Paper

Critical Infrastructure Risk Assessment Using Markov Chain Model

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

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

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

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

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

1. Introduction

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

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

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

2. Application of the Markov Chain Model in the Cybersecurity

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

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

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

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

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

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

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

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

3. Threat Imaging Model

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

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

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

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

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

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

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

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

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

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

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

$$n^1 = n^2 = \ldots = n^R = n \tag{3}$$

and

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

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

$$\pi(k+1)^T = \pi(k)^T P(k) \ , \tag{5}$$

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

Such a description allows us to illustrate well the general situation, assuming that at a given stage the OC knows the states of models of particular system services. It is possible to assign to these services various criticalities corresponding to the assessment of the relative importance of a given service from the point of view of the functioning of the entire state organism.

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

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

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

4. A Real Life Example

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

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

Let us suppose that one may estimate, based on the analysis carried out at the level of operators, in the system's normal state, described by pair (S^1_0,S^2_0), the probabilities of an increased risk of relevant IT infrastructures, i.e., respectively, $p^1_{01}(S^2_0) = 0.01$ and $p^2_{01}(S^1_0) = p^2_{01}(S^1_1) = p^2_{01}(S^1_2) = p^2_{01} = 0.005$ (we assume that S^1 has no influence on S^2). Let at the same time $p^1_{02}(S^2_0) = 0.001$ and $p^2_{02}(S^1_0) = p^2_{02}(S^1_1) = p^2_{02}(S^1_2) = p^2_{02} = 0.001$ – we assume that in the normal state, the probability of withholding the services in question is very small. The values of probabilities refer to, say, the time interval between moments k and $k+1$ equaling one day. In the case of changing the time scale considered in our model, these values have to be changed accordingly.

Then, in the situation when $S^1(k) = S^1_0$ but $S^2(k) = S^2_1$, i.e., an increased risk has taken place in the service model associated with the delivery of energy, we evaluate $p^1_{01}(S^2_1)$ equal to 0.1. In this case an increased risk of information services 2 associated with the observed digital attack and the violation of the corresponding susceptibility of the operator of the service increases the potential threat to service 1. At the same time we can estimate $p^1_{02}(S^2_1)$ as equal to 0.05 – we seriously expect that the observed increased risk of service 2 $(S^2(k) = S^2_1)$ makes it possible to suspend the provision of service 1.

Further, when $S^1(k) = S^1_0$ but $S^2(k) = S^2_2$, i.e., service 2 is not provided, we assess $p^1_{01}(S^2_2)$ as also equal to 0.1, but, at the same time $p^1_{02}(S^2_2) = 0.4$ – the probability of interrupting the operation of the hospital is high. This means that the lack of service 2 does not influence, in itself, the state of IT security of service 1, but substantially decreases the ability to maintain service 1. If we are able to determine, in a similar manner, the value of the probability p^2_{12}, e.g., $p^2_{12} = 0.2$, and of other necessary probabilities, including the return to normal states $p^1_{10}(S^2_0)$, $p^1_{10}(S^2_1)$, $p^1_{10}(S^2_2)$, $p^1_{20}(S^2_0)$, $p^1_{20}(S^2_1)$, $p^1_{20}(S^2_2)$ and finally p^2_{10} and p^2_{20}, we can, starting from any state at time k, conduct further simulation analysis of the system behavior. We can also calculate stationary probabilities which allow to assess the long-term behavior of the entire system if external and internal conditions remain unchanged.

This example clearly shows how many values of relevant probabilities need to be estimated in order to be able to dynamically analyze the development and propagation of threats. It seems that little can be done about it. It is necessary to count on the fact that the development of threats within a given service will actually depend on the condition of a few other services. This should, to a large extent, alleviate the difficulty of estimating a large number of probabilities. The example also shows that dynamic threat analysis limited to the analysis regarding the nearest time perspective in the currently observed condition of services only, requires knowledge of the values of probabilities related to this state. If, suppose, our exemplary system is currently in state $S^1(k) = S^1_0, S^2(k) = S^2_1$, then, for such an analysis, we need to know the values of p^2_{10}, p^2_{12} and, as specified above, $p^1_{01}(S^2_1)$ and $p^1_{02}(S^2_1)$. In particular, knowing the approximate values of these probabilities, we can, being also aware of the short-term effects of individual states expressed in the appropriate scale, determine the expected value of these effects, i.e., the degree of a given risk.

5. Implementation and a Numerical Test

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

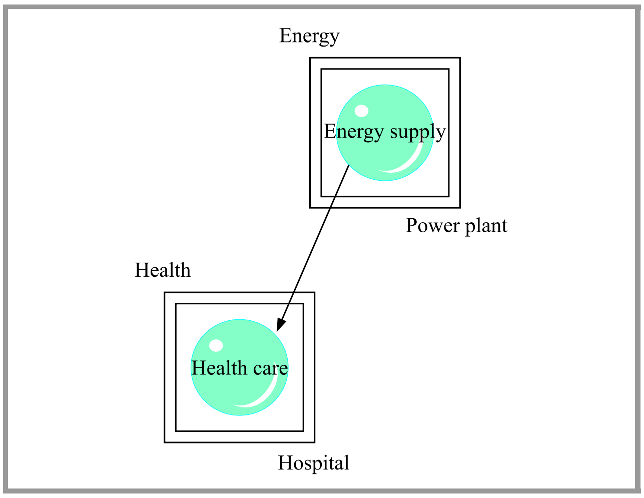
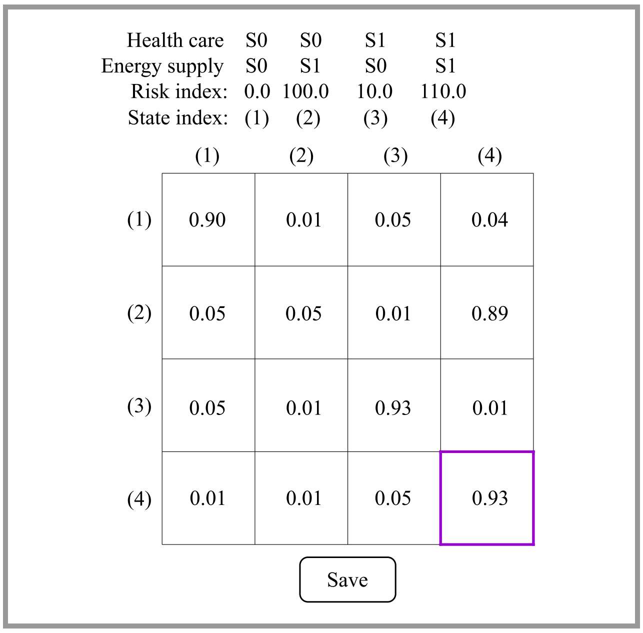


Fig. 1. Graph depicting the services.

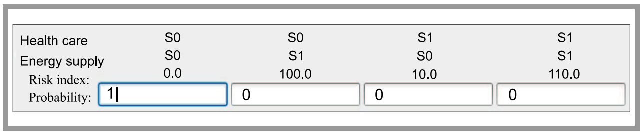
When configuring the model, the user enters the number of iterations (stages), the transition matrix P and the vector of initial input probabilities $\pi(0)$. If we assume that each service can have two states, this matrix will be of size 4 × 4 (Fig. 2). Accordingly, the vector of input probabilities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



Health care	S0	S0	S1	S1
Energy supply	S0	S1	S0	S1
Risk index:	0.0	100.0	10.0	110.0
State index:	(1)	(2)	(3)	(4)

	(1)	(2)	(3)	(4)
(1)	0.90	0.01	0.05	0.04
(2)	0.05	0.05	0.01	0.89
(3)	0.05	0.01	0.93	0.01
(4)	0.01	0.01	0.05	0.93

Fig. 2. Transition matrix.



Health care	S0	S0	S1	S1
Energy supply	S0	S1	S0	S1
Risk index:	0.0	100.0	10.0	110.0
Probability:	1	0	0	0

Fig. 3. Probabilities and risk index vector.

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

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

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

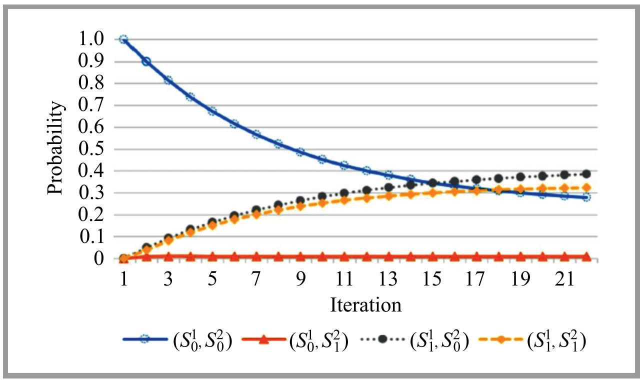


Fig. 4. Time series of probabilities of different states of the Markov chain.

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

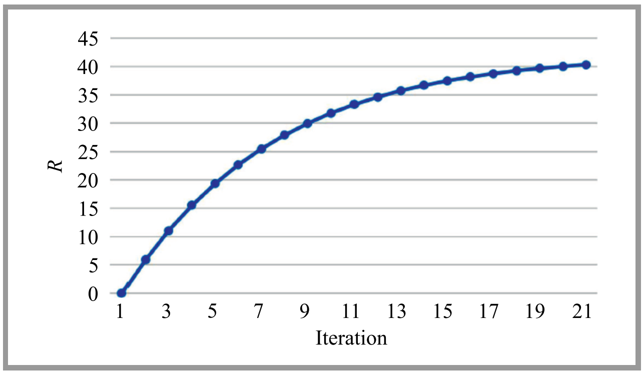


Fig. 5. Time series of the total risk level *R*.

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

6. Perspectives

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

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

7. Conclusions

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

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

Acknowledgements

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

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

References

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

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

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

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

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

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

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

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

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

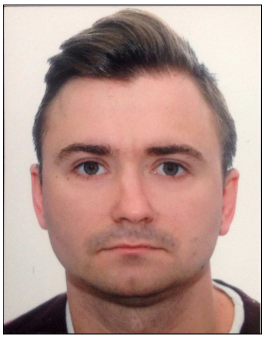
Andrzej Karbowski received his Ph.D. (1990) and D.Sc. (2012) in Automatic Control and Robotics from the Warsaw University of Technology, Faculty of Electronics and Information Technology. Currently he is an Associate Professor at the Institute of Control and Computation Engineering of Warsaw University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

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

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

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

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



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

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

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

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