. Abaev, I. Uglov, and R. Razumchik, "Statistical analysis and modelling of SIP traffic for parameter estimation of server hysteretic overload control", *J. Telecommun. Inform. Technol.*, no. 4, pp. 22–31, 2013.

[23] A. Heyde and L. Stewart, "Using the Endace DAG 3.7GF Card With FreeBSD 7.0", Tech. Rep. CAIA 080507A, 2008-05.

[24] "SIP: Session Initiation Protocol", IETF, RFC 3261, 2002-06.

[25] G. Casale, E. Zhang, and E. Smirni, "KPC-toolbox: Simple yet effective trace fitting using markovian arrival processes", in *Proc. 5th Int. Conf. Quantit. Eval. Syst. QEST 2008*, St. Malo, France, 2008, pp. 83–92.

Pavel Abaev received his Ph.D. in Computer Science from the Peoples Friendship University of Russia in 2011. He has been an Associate Professor in the Department of Applied Informatics and Probability Theory of Peoples' Friendship University of Russia. His current research focus is on NGN signalling, QoS analysis of SIP, and mathematical modeling of communication networks.
E-mail: pabaev@sci.pfu.edu.ru
Department of Applied Informatics and Probability Theory
Peoples' Friendship University of Russia
Miklukho-Maklaya st 6
117198 Moscow, Russia

Rostislav Razumchik received his Ph.D. in Physics and Mathematics in 2011. Since then, he has worked as a senior research fellow at the Institute of Informatics Problems of the Russian Academy of Sciences. His current research activities focus on stochastic processes and queuing theory.

E-mail: rrazumchik@ieee.org
Institute of Informatics Problems of RAS
Vavilova st 44-1
119333 Moscow, Russia

Ivan Uglov works at the Department of Information Security, Moscow Technical University of Radio Engineering, Electronics and Automation. His research interests include telecommunication network modeling, simulation and quality of service provisioning.

E-mail: uglov_ivan@mail.ru
Moscow Technical University of Radio Engineering,
Electronics and Automation
Vernadskogo st 78, 21-88
119454 Moscow, Russia

Paper

FTTH Network Optimization

Hoang Nghia Le

Suntech S.A., Warsaw, Poland

Abstract—Fiber To The Home (FTTH) is the most ambitious among optical technologies applied in the access segment of telecommunications networks. The main issues of deploying FTTH are the device price and the installation cost. Whilst the costs of optical devices are gradually decreasing, the cost of optical cable installation remains challenging. In this paper, the problem of optimization that has practical application for FTTH networks is presented. Because the problem is Non-deterministic polynomial-time hard (NP-hard), an approximation algorithm to solve it is proposed. The author has developed the algorithm in a C# program in order to analyze its performance. The analysis confirms that the algorithm gains near-optimal results with acceptable time consumption. Therefore, the algorithm to be applied in a network design tool for FTTH network planning is proposed.

Keywords—cost optimization, development optimization, FTTH, optical technology, telecommunications network.

1. Introduction

Unlike in other technologies, in FTTH the digital data stream is transmitted through the optical medium directly to the subscriber's terminal. Thanks to this approach, FTTH allows for data transmission with higher speed and better quality than other networks based on radio, copper, coaxial and optical-coaxial mixed technologies. Moreover, FTTH is future proofed – a greater transmission speed requires only faster terminals and routers, with the fibers remaining unchanged.

However, nowadays the FTTH development in the world (also in Europe) is unequal. In annual ranking of FTTH Council based on FTTH coverage (the percentage of Internet subscribers using FTTH) in particular countries [1], apart from about 20 countries (led by South Korea, United Arab Emirates and Japan) with FTTH technology widely developed (FTTH coverage larger than 25%), for the rest of the world this key factor is still less than 5%. The problem is due to economic issues – FTTH requires high cost of devices and optical cable installation. Below a brief overview of the technology FTTH is presented.

The FTTH network starts from an Optical Line Terminal (OLT), an endpoint of the core network (Fig. 1). The optical signals that carry the digital data streams to the subscribers are firstly transmitted in a common cable. This is possible thanks to Wave Division Multiplexing technology (WDM), which allows a fiber to simultaneously transmit several tens of optical signals, each of them in a separate waveband. Later, the signals are split into different routes, by means of splitters, and end in the Optical Network Units (ONUs) installed in the subscribers' homes. Unlike other networks, in an FTTH network copper cables are not used. Therefore, optical to electrical conversion, which severely lowers the limit of data transmission speed for a single user, is not needed.

Whilst the prices of optical devices (OLTs and ONUs), the most problematic issue so far, are gradually decreasing, the cost of optical cable installation remains unchanged. The cost is made up of several factors as:

- the duct digging,
- the drilling the conduits in new or existing ducts,
- the laying the cables in new or existing conduits,
- the cable.

In this paper, a new method for FTTH network optimization with the focus on cable installation minimization is proposed. After analyzing the previous work, the FTTH network optimization issues as a mathematical problem is presented, called the problem of FTTH Network Optimization (FNO). An exact algorithm to solve FNO is proposed, modeling it as an Integer Linear Programming (ILP) problem. Due to the NP-hardness of FNO, the exact algorithm allows to solve the problem only for small FNO instances (with less than ten subscribers). Therefore, for larger FNO instances, the author proposes an approximation algorithm. Although the algorithm does not guarantee the ideal solution, it allows for finding the solution closed to optimum. The algorithm computation complexity is polynomial, which allows for its application in computer system with acceptable cost for FTTH network planners. In order to evaluate presented algorithms, the result of their operations in examples is presented.

2. Related Work

The optimization issues in FTTH network planning are considered in various surveys, among others [2]. Detailed studies about FTTH optimization focus on 3 areas:

- device installation optimization [3],
- cable installation optimization [4]–[7],
- bandwidth utilization optimization in an FTTH existing network [8].

In [3], the network cost to be optimized is composed of two parts: CAPEX – cost of device installation, and OPEX – cost of network element maintenance. The net-

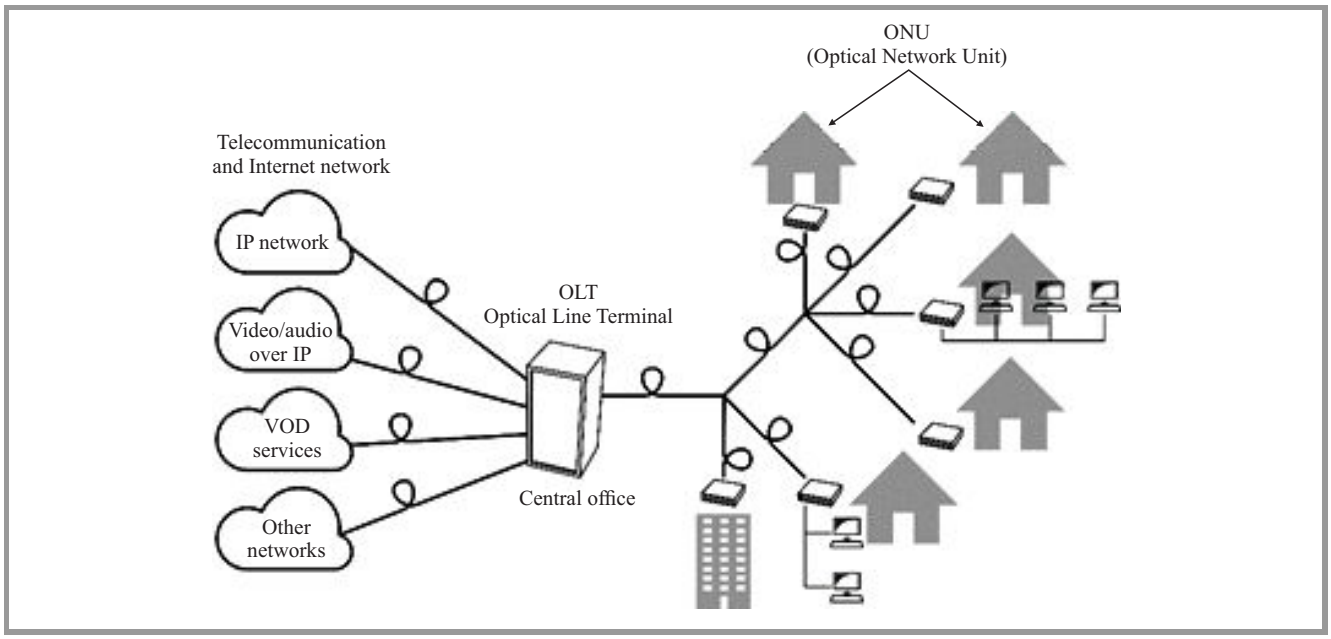


Fig. 1. FTTH network structure.

work optimization is modeled as an Integer Linear Programming (ILP) problem. Due to the NP-hardness property of the problem, an approximated solution is proposed. Cable installation cost optimization is not considered in the paper.

In [4]–[7], the cable installation cost optimization issues are considered. However, the authors have limited the research scope to the problem of selection of the best cable routes from among the predefined ones. Thus, this approach makes the result strongly depended on the subjectively predefined cable routes. In [7], the robustness of the network is also considered. The network should operate without loss after a failure of a single cable. In [8], another category of optical network optimization is considered: optimization of bandwidth distribution in an existing FTTH network.

After thorough analysis of the previous studies, it could be concluded that the problem of FTTH network optimization in the full format of geographical optimization – finding the optimal allocation of devices and cables in a given area, with the geographical aspects considered has not been resolved yet. Therefore, the aim of this study is to fill this research gap.

Geographical optimization is applied in various areas, including energy, transport, industry, and also in telecommunications (especially for core networks). The basic geographical optimization problems are the problems of Euclidean Traveling Salesman (ETS) and Euclidean Steiner Tree (EST) [9], [10]. The first of these problems is to find the shortest tour to visit a set of points in a plane, whilst the later problem is to find the shortest tree-network that connects a set of points in a plane.

The author has analyzed the attempts to extend EST problem with geometrical conditions in previous studies [11], [12]. In those studies, the algorithms to find the EST that avoid given obstacle areas are proposed. In this paper, the problem further by considering the following aspects is extended:

- The geographical aspect. In EST, the optimization objective is to find the shortest network. In practice, it may not be the network with the lowest cost, if some of its links have to be provided across areas, where cable installation is difficult or impossible. In this work, the cable installation cost resulting from the terrain condition is assigned to each point of the plane and the algorithm finds the network with the lowest total cost.
- The cable capacity limitation.
- The existing network resources. This extension is essential for using the algorithm in frequent practical situation, in which the network planner task is rather to develop an existing network than to create a new network for a “green-field”.

3. FTTH Network Optimization Problem

In this section, the formal description of the FTTH network optimization problem (FNO) is presented.
It starts with geometrical input data:

- finite set of source points in the plane $S \subset R^2$ (a source point represents an OLT);
- finite set of destination points in the plane space $D \subset R^2$ (a destination point represents an ONU);
- finite set of existing transit points in the plane $T_1 \subset R^2$ (a transit point represents a splitter);

- finite set of lines connecting the points in the sets S, D and $T_1 : E_1 \subset (S \cup D \cup T_1)^2$ (a line represents a linear segment of a cable).

In Fig. 2 the model of an FTTH network is presented.

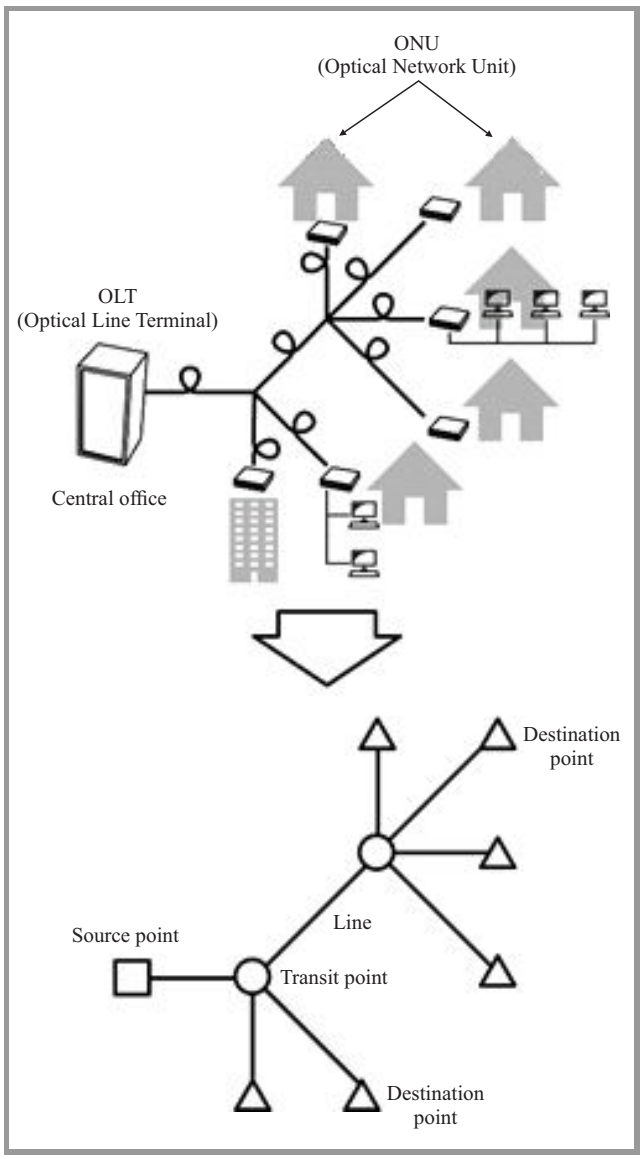


Fig. 2. Modeling FTTH network in FNO problem.

Other input data:

- Cable capacity C. It represents the maximum number of WDM channels that can be transmitted via the cable;
- Density function of cable installation cost in the area g: $R^2 \to R$. The cost of cable installation depends on the terrain of the area and the infrastructure existing in the area. The cost of cable installation can be: quite low if the cable is laid along a road, quite high if the cable is laid across a road, or infinite if the cable has to cross a building or a housing estate (impossible to install).

Function $g(x)$ describes the installation cable cost with a unit length at the point $x \in R^2$. Having the function g, the installation cost of a cable e by means of the following integral can be calculated:

$$f(e) = \int_{r=0}^{1} g\big((1-r)\cdot \text{in}(e) + r \cdot \text{out}(e)\big)\text{d}r, \qquad (1)$$

where $\text{in}(e)$ denotes the input point of line e, $\text{out}(e)$ denotes the output point of line e.

It is assumed that function g is described by means of a finite and sorted collection of polygons, each of which has an assigned cost value, and called the g-polygons. The value $g(x)$ for point x in R^2 is the cost of the first g-polygon that contains x. If x does not belong to any g-polygon, the $g(x) = 1$. A g-polygon represents an area with the same cost. For example: a roadside (low cost), a road (high cost), a building (infinite cost).

In Fig. 3, the cost of cable installation from A to B is $f(\text{AB}) = ||\text{AT}_1|| + ||\text{T}_1\text{T}_2|| \cdot m_1 + ||\text{T}_2\text{T}_3|| \cdot m_2 + ||\text{T}_3\text{T}_4|| \cdot m_1 + ||\text{T}_4\text{B}||$, where m_1, m_2, m_3 are the costs of the highlighted areas, respectively.

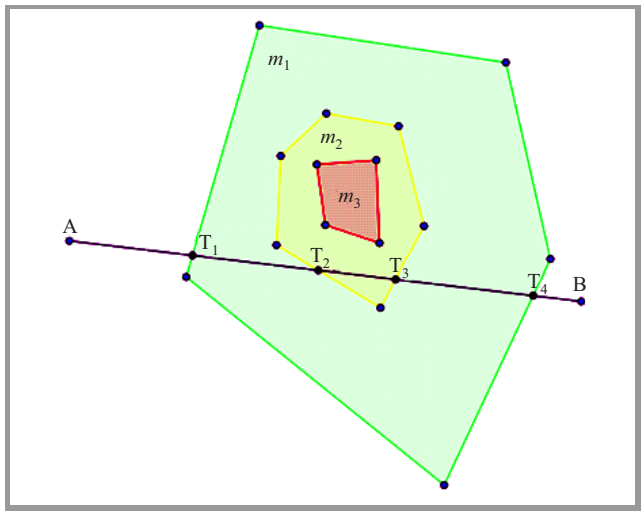


Fig. 3. The cost of installing cables through g-polygons.

The next step is to find:

- finite set of transit points $T \subset R^2$,
- finite set of lines connecting the points in the sets S, D and T: $E \subset (S \cup D \cup T)^2$,
- finite set of paths (sequences of connected lines) $P = \{p : p = (e_1, e_2, \ldots, e_n);\ \forall i = 1 \ldots n,\ e_i \in E,$ where $\forall j = 1 \ldots n-1,\ \text{out}(e_j) = \text{in}(e_{j+1})\}$.

Conditions:

- The **connectivity condition**. Each destination point is connected to at least one source point, either directly via one line or a sequence of connected lines. In other words, for each point $d \in D$, there exists a path $p \in P$ so that $\text{in}(p) \in S$, $\text{out}(p) = d$, where

in(p) denotes the input point of the first line of path p, and out(p) denotes the output point of the last line of path p;

- The **capacity condition**. The number of path containing a line should not exceed the predefined capacity of the line: $\forall e \in E$, $\sum_{p \in P: e \in p} 1 \leq C$. In the context of WDM technology, C is the number of channels that can be transmitted through an optical cable.

Optimization goal:

- The optimization objective is to get seek solution with the least total cost of installation of the cables:

$$\text{Minimize} \sum_{e \in E \setminus E_1} f(e). \tag{2}$$

4. Exact Algorithm for FNO

In this paper, the two algorithms for FNO are proposed. The main one is an approximation algorithm that allows for effective finding of a near optimal solution of the problem. In addition an exact algorithm modeled as an Integer Linear Programming (ILP) is proposed, which is effective only for small problem instances. The exact algorithm is used to evaluate the quality of the solution obtained from the main algorithm.

FNO is strongly related to the family of Steiner Tree Problems (STP). Apart from the EST already mentioned earlier, FNO is also related to the topological version of the STP. The descriptions of the two problems are as follows:

- the Topological Steiner Tree (TST): given a graph consisting of node set V and link set E (each link has a cost value assigned), interconnect a given subset T of V by a sub-graph with the shortest total link cost;
- the Euclidean Steiner Tree (EST): given n points in the plane (called the terminal points), connect them by line segments of the minimum total length in such a way that any two terminal points may be interconnected by the line segments either directly or via other points (called the Steiner points).

TST will be used multiple times as a subroutine of the algorithms for FNO, whilst EST is a special case of FNO when S is a one-single-element set, g is a constant function, and C is larger than $|D|$.

Because EST has been intensively studied in the last century, the author will construct the exact algorithm using the knowledge collected in the studies on EST. EST is proved to be an NP-hard problem [13].

Transferring the EST and its derived problems, like FNO, into an ILP form is difficult, because the Steiner points to be found are derived from a continuum and unconstrained set, whilst an ILP is assumed to have discrete and limited set of variables and equalities. Therefore, in order to transfer FNO into an ILP, there is need to "discretize" the problem data space. In other words, the aim is to construct a limited and discrete set of points that contains the sought Steiner points. The author calls these points the candidate points.

4.1. Candidate Points for EST and FNO

There are two approaches for discretizing the space of EST deriving problems:

- by means of a grid of pixels on the plane – the candidate points are defined as the vertices of the grid;
- by generating the candidate points, based on geometrical properties of EST.

The first approach is practical for an approximation algorithm. However, it does not allow for finding the exact solution. The quality of the solution depends on the grid granularity. The second approach is used in presented exact algorithm.

Firstly, the set of candidate points for EST is found, then the set of candidate points for FNO is extended. The symbol EST(n) is used to denote the EST of the given value of n. EST(2) is trivial. The solution consists of the line segment connecting the two given points.

EST(3) is equivalent to the Fermat Point Problem – given a triangle ΔABC, find a point F in the plane such that the total distance from the three vertices of the triangle to the point is minimum. The problem was first raised in year 1643 by the famous French mathematician Fermat, as a challenge to the Italian mathematician Torricelli. Fermat resolved the problem (Fig. 4) by:

- constructing 3 equilateral triangles (ΔBCA$'$, ΔACB$'$ and ΔABC$'$), each of which shares an edge of the given triangle;
- constructing the line segments AA$'$, BB$'$ and CC$'$, which meet at one point. If this point belongs to the ΔABC area, it will be the Fermat point.

Torricelli announced another, equivalent, solution (see Fig. 5):

- construct a point P, so that ΔBCP is an equilateral triangle which does not cut ΔABC. P is called the Torricelli substituting point of the pair of points B and C;
- construct the circumscribed circle of ΔBCP. We call the short arc BC of this circle the Torricelli arc of BC;
- if line AP will meet the Torricelli arc of BC at a point, this point will be the Fermat point.

The Torricelli solution is more useful for further solving the EST(n) problem with $n > 3$. The solution is based on the fact that for any point T lying on the Torricelli arc, the following equation holds: $|\text{TP}| = |\text{TB}| + |\text{TC}|$. There-

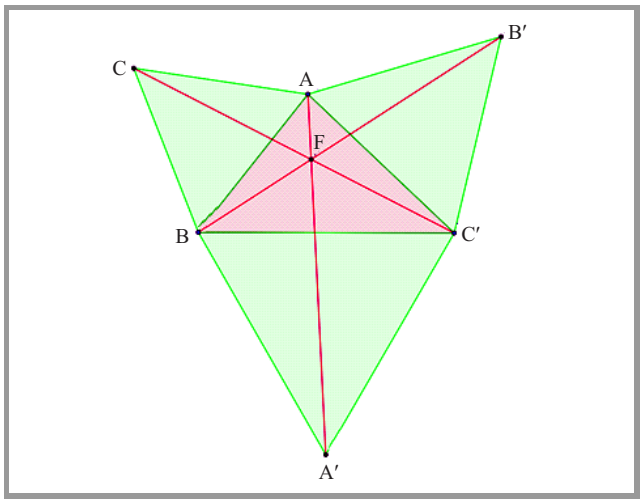


Fig. 4. Fermat Point Problem and its original solution.

fore, the sum of $|TA|+|TB|+|TC|$ will be minimized if $|TA|+|TP|$ is minimized, which will happen if T belongs on AP.

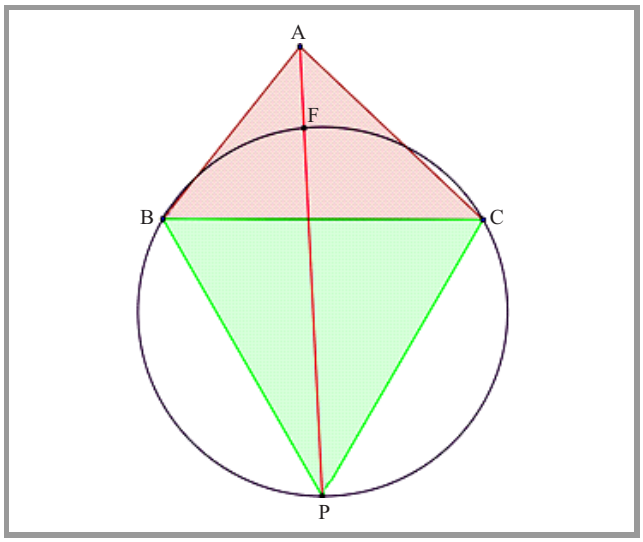


Fig. 5. Torricelli solution for Fermat Point Problem.

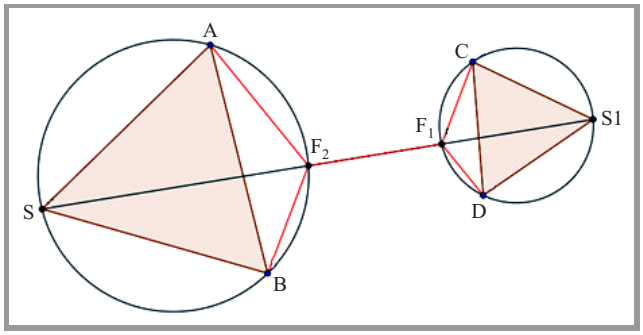


Fig. 6. Solution of EST(4).

Both Fermat and Torricelli solutions are valid only for a triangle with angles less than 120°. Otherwise, F will be the vertex of the triangle with the widest angle.

EST(4) problem can be solved as follows (Fig. 6):

- choose two points from the 4 points (the chosen points are called A and B, and the remaining points C and D);
- construct the Torricelli substituting point and Torricelli arc of A, B: S = S(A,B) and $\alpha = \alpha$(A,B);
- construct the Fermat point of C, D and S: F_1 = F(C,D,S);
- if α cuts the line segment SF_1 at F_2, then we have the EST solution consisting of AF_2, BF_2, F_1F_2, CF_1 and DF_1;
- otherwise, return to the beginning of the procedure, and choose another pair A, B. It has been proven that the solution will be found for at least one A, B pair.

The method proposed for EST(4) can be generalized for EST(n) with $n > 4$ as follows:

- choose two points from the n points (we call the chosen points A and B);
- construct the Torricelli substituting point and Torricelli arc of A, B: S = S(A,B) and $\alpha = \alpha$(A,B);
- find the solution of the EST($n-1$) problem for the set of points consisting of S and the remaining points. Let F_1 be the first point, through which S is connected to the remaining points of the EST($n-1$) solution.
- if α cuts the line segment SF_1 at F_2, then we have the solution of the EST(n) problem consisting of AF_2, BF_2, and the element of the EST($n-1$) problem solution reduced by SF_2;
- otherwise, return to the procedure beginning, and choose another pair A, B.

The given algorithm has the complexity of $O(n!)$. It has application in practice for small value of n. For large value of n, it is impossible to use this algorithm to find the EST in a sensible time. However, an essential property of the algorithm will be reused in proposed algorithm, in order to construct the set of candidate points. Thus, a candidate point should be either: the Torricelli substituting point of a pair of points, each of which is a terminal point or another candidate point, or the Fermat point of a triple of points, each of which is a terminal point or another candidate point. Another proven fact is that the number of Steiner points cannot excess $n-2$ [9].
Therefore, the set of candidate points can be generated as shown in Fig. 7.
Up to now, we have been finding the candidate points for EST. The FNO, however, has a larger set of candidate points, due to the impact of g function, described by means of a collection of g-polygons. Each g-polygon has an assigned cost value. Providing the g-polygons causes

```
procedure GenerateESTCandidates(in
  terminals; out candidates)
begin
  candidates = terminals
  n = Cardinality(terminals)
  for i=1 to n-2 do
  begin
    candidates += {set of points, each of
      which is a Torricelli substituting
      point of a pair of points in
      candidates}
    candidates += {set of points, each of
      which is a Fermat point of a triple
      of all triple of points in
      candidates}
  end
  candidates -= terminals
```

Fig. 7. Method of generating set of candidate points.

the straight line between two points to not always be the least cost line.

Let us consider a situation in Fig. 8, in which the plane is divided into two half-planes with different costs (m_1 and m_2). The goal is to find the lowest-cost line that connects two points A and B belonging to the two half-planes.

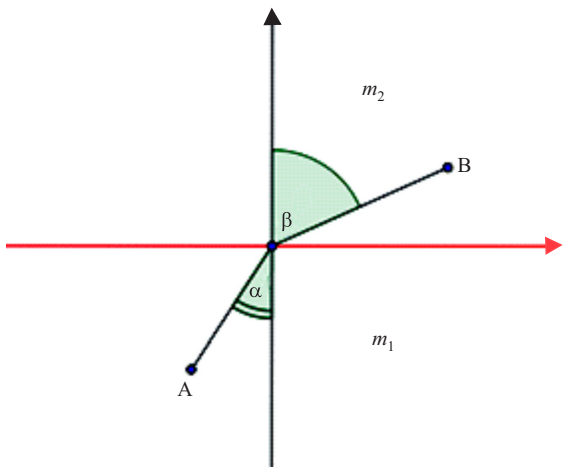


Fig. 8. Fermat Principle.

According to Fermat Principle, the line with lowest cost is the two-segment polyline A-O-B, where O belongs to the interface between the two half-planes and fulfills following condition:

$$\frac{\sin\alpha}{\sin\beta} = \frac{m_1}{m_2}. \tag{3}$$

The Fermat Principle has wide applications in physics; among others, it explains the phenomenon of light refraction. The point O is called the refraction point of A, B through the interface line.

In FNO, the Fermat Principle allows for finding a new subset of candidate points, each of which is the refraction point of a pair of other candidate points through an edge of a g-polygon. Taking refraction points into consideration, the candidate points of FNO can be generated by means of procedure shown in Fig. 9.

```
procedure GenerateFNOCandidates(in sources,
  destinations, g-polygons; out candidates)
begin
  candidates = sources + destinations +
    {set of vertices of the g-polygons}
  n = Cardinality(sources + destinations)
  for i=1 to n-2 do
  begin
    candidates += {set of points, each of
      which is the Torricelli substituting
      point of a pair of points in
      candidates}
    candidates += {set of points, each of
      which is the Fermat point of a triple
      of all triple of points in
      candidates}
    candidates += {set of points, each of
      which is the refraction point of a
      pair of points in candidates through
      an edge of a g-polygon}
  end
  candidates -= sources + destinations;
end
```

Fig. 9. Generating procedure of NFO candidate points.

The cardinality of the set of the candidate points grows according to $O\big((n+m)^{3n}\big)$, where n is the total number of source and destination points, whilst m is the total number of the g-polygons vertices.

4.2. Transformation of FNO into ILP

In FNO problem, let K denote the set of candidate point generated for S, D and the given g-polygons. Let V denote the sum of S, D, T_1 and K.

For each pair of $u, v \in V$ a binary variable $x_{uv} \in \{0,1\}$ is defined. In addition the cost of the line segment u-v is calculated by means of the given cost density function g:

$$c_{uv} = \int_{r=0}^{1} g\big((1-r)u + rv\big)\mathrm{d}r. \tag{4}$$

Because the exact algorithm is not the main goal of this work, the author leaves the capacity constraints to future work.

The FNO problem can be transferred into ILP format, denoted by ILP_FNO(V, S, D, c), as follows:

Minimize

$$\sum_{u,v\in V} c_{uv}x_{uv}$$

Subject to:

$$\sum_{u\in M, v\in V\setminus M} x_{uv} \geq 1$$

for each set $M \subset V$, $M \cap S \neq \emptyset$ and $V\setminus M \cap D \neq \emptyset$.

ILP_FNO can be resolved by means of an integer linear programming package. Furthermore, ILP_FNO has a very similar form to the ILP of the TST problem [14]. In particular, the ILP_FNO into the ILP form of TST is derived by creating an artificial "super source node" connected to all

nodes of S by artificial links with zero cost. Hence, the algorithms proposed for TST to find the exact or approximate result of ILP_FNO can be reused.

For a FNO instance presented in Fig. 10 (Example 1), with the only g-polygon is the brown triangle with assigned cost = 2, the exact algorithm provides the optimal result presented by the bold polylines: AS_2, BS_3, CS_1, S_1S_2, S_1S_3, with the total cost = 10.59. If the g-polygon was not considered in the algorithm, the total cost would be 10.96 (3.5% more expensive).

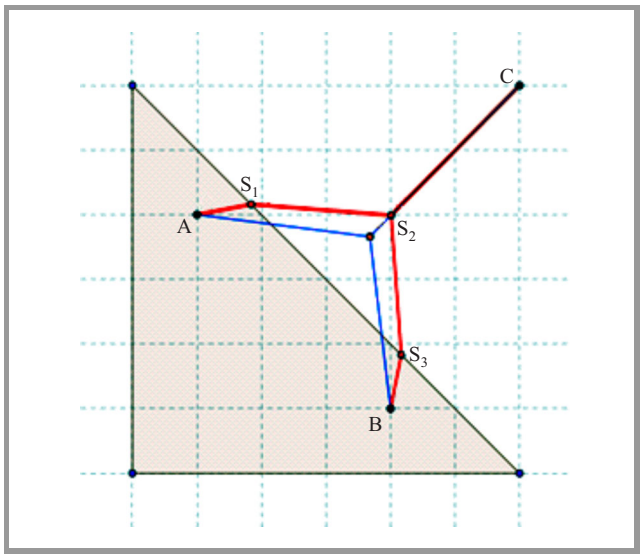


Fig. 10. FNO instance resolved by exact algorithm.

Since the FNO problem is NP-hard, the exact algorithm allows to find exact solutions only for small instances of FNO. The algorithm has been developed and conducted performance tests, which have shown that for typical configurations of the computer systems used by FTTH network planners, it is possible to apply the exact algorithm for a network with less 10 users. This limitation is unacceptable in practice, since a typical FTTH network is to serve several hundred users.

5. Approximation Algorithm for FNO

In the previous section, the mathematical properties of the EST have been applied in order to find the candidate points for optimization. This approach allows for finding the exact optimal solution, but due to the enormous cardinality of the candidate points set, it is impossible to use it for a larger instance of FNO in a sensible time. However, parts of the work on the exact algorithm can be reapplied in construction the approximation algorithm.

5.1. Approximation Algorithm Strategy

In the approximation algorithm, instead of starting already with the full set of candidate points, as the exact algorithm, the author starts the algorithm with a basic candi-

```
procedure CalculateCostVector
(in candidates; out cost_vector)
begin
  foreach v1,v2 in candidates do
  begin
    cost_vector[v1,v2] = the cost of
      the g-polygons containing v1 and v2.
  end
end

procedure CalculateILP_FNO(in candidates,
  sources, destinations, cost_vector; out
  steiner_points, steiner_lines)
begin
  Resolve the ILP by means of CPLEX, MS
  Solver, or Steiner algorithms
end

procedure FNO_Main(in PEC, LVR; in sources,
  destinations, existingTransits,
  g-polygons; out steiner_points,
  steiner_lines)
begin
  candidates = sources + destinations +
    existingTransits + vertices(g-polygons)
  for i=1 to PEC do
  begin
    foreach a, b in candidates do
    begin
      if a, b belongs to different
        g-polypons then
      begin
        Construct the cut points of line
          segment (a,b) with the
          g-polygons. Call them x1, x2, ..
          xn
        candidates += {x1, x2, .. xn}
      end
    end

    for j=1 to LVR do
    begin
      foreach a, b, c in candidates do
      begin
        if a, b, c belong to the same
          g-polygon then
        begin
          Construct the Fermat point for
            the triple a, b, c. Call it f
          candidates += {f}
        end
      end
    end

    cost_vector =
      CalculateCostVector(candidates)
    CalculateILP_FNO(candidates, sources,
      destinations, cost_vector,
      steiner_points, steiner_lines)
    foreach s in steiner_points do
    begin
      if s belongs to the boundary of a
        g-polygon then
      begin
        Find the nearest (clockwise and
          anti-clockwise) candidate
          points to s in the g-polygon
          boundary: v1 and v2

        Establish the midpoints of line
          segments: v1-s and
          v2-s and call them x1 and x2
        candidates += {x1,x2}
      end
    end
  end
end
```

Fig. 11. Algorithm details.

date point set consisting only of given points: the sources, destinations, existing transit points and the vertices of the g-polygons. After resolving the ILP_FNO for those points, the result will be improved in iterations. In each iteration, new points are added to the candidate point set. The number of the iterations is preset by means of the algorithm configuration parameters.
The main configuration parameters of the algorithm are:

- **Loose Vertices Resolution (LVR)** – the number of iterations, in each of which we find the Fermat point for each triple of candidate points lying on the same g-polygon. This way, we can locally improve the solution quality;
- **Polygon Edge Cut (PEC)** – the number of iterations, in each of which we find the quasi-refraction points and add them to the set of candidate points.

For the ILP_FNO implementation, beside using the commercial optimization packages, the author also created his own algorithm based on the known algorithms for the TST) [14]–[16].
The details of the algorithm are presented in Fig. 11.
The complexity of the approximation algorithm is $O(n^4) \cdot PEC \cdot LVR + S(n^{4 \cdot PEC}) \cdot PEC$, where n is the cardinality of the starting candidate point set (consist of S, D and the g-polygon vertices), and $S(k)$ is the complexity of the algorithm that resolve the TST problem for a k-element graph.

6. FNO Algorithm Evaluation

6.1. Comparison with Exact Algorithm

In order to compare the results of the approximation and exact algorithms, the FNO instance in Example 1, which has been resolved by the exact algorithm (Fig. 8) is considered. The approximation algorithm operates as follows:

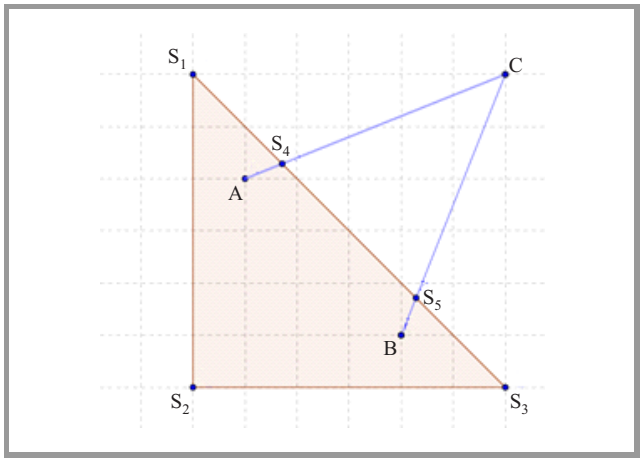


Fig. 12. Approximate algorithm for Example 1 (step 2).

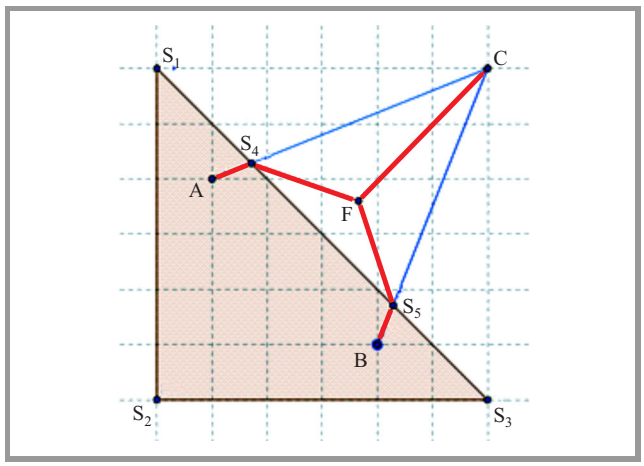


Fig. 13. Approximate algorithm for Example 1 (step 4).

1. It starts with the basic candidate points A, B, C (the given points), S_1, S_2 and S_3 (the vertices of the g-polygon).
2. Next, we add to the candidate point set the cut points of AC and AB with the boundary of the g-polygon: S_4 and S_5 (Fig. 12).
3. The Fermat point of all point triples that belong to the same g-polygon is constructed. In this example, the most interesting is the Fermat point of (C, S_4 and S_5).
4. The ILT_FNO for (A, B, C, F, $S_1, \ldots, S_5$) is resolved. The result is the red (bold) polyline presented in Fig. 13.
5. The midpoints of the line segments of the candidate points belonging to the g-polygon edges (S_1S_4, S_4S_5, etc.) is constructed. The constructed midpoints are treated as the quasi-refraction points, and added to the candidate point set.
6. The PEC is decreased by one, and repeat step 2 until PEC is zero.

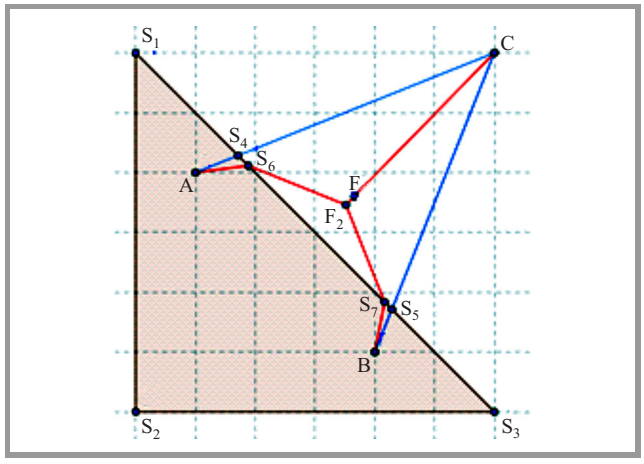


Fig. 14. Approximate algorithm for Example 1 (final result).

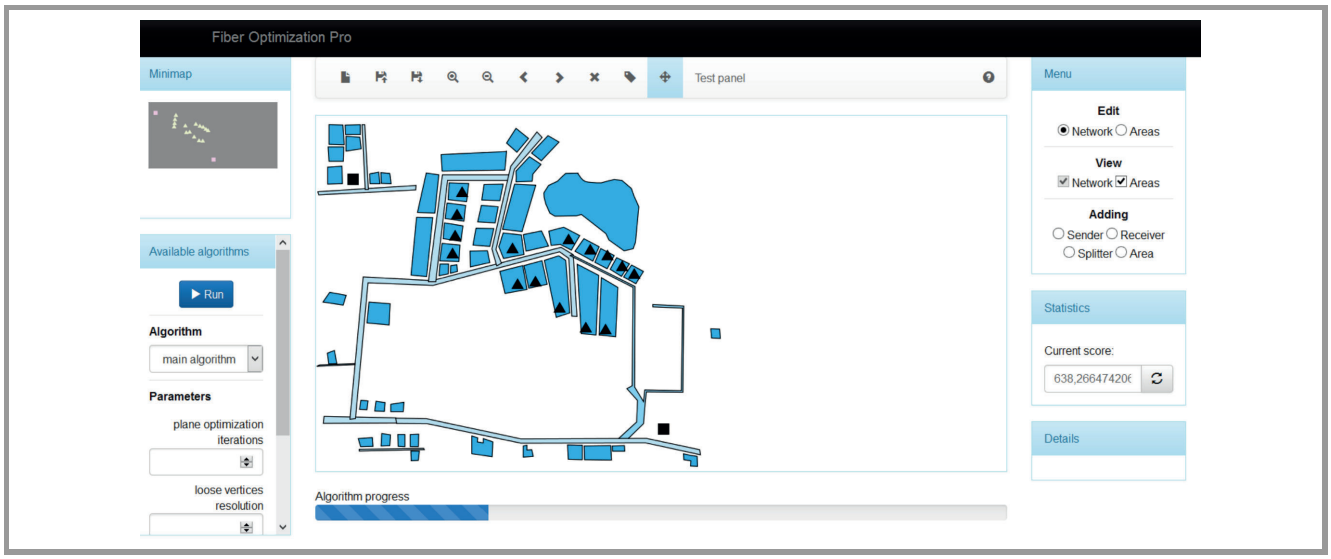


Fig. 15. FNO testing Web application – main page.

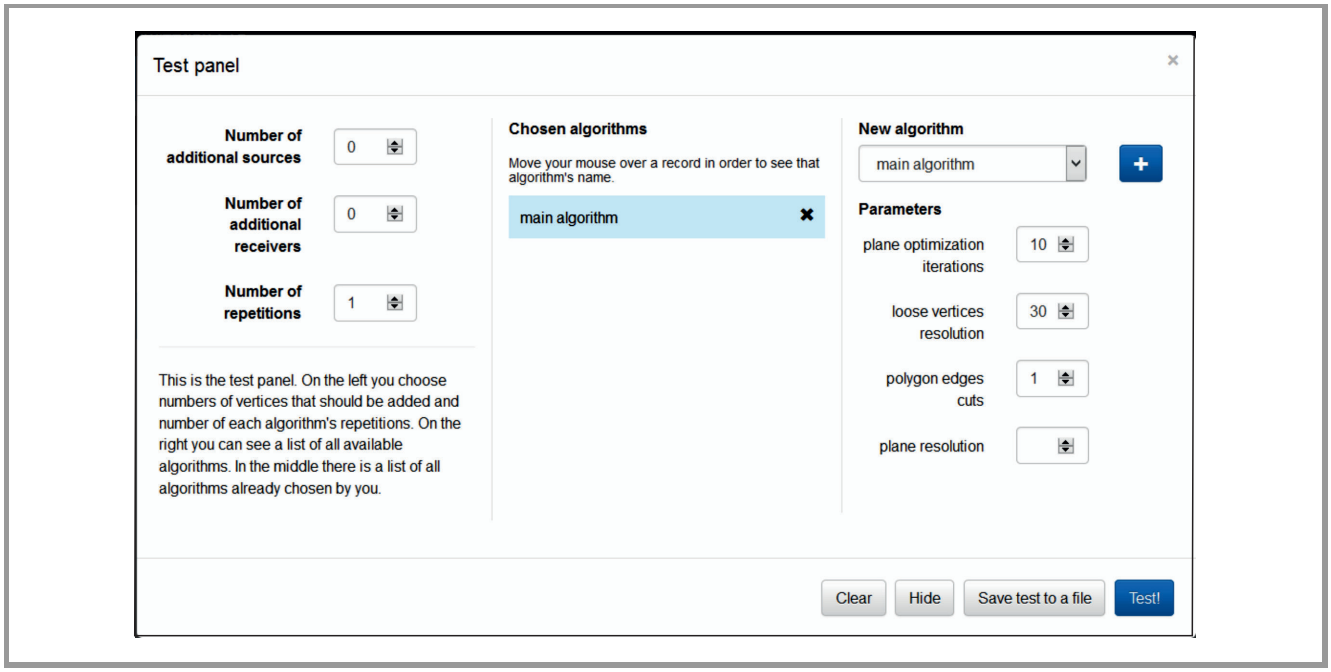


Fig. 16. FNO testing Web application – mass test panel.

The final result for PEC = 20 is presented in Fig. 14. It is very close to the exact algorithm result (0,001% cost difference).

6.2. Analysis of Algorithm Performance in Practical Example

In order to evaluate the effectiveness of the algorithm, the author has developed it in a .net C# program (Fig. 15). The program has been run in a PC based on Intel Core i5 2.66 GHz and 8 GB RAM.

The Web application includes a test panel that allows for mass testing of the algorithm problem for different values of configuration parameters PEC and LVR (Fig. 16).

In order to explain how the configuration parameters impact the result quality and the time consumption, let us consider an FNO instance (Example 2), in which we have 1 source (the square symbol), 3 destinations (triangles) to be connected through 3 high-cost polygons.

For PEC = 1 and LVR = 1 (Fig. 17), the cost is quite high (644.9) but the algorithm runs exceptionally fast (0.7 s duration).

When LVR is increased to 10 (Fig. 18), the cost is improved significantly (638.3). However, the algorithm runs slower (6 s), though the duration is still acceptable (near real-time).

Additional increasing LVR up to 20 (Fig. 19), causes minimal cost improvement (638.2). However, the algorithm

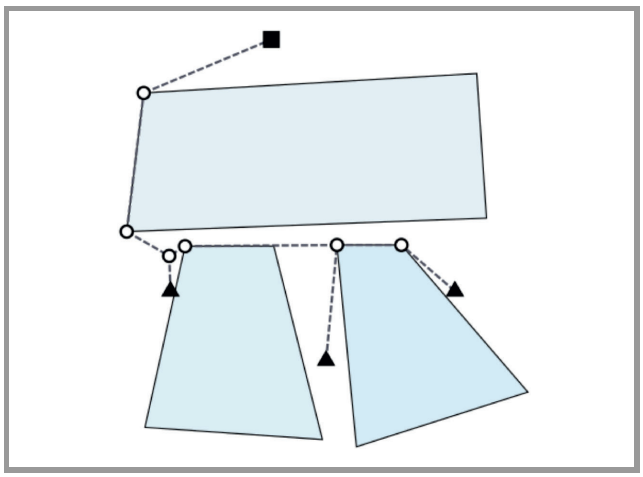


Fig. 17. Algorithm result for Example 2, PEC = 1, LVR = 1, cost = 644.9.

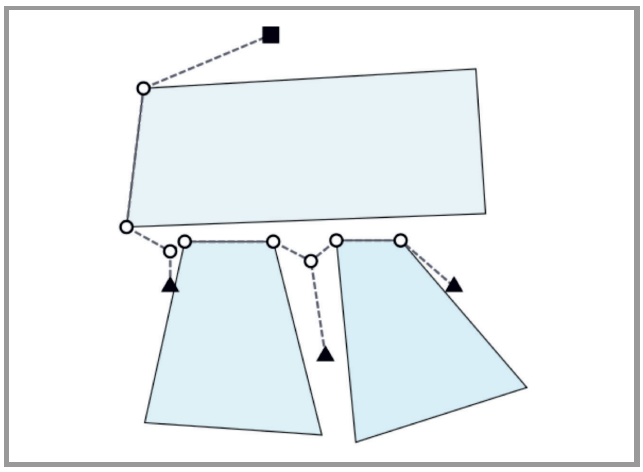


Fig. 18. Algorithm result for Example 2, PEC = 1, LVR = 10, cost = 638.3.

runs much slower (374 s), and the duration is unacceptable for a network design tool.

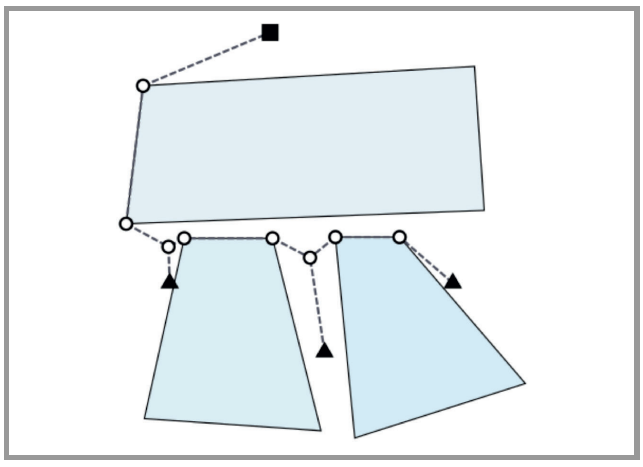


Fig. 19. Algorithm result for Example 2, PEC = 1, LVR = 20, cost = 638.2.

More detailed impact analysis of the configuration parameters PEC and LVR on the algorithm operation has been conducted by means of the mass testing on a practical example of FTTH network optimization for a housing estate in Warsaw (Example 3, Fig. 20). The mass testing relies on running the algorithm multiple times, changing the configuration parameters for each iteration.

In Fig. 21, the tendency regarding the result quality when PEC and LVR increase is presented. It can be observed that increasing LVR from 0 to 1 causes significant improvement of the result quality. Increasing LVR from 1 to 2 gives only modest improvement, whilst further increment of this parameter does not causes any noticeable effect. This tendency is logical, because parameter LVR only decides on local improvement of the algorithm result relying on finding the Fermat points.

The PEC impact on the algorithm is different. The author has observed that, a number of iteration is needed (PEC = 20 for LVR = 0 and PEC = 7 for LVR = 1), in order to gain a significant improvement of the result quality. This tendency is logical, because parameter PEC decides on the cardinality of the set of candidates points, whilst the algorithm needs the set large enough in order to return the converging the optimum.

The performance of the algorithm is presented in Fig. 22. It can be observed that each increment of LVR causes a significant growth of operation time, whilst the LVR rise causes rather modest increment of operation time.

The conclusion of mass testing analysis is that in practical situation, it is recommended to run the algorithm with LVR to be 1, 2 or 3, whilst PEC should be set to be as large as possible. The mass testing analysis confirms that, although the algorithm does not guarantee the ideal solution, it allows for finding the solution closed to the optimum. This allows the algorithm to be applied in computer systems used by FTTH network planners.

7. Conclusion

In the paper, a new method for FTTH optimization focused on minimizing the cost of cable installation is presented. This method is a development of the previous work result on geometric optimization. The author added new aspects not considered in previous work, in particular geographical aspect and the aspect of existing network resources.

The optimization problem FTTH has been formulated as a mathematical problem called FTTH Network Optimization (FNO). FNO problem has been transformed into an Integer Linear Programming. Since FNO problem is NP-hard, its exact algorithm allows to find optimal solutions only for small FNO instances (for less than ten end-users). The algorithm has been developed and performance tests were conducted, which have shown that for typical configurations of the computer systems used by FTTH network planners, it is possible to apply the exact algorithm for a network with less than 10 users. This limitation is un-

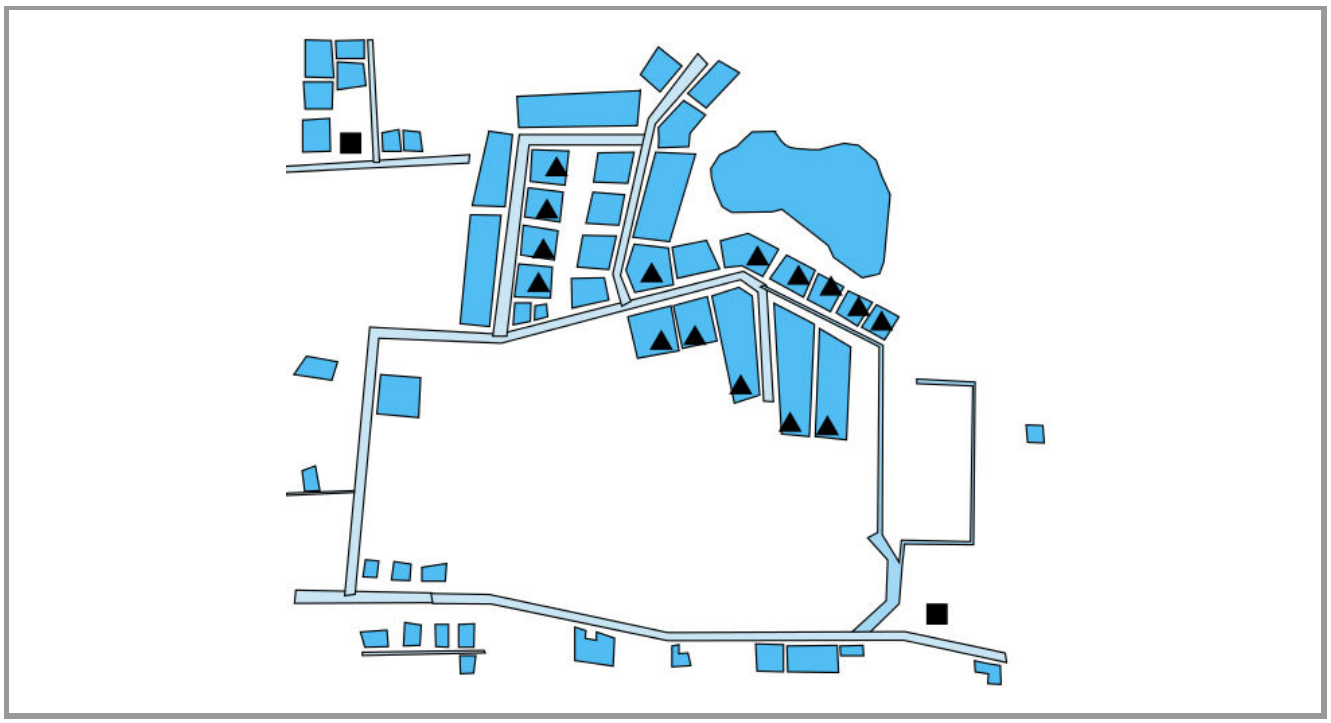


Fig. 20. Example 3, testing for housing estate in Warsaw.

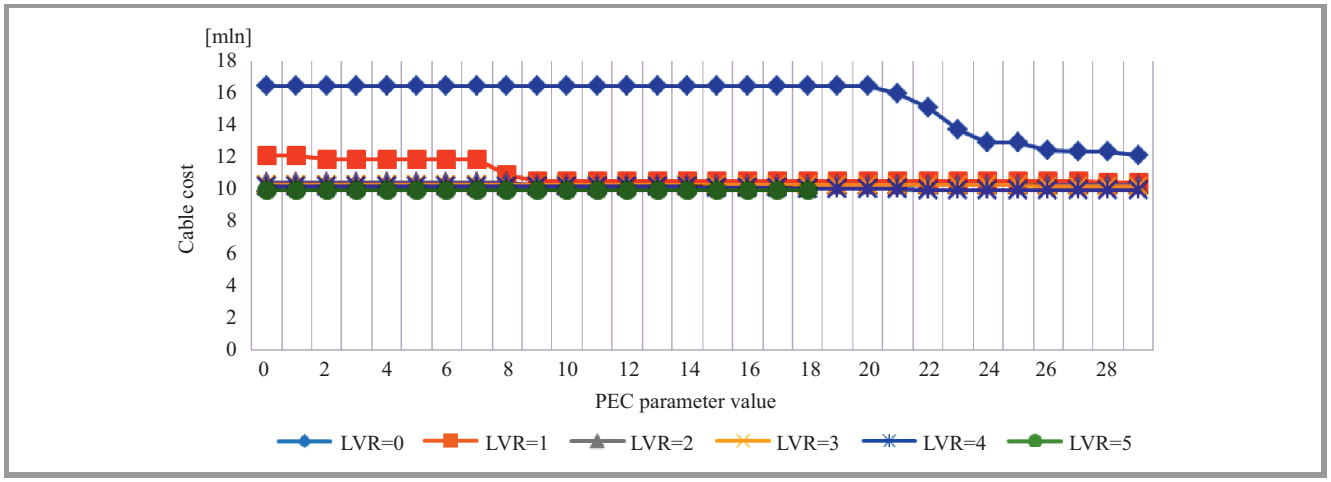


Fig. 21. Result quality dependence on parameters PEC and LVR for Example 3.

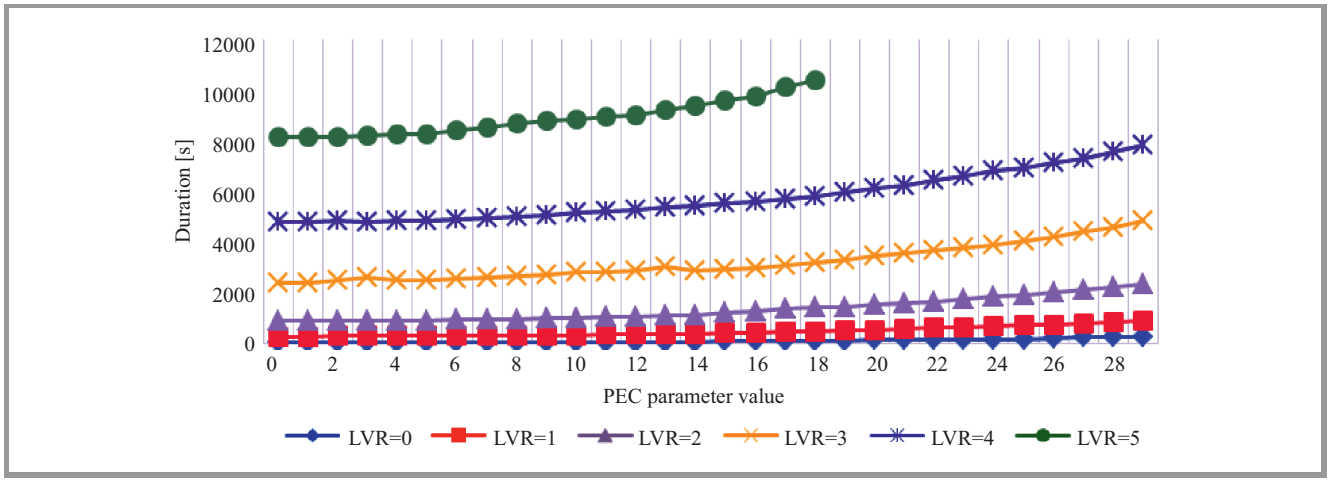


Fig. 22. Performance dependence on parameters PEC and LVR for Example 3.

acceptable in practice, since a typical FTTH network is to serve several hundred users.
Therefore, for larger FNO instances, an approximation algorithm have been proposed. Although the algorithm does not guarantee the ideal solution, it allows for finding the solution closed to optimum. The algorithm computation complexity is polynomial. It can be applied in typical computer systems used by FTTH network planners.
In the paper, the approximation algorithm has been described. In order to confirm its performance in practice, the author has developed the algorithm in a .net C# program. In order to verify the result quality and evaluate the impact of the algorithm configuration parameters, the mass testing on a practical example was conducted. As a conclusion after analyzing the test results, the recommendation for algorithm usage in practice has been presented.

References

[1] B. Williams, "FTTH council global alliance updates", in *Proc. 2013 FTTH LATAM Ann. Conf.*, Sao Paulo, Brazil, 2013.

[2] B. Deutsch, R. Whitman, and C. Mazzali, "Optimization of FTTH passive optical networks continues", *Lightwave Mag.*, Jan. 2005 [Online]. Available: http://www.lightwaveonline.com/articles/2005/01/optimization-of-ftth-passive-optical-networks-continues-53911092.html

[3] M. Chardy and C. Hervet, "FTTH network design under OA&M constraints", in *Proc. 5th Int. Conf. on Netw. Optimiz. INOC'11*, Hamburg, Germany, 2011, pp. 98–104.

[4] S. van Loggerenberg, L. Grobler, and F. Terblanche, "Optimization of PON planning for FTTH deployment based on coverage", in *Proc. Southern African Telecommun. and Netw. Access Conf. SATNAC 2012*, Fancourt in George, Sth. Africa, 2012.

[5] M. Grötschel, C. Raack, and A. Werner, "Towards optimizing the deployment of optical access networks", *EURO J. Comput. Optimiz.*, vol. 2, no. 1–2, 2013.

[6] M. Chardy, M.-C. Costa, A. Faye, and M. Trampont, "Optimizing splitter and fiber location in a multilevel optical FTTH network", *Eur. J. Operat. Res.*, vol. 222, no. 3, 2012.

[7] C. Hervet, A. Faye, M. Costa, M. Chardy, and S. Francfort, "Solving the two-stage robust FTTH network design problem under demand uncertainty", *Elec. Notes in Discrete Mathem.*, vol. 41, 2013.

[8] D. Kadhim and N. Hussain, "Link and cost optimization of FTTH network implementation through GPON technology", *Commun. and Netw.*, vol. 5, 2013.

[9] M. Brazil, "On the history of the Euclidean Steiner tree problem", *Archive for History of Exact Sciences*, vol. 68, no. 3, 2014.

[10] S. Arora, "Polynomial time approximation schemes for Euclidean traveling salesman and other geometric problems", *J. of the ACM*, vol. 45, no. 5, 1998.

[11] L. Chung-Wei *et al.*, "Efficient obstacle-avoiding rectilinear Steiner tree construction", in *Proc. Int. Symp. on Physical Design ISPD'07*, Austin, TX, USA, 2007.

[12] M. Zachariasen and P. Winter, "Obstacle-avoiding Euclidean Steiner trees in the plane: an exact algorithm", in *Algorithm Engineering and Experimentation*, M. T. Goodrich, C. C. McGeoch, Eds., *LNCS*, vol. 1619, pp. 286–299. Springer, 1999.

[13] M. Garey, "The complexity of computing Steiner minimal trees", *SIAM J. of Appl. Mathem.*, vol. 32, no. 4, 1977.

[14] J. W. Van Laarhoven. "Exact and heuristic algorithms for the Euclidean Steiner tree problem", PhD thesis, University of Iowa, 2010.

[15] K. Mehlhorn. "A faster approximation algorithm for the Steiner problem in graphs", *Inform. Process. Lett.*, vol. 27, no. 3, 1988.

[16] V. V. Vazirani, *Approximation Algorithms*. Berlin: Springer, 2001.

Hoang Nghia Le received his M.Sc. degree from Warsaw University of Technology, Faculty of Electronics and Information Technology, Institute of Telecommunications in 1998. Currently he is a product manager at Suntech S.A., a software company specialized in producing OSS (Operations Support Systems) for telecommunication networks. His scientific interests cover optimization issues in optical and wireless networks.
E-mail: NghiaLe.Hoang@suntech.pl
Suntech S.A.
Puławska st 107
02-595 Warsaw, Poland

Paper

Efficient Performance and Lower Complexity of Error Control Schemes for WPAN Bluetooth Networks

M. A. M. El-Bendary and M. A. R. El-Tokhy

Faculty of Industrial Education, Helwan University, Helwan, Egypt

Abstract—This paper presents a new technique of reduction retransmission time by decreasing the discarded packets and combating the complexity through error control techniques. The work is based on Bluetooth, one of the most common Wireless Personal Area Network. Its early versions employ an expurgated Hamming code for error correction. In this paper, a new packet format using different error correction coding scheme and new formats for the EDR Bluetooth packets are presented. A study for the Packet Error Probability of classic and Enhanced Data Rate (EDR) packets is also presented to indicate the performance. The simulation experiments are performed over Additive White Gaussian Noise (AWGN) and Rayleigh flat-fading channels. The experimental results reveal that the proposed coding scheme for EDR packets enhances the power efficiency of the Bluetooth system and reduce the losses of EDR packets.

Keywords—Bluetooth, EDR, packet loss, power efficiency, Wireless Personal Area Network.

1. Introduction

Bluetooth is a short-range radio communication technology specified in the IEEE 802.15.1 standard, which evolved as a wireless alternative to cable connections [1]. It provides a universal wireless interface for different devices to communicate with one to another. The low cost of implementation and low power of Bluetooth systems have fueled popularity this technology, which has emerged as a good solution to form Wireless Personal Area Networks (WPANs) [2].

Bluetooth operates in the Industrial Scientific Medical (ISM) 2.4 GHz band with Frequency Hopping Spread Spectrum (FHSS) modulation to avoid interferences caused by other wireless technologies, i.e., IEEE 802.11b-g, IEEE 802.15.4 [3] or cordless telephones. The Bluetooth supports industrial specifications for WPANs [4], where it provides wireless media to connect and exchange information between devices.

Bluetooth employs variable-size packets occupying different numbers of 625 μs time-slots up to a maximum of five. There are several types of packets, which are chosen according to the channel conditions. Big packets increase the throughput of the system and are used with good conditions. For bad channel conditions, small packets are used, which decreases the throughput.

Bluetooth 2.1 has introduced the EDR packets types using Differential Phase Shift Keying (DPSK) modulation [5] and supports 2–3 Mbit/s air rates of through π/4-DQPSK and 8-DPSK modulation formats [6]–[8].

The performance of classic Bluetooth packets with expurgated Hamming (15, 10) code was analyzed in [9]. The concept of Forward Error Correction (FEC) bearing Data Medium (DM) packets for EDR was proposed in [10].

In this paper, the authors investigate the performance of EDR Bluetooth packets with the Hamming (15, 10) code and different error controls, i.e. convolutional codes. The Packet Error Probability (PEP) of classic and EDR Bluetooth are analytically presented. $2DM_1$ and $2DM_5$ packets are employed in presented simulations, carried out over AWGN and Rayleigh flat-fading channels [11].

This paper is organized as follows. In Section 2, the Bluetooth system is described. Section 3 highlights the issue of channel coding in Bluetooth. In Section 4, the Packet Error Probability is discussed. The proposed modifications are presented in Section 5. The simulation and the results are introduced in Section 6. The computational complexity is discussed in Section 7. Finally, the paper is concluded in Section 8.

2. Bluetooth System

The Bluetooth standard encompasses two types of links: Synchronous Connection Oriented (SCO) and Asynchronous Connection Less (ACL). SCO are aimed for transmitting real-time signals, which is delay-sensitive, i.e. voice. ACL links are intended for transmitting asynchronous data traffic (file transfer). The recent versions introduced a different packet format [12], i.e. Bluetooth v2.1+EDR add a number of ACL formats to the basic rate packets. Generally, the Bluetooth packet contains three main fields: access code (AC), header (HD), and payload (PL). AC identifies the packets exchanged within a piconet, with unique access code and used to synchronize the slaves in a piconet to its master [13]. The main function of HD is to determine an individual slave address in the piconet by Logical Transport-Address (LT_ADDR). The last field of the Bluetooth packet is the payload [14].

EDR achieves higher data throughput by using Phase Shift Keying (PSK) modulation, instead of Gaussian Frequency Shift Keying (GFSK). PSK is used in EDR packets for payloads field only, the rest of EDR packets still use GFSK in headers (AC and HD fields). This papers focus on Asyn-

chronous Connectionless Link packets, and its types: DM_x, DHM_x, and EDR DHM_x. The M refers to medium data rate, while H to high data rate. The symbol x denotes the number of time slots between two hops used in the frequency hopping system [15]. It takes value 1, 3, 5 referring to 1, 3, or 5 time slots between consecutive frequency hops. Always DMM_x are coded and DHx are uncoded.

3. Channel Coding in Bluetooth

To protect data in wireless communication against errors channel coding is required. There are implemented several channel coding schemes using data payload to reduce retransmission times [16]. There are three types of error control coding systems: rate 1/3 error control code, rate 2/3 error control code, and ARQ (Automatic Repeat Request). Research concentrates on varying PL field coding schemes, which means dividing the payload between data and checksum.

The performance of classic Bluetooth packets with the expurgated Hamming (15, 10) code have been analyzed in many papers [15]. The most appreciable work in the coding of the payload field and EDR was introduced by Galli *et al*. and Ling *et al*. in [17]. The authors of [14] proposed other error control codes for improving performance such as convolutional codes. They improved the performance but reduced the PL field length. The propositions of Forward Error Control (FEC) bearing DM packets for EDR were proposed in Chen [12]. In [13] the improvements of EDR packets through FEC and interleaved FEC were investigated. In the same manner, all proposed cases improved the performance with throughput reduction.

4. Packet Error Probability

The throughput performance is affected by the PEP, which is related to packet size as [8]:

$$PEP = 1-(1-P_b)^L \tag{1}$$

$$P_b = \frac{1}{2}\left(1-\sqrt{\frac{E_b/N_o}{1+E_b/N_o}}\right) \cong \frac{1}{4E_b/N_0},$$

where P_b is Bit Error Probability (BEP) of single bit and L stands for packet length.

PEP value is decreased on low packet sizes. In the following analysis, the perfect interleaved channel is assumed for independent error over wireless channel. Eq. (1) gives PEP of uncoded packets. In the case of encoded packets, the PEP equation is [9]:

$$PEP_{FEC} = 1-(1-P_{CW})^{Nc}, \tag{2}$$

where PEP_{FEC} is packet error probability of encoded packet, P_{CW} is the codeword error probability and Nc is the number of codeword in the packet.

The codeword error probability is a function of BEP, the number of correctable error t, and the length of codeword N_b. It can be expressed as

$$P_{CW} = \sum_{n=t+1}^{N_b} \binom{N_b}{n} P_b^n (1-P_b)^{N_b-n}. \tag{3}$$

The Bluetooth classic and EDR packet contains three main fields: access code, header and payload. Therefore, the encoded and uncoded PEP is given by:

$$PEP_{BT} = 1-(1-P_{AC})(1-P_{HD})(1-P_{PL}), \tag{4}$$

where P_{AC} is the access code error probability, P_{HD} stands for header error probability and P_{PL} is the payload error probability.

The AC and HD fields are encoded by BCH (64, 30) code and repetition (3, 1) code. P_{ecw}, and P_{HD} are given by Eqs. (5)–(7) [7], [14]:

$$P^{AC} = \sum_{i=7}^{64} \binom{64}{i} P_b^i (1-P_b)^{64-i}, \tag{5}$$

$$P_{ecw}^{HD} = \sum_{i=3}^{3} \binom{3}{i} P_b^i (1-P_b)^{3-i}, \tag{6}$$

$$P_{HD} = 1-(1-P_{HDW})^{18}. \tag{7}$$

The last field in Bluetooth packets is the payload. There are two types of PL: uncoded and encoded.

4.1. Classic Bluetooth Encoded Packets

The error probability for classic encoded Bluetooth packets is described in [9]. These packets are encoded by expurgated Hamming code (15, 10). The codeword error probability can be expressed as

$$p_{ecw}^{PL} = \sum_{i=2}^{15} \binom{15}{i} p_b^i (1-p_b)^{15-i}. \tag{8}$$

Then the probability of encoded payloads is

$$P_{PLm} = 1-(1-P_{PLW})^m, \tag{9}$$

where $m = 16, 100, 183$ for the DM_1, DM_1, and DM_5 packets, respectively.

$$P_{BT_{coded}} = 1-(1-P_{AC})(1-P_{HD})(1-P_{PLm}). \tag{10}$$

4.2. Classic Bluetooth Uncoded Packets

DH are uncoded Bluetooth packets. Its payloads are transmitted without FEC. The PEP of these packets is given by

$$P_{PL_{uncoded}} = 1-(1-P_b)^L, \tag{11}$$

where L is the length of uncoded payloads and $L = 240$, $1500, 2745$ for the DH_1, DH_3, and DH_5 packets, respectively. Then the uncoded classic Bluetooth packets error probability $P_{BT_{uncoded}}$ can be expressed as

$$P_{BT_{uncoded}} = 1-(1-P_{AC})(1-P_{HD})(1-P_{PL_{uncoded}}). \tag{12}$$

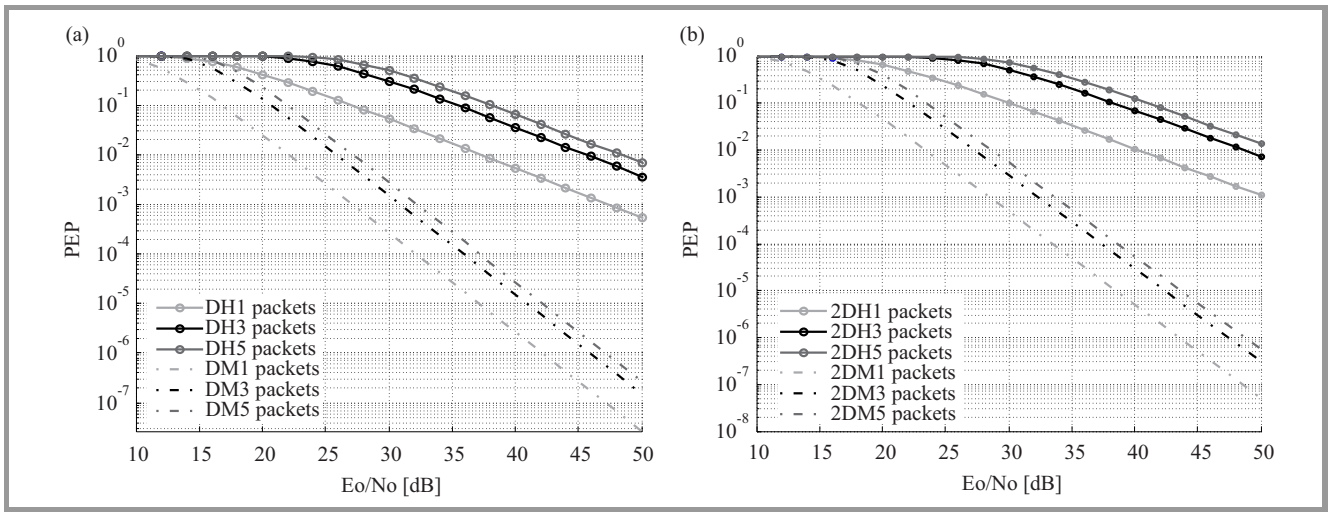


Fig. 1. PEP versus E_b/N_o of DHM_x and DMM_x packets over fading channel: (a) classic Bluetooth and (b) EDR.

Figure 1a gives the PEP versus Eb/No parameter for classic packets and Fig. 1b relates to EDR DHM_x and DMM_x packets. As shown the encoded packets performs better than uncoded ones. The PEP of the EDR packets is higher than the PEP of classic packets for the same E_b/N_o.

4.3. Uncoded EDR Packets

The PEP of EDR packets is given by Eq. (13). The difference is the last term $P_{PL_{uncoded}}$, which is affected by the length of payloads.

$$P_{PL_{EDR-uncoded}} = 1-(1-P_b)^{L_{EDR}}, \tag{13}$$

where $P_{PLE_{EDR-uncoded}}$ is PEP of EDR payloads, P_b is Bit Error Probability and L_{EDR} is the length of EDR payloads. The PEP of EDR Bluetooth packets can be expressed as

$$P_{BT_{uncoded}} = 1-(1-P_{AC})(1-P_{HD})(1-P_{PL_{EDR-uncoded}}). \tag{14}$$

4.4. Encoded EDR Packets

DM packets are encoded packets in classic Bluetooth using FEC schemes, called $2DMM_1$, $2DMM_3$, and $2DMM_5$ [18]. The PEP of encoded EDR packets can be expressed as Eqs. (9)–(10). The difference in PEP of classic Bluetooth packets and encoded EDR ones is the number of codeword in the packets with using the same FEC scheme [19].
It can be concluded from the previous studying that the EDR long packets performance is degraded than the classic ones. Several of papers proposed different error control schemes such as convolutional codes. Its complexity increases with the length of packet. Splitting packet or segmented packet format can decrease the complexity and enhance the EDR performance.

5. Proposed Modifications

This section proposes the usage of different schemes, the use of error correction schemes in Bluetooth EDR packets and investigates the effect of segmentation of EDR packets using expurgated Hamming (15, 10) code for encoding PL_1 field 1 and convolutional code (1, 2, and $K = 3$) for PL_2 [16].
Figure 2 shows the proposed packet format called segmented encoded EDR packets. The proposition depends on using error control for reduction the number of dropped packets and leads to reduce the retransmission requirements.

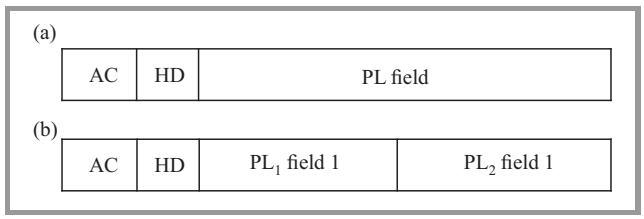


Fig. 2. Bluetooth packet contents: (a) standard format and (b) the proposed segmented encoded EDR packets.

There are two motivations for presenting the proposed technique of packet splitting. The EDR packets performance is much degraded compared to the classic version, and therefore, this work shows the error control schemes of classic packets for EDR with its evaluation. Also, the FEC utilizing causes more complexity to the data transmitting and receiving process especially with the complex encoding and decoding. Then the second motivation is decreasing the complexity of FEC scheme (convolutional codes) through reducing the input data length (processed data). It is worth to note that the complexity of convolutional codes is proportional to the number of input bit streams.

6. Simulation and Results

The Monte Carlo simulation method is used in the simulation experiments to compare between the traditional expurgated Hamming (15, 10) code used in the standard Blue-

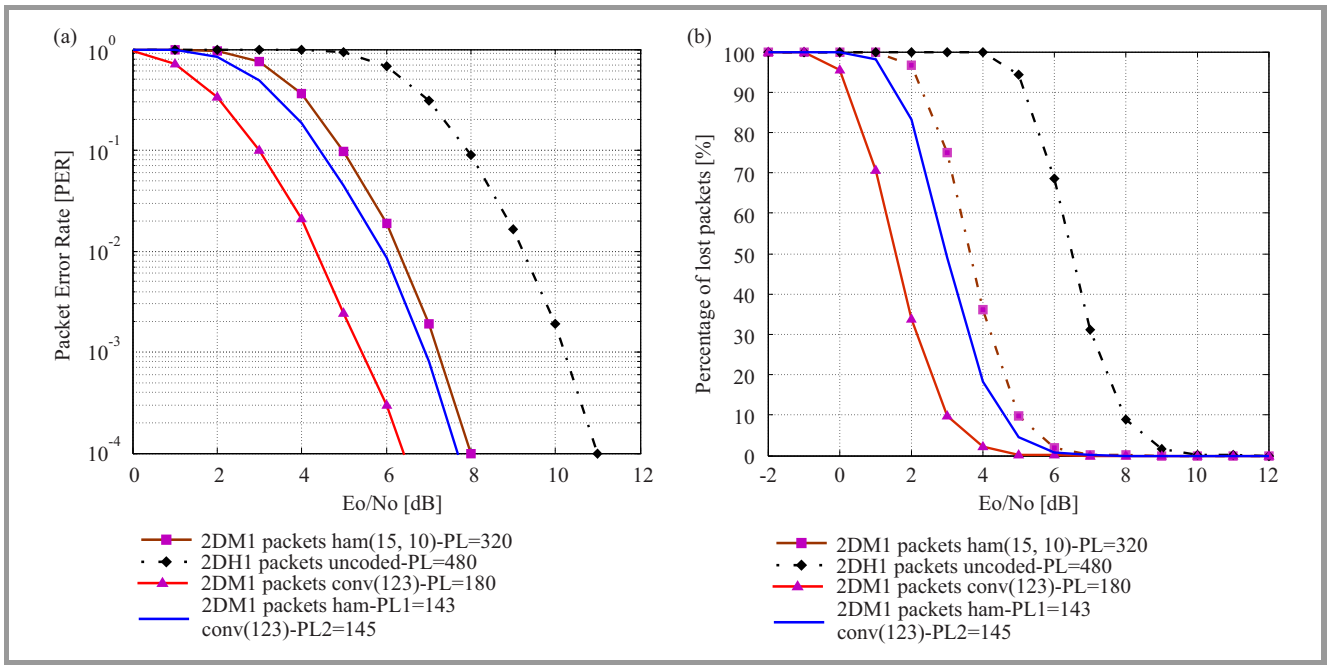


Fig. 3. (a) PER and (b) NLP versus E_b/N_o for $2DH_1$ and $2DM_1$ over AWGN channel with EDR and segmented EDR packets.

tooth packets and the proposed schemes. This method ensures obtaining correct statistical results. The simulation experiments are carried out over AWGN and Rayleigh flat-fading channels [24].

An important assumption used in the simulation is that a packet is discarded if there is an error in the AC, HD, or PL (after decoding), which was not corrected using the error correction. This is a realistic assumption to simulate the real Bluetooth systems operation. In this simulation, hard decision is assumed at the receiver in the decoding process for all channel codes. In the simulation, the interference effects are neglected. The packets lengths in all experiments are kept fixed for all coding schemes. This is at the expense of payload lengths. In some simulation experiments, a block-fading channel is assumed. It is slow and frequency nonselective channel, where symbols in a block undergo constant fading effect [22].

The experiments are concentrated on $2DH_1$ and $2DH_5$ (the shortest and longest uncoded EDR packets), the proposed encoded EDR packets ($2DM_1$ and $2DM_5$), and the proposed segmented encoded EDR packets, the results can be generalized for the rest EDR. Theses cases are expected improve the performance of the rest packets. MATLAB was used for carrying our simulation experiments of different cases. All simulations results have been gotten by transmission of 10000 trails (packets) over several SNR values [23].

6.1. AWGN Channel

This section is devoted to measure the number of packet loss and the efficiency of power transmission using classic, EDR, and proposed EDR Bluetooth packets. The first experiment is performed for uncoded $2DH_1$, proposed $2DM_1$, $2DM_1$ using convolutional code, and segmented $2DM_1$ packets transmission over an AWGN channel. The segmented $2DM_1$ packets using expurgated Hamming code (15, 10) for first part from PL_1 field and convolutional code (1, 2, and $K = 3$) for second part from PL_2 field. The results of these experiments are shown in Fig. 3a, $2DM_1$ EDR packets perform better than $2DH_1$, which means improving the Bluetooth power efficiency by using encoded EDR packets. As shown in Fig. 3b, the Number of Packets Loss (NPL) is decreased with using encoded EDR. The proposed segmented encoded EDR ones performs better than $2DM_1$ with using standard coding scheme and the redundancy is lesser than convolutional code for encoded EDR packets.

The first experiment is repeated over AWGN channel for $2DH_5$ and $2DM_5$ using different cases. The result of this experiment is shown in Fig. 4a,b, these figure reveals, segmented EDR packets perform better than $2DH_5$ and $2DM_5$ packets also, and this packet has lesser redundancy than EDR packets with convolutional code. The proposed format improves the power efficiency and reduces the number of packet losses. As shown in the results the proposed schemes are effective in the case of $2DM_5$ more than $2DM_1$.

6.2. Fading Channel

The previous experiments were repeated over Rayleigh flat-fading channel. The results of $2DH_1$ and $2DM_1$ packets are shown in Fig. 5a,b, PER and NPL respectively. The error control schemes are useful for improving the power efficiency and reduce the probability of retransmission request.

Same result of $2DH_5$ and $2DM_5$ packets over Rayleigh flat-fading channel are shown in Fig. 6a,b. The error control schemes are useful for improving the power efficiency espe-

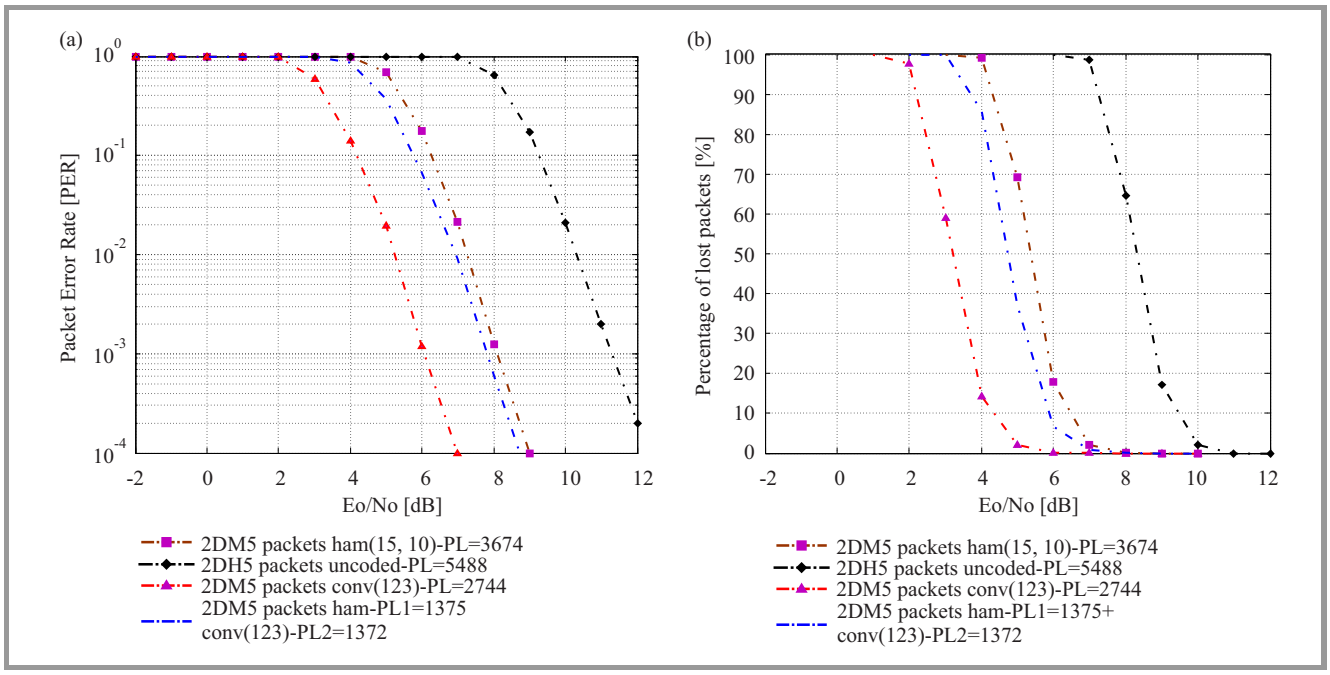


Fig. 4. (a) PER and (b) NLP versus E_b/N_o for $2DH_5$ and $2DM_5$ over AWGN channel with EDR and segmented EDR packets.

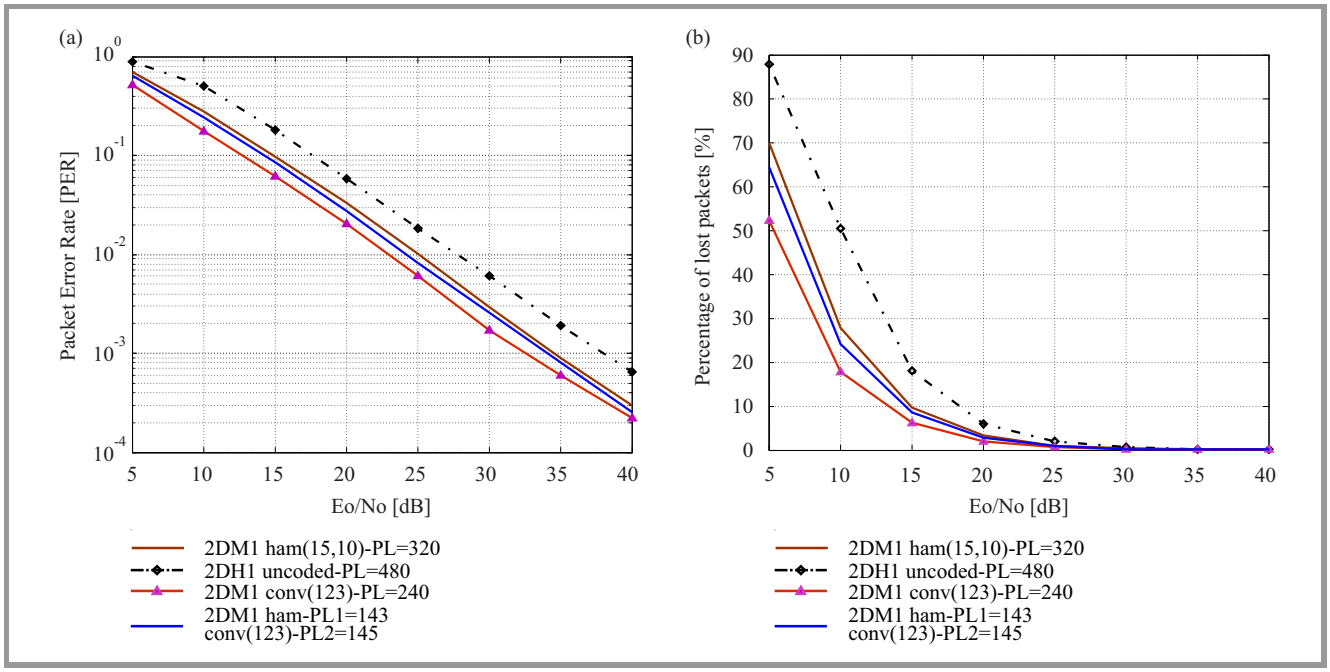


Fig. 5. (a) PER and (b) NLP versus E_b/N_o for $2DH_1$ and $2DM_1$ over fading channel with EDR and segmented EDR packets.

cially in the case of longer packets such as $2DHM_5$ packets. The proposed formats perform better than standard one. The segmented encoded EDR 2DM packets are trade-off between NPL and the redundancy.

The segmented encoded EDR packet gives performance better than encoded EDR. It reduces the redundancy bits more than convolutional code. The effectiveness of proposed schemes is good in the case of longer packets as shown in the results. With increasing the SNR this negative effect is reduced.

The throughput is related to the payload length and the PEP. Equation (15) gives the formula of the throughput calculating of Bluetooth system [24].

$$Throughput = \frac{PL(1-PSER)}{(x+1)t}. \tag{15}$$

PL is the user payload length, x is the number of time slots occupied by the packet, and t is the duration of the Bluetooth time slots. Figure 7a gives the amount of throughput variation with the channel SNR for $2DH_1$ and $2DM_1$

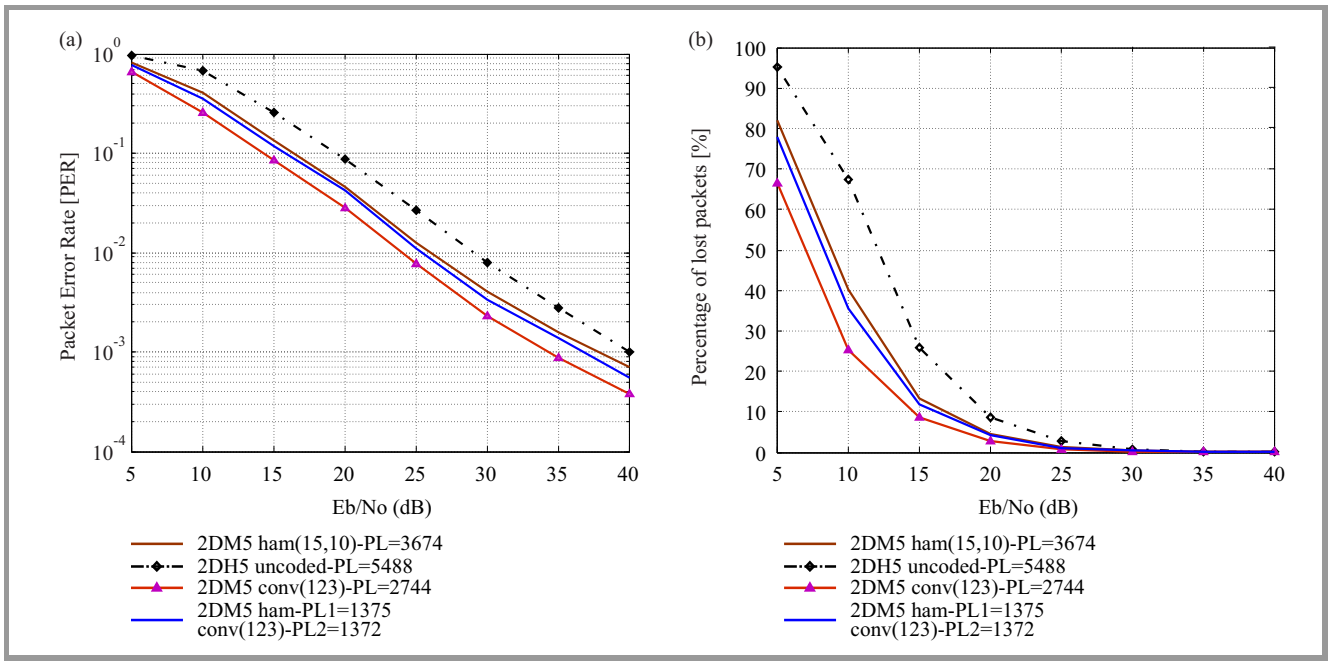


Fig. 6. (a) PER and (b) NLP versus E_b/N_o for $2DH_5$ and $2DM_5$ over fading channel with EDR and segmented EDR packets.

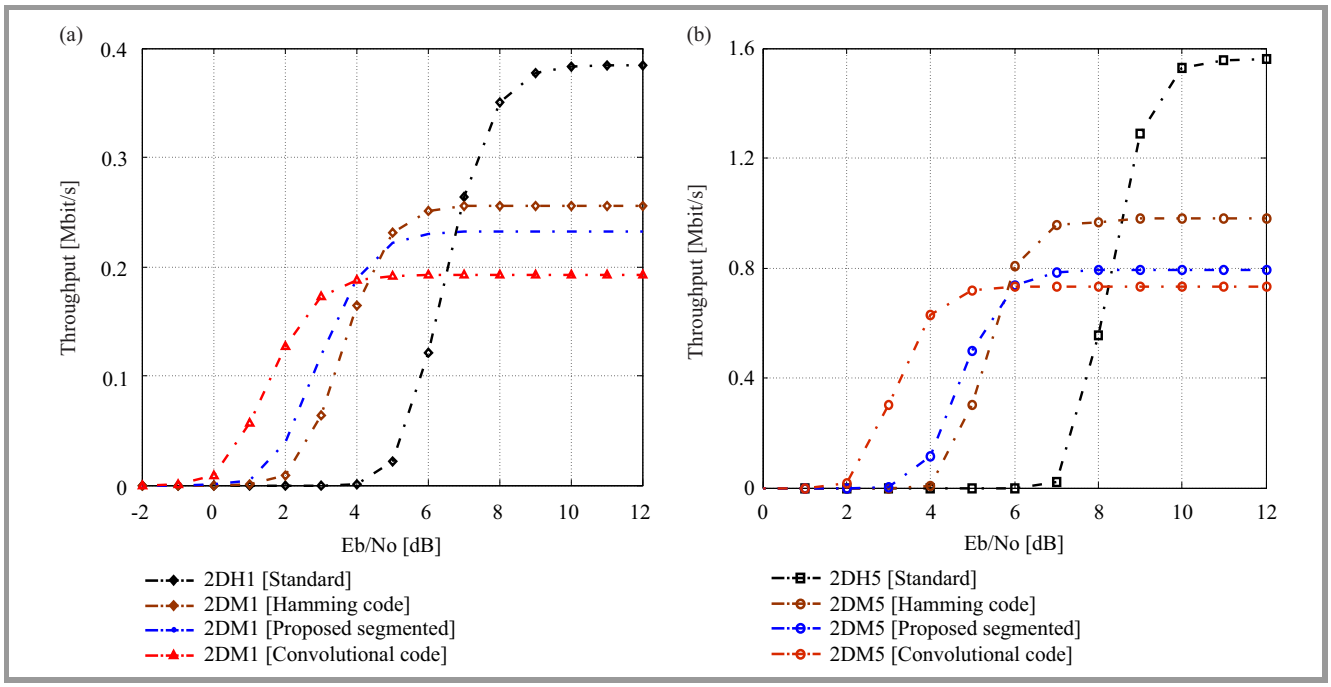


Fig. 7. Throughput versus E_b/N_o for AWGN with EDR and segmented EDR packets for: (a) $2DH_1$ and $2DM_1$ and (b) $2DH_5$ and $2DM_5$.

packets with the standard and proposed schemes over AWGN channel. As shown, the proposed schemes packets give high throughput at lower SNR values. Figure 7b shows the throughput with the SNR of the channel for $2DH_5$ and $2DM_5$ with different schemes. The proposed encoded packets using different error control scheme have different extra redundant bits. The segmented encoded packet format balances the PEP and the length of the redundant bits.

7. Computational Complexity

In many communications systems, the error control schemes have become an important tool in the computational complexity. In addition, the length of the transmitted and processed data increases the complexity.

The EDR packets are longer and their performance is worse than the classic ones. Many of papers proposed and studied different error control schemes for EDR packets such as the

convolutional codes. Its complexity is proportion to the length of input data. This work presents a simple method to decrease this complexity through segment or splitting the packet to two fields, as shown in Section 5.

The block codes are defined by (n, k) where k is the number of input data bits and n is the number of bits in the encoded frame, i.e. Hamming code [21]. These codes have low complexity than the other schemes. The computational complexity of the block codes is determined by the values of n and k.

The computational complexity of convolutional codes is higher than block codes. In general, convolutional code, the input information sequence contains $k \times L$ bits, where k is the number of parallel information bits at one time interval and L is the number of time intervals. These results in $m+L$ stages, in trellis diagram there are exactly $2^k \times L$ distinct paths in the trellis diagram. As a result the ML sequence would have a computational complexity on the order of $O[2^k \times L]$ the Viterbi algorithm reduces it by performing the ML search on stage at a time in the trellis at each node (state) of trellis, there are 2^k calculations. The number of nodes per stage in the trellis is 2^m. There for the complexity of Viterbi calculation is on the order of $O[(2^k)(2^m)(m+L)]$. In this work, the value of $k = 1$, $m = 2$, and $L =$ length of uncoded payload, it is different according to the packet type [22], [23]. As mentioned before, the reduction of bits stream leads to decreasing the complexity. The splitting of packets to two FEC schemes provides a trade-off between performance upgrading and the redundant bits. It is cleared from the previous simulation experiments, the proposed technique results curve located between the traditional FEC of classic packets and the convolutional codes curves as shown in Figs. 4–5. Also, the length of user data is increased at the expense of the overall redundant bits of the encoded packets. The overall redundant bits intended to the sum redundant bits of two FEC schemes, which is utilized to encode the two-segmented packet.

8. Conclusions

The authors have proposed a new segmented EDR packets type in Bluetooth using expurgated Hamming (15, 10) and convolutional code. The experimental results reveal that at low SNR values, $2DM_1$ and $2DM_5$ packets perform better than uncoded $2DH_1$ and $2DH_5$ packets, respectively. At high SNR values, the effect of proposed schemes is decreased. Therefore, the $2DH_1$ and $2DH_5$ packets are better on high throughput. Using convolutional codes with $2DM_1$ packets reduces the probability of retransmission process. It improves the performance especially at low SNR values. Segmented encoded EDR packets reduce the loss of packets with decreasing the redundancy compared to the use of convolutional codes. In the case of applying proposed schemes over $2DM_5$ packets, it was more effective than $2DM_1$. Proposed schemes improve the power efficiency and reduce the losses of packets. The segmented encoded EDR packet improves the performance of $2DM_5$ with redundancy reduction. Finally, segmented encoded EDR $2DM_x$ packets are trade-off between NPL and the redundancy.

References

[1] M. A. M. Mohamed, A. Abou El-Azm, N. El-Fishwy, M. A. R. El-Tokhy, and F. E. Abd El-Samie, "Optimization of Bluetooth packet format for efficient performance", *Progr. Electromag. Res. M*, vol. 1, pp. 101–110, 2008.

[2] P. Johansson, R. Kapoor, M. Kazantzidis, and M. Gerla, "Bluetooth: An enabler for personal area networking", *IEEE Netw. Mag.*, vol. 15, no. 5, pp. 28–37, 2001.

[3] "IEEE 802.11, the working group setting the standards for wireless LANS" [Online]. Available: http:// grouper.ieee.org/groups/802/11

[4] W. Feng, A. Nallanathan, and H. K. Garg, "Introducing packet segmentation for IEEE 802.11b throughput enhancement in the presence of Bluetooth", in *Proc. 59th IEEE Vehicular Technol. Conf., VTC 2004-Spring*, Milan, Italy, 2004, pp. 2252–2256.

[5] S. Galli, D. Famolari, and T. Kodama, "Bluetooth: channel coding considerations", in *Proc. 59th IEEE Vehicular Technol. Conf., VTC 2004-Spring*, Milan, Italy, 2004, vol. 5, pp. 2605–2609.

[6] R. Razavi, M. Fleury, and M. Ghanbari, "Energy-efficient video streaming over Bluetooth using rateless coding", *Elec. Lett.*, vol. 44, no. 22, pp. 1309–1310, 2008.

[7] A. Zanella, "A mathematical framework for the performance analysis of Bluetooth with enhanced data rate", *IEEE Trans. Commun.*, vol. 57, no. 8, pp. 2463–2473, 2009.

[8] A. Zanella, "A complete mathematical framework for the performance analysis of Bluetooth in fading channel", Dept. Information Engineering, University of Padova, Italy, Dec. 2007.

[9] A. Zanella and M. Zorzi, "Throughput and energy efficiency of Bluetooth v2 + EDR in fading channel", in *Proc. IEEE Wirel. Commun. Netw. Conf. WCNC 2008*, Las Vegas, NE, USA, 2008, pp. 1661–1666.

[10] R. Razavi, M. Fleury, and M. Ghanbari, "Correct Bluetooth EDR FEC performance with SEC-DAEC decoding", Elec. Let., vol. 43, no. 22, pp. 1209–1211, 2007.

[11] L.-J. Chen, T. Sun, and Y.-C. Chen, "Improving Bluetooth throughput using FEC and interleaving", in *Proc. Int. Conf. Mob. Ad Hoc Sensor Netw.*, Hong Kong, 2006, pp. 726–736.

[12] M. A. M. Mohamed *et al.*, "Bluetooth performance improvement with existing convolutional codes over AWGN channel", in *Proc. 2nd Int. Conf. Elec. Engin. Design and Technol. ICEEDT'08*, Hammamet, Tunisia, 2008.

[13] N. Golmie, R. E. Van Dyck, and A. Soltanian, "Interference of Bluetooth and IEEE 802.11: Simulation modeling and performance evaluation", in *Proc. ACM Int. Worksh. Model., Anal. Simul. Wirel. Mob. Sys.*, Rome, Italy, 2001, pp. 11–18.

[14] T. Y. Chui, F. Thaler, and W. G. Scanlon, "A novel channel modeling technique for performance analysis of Bluetooth baseband packets", in *Proc. IEEE Int. Conf. Commun. ICC 2002*, New York, USA, 2002, pp. 308–312.

[15] J. C. Haartsen and S. Zürbes, "Bluetooth Voice and Data Performance in 802.11 DS WLAN Environment", Ericsson Rep., 1999.

[16] M. Lentmaier and K. Sh. Zigangirov, "On generalized low-density parity-check codes based on Hamming component codes", *IEEE Commun. Lett.*, vol. 3, no. 8, pp. 248–250, 1999.

[17] D. Haccounand and G. Begin, "High-rate punctured convolutional codes for Viterbi and sequential decoding", *IEEE Trans. Commun.*, vol. 37, no. 11, pp. 1113–1125, 1989.

[18] M. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, "Efficient erasure correcting codes", *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 569–584, 2001.

[19] M. Kaiser, W. Fong, and M. Sikora, "A comparison of decoding latency for block and convolutional codes", in *Proc. 10th Int. Symp. Commun. Theory Appl. ISCTA'09*, Ambleside, UK, 2009.

[20] J. Hagenauer and L. Papke, "Iterative decoding of binary block and convolutional codes", *IEEE Trans. Infor. Theory*, vol. 42, no. 2, pp. 429–445, 1996.

[21] I. Howitt, "WLAN and WPAN coexistence in UL band", *IEEE Trans. Veh. Technol.*, vol. 50, no. 4, pp. 1114–1124, 2001.

[22] A. Conti, D. Dardari, G. Paolini, and O. Andrisano, "Bluetooth and IEEE 802.11b coexistence: analytical performance evaluation in fading channels", *IEEE Trans. Selec. Areas Commun*., vol. 21, no. 2, pp. 259–269, 2003.

[23] J. Mikulka and S. Hanus, "Bluetooth and IEEE 802.11b/g coexistence simulation", *Radioengin.*, vol. 17, no. 3, pp. 66–73, 2008.

[24] M. C. Valenti, "On the throughput of Bluetooth data transmissions", in *Proc. IEEE Wirel. Commun. Netw. Conf.*, Orlando, FL, USA, 2002, pp. 119–123.

Mohsen A. M. Mohamed Kaseem El-Bendary received his B.S. in 1998, M.Sc. in 2008, Ph.D. in 2012 all in Communication Engineering, from Menoufia University, Faculty of Electronic Engineering. He is now a lecturer in Electronics Department, Helwan University, Cairo, Egypt. His research interests cover wireless networks, wireless technology, channel coding, QoS over Bluetooth system and Wireless Sensor Network (WSN), and security systems which use wireless technology, such as fire alarm and access control systems.
E-mail: mohsenbendary@hotmail.com
Faculty of Industrial Education
Helwan University
Helwan, Egypt

Mostafa A. R. El-Tokhy received his B.S. degree from Zagazig University, Banha branch, Egypt and M.Sc. degree from Technical University, Eindhoven, The Netherlands in 1993 and 1998 respectively. He received his Ph.D. degree from Osaka University, Osaka, Japan in 2003. Presently, he is an Assistant Professor of Electronics Engineering at Industrial Education College, Higher ministry of Education, Cairo, Egypt. His current research interests are high performance digital and analog circuits.
E-mail: mostafaeltokhy@hotmail.com
Faculty of Industrial Education
Helwan University
Helwan, Egypt

Paper

Design and Development of Miniature Dual Antenna GPS-GLONASS Receiver for Uninterrupted and Accurate Navigation

N. S. Sudhir and S. S. Manvi

[1] *GNSS and Embedded Systems Lab, Accord Software Systems Pvt. Ltd., Bangalore, India*
[2] *Wireless Research Lab, Reva Institute of Technology and Management, Bangalore, India*

Abstract—Global Positioning System (GPS), Global Navigation Satellite System (GLONASS), and GPS-GLONASS receivers are commonly used for navigation. However, there are some applications where a single antenna interface to a GPS or GPS-GLONASS receiver will not suffice. For example, an airborne platform such as an Unmanned Aerial Vehicles (UAV) will need multiple antennae during maneuvering. Also, some applications will need redundancy of antenna connectivity to prevent loss of positioning if a link to satellite fails. The scope of this work is to design a dual antenna GPS-GLONASS navigation receiver and implement it in a very small form-factor to serve multiple needs such as: provide redundancy when a link fails, and provide uninterrupted navigation even under maneuvering, also provide improved performance by combining data from both signal paths. Both hardware and software architectures are analyzed before implementation. A set of objectives are identified for the receiver which will serve as the benchmarks against which the receiver will be validated. Both analysis and objectives are highlighted in this paper. The results from the tests conducted on such a dual antenna GPS-GLONASS receiver have given positive results on several counts that promise a wider target audience for such a solution.

Keywords—dual-antenna receiver, embedded system, GLONASS, GPS, miniaturization.

1. Introduction

Typical single antenna navigation receiver architecture consists of a few critical blocks as shown in Fig. 1: RF front-end, correlator, and navigation processor [1], [2]. The RF front-end block consists of amplifiers, filters, down-conversion and Analog to Digital Converter (ADC) blocks for each of the signals. The ADC output is then relayed onto the correlator block, which generates the appropriate carrier frequencies and code bit streams in order to perfectly match with the incoming signal. The results of this process are passed on to the navigation processor, which estimates the location information. The navigation processor also generates appropriate messages to interface receiver with the host.

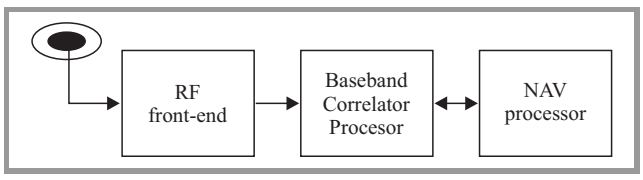


Fig. 1. Typical navigation receiver architecture.

Navigation receivers are available today in varied hues. There are both single constellation and multi-constellation receivers serving the needs of myriad user communities. GPS, GLONASS, and dual GPS-GLONASS receivers are commonly used for navigation. GPS is a USA satellite based navigation system providing reliable and uninterrupted location guidance services to global users [3], [4]. Launched in the 80's, it is one of the most popular navigation systems used world-wide across a multitude of applications. GPS is a typical single constellation receiver installed in mobile phones, PNDs, wireless base stations, and vehicles.

GLONASS is the Russian equivalent of GPS. Launched as a competitive system to GPS during the days of cold war, it went into degeneration during the disintegration of Soviet Union and was recently revived back to its full constellation. GLONASS has proven to be both an alternative as well as a companion to GPS for multi-constellation receivers. A multi-constellation receiver is slowly finding its relevance today with the stabilization of the GLONASS constellation. Typically, GPS is combined with GLONASS and offered as a higher performance platform, but at a premium value.

Most of today's navigation receivers are equipped with single antenna interface. However, there exists a niche segment that demands multiple antenna interfaces. An example would be that of an Unmanned Aerial Vehicle (UAV). UAVs today are used in several wartime applications. However, they have found their use in several civil and commercial applications as well. A few of them are: wildfire management, disaster management, pipeline and homeland security, and earth science research and applications.

The primary use of multiple antenna interfaces would be to have an uninterrupted navigation data even when the vehicle maneuvers. Navigation receiver's antenna need to have a clear view of the sky to catch the signals transmitted from the satellites. In vehicles such as UAVs, there is a high probability that a single antenna may not always see the sky and therefore continuous navigation may not be possible.

Another application that would greatly benefit the use of multiple antennas is that of in-vehicle navigation. In big cities with tall buildings, a single antenna may have a limited sky view. With a two antenna architecture with an antenna each placed on the dash and on the rear parcel tray enables more coverage of the sky and leads to a higher percentage of navigation guidance.

During a study of past and current developments, it has been found that most receivers are developed to address a single parameter such as multipath, interference mitigation or redundancy. These receivers are high-end and targeted at very specific applications.

The challenge now is to come up with a new architecture that can support multiple antennas, build system redundancy, and provide improved navigation availability, lower power consumption and a miniature form-factor package. The receiver incorporates two independent channels to receive dual-frequency signals simultaneously.

There are receivers with multiple antenna interfaces and multi-constellation architectures [6]–[8], but these are designed to address a different class of applications. For instance, the solution proposed to overcome severe vehicle maneuvering in GPS receivers is discussed in [6] where a GPS receiver is connected to 3 GPS antennas through a RF switch. The RF switch is controlled using software to periodically sample the signal from each path in order to determine the signal availability and quality. This approach avoids duplication of the signal processing blocks, but can take more time for a position fix. Again, the multiple antenna solutions in [6] and [7] are more driven towards multipath mitigation using antenna array technology.

The work given in [8] presents combined GPS and GLONASS receiver for consumer market. A fully integrated dual-channel reconfigurable GNSS receiver supporting Compass/GPS/GLONASS/Galileo systems is implemented in 65 nm CMOS semiconductor technology [9]. The target multi-system GNSS receiver architecture based on an PCI ExpressCard peripheral card for the PC computer is described in [10]. The work given in [11] presents a practical design of smart antenna system for GPS/GLONASS anti-jamming based on adaptive beamforming.

The authors have noticed very few works on such designs in a small foot-print. Hence, GPS-GLONASS navigation receiver is designed and developed in a very small form-factor to serve the multiple needs such as:

– provide redundancy when one link fails,

– provide uninterrupted navigation even under maneuvering,

– provide improved performance by combining data from both signal paths.

The rest of the paper is organized as follows. The multi-constellation GNSS (GPS-GLONASS) versus stand-alone GPS or GLONASS is debated in Section 2 along with a glimpse into the architecture proposed and implemented for a miniature multi-antenna navigation receiver. Hardware and software implementation details of the receiver are presented in Section 3. Measurements and results are given in Section 4, and the conclusion is presented in Section 5.

2. Proposed Dual Antenna GNSS Receiver Architecture

Multiple-constellation GNSS receivers offer significant performance advantages over single constellation receivers in almost all positioning applications. Increased availability, improved accuracy, and less susceptibility to jamming are ones that are readily apparent. With the exponential increase in the number of GPS receivers deployed in conditions where the satellite visibility is limited, a multiple-constellation receiver can continue to provide fairly accurate positioning even when a GPS-only receiver is unable to do so, resulting in a much more satisfactory user experience.

Until recently, GPS was the only satellite based navigation system with full operational capability. However, the GLONASS constellation has also reached its full deployment configuration. The main advantage of having multiple satellite constellations is in the availability of more satellites and improvement in Geometric Dilution of Precision (GDOP) [5]. The GNSS receiver by virtue of tracking more number of satellites is capable of providing a faster time to fix. In addition, a stand-alone (single constellation) receiver may not be able to compute a position fix in situations where the antenna is obscured, but with a multi-constellation GNSS receiver, it is highly probable that the combination of the available satellites from different satellite constellations can provide a navigation solution.

The multi-constellation GNSS receiver architecture proposed involves two independent RF and base-band processing paths. Each of the two independent paths can act as a stand-alone GPS-GLONASS position engine. This dual RF processing maximizes the satellite availability during vehicle maneuvers or signal blockage. This in turn, ensures near complete visibility of all the satellites from both the constellations and hence increases the probability of a faster time to fix.

The GNSS receiver architecture is depicted in Fig 2. As seen, there are two antenna paths with each path supporting a GPS and a GLONASS RF front-end (GLSRF and GPSRF). The output of the GPS front-end is fed to the GPS correlator and that of the GLONASS front-end to the GLONASS correlator. It is obvious that there are two such correlator pairs, one for each signal path. The data from all four paths are fed to the navigation processor where the

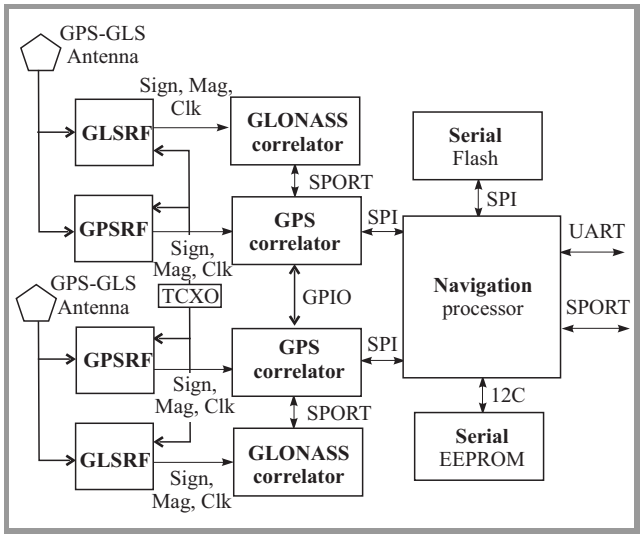


Fig. 2. Dual-antenna GPS-GLONASS receiver architecture.

data is decoded and the navigation data is computed. In addition to the main components described above, there are other important blocks that contribute to making a complete receiver. The memory is interfaced to the navigation processor and serves two important purposes – holds the boot program for the baseband correlators and navigation processor and stores the runtime configuration and satellite data.

In the proposed receiver architecture, the design is optimized to balance the trade-off between the factors as: components size, performance, consumed power and cost.

3. Hardware and Software Details of GNSS

3.1. Hardware Implementation

With reference to the receiver block diagram in Fig. 2, hardware details are provided. Each antenna port is immediately followed by a power splitter. The power splitter matches the impedance to 50 Ω at both its input and output. The two output ports from each splitter feed the front-ends of a pair of GPS and GLONASS RF chips. The down conversion of L1 frequency is performed in a single mixer stage to generate IF frequencies in each RF chip. The local oscillator frequency required for mixing operation is derived from a common reference clock. The final output from the RF front end is a digitized IF signal.

The digitized IF signal is separately processed in GPS and GLONASS base-band processor blocks. This feature is duplicated across two paths resulting in dual independent base-band processing of the signal received from the two antennas. The respective baseband processors work on the IF outputs from the RF chips, run signal acquisition and tracking algorithms, receive the data bits from the satellites and deliver the results to the navigation processor.

The key hardware specifications of the RF front end are listed in the Table 1 (QFN denotes "quad-flat no-leads" plastic package, and RLC denotes resistors and inductors and capacitors). The digitized IF signal is separately processed in GPS and GLONASS base-band processor blocks. This feature is duplicated across two paths resulting in dual independent base-band processing of the signal received from the two antennas. The respective baseband processors work on the IF outputs from the RF chips, run signal acquisition and tracking algorithms, receive the data bits from the satellites and deliver the results to the navigation processor. The key hardware specifications of the baseband processors are shown in Table 2 (FBGA means "Fine pitch Ball Grid Array"). The navigation processor in turn intelligently weighs the measurements and computes the navigation solution in three modes: GPS only position, GLONASS only position, and GPS-GLONASS combined position. The key hardware specifications of the navigation processor are listed in Table 3. The navigation processor has adequate internal memory and hence the only memory device required to hold the boot program is a Flash memory. A serial Flash is selected in order to minimize the package area and avoid PCB routing of address and data bus. The key hardware specifications of the memory are presented in Table 4. The receiver provides several industry standard interfaces such as Universal Asynchronous Receiver Transmitter (UART), Serial Peripheral Interface (SPI), Serial Port (SPORT) and two-wire synchronous interface thereby providing multiple options for connectivity with the host system. The key specifications of the interface section are shown in Table 5. The power supply

Table 1
Key specifications of the RF front-end

Size	4 × 4 mm
Package	QFN, 24-lead
Number of external components	23 RLC
Occupied PCB area	9 × 9 × 4 mm

Table 2
Key specifications of baseband processor

Size	7 × 7 mm
Package	FBGA, 24-lead
Number of external components	11 RC
Occupied PCB area	8 × 8 × 2 mm

Table 3
Key specifications of navigation processor

Size	7 × 7 mm
Package	FBGA, 24-lead
Number of external components	11 RC
Occupied PCB area	7 × 7 × 1 mm

Table 4
Key specifications of memory

Size	6 × 4 mm
Package	DSM, 24-lead
Number of external components	4 RC
Occupied PCB area	7 × 5 × 1 mm

Table 5
Key specifications of interface

UART	115200 b/s, 8 data bits, 1 start bit, 1 stop bit
SPI	22.5 Mb/s, 16-bit data interface, full-duplex
Synchronous interface	40 MHz half duplex
Serial port (SPORT)	22.5 MHz full duplex

to the hardware should be able to supply 1.5 A at 3.3 V. On-board, the power supply section converts the input voltage of 3.3 V into 1.2 V and 2.5 V to supply the core of the different chips. The key hardware specifications of the power supply section are listed in the Table 6 (DFN indicates "Dual flat no leads" package). The PCB is a crucial hardware component that determines the receiver size. The PCB should be small enough to meet the constraint of miniaturization, but should not impose severe penalties in terms of using expensive PCB manufacturing technologies. The PCB should support mechanical structures such as RF connector, interface connector and an enclosure.

Table 6
Key specifications of power supply

Size	4 × 3 mm
Package	DFN, 12-lead
Number of external components	12 RLC
Occupied PCB area	7 × 9 × 2 mm

3.2. Software Implementation

The presence of multiple processing elements in the design brings with it the challenges for the software in terms of performing the power on initializations for each processor, managing the inter-processor communication, weeding out the unwanted measurement from the several that enter the receiver and finally managing the man-machine interface through one of the many interfaces on the receiver. Figures 3 to 6 depict flowcharts for initialization, inter-processor communication, boot sequence program, and measurement.

Upon power up, each of the four processing elements comprising of the two baseband processors, the navigation processor and the FPGA will need to be initialized with their respective programs. Since the entire system has a single Flash memory, the individual program files are allocated specific segments. The Flash is interfaced with the navigation processor and upon power up, the boot program is brought into the navigation processor.

The boot program sequentially manages the initialization by bring in the program of each processing element in turn and then transferring the same to the corresponding processor. In addition, once a processor is loaded with its program, it should not immediately start executing. It is important to maintain synchronization with the other processors and towards this, signaling is performed to ensure that all processors start at the same instant. Once the system is up

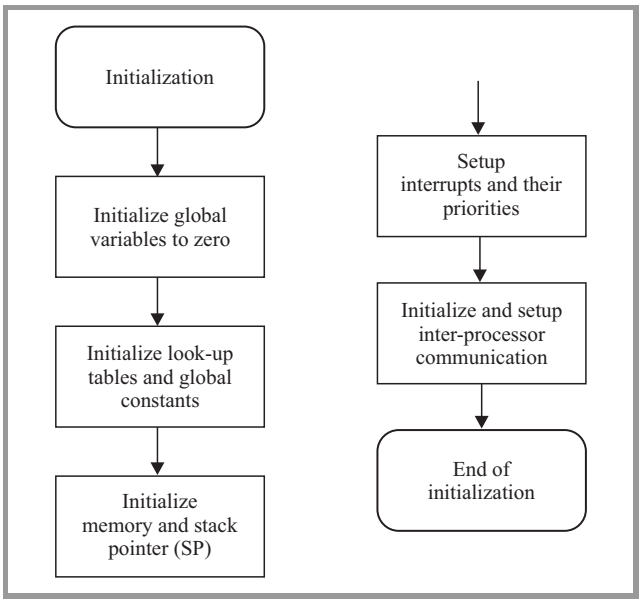


Fig. 3. Initialization.

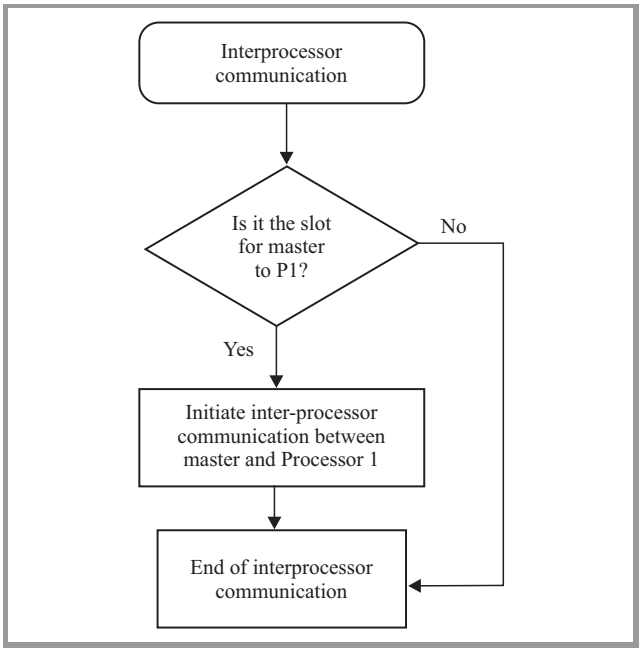


Fig. 4. Interprocess communication.

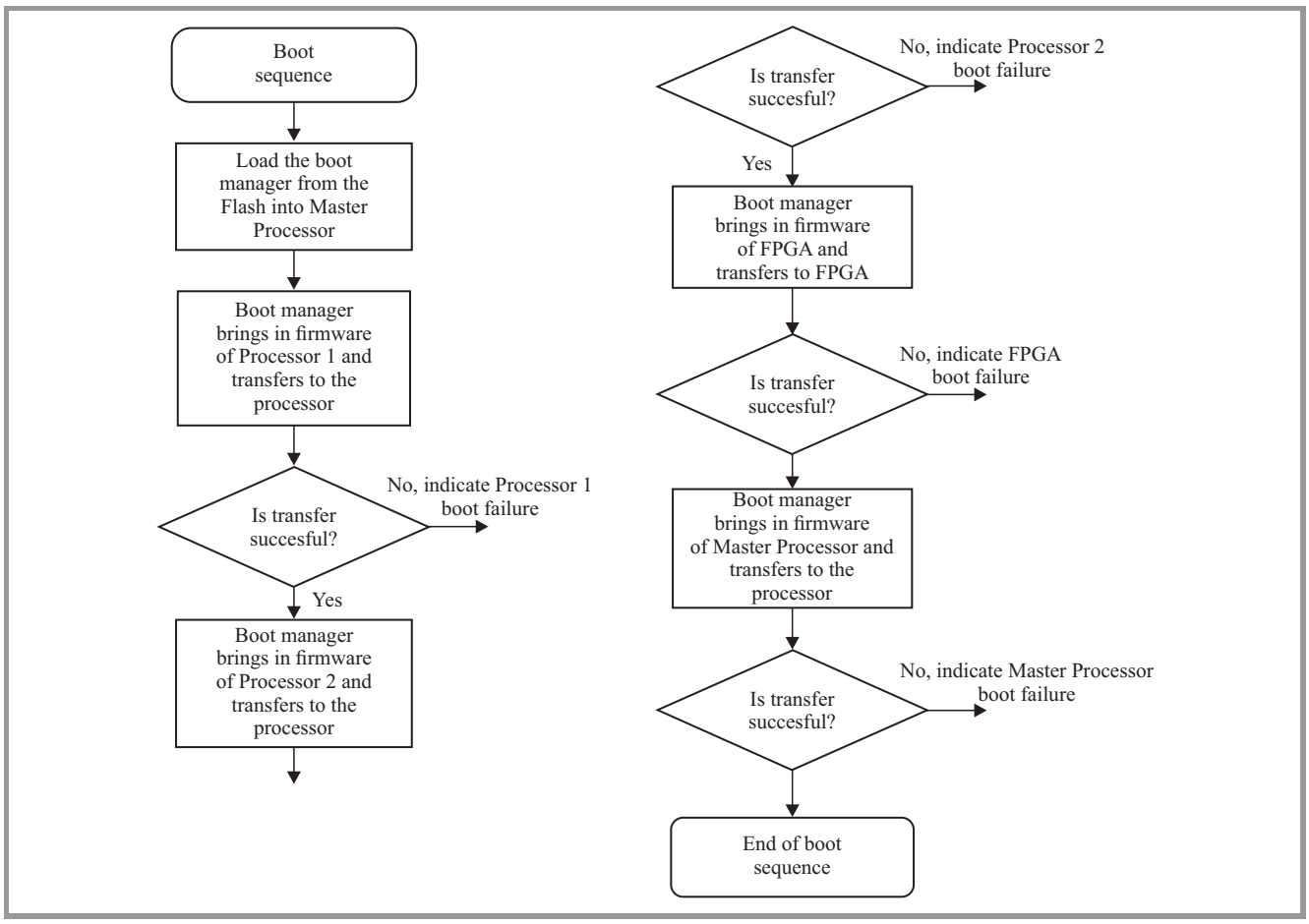


Fig. 5. Boot sequence.

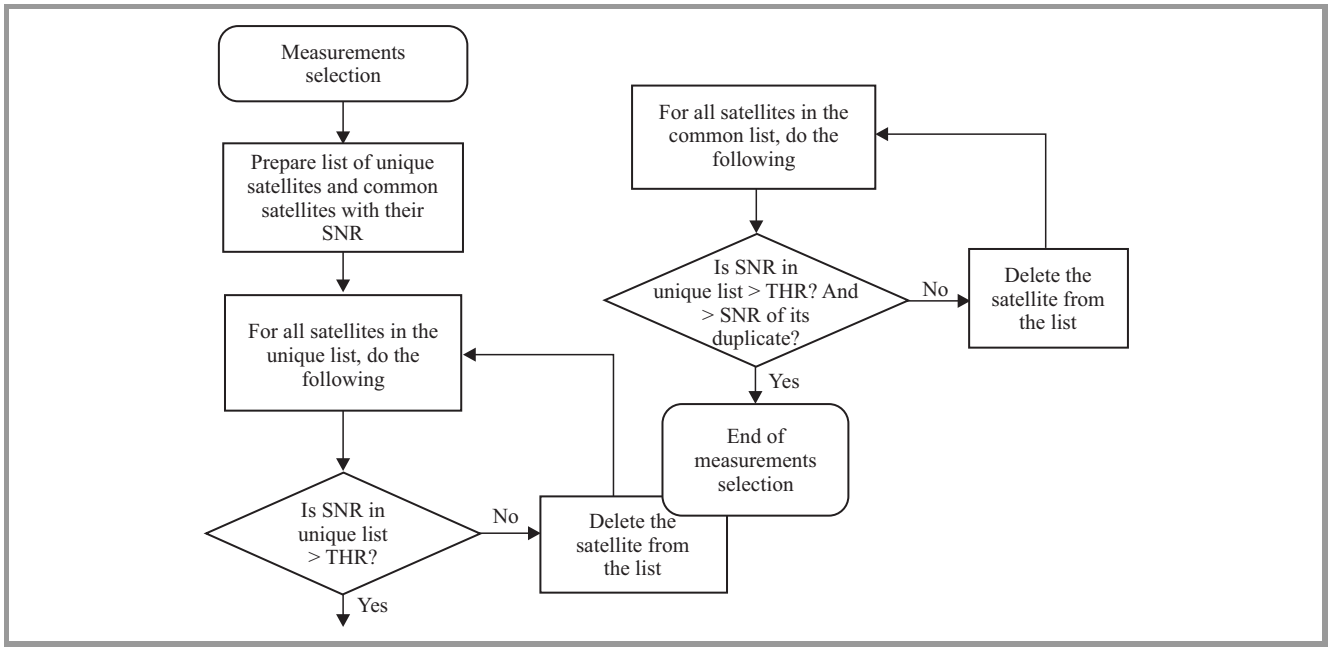


Fig. 6. Measurement selection.

and running, it is important to seamless exchange data between the different processing entities. The results from the signal processing have to be passed from the correlators to the navigation processor while any configuration to be done from the navigation processor is passed back to the correlators. This happens through the SPORT interface, which is programmed to work as SPI. In a dual-antenna system, the number of measurements is double that of a single antenna system. Further, some of the satellite signals enter through both antennas and arrive with different characteristics. It is important for the navigation processor to apply selection criteria to reject the unwanted measurements. The simplest and reliable means of discarding a measurement is to look at the signal level of the measurement. A threshold can be set based on experiments and any measurement whose signal level falls below the threshold can be rejected. Finally, the navigation solution computed in the receiver has to be brought out and delivered to the other entities which are part of the bigger system. The receiver has multiple interfaces to address such needs – UART, SPI, and synchronous communication. The UART is normally used to connect to a PC. The SPI and synchronous communication interfaces are more suited for embedded interfaces where the inter-connection happens between two or more processors.

4. Measurements and Results

To validate the dual antenna GPS-GLONASS receiver, several tests were conducted to justify the creation of such a receiver. Some of the key measurements and results are presented in this section.

4.1. Size

The miniature dual antenna GPS-GLONASS receiver is realized using indigenous as well commercial-off-the-shelf components. The design is implemented in a tiny $40 \times 40 \times 1$ mm (length $\times$ width $\times$ height) form-factor with dual row 50-pin connector for data and power supply interfaces along with the two antenna ports. A snapshot of the receiver module is shown in Fig. 7.

Fig. 7. Miniature dual antenna GPS-GLONASS receiver.

4.2. Power Consumption

The power consumption was measured by connecting a GPS-GLONASS antenna to each of the two ports and allowing the receiver to capture as many satellites as possible and computing the navigation solution. The current consumed was measured at multiple instances over a 12 hour period and the average of the current consumed was recorded. The current was measured to be 310 mA which amounts to a shade over 1 W. This result is encouraging as it enables the receiver to be used across several applications where power consumption is important.

4.3. Time to First Fix

The Time to First Fix (TTFF) is an important factor of a receiver. This indicates the speed at which the receiver is able to lock onto satellites and deliver the navigation output. The test setup consisted of the following: dual antenna GPS-GLONASS receiver, GPS-GLONASS antennae, and host PC to process the receiver output. The test results were recorded under open sky conditions. It can be seen in Table 7 that the TTFF in the combined mode is better than the worst case seen in a stand-alone receiver.

Table 7
Time to first fix for receivers

TTFF	Trial [s]	Trial 2 [s]	Trial 3 [s]
GPS	32	34	27
GLONASS	23	18	35
GPS-GLONASS	30	31	34

4.4. Accuracy

Using the same test setup, another important parameter was measured – position accuracy as shown in Fig. 8. The navigation data output from the receiver was recorded for over 24 hours with the antenna kept under a clear sky view. The plot of the position coordinates from GPS-only, GLONASS-only and combined modes are plotted in the same graph.

4.5. Field Test

Another test conducted on the receiver was a field test. Here, the advantage of having two antennas was exploited. The test setup consisted of the following: dual antenna GPS-GLONASS receiver, Stand-alone GPS receiver, GPS-GLONASS antennae with splitter, and host PC to process the receiver output. The objective of this test is to justify the presence of multiple constellation and dual antenna interface on the receiver. The receiver is installed in a vehicle with the two antennas placed on the dash and rear parcel tray respectively. A stand-alone high performance GPS receiver is also used in the test and the antenna placed on the dash is connected to this receiver through a splitter. The

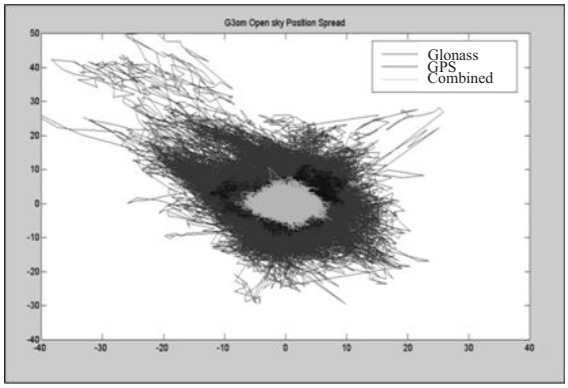
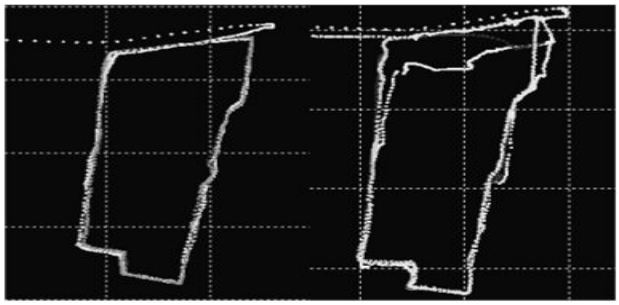


Fig. 8. Position accuracy.

vehicle is driven in a designated test route with buildings on either side of a narrow street. The performance of the receivers is compared and the plot from the test is shown in Fig. 9. The test results in Fig. 9, clearly demonstrates



Position plot from dual antenna GPS-GLONASS receiver | Position plot from a stand-alone GPS receiver

Fig. 9. Position trace from field test.

the benefits of satellites increased availability in the dual-antenna GPS-GLONASS combined mode. As a result, the plot of the receiver on the left looks much clean compared to the plot shown on the right for a GPS-only receiver. The field tests were conducted in a land-vehicle by placing one antenna on the dashboard and another on the rear parcel tray. When the vehicle moves in a narrow lane with reasonably tall buildings on either side, the satellite visibility is mostly restricted in the direction of vehicle. With a single antenna single constellation receiver, the number of satellites that are visible is limited to a single constricted view (either out of the front pane or the rear pane. A dual antenna multi-constellation receiver has the advantage of increased number of satellites from two constellations and also of seeing two different views out of the front and rear of the vehicle.

5. Conclusions

The key takeaway from this work is the realization that a multiple constellation receiver is better than a single constellation receiver. Further, dual-antenna multiple constellation receiver performs better than a single-antenna multiple constellation receiver.

The dual-antenna GPS-GLONASS receiver has no peers as it is a unique design in its class of receivers. It is designed to be a miniaturized receiver that is capable of being integrated into several classes of applications.

References

[1] B. W. Parkinson and J. J. Spilker, *Global Positioning System: Theory and Applications. Vol. I.* Progress in Astronautics and Aeronautics Serie, vol. 163. American Institute of Aeronautics and Astronautics, 1996.

[2] P. Misra and P. Enge, *Global Positioning System: Signal Measurements and Performance*. Lincoln, MA: Ganga-Jamuna Press, 2001.

[3] E. D. Kaplan and C. J. Hegarty, *Understanding GPS: Principles and Applications*, 2nd ed. Artech House, 2006.

[4] J. Bao and Y. Tsui, *Fundamentals of Global Positioning System Receivers*. Wiley, 2000.

[5] S. B. Vijay and G. Vyasaraj, "Innovative approach to overcome GPS signal masking during maneuvers of aircraft and satellites", in *Proc. 20th Int. Technical Meeting of the Satellite Division of The Institute of Navigation ION GNSS 2007*, Fortworth, TX, USA, 2007, pp. 2999–3007.

[6] A. T. Balaei, "Characterization of interference effects in multiple antenna GNSS receivers", in *Proc. Int. Conf. Image and Sig. Proces. ICISP 2010*, Trois-Rivieres, Canada, 2010, vol. 8, pp. 3930–3934.

[7] G. S. Granados, "Antenna arrays for multipath and interference mitigation in GNSS receivers", *Ph.D. Thesis*, Universitat Politecnica De Catalunya, July 2000.

[8] A. L. Botchkovski, N. V. Mikhaylov, and S. S. Pospelov, "GPS/GLONASS receiver in land vehicle: Expectations and reality", in *Proc. of 11th Int. Conf. ITS Telecommun. ITST 2011*, St. Petersburg, Russia, 2011, pp. 287–292.

[9] N. Qi *et al.*, "A dual-channel Compass/GPS/GLONASS/Galileo reconfigurable GNSS receiver in 65 nm CMOS with on-chip I/Q calibration", *IEEE Trans. Circ. Syst. I*, vol. 59, no. 8, pp. 1720–1732, 2012.

[10] P. Kovar, P. Kacmarik, and F. Vejrazka, "Interoperable GPS, GLONASS and Galileo software receiver", *IEEE Aerosp. Elec. Sys. Mag.*, vol. 26, no. 4, pp. 24–30, 2011.

[11] X.-H. Wang *et al.*, "Smart antenna design for GPS/GLONASS anti-jamming using adaptive beamforming", in *Proc. Int. Conf. Microw. Millim. Wave Technol. ICMMT 2010)*, Chengdu, China, 2010, pp. 1149–1152.

N. S. Sudhir is a senior Manager in the GNSS group at Accord Software and Systems, Bangalore. He has over 17 years of experience in R&D and design and development of software, hardware and algorithms for several GNSS embedded products. He has been building several variants of GNSS receivers for commercial use in various segments for consumer electronics, automotive, infrastructure and industrial applications.

E-mail: nssudhir@yahoo.com
GNSS and Embedded Systems Lab
Accord Software Systems Pvt. Ltd.
Bangalore, India

S. S. Manvi received the M.E. degree in Electronics from the University of Visvesvaraya College of Engineering, Bangalore and Ph.D. degree in Electrical Communication Engineering from Indian Institute of Science, Bangalore, India. He is presently working at Reva Institute of Technology and Management, Bangalore, India, as Dean of Research and Development. He is involved in research of agent-based applications in multimedia communications, grid computing, vehicular ad-hoc networks, e-commerce and mobile computing. He has published about 140 papers in national and international conferences, 90 papers in national and international journals, and 3 books. He is a fellow IETE (FIETE, India), fellow IE (FIE, India) and member ISTE (MISTE, India), member of IEEE (MIEEE, USA).

E-mail: sunil.manvi@revainstitution.org
Wireless Research Lab
Reva Institute Technology and Management
Rukmini Knowledge Park Yelhanka
Bangalore, India

Paper

Model that Solve the Information Recovery Problems

Nadia Kazakova[1], Oleksandr Skopa[1], and Mikołaj Karpiński[2]

[1] *Odessa National Economic University, Odessa, Ukraine*
[2] *University of Bielsko-Biala, Bielsko-Biala, Poland*

Abstract—The main part of the information ensuring in information and communication systems (ICS) is the provision for the development of methods for monitoring, optimization and forecasting facilities. Accordingly, an important issue of information security is a challenge to improve the monitoring systems accuracy. One way is to restore the information from the primary control sensors. Such sensors may be implemented in the form of technical devices, and as a hardware and software systems. This paper reviews and analyzes the information recovery models using data from monitoring systems that watch the state of information systems objects and highlights its advantages and disadvantages. The aim of proposed modeling is to improve the accuracy of monitoring systems.

Keywords—accuracy, information recovery, model, monitoring.

1. Introduction

Solving direct mathematical problems require accurate functions that will be able to describe physical phenomena, e.g., sound propagation, heat distribution, seismic vibrations, electromagnetic waves, etc. Medium properties in which the changes occur are described by equation coefficients. Equations coefficients are chosen to provide boundary conditions for the existence of phenomena in the environment. These values describe the initial state of the process, its properties, the boundary of data, reliability, etc. Such indicators are considered known. The therm called verge of reliability occurs when research area has limitations or during the stationary cases study, when the lack of dynamics does not allow to set the exact boundaries of the measured values deviation.
Indicated provision of the data unreliability can be distributed to informational medium. It may be also extended to those phenomena, which are investigated within them. Information environments have high physical and informational complexity, and their properties are often unknown. It means that there is need to formulate and solve the inverse problems to specify:

- the equations coefficients,
- unknown primary and/or boundary conditions,
- location, boundaries and other physical and information spaces that include under study processes.

These tasks are improper in most cases because they disrupt at least one of three common correctness properties. At the same time, the sought equation coefficients are usually density, electrical or thermal conductivity and other investigated medium important properties. When analyzing information medium, there an additional coefficients can be applied:

- data reliability as a property to preserve the semantic meaning,
- data reliability as a property to secure the electrical signals recovery, and so on.

The analysis of information and communication or software and hardware systems, e.g., the monitoring information space systems by search engines also requires the inverse problems solution. They arise while finding location of a given physical or logical object, its form, structure, or type of information impurities, defects in the information environment, sources defects, etc.
As can be seen in this software and hardware applications set, nowadays the theory of inverse and ill-posed problems is rapidly evolving science area.
Total requirements for software and hardware information and communication systems have become the basis for the systematic development of the converged architecture basic principles. This work is based on centralized services. Typically, services are combined into a single group (pool), which reduces the cost of their use. On this basis, cloud data processing technology has been developed and implemented. Data processing can be done by the user through existing network services, which are designed to serve a wide range of queries. They provide interaction between distributed software and hardware environment for cross-platform. In this case, any information about the user's location or his hardware and software configuration is unknown. Details are located in secure data centers. Data comes in data centers through special monitoring system and its reliability must be extremely high. Any distortion leads to the need for inverse problems solutions. Lack of data when modeling such systems also requires the inverse problems solution. Most of these are ill-posed. Their solutions have been developed over entire period of physical-information environments existence. The appearance of the fundamental works by A. M. Tikhonov allowed creating the modern theory of inverse problems solution. The concept

of a regularizing algorithm was taken as a basis for the theory. The author observed the class of problems in which small changes in the initial data values lead to significant variations in the processing of measurements in physical environments. Later, the theory was extended to the problems of:

- unstable convolution type integral equations solution,
- incoming signal restoration by the outgoing signal values, considering the system impulse response.

Much later, the Tikhonov's theory for solving inverse problems allowed to get solutions for:

- processes of multi-DF (Direction Finding) signal on one frequency,
- radio emission sources identification, which was the beginning of the monitoring systems.

Nowadays monitoring systems are a broad class of devices. They have extensive physical and information functions and are based on ICS. The term "monitoring" implies that it is the observing and recording data process about phenomena or objects, or about changing their information status. The authors take into account that this process occurs at time intervals that are adjacent to one another. During these intervals the data value is not significantly changed. The most recent observation about the irrelevance of information changing and its consequences, is one of the major challenges in this article.
In general, the data recovery problem in ICS can be displayed by an operator equation of the form [1]–[6]:

$$Ay = f\,, \tag{1}$$

where A is the compact linear operator, y is the function, which aims to solve mathematical inverse problem of restore information about the objects status of information-control systems, and f stands for function, based on the results of the experiment.
According to [7] the inverse operator A^{-1} may not exist causing the problem incorrect [8], [9]. This shows that there is not only one or unstable solution. An example of this is degenerate or fuzzy defined System of Linear Algebraic Equations (SLAE) (1).
Difficulties in dealing with degenerate and fuzzy defined algebraic equations are well known in practical problems related to digital signal processing. This is explained by the fact that the digital processing calculations are performed with finite precision. Naturally, in this case no one can determine whether a given system of equations are degenerated or fuzzy defined. This implies that fuzzy defined and degenerated systems can be indistinguishable within the specified accuracy. Thus, the objectives formulation and purpose of the article is to analyze models of problem that solve information retrieval, information in which can be obtained by monitoring systems that watch the state of information systems objects in purpose to increase the data accuracy and an overview of their advantages and disadvantages.
Solutions of applied tasks in information retrieval monitoring systems are based on the Fredholm integral type I equation. It uses a variety of methods that providing for the regulating parameters imposition. These include methods mentioned in the researches and publications analysis given below. However, existing methods for finding the regularization parameter is not always ensure finding the optimal value at which the error of solution may be minimal. The article is devoted to the unsolved part of the overall problem. The essence of the article and it's scientific innovation are in the need to find a multi-criteria model for data recovery, providing a choice point solutions on the Pareto set. It is necessary to identify and take into account possible limitations on the permissible vector criterion range, if the Pareto set belongs to this area. Besides, it is necessary to find and show the selected model shortcomings.

2. Analysis of Approaches that Solve Ill-Posed Information Restoring Problems

Nowadays there is a wide range of different approaches to solve ill-posed problems. The basis for the research in this area is the A. M. Tikhonov's work, who created the mathematical theory of ill-posed problems. These include his method of regularization, Lavrentiev's method of replacing, Ivanov's method of selection and quasi-solution and others. Also, there were developed methods for iterative, statistical, local, descriptive regularization, suboptimal filtering, solutions on the compact and others. Foreign development methods are optimal filtration of the Kalman-Bucy and Wiener, method of controlled linear filtering (Beykusa-Gilbert), and others. Although these methods are in principle more precise, the methods proposed by mentioned scientists (primarily Tikhonov regularization method) require much less additional information about the solution and therefore are more widely used when solving ill-posed problems.
To study the behavior of complex physical objects or processes, the authors use a systematic approach, which is characterized by the determination of a set of properties and relationships inherent in the object or process. Researching properties often contradict each other, but neither one of them cannot be neglected, because only all together they give a complete object picture. For ill-posed problems, such contradictory properties or partial quality criteria in multiobjective formulation can be resulting solution stability and accuracy. Multicriteria problems are complex because their computational complexity depends linearly on the vector criterion dimension and exponentially on the desired solution dimension vector. In addition in many studies the effectiveness of multi-objective optimization is the assertion for a wide class of problems.

3. Analysis of Finding the Optimal Regularization Parameter Methods

In practical tasks the right side of the operator Eq. (1) and matrix elements (i.e., the coefficients of the system) are frequently given by their approximations $\left\|\tilde{f}-f\right\|_{L_2} \leq \delta$ and $\left\|\tilde{A}-A\right\| \leq \xi$ with the upper bound of the right part and the operator. In this case this type of equation is solved: $\tilde{A}\tilde{y}=\tilde{f}$, where $\tilde{y} \in L_2$ – approximate solution, $\tilde{f} \in L_2$ – approximate function that most closely matches the experimental results, L_2 – common designation of studied events multitude. But it should be noted that there are an infinite number of system with this type input data, i.e. (A, f). Within the accuracy that can be a priori given with unknown tolerances, errors may be unnoticeable. In this case an approximate system $\tilde{A}y=\tilde{f}$ can be solved.

This paper introduces the concept of normal solution for solving degenerate and ill-conditioned SLAE system (1), which is stable against input data small changes. Here the normal solution of SLAE on the vector y^1 is called solution y^0, for which $\left\|y^1-y^0\right\| = \inf\limits_{y \in F_A} \left\|y-y^1\right\|$, where $\left\| y^0\right\| = \sqrt{\sum_j^n y_j^2}$. Thus, the problem of solving SLAE is reduced to minimize the functional $\left\| y^0-y^1\right\|^2$ on the set of vectors that satisfy the inequality $\left\| Ay-\tilde{f}\right\| \leq \delta$, so according to [10], [11], there is need to find vector that minimizes the smoothing functional:

$$M^{\alpha}\left[y, \tilde{f}, \alpha\right] = \alpha\left\|y^0-y^1\right\|^2 + \left\|Ay-\tilde{f}\right\|^2, \qquad (2)$$

where α is the regularization parameter.

According to the foregoing, it is necessary to stave the parametric optimization problem, which is connected with great challenges (e.g. [1]–[6], [8]–[11]). It is also called the position of finding the optimal regularization parameter question. This follows from the fact that by definition of the general case, it should be searched with infinite precision in the interval $0 \leq \alpha \leq 1$.

When Eq. (1) is a linear integral operator with constant limits of integration, the signal reconstructing problem can be represented by "truncated" Fredholm's linear integral equations of the first kind, which is:

$$\int_a^b Q(x,s) \cdot y(s) ds = f(x), x \in [c,d], \quad s \in (a,b). \qquad (3)$$

To solve the signal restoration problem for the Eq. (3) means finding the kind of signal $y(s)$, distorted by monitoring instrumentation with hardware function $Q(x,s)$ to a signal $f(x)$. Existing methods for solving the problem of information recovery typically use regularization, and they are extremely sensitive to errors in the results obtained in the monitoring process. In addition, they are not universal due to the fact that they shows acceptable results only for recovery tasks defined types, such as those that have precise initial conditions and well-conditioned system of equations, which can be reduced to Eq. (3).

4. Providing the Optimal Regularization Parameter Conditions

Methods mentioned in Section 3 for finding the regularization parameter are not always provide the optimal regularization parameter in which solution error given by Eq. (3) can be minimalized, i.e.:

$$\delta_y = \frac{\|y_\alpha - \bar{y}\|_{L_2}}{\|\bar{y}\|_{L_2}} \rightarrow \min, \qquad (4)$$

where y_α and $\bar{y}$ are obtained and exact solutions of the Eq. (3).

In this paper the concept of partial quality criteria is used, that are typical for multiobjective optimization, to identify the conditions for the solution to find. The quality of the Eq. (3) solution is estimated by set of frequency criteria:

$$I_j = \Phi_j[x, a, b, c, d, y], \qquad (5)$$

where $j = 1, 2, 3, \ldots, P$, functions Φ_j have continuous partial derivatives on y, and partial criteria given by Eq. (5) are the components of P-dimensional vector criterion $I = (I_1, I_2, \ldots, I_p)$.

Suppose vector's I criterion is limited by permissible area $I \in \Omega(I)$. Each component of the vector's criterion I is described by Eq. (5), which is specified on solutions $Y \in Y$ of integral Eq. (3). Solution's multicriteria problem IP is to determine the extremes $\{y^*(s)\}, y^* \in Y, I^* \in (I)$ (that under the given circumstances conditioned by the degree of a priori information about the solution $y(s)$, which optimize the vector's criterion I.

Let's take Y as the given set of possible solutions, composed of vectors $y = \{y_i\}_{i-1}^n$ n – dimensional Euclidean space. The solution quality can be evaluated by set of conflicting partial criteria, which forms P – dimensional vector $Y(y) = \left\{I_j(y)\right\}_{j-1}^P \subset F$ specified on the set Y, which belongs to the class F admissible vectors effectiveness and which is limited by acceptable area $I \in \Omega$. Therefore, there is need to define a solution $y^* \in Y$, that under given conditions and constraints optimizes the solution $y(s)$ of Eq. (3). So the components of the vector $y(s)$ should be subjected to normalization, since the solution is defined on the set of efficient points (Pareto's area) only if all partial criteria reduced to a single dimension or dimensionless form. In [7] an objective normalization method which does not disrupt any of the equality of partial criteria and which does not depend on the scale was presented. In this case the components of normalization vector y_0 as partial criteria extremes are taken, which defined on the space of solutions:

$$y_0 = \left\{\sup_{s \in S} y_j(s)\right\}_{j=1}^P. \qquad (6)$$

Let's perform the efficiency vector $I(y)$ normalization by constrained vector I_{jm} and obtain the vector of relative partial criteria, i.e. normalized efficiency vector:

$$I_0(y) = \left\{I_j(y)/I_{jm}\right\}_{j=1}^P = \left\{i_0(y)\right\}_{j=1}^P. \qquad (7)$$

Assume that all partial criteria $I_j(y)$ require minimization and they all are non negative and constrained:

$$\Omega = \left\{ I \left| 0 \le i_j(y) \le I_{jm}, j \in [1,P] \right. \right\}. \tag{8}$$

According to the literature analysis, case given by Eq. (8) is the most common. The system of inequalities (8) is a structured demonstration of acceptable area $y \in \Omega$. In this area efficiency vector (6) has the form of given constrained vector:

$$y_0 = \left\{ I_{jm} \right\}_{j=1}^{P}, \tag{9}$$

as the supremum of partial criteria are specified constraints I_{jm}.

5. Restrictions on Finding the Optimal Solution

Depending on the presence and prior information type, approaches to solving multicriteria problems may be different. In the absence of such information just find any vector solution y^*, that provides only the condition (8) to limit [14], [15]:

$$I^* \in \Omega = \left\{ I | 0 \le I_j(y^*) \le I_{jm}, j \in [1,r] \right\}, y^* \in Y = Y^k \cup Y^C, \tag{10}$$

where $y^* \in Y = Y^k \cup Y^C$ is solution belongs to two areas: compromises Y^k (the Pareto's area) and agreement Y^C [16], [17]. With this method the optimal solution it often approximated. The main criteria method is often recommended for practical use. It assumes that for the optimization from a set I_j, where $j \in [1,P]$, only one of the possible criteria (e.g. first) is chosen as a criterion, and others are transferred to the constraints category. Thus output multicriterion problem artificially replaced by a single-criterion with constraints is:

$$y^* = \arg\min_{y \in Y} I_1(y), 0 \le i_j(y) \le A_j, j \in [1,P]. \tag{11}$$

Although this method can be justified only for the complex systems optimization, i.e., when to perform even the simplest coordination of contradictory criteria is not easy, one still could argue that ill-posed problems are also a complex systems [18]–[20], and the replacement of multicriterion optimization by single-criterion will be expedient.

6. Modeling Multicriteria Problems in Data Restoring Technology

In [21], [22] some of multicriteria models are reviewed. According to the first model, resulted in the sources, multicriterion problem defined by Eqs. (3)–(7) is reduced to minimize the linear form component scalar criterion with constant weighting coefficients:

$$I_{M_1} = \sum_{j=1}^{P} \alpha_j I_j, \alpha_j > 0, \ \sum_{j=1}^{P} \alpha_j = 1. \tag{12}$$

In this case there is the problem of choosing weighting coefficients $\alpha_j, j = \overline{1,P}$. The scheme (12) in [12], [13] and [21], [22] is called the *integration optimality* model.

The second model in [21], [22] is defined as the *ideal (optimal) point in the space of quality criteria*. In each partial criterion (5) is optimized separately from others in the system of constraints (7). The result can be obtained by P optimal solutions, which are characterized by vectors $Y^{(j)}$, where $j = \overline{1,P}$. These solutions corresponds to the definition of partial criteria (7) $I_j^0(Y^{(j)}$, where $j = \overline{1,P}$, which are the coordinates of the ideal (optimal) point. Later the problem of minimizing the generalized norm puts up in the system of constraints (7):

$$I \left(\sum_{j=1}^{P} \left[I_j(y) - I_j^0 \left(y^{(j)} \right) \right]^L \right)^{\frac{1}{L}}, \ L \ge 1, \tag{13}$$

The expression (13) with $L = 1$ represents a linear combination of vector components $I(y)$ and $I^0(0)$. For $L = 2$ the expression (13) coincides with the Euclidean norm $\left\| I(y) - I^0(y) \right\|$, and if $L \to \infty$ it is reduced to the form: $\max_j \left\{ I_j(y) - I_j^0 \left(y^{(j)} \right) | j = \overline{1,P} \right\}$.

In some cases, the multicriterion model (13), treats the function (7) minimizing problem by the relative deviations sum of squares from their optimal values:

$$I_{M_2} = \sum_{j=1}^{P} \left[\frac{I_j(y) - I_j^0 \left(y^{(j)} \right)}{I_j^0 \left(y^{(j)} \right)} \right]^2. \tag{14}$$

For such cases multicriteria problem given by Eqs. (3)–(7) is reduced to minimize the function (14), and solution vector is chosen from the condition of minimization of the distance from the point corresponding to the space criteria selected solution vector to the ideal (optimal) point.

Modeling the multicriterion task by Eqs. (3)–(7) and Eq. (14) does not require weighting coefficients preselection α_j in the Eq. (12), but has a high computational complexity. This is due to solving P optimization problems in (3)–(7) for each partial criterion I_j to identify the ideal point coordinates $\left\{ I_1^0(y^1), I_2^0(y^2), \ldots, I_P^0(y^P) \right\}$ and solving the problem of minimizing additional functions in (7) to determine the optimal solution vector.

Next multicriteria model based on the scalar contraction of partial criteria for nonlinear compromise scheme [23], [24] is presented. It was was introduced in the theory of information recovery in [12], [13] does not require selection of weighting coefficients in the expression (12) and does not need a solution $P+1$ of optimization tasks, which is necessary for implementation in the others. Multicriterion problem given by (3)–(8) is reduced to the solution of a single optimization problem in expression [12]–[15] under the conditions (8):

$$I_{M_3} = \sum_{j=1}^{r} \frac{1}{1 - \frac{I_j}{T}}. \tag{15}$$

To set a certain criteria priority and achieve different sensitivity to variation problem parameters, instead of a unit

in the expression (15) numerator the weight coefficients α_j must be entered which imposed constraints $\sum a_j = 1$.
Necessary conditions for a minimum I_{M_3} give a finite system of equations:

$$\frac{\partial I_{M_3}}{\partial y_i} = 0, i = \overline{1,n}. \tag{16}$$

After differentiation of Eq. (16), a low dimensioned system of nonlinear equations (SNE) is obtained, which leads to for example using Newton's method for SLE.
When the function $y_0(x), j = \overline{1,m}$ – continuous and strictly convex parallelepiped $\Pi_x = \left\{x \in E^n \middle| a_i \le x_i \le b_i, i = \overline{1,n}\right\}$, a scalar convolution by nonlinear scheme of compromise $\Phi(x) = \sum\limits_{j=1}^{m} \alpha_j \left(1 - y_{0j}(x)\right)^{-1}$, $x \in \Gamma_x$, when normalization of partial criteria using expressions $y_{0j} = \frac{y_j(x)}{A_j}$, $A_j = \sup\limits_{x \in \Gamma_x} u_j(x) j = \overline{1,m}$, has a single minimum on parallelepiped Π_x, which means being unimodal. Therefore, for the partial criteria it should be selected strictly convex function in order to problem of optimizing by the scheme (15) has a unique solution.
Multicriterial model given by Eq. (15) is sensitive to parameters changes defined by Eqs. (3)–(8). If there's one partial criteria I_j close to the upper limit I_{jm} allowable values (8) multicriteria model (15) implements the Chebyshev's action (minimax) operator in this partial criterion. In other cases multicriteria model (15) is equivalent to the integrated optimality operator with varying degree of equalization of partial criteria. The deterioration one of the partial's criteria is offsets by another partial improvement.

7. Conclusions

The presented analysis shows that multicriteria model provides selection of a point on Pareto's set. Thus if Pareto set belongs to this area it is necessary to take into account specified constraints on the range of allowable vector criterion. Accordingly, for solving multicriteria problems, which set constraints (8) on the components of the vector criterion, model (15) is recommended.
However, the drawbacks of the model should be taken into account:

- cumbersome of equations when a large dimension,
- CHP (16) can have many roots,
- if the solution lies on the constraints border, it will be found with an error, although less than required (i.e., it means that there is essentially exact solution).

As presented, the SLAR solution is unstable. The instability is the result of the presence of a large numbers, its representation and tolerances. Thus, the goal of future researches is to show that:

- if the solutions of these equations does not exist, then is there any point in using the Gauss method of least squares, which can lead to a pseudo-solution,
- if there is no unique solution, whether it may be possible to use the Moore-Penrose matrix pseudo-inverse, where the normal solution can be obtained,
- if the solution is unstable, whether it may be appropriate to use regular or sustainable methods, i.e. regularization or filtering.

The experts of data recovery in inverse and ill-posed problems are involved in the study of the properties and non-stable problems regularization methods. These tasks are distributed into a large set of physical and information processes. For IT processes and for information space monitoring systems, these problems are only in their developmental stage. Nowadays scientists are trying to create new methods to solve non-stable problems. While doing so, they suggest that the methods are suitable for use in informatization systems. In terms of linear algebra, this is equivalent to find approximate methods to search the normal pseudo-solution in algebraic linear equations systems. It is assumed that the methods can be applied to calculations in rectangular, degenerate or poorly conditioned matrices. It is the aim of the further researches on the issue which was discussed in this paper.

References

[1] G. Weikum and G. Vossen, *Transactional Information Systems: Theory, Algorithms, and the Practice of Concurrency Control and Recovery*. Morgan Kaufmann, 2001.

[2] N. F. Kazakova and O. O. Skopa "Definition of parameters for solving predictive control multi-service telecommunication networks", *Modern Inform. Secur.*, no. 4, Special Issue, pp. 55–61, 2010 (in Ukrainian).

[3] V. S. Frost and B. Melamed "Traffic modeling for telecommunications networks", *Commun. Mag.*, vol. 32, no. 3, pp. 70–81, 1994.

[4] N. F. Kazakova, N. M. Bilyk, and G. A. Gunderich, "Fundamental problems of classification and analysis of models for software and predictive control of multi-telecommunication networks", *Nat. Univ. Shipbuilding (NUS Journal)*, no. 2 [431], pp. 125–132, 2010 (in Russian).

[5] J. Wu, J. Meng, and W. Liu, "Iterative solutions for a class of systems of abstract binary operator equations", in *Proc. 5th Int. Conf. Comput. Inform. Sci. ICCIS 2013*, Shiyan, China, 2013, pp. 888–890.

[6] N. F. Kazakova, "Application software implemented predictive control in the sense of solving practical problems of quality assurance services in secure information networks", *A Modern Special Technique*, no. 2, pp. 86–95, 2012. (in Ukrainian).

[7] C. G. Park, "On the stability of the linear mapping in Banach modules", *J. Mathem. Anal. and Appl.*, vol. 275, no. 2, pp. 711–720, 2002.

[8] E. J. Candès, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information", *IEEE Trans. Inform. Theory.*, vol. 52, no. 2, pp. 489–509, 2006.

[9] V. L. Baranov *et al.*, *Recovery and Optimization of Information Systems in Decision Making*. Kiev: State University of Information and Communication Technologies, 2009 (in Ukrainian).

[10] M. E. Kilmer and D. P. O'Leary, "Choosing regularization parameters in iterative methods for ill-posed problems", *SIAM J. Matrix Anal. Appl.*, vol. 22, no. 4, pp. 1204–1221, 2001.

[11] A. N. Tikhonov and V. Y. Arsenin, *Solutions of Ill-Posed Problems*. Washington, D.C.: Wiley, 1977.

[12] J. Zhu, C. K. Zhong, and Y. J. Cho, "Generalized variational principle and vector optimization", *J. Optimiz. Theory Appl.*, vol. 106, no. 1, pp. 201–217, 2000.

[13] A. N. Voronin, *Multicriteria Synthesis of Dynamic Systems*. Kiev: Naukova Dumka, 1992 (in Russian).

[14] B. P. Zeigler, H. Praehofer, and T. G. Kim, *Theory of Modelling and Simulation: Integrating Discrete Event and Continuous Complex Dynamic Systems*. Academic Press, 2000.

[15] A. N. Voronin, J. K. Ziatdinov, A. I. Kozlov, and V. S. Chabanyuk, *Vector Optimization of Dynamic Systems*. Kiev: Technika, 1999 (in Russian).

[16] K. Deb and H. Gupta, *Searching for robust Pareto-optimal solutions in multi-objective optimization*, Lecture Notes in Computer Science, vol. 3410, pp. 150–164, Springer, 2005.

[17] V. V. Podinovskii and V. D. Nogin, *Pareto-Optimal Solutions of Multiobjective Problems*. Moscow: Nauka, 1982 (in Russian).

[18] J. Haupt and R. Nowak. "Signal reconstruction from noisy random projections", *Information Theory, IEEE Transactions on.*, 2006, vol. 52, no. 9, pp. 4036–4048.

[19] V. L. Baranov, I. A. Zhukov, and A. A. Zasyadko, "Using the main criterion for solving the problem of signal restoration", *Bull. National Aviation University*, no. 1, pp. 9–13, 2003 (in Ukrainian).

[20] A. A. Zasyadko, "Comparison of the Tikhonov method and the method of multicriteria optimization for solving the signal restoration problem", *J. Autom. Inform. Sci.*, vol. 35, no. 9, pp. 45–52, 2003.

[21] K. E. Parsopoulos and M. N. Vrahatis, "Particle swarm optimization method in multiobjective problems", in *Proc. ACM Symposium on Applied Computing SAC 2002*, Madrid, Spain, 2002, pp. 603–607.

[22] A. A. Zasyadko, "Multiple objective restoration process signals", *Electr. Simul.*, vol. 26, no. 4, pp. 13–21, 2004 (in Russian).

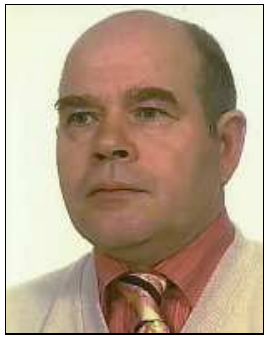
[23] T. Lobos *et al.*, "High-resolution spectrum-estimation methods for signal analysis in power systems", *IEEE Trans. Instrum. Measur.*, vol. 55, no. 1, pp. 219–225, 2006.

[24] S. M. Kay and S. L. Marple (Jr), "Spectrum analysis – A modern perspective", *Proc. IEEE*, vol. 69, no. 11, pp. 1380–1419. 1981.

Nadia Kazakova received the M.Sc. degree in Telecommunications in Odessa National Academy of Telecommunications named after O. S. Popov, Ukraine, in 2001. She received her Ph.D. in Technical Sciences in 2005 from the Ukrainian Scientific Research Institute of Communications. Currently she is an Associate Professor in Department of Information Systems in Economics at the Odessa National Economic University. Her research interests are in the theory of information security systems.

E-mail: kaz2003@ukr.net
Department of Information Systems in Economics
Odessa National Economic University
Gogolya st 18
65082, Odessa, Ukraine

Alexander Skopa received the M.Sc. degree in Telecommunication Engineering in Odessa National Academy of Telecommunications named after O. S. Popov, Ukraine, in 1986, and received his D.Sc. in Technical Sciences in 2011 from Lviv Polytechnic National University, Ukraine. He is an Associate Member of the Ukrainian Communications Academy. Currently he is a Head of Department of Information Systems in Economics at the Odessa National Economic University. His research interests are in the theory of information security systems.
E-mail: skopa2003@ukr.net
Department of Information Systems in Economics
Odessa National Economic University
Gogolya st 18
65082, Odessa, Ukraine



Mikołaj Karpiński received the M.Sc. degree in Electrical Engineering from the Lviv Polytechnic, Ukraine, in 1980, Ph.D. and D.Sc. degree in Electrical and Computer Engineering from the Academy of Sciences of Ukraine, Kiev, in 1989, and from the Lviv Polytechnic, in 1995, respectively. Currently he is a Chairman of Unit of Computer Science at the University of Bielsko-Biała. Prof. Karpinski is the author or co-author of 5 books, 5 book chapters and over 100 scientific papers. His research interests are in the cybersecurity, computer systems and wireless networks, especially their security, in particular cryptographic methods of information defense, lighting engineering, electric and photometric measurements, computer engineering.
E-mail: mkarpinski@ath.bielsko.pl
Unit of Computer Science
University of Bielsko-Biała
Willowa st 2
43-309, Bielsko-Biała, 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 author's JTIT LATEX style file is available:
http://www.nit.eu/for-authors

Papers published should contain up to 10 printed pages in LATEX author's style (Word processor one printed page corresponds approximately to 6000 characters).

The manuscript should include an abstract about 150–200 words long and the relevant keywords. The abstract should contain statement of the problem, assumptions and methodology, results and conclusion or discussion on the importance of the results. Abstracts must not include mathematical expressions or bibliographic references.

Keywords should not repeat the title of the manuscript. About four keywords or phrases in alphabetical order should be used, separated by commas.

The original files accompanied with pdf file should be submitted by e-mail: redakcja@itl.waw.pl

Figures, tables and photographs. Original figures should be submitted. Drawings in Corel Draw and PostScript formats are preferred. Figure captions should be placed below the figures and can not be included as a part of the figure. Each figure should be submitted as a separated graphic file, in .cdr, .eps, .ps, .png or .tif format. Tables and figures should be numbered consecutively with Arabic numerals.

Each photograph with minimum 300 dpi resolution should be delivered in electronic formats (TIFF, JPG or PNG) as a separated file.

References. All references should be marked in the text by Arabic numerals in square brackets and listed at the end of the paper in order of their appearance in the text, including exclusively publications cited inside. Samples of correct formats for various types of references are presented below:

[1] Y. Namihira, "Relationship between nonlinear effective area and mode field diameter for dispersion shifted fibres", *Electron. Lett*., vol. 30, no. 3, pp. 262–264, 1994.

[2] C. Kittel, *Introduction to Solid State Physics*. New York: Wiley, 1986.

[3] S. Demri and E. Orłowska, "Informational representability: Abstract models versus concrete models", in *Fuzzy Sets, Logics and Knowledge-Based Reasoning*, D. Dubois and H. Prade, Eds. Dordrecht: Kluwer, 1999, pp. 301–314.

Biographies and photographs of authors. A brief professional author's biography of up to 200 words and a photo of each author should be included with the manuscript.

Galley proofs. Authors should return proofs as a list of corrections as soon as possible. In other cases, the article will be proof-read against manuscript by the editor and printed without the author's corrections. Remarks to the errata should be provided within one week after receiving the offprint.

A copy of the JTIT is provided to each author of paper published.

Journal of Telecommunications and Information Technology has entered into an electronic licencing relationship with EBSCO Publishing, the world's most prolific aggregator of full text journals, magazines and other sources. The text of *Journal of Telecommunications and Information Technology* can be found on EBSCO Publishing's databases. For more information on EBSCO Publishing, please visit www.epnet.com.

(*Contents Continued from Front Cover*)

INSTYTUT ŁĄCZNOŚCI
PAŃSTWOWY INSTYTUT BADAWCZY

Editorial Office
National Institute
of Telecommunications
Szachowa st 1
04-894 Warsaw, Poland

tel. +48 22 512 81 83
fax: +48 22 512 84 00
e-mail: redakcja@itl.waw.pl
http://www.nit.eu

JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY 4/2014