Advances in Intelligent Systems and Computing 1173

Wojciech Zamojski ·
Jacek Mazurkiewicz ·
Jarosław Sugier · Tomasz Walkowiak ·
Janusz Kacprzyk *Editors*

Theory and Applications of Dependable Computer Systems

Proceedings of the Fifteenth International Conference on Dependability of Computer Systems DepCoS-RELCOMEX, June 29 – July 3, 2020, Brunów, Poland

Springer

Contents

Sequence Mining and Property Verification for Fault-Localization in Simulink Models 1
Safa Aloui Dkhil, Mohamed Taha Bennani, Manel Tekaya, and Houda Ben Attia Sethom

Handwritten Text Lines Segmentation Using Two Column Projection 11
Tomasz Babczyński and Roman Ptak

Convolutional Neural Networks for Dot Counting in Fluorescence in Situ Hybridization Imaging 21
Adrian Banachowicz, Anna Lis-Nawara, Michał Jeleń, and Łukasz Jeleń

Classification of Local Administrative Units in Poland: Spatial Approach 31
Jacek Batóg and Barbara Batóg

Development of Methodology for Counteraction to Cyber-Attacks in Wireless Sensor Networks 41
Olexander Belej, Kamil Staniec, Tadeusz Więckowski, Mykhaylo Lobur, Oleh Matviykiv, and Serhiy Shcherbovskykh

The Need to Use a Hash Function to Build a Crypto Algorithm for Blockchain 51
Olexander Belej, Kamil Staniec, and Tadeusz Więckowski

Common Criteria Vulnerability Assessment Ontology 61
Andrzej Bialas

Risk Management Approach for Revitalization of Post-mining Areas 71
Andrzej Bialas

Performance Assessment of Selected Techniques and Methods Detecting Duplicates in Data Warehouses 221
Paweł Dymora and Mirosław Mazurek

An Overview of DoS and DDoS Attack Detection Techniques 233
Mateusz Gniewkowski

Biometric Data Fusion Strategy for Improved Identity Recognition 242
Zbigniew Gomolka, Boguslaw Twarog, Ewa Zeslawska, and Artur Nykiel

Non-homogeneous Four State Semi-Markov Reliability Model of Operation Process 252
Franciszek Grabski

The Efficiency of Energy Storage Systems Use for Energy Cost Mitigation Under Electricity Prices Changes 263
Alexander Grakovski and Aleksandr Krivchenkov

Capacitated Open Vehicle Routing Problem with Time Couplings 273
Radosław Idzikowski

Mobile Application Testing and Assessment 283
Marcin J. Jeleński and Janusz Sosnowski

Crypto-ECC: A Rapid Secure Protocol for Large-Scale Wireless Sensor Networks Deployed in Internet of Things 293
Wassim Jerbi, Abderrahmen Guermazi, and Hafedh Trabelsi

Redundancy Management in Homogeneous Architecture of Power Supply Units in Wireless Sensor Networks 304
Igor Kabashkin

Successive-Interference-Cancellation-Inspired Multi-user MIMO Detector Driven by Genetic Algorithm 315
Mohammed J. Khafaji and Maciej Krasicki

The Availability Models of Two-Zone Physical Security System Considering Cyber Attacks 325
Vyacheslav Kharchenko, Yuriy Ponochovnyi, Al-Khafaji Ahmed Waleed, Artem Boyarchuk, and Ievgen Brezhniev

Automatically Created Statistical Models Applied to Network Anomaly Detection 334
Michał Kierul, Tomasz Kierul, Tomasz Andrysiak, and Łukasz Saganowski

Sparse Representation and Dictionary Learning for Network Traffic Anomaly Detection 344
Tomasz Kierul, Michał Kierul, Tomasz Andrysiak, and Łukasz Saganowski

The Availability Models of Two-Zone Physical Security System Considering Cyber Attacks

Vyacheslav Kharchenko[1,2], Yuriy Ponochovnyi[3(✉)], Al-Khafaji Ahmed Waleed[1], Artem Boyarchuk[1], and Ievgen Brezhniev[1,2]

[1] National Aerospace University KhAI, Kharkiv, Ukraine
{V.Kharchenko, a.boyarchuk, e.brezhnev}@csn.khai.edu, eng_ahmed.waleed@yahoo.com
[2] Research and Production Company Radiy, Kropyvnytskyi, Ukraine
[3] Poltava State Agrarian Academy, Poltava, Ukraine
yuriy.ponch@gmail.com

Abstract. Relevance of the paper is confirmed by the need to protect the security systems themselves, not only from physical damage, but also from cyber attacks by intruders. The paper explores the Markov model of the two-zone cyber-physical security system. Evaluation of the functioning of the multi-zone system was carried out taking into account two degrees of degradation (operative condition - the failure state of all zones). The state space of the model (or one fragment) has a dimension of 9 states. In the proposed model, hardware failures caused by vandal attacks on objects of the first zone and software failures due to cyber attacks on the functions of the second zone are considered. The simulation results illustrate different transition intervals of availability indicators of various levels of degradation to a stationary state. For different degrees of degradation, the minimum value of the availability function, the time interval of the transition of the availability function to the stationary mode, and the value of the availability function in the stationary mode are determined. When eliminating software defects and vulnerabilities, the increase in the availability function is 0.23% for a zero level of system degradation.

Keywords: Cyberphysical security system · Availability indicators · Markov model · Degradation levels · Multi-Zone architecture

1 Introduction

Modern physical protection systems have powerful cybernetic components that require full or temporary connection to an open Internet network for full functioning. If before there was a dilemma for ensuring the protection of physical security systems themselves only against physical damage, now such systems are an object for cyber attacks by cybercriminals.

The security system is represented by a set of subsystems, each of which is considered as a separate "zone". Each subsystem contains constituent elements. In aggregate, such a hierarchy is presented in Fig. 1 [1]. Each subsystem is represented by

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2020
W. Zamojski et al. (Eds.): DepCoS-RELCOMEX 2020, AISC 1173, pp. 325–333, 2020.
https://doi.org/10.1007/978-3-030-48256-5_32

the failure state spaces of hardware components (HW, hardware) and software/functions (SW, software), which arise due to the manifestation of physical defects (pf), design defects (df), operator errors (hf), and interaction defects (if).

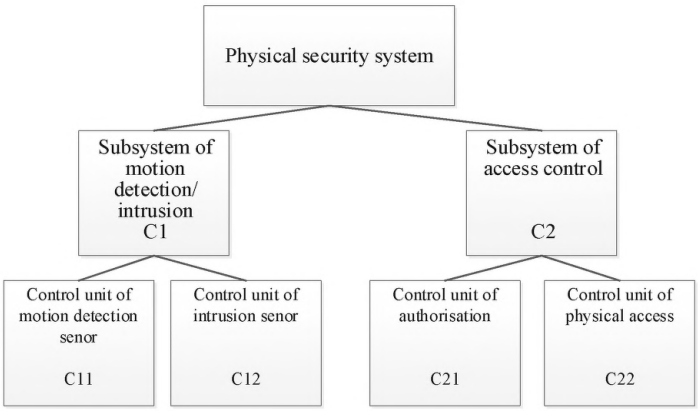

Fig. 1. Two-zone architecture of physical security system

The zonal architecture of physical security systems (PSS, physical security systems), their multifunctionality and functioning in an aggressive external environment require appropriate adequate representation in the construction and analysis of models. The use of the mathematical apparatus of Markov modeling [2, 3], on the one hand, provides a direct assessment of the resulting availability indicator, meets the requirements of standards and normative documents [4, 5]. But, on the other hand, Markov models are limited by assumptions on the simplest flows of events [6], and are also prone to the problem of increasing dimensionality when taking into account a large number of external factors. In [7], a structurally automatic approach to modeling large-dimensional systems is considered. The use of multi-fragment modeling apparatus [8] allows us to study systems with variable parameters, but does not solve the dimensional problem.

In [9], to study systems with variable parameters, it was also proposed to codify Continuous-Time Markov Chains. In [10, 11], Markov and multi-fragment models of hardware and software systems for various purposes for specific architectures are considered. In [12], the Semi-Markov reliability model with variable parameters of event flows was considered.

However, the well-known papers did not consider the influence of zonal architecture on the availability of the system from the standpoint of both reliability and security.

The aim of this study is to develop and analyze the classic Markov model of two-zone PSS availability. The development of the model is based on the determination of many states and mechanisms of interaction taking into account the degree of degradation. Assessment of the availability functions of various degrees of degradation was performed for various sets of input data.

The paper is structured as followed. Next Sect. 2 describes two PSS availability Markov models, their assumptions, states and transitions between them (Subsects. 2.1 and 2.2). The results of the PSS modeling and availability assessment are analyzed in Sect. 3. Section 4 concludes and describes future steps.

2 Development and Research of the Availability Model of Physical Security Systems

2.1 Development of the Initial Model

The availability model of a two-zone cyberphysical security system allows us to study the simultaneous effect of failures of the hardware component of zones and their functions implemented through software. The paper considers a two-zone PSS model (Fig. 1), in which the first zone has an external perimeter and is susceptible to vandal attacks, and the second zone implements access control functions via a remote connection (therefore, it is susceptible to cyber attacks).

The main assumptions of the M_{PSS0} model are:

- the flow of events that transfers the system from one functional state to another has the properties of stationarity, ordinaryness and the absence of aftereffect, the input parameters of the model are assumed to be constant;
- the probability of failure of the cloud service is negligible;
- acts of vandalism (γ_{HW}) are committed on the objects of the first zone, which are located outside the protected perimeter;
- vulnerability attacks (γ_{SW}) are carried out on the functions of the second zone, which are accessible through a public network.

The state space of the model has a dimension of 9 states (Fig. 2), according to combinations of hardware and functional component failures in each of the zones. Also, in Fig. 2, three levels of degradation of the system (0, I and II) are highlighted.

State	Combination of hw/sw failures				Degradation level
S1	1h	2h	1s	2s	0
S2	1h	2h	1s	2s	I
S3	1h	2h	1s	2s	
S4	1h	2h	1s	2s	
S5	1h	2h	1s	2s	
S6	1h	2h	1s	2s	II
S7	1h	2h	1s	2s	
S8	1h	2h	1s	2s	
S9	1h	2h	1s	2s	

Fig. 2. Combinations of zone failures that determine the states of the M_{PSS0} model and degradation levels

In this work, independent failures of hardware and software of two CPSS zones are considered. They are not physically and logically linked and, from the position of Markov modeling, cannot happen simultaneously in an ordinary stream of events.

Figure 3 shows the marked graph of the model, which has end-to-end numbering of states and is developed using the modified grPlot_marker function [13].

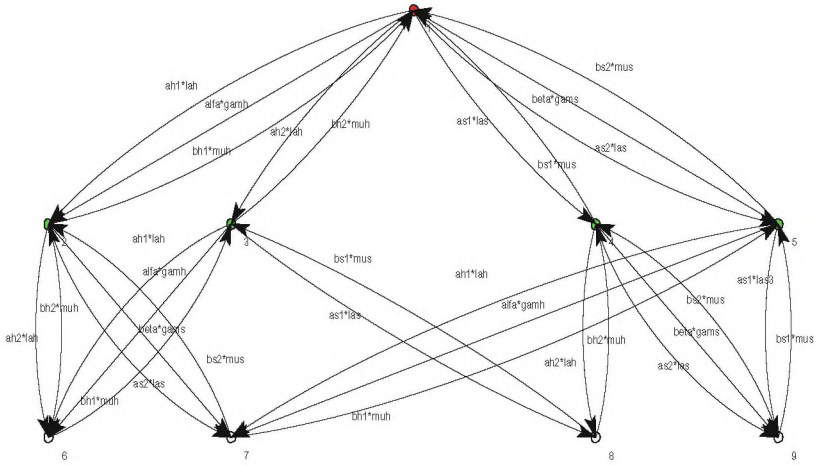

Fig. 3. Marked oriented graph of the two-zone M_{PSS0} model

When constructing the model graph (Fig. 3), a vertical hierarchy of states was used to display the levels of degradation. The upper level is S1 state. It indicates an operative state without failures. The second stage is S2, S3, S4, S5 states. They indicate the state of the first level of system degradation, in which either hardware or functional (software) failure occurred in one of the zones. At the lower level (states S5, S6, S7, S8), the states of complete failure of all zones of the system are indicated. When marking the graph and compiling a system of differential equations, we used the weight coefficients ah1, ah2, as1, as2 to distinguish the failure rates of different zones; and to distinguish the recovery rates, the coefficients bh1, bh2, bs1, bs2 were used.

Hardware failures caused by vandal attacks on objects of the first zone are modeled by transitions - arrows weighted by the index $\alpha^*\gamma_{HW}$. Software failures caused by cyberattacks on the functions of the second zone are modeled by transitions—arrows, weighted by $\beta^*\gamma_{SW}$.

Availability functions for different levels of degradation are defined as:

$$A^{(0)}(t) = P_1(t); \quad A^{(I)}(t) = \sum_{i=1}^{5} P_i(t) \tag{1}$$

Baseline conditions: $t = 0$, $P_0(t) = 1$.

2.2 Development of a Multi-fragment Model for Updating Software Functions

In the previous M_{PSS0} model, the assumption was made that the parameters of the functional components of individual zones of the cyberphysical security system are constant. However, modern systems can receive updates and patches of the software component as part of the development and modification cycles. After installing the update or patch, the program code and/or configuration files change, which directly affects the value of the input parameters of the failure flows and cyberattacks. In [8, 11], such changes are modeled using the multi-fragment approach, which is the basis of the M_{PSSm} model.

The assumptions of this M_{PSSm} model are expanded (in comparison with the assumptions of M_{PSS0}):

- the flow of events that transfers the system from one functional state to another one within the same fragment has the properties of stationarity, ordinaryness and the absence of aftereffect, the model parameters within one fragment are assumed to be constant;
- during the upgrade process, the elimination of software defects and vulnerabilities occurs, new defects and vulnerabilities are not introduced.

The state space of the M_{PSSm} model within one fragment, like M_{PSS0}, has a dimension of 9 states (Fig. 2) and three levels of system degradation.

Figure 4 shows a marked graph of three fragments of the M_{PSSm} model. Each fragment of the model is a mapping of the M_{PSS0} graph (Fig. 3), but for compactness, a vertical arrangement of states was performed.

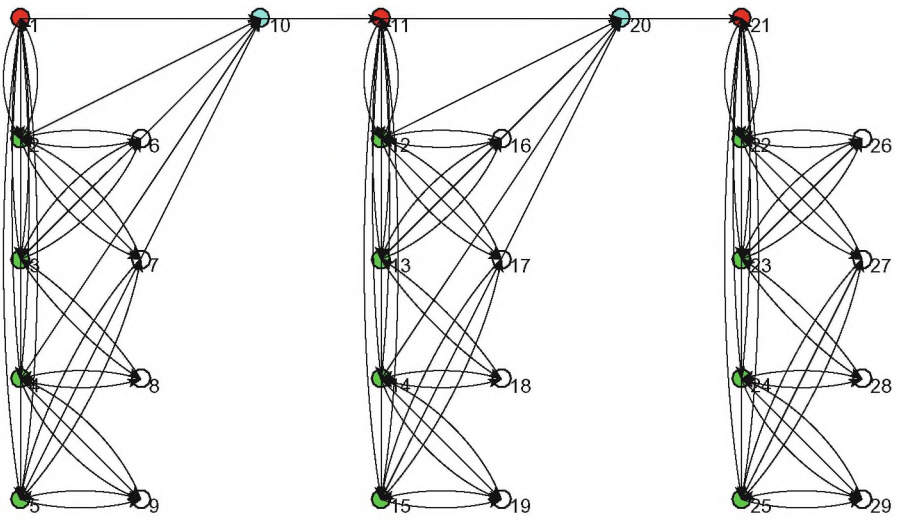

Fig. 4. Marked graph of the three-fragment M_{PSSm} model

When constructing the graph of the model (Fig. 4), the color marking of the states ("Red", "Green", "White") was used to indicate that the states belong to different levels of degradation. Additionally, a "blue" marker was used to highlight SW update states (S10, S20), the system is inoperative in these states.

Availability functions for different levels of degradation are defined as:

$$A^{(0)}(t) = \sum_{i=1}^{Nf} P_{10i-9}(t); \quad A^{(I)}(t) = \sum_{i=1}^{Nf} \sum_{j=1}^{5} P_{(10i-10)+j}(t) \tag{2}$$

3 Simulation and Comparative Analysis

The primary input parameters of Markov models were determined on the basis of certification data [1, 5] for the previous CPSS versions samples. Their values are presented in Table 1. To build the matrix of Kolmogorov-Chapman system of differential equations (SDE) in Matlab, matrix A function was used [14].

The Kolmogorov-Chapman SDE can be solved using analytical methods (substitutions, Laplace transforms, etc.). But this approach is applicable for systems of small dimension. In this paper, we consider a single-fragment model of medium dimension (9 states) and a multi-fragment model of large dimension (29 states), therefore, an approach that is universal for both models to the numerical solution of SDEs was chosen.

Table 1. Values of simulation processing input parameters

#	Sym	Parameter	Value
1	λhw	HW failure rate due to unintentional physical and design defects (pf and df)	1e-3 (1/hour)
2	λsw	SW failure rate due to design defects of an unintentional nature (df)	5e-3 (1/hour)
3	γhw	HW failure rate due to intentional actions (if, vandalism)	1e-3 (1/hour)
4	α	The coefficient of "aggression" of physical attackers, depends on external factors	1..100
5	γsw	SW failure rate due to intentional actions (if, viruses, cyberattacks)	5e-3 (1/hour)
6	β	The coefficient of "aggression" of cyber attackers, depends on external factors	1..10
7	μhw	HW recovery rate after failure, averaging is performed in the research and recovery is considered for all causes of failures (pf, df, hf, if)	1 (1/hour)
8	μsw	SW recovery rate after failure, averaging is performed in the research and recovery is considered for all causes of failures (pf, df, hf, if), the recovery does not provide for the elimination of the causes of failure	2 (1/hour)
9	ah1, ah2, as1, as2	The weight coefficients to distinguish the HW failure rates (ah1, ah2) and SW failure rates (as1,as2) of different zones	[1 2 1.5 1.2]
10	bh1, bh2, bs1, bs2	The weight coefficients to distinguish the HW recovery rates (bh1, bh2) and SW recovery rates (bs1,bs2) of different zones	[1 2 1.3 1.25]

In [15], for the Kolmogorov-Chapman SDE solution, it was proposed to use a software implementation of the Runge-Kutta method. In this papers the SDE solution is obtained using the ode15s function [16]. The simulation results are shown in Fig. 5. The graphs of the M_{PSS0} model (Fig. 5, a) illustrate the typical nature of the change in the availability function with a decrease to a stationary coefficient during the first 10 h of operation. Thus, in further analysis of the results, it is necessary to take into account the values of two levels of availability degradation:

- $A^{(0)}M_{PSS0} = 0,9638$;
- $A^{(1)}M_{PSS0} = 0,9997$.

The graphs of the M_{PSSm} model (Fig. 5, b) illustrate the typical nature of the change in the availability function for multi-fragment models [8, 11, 14]. In the initial period of operation, the availability of the system is reduced to a minimum, and then, as the elimination of SW defects and vulnerabilities, strive for a stationary value.

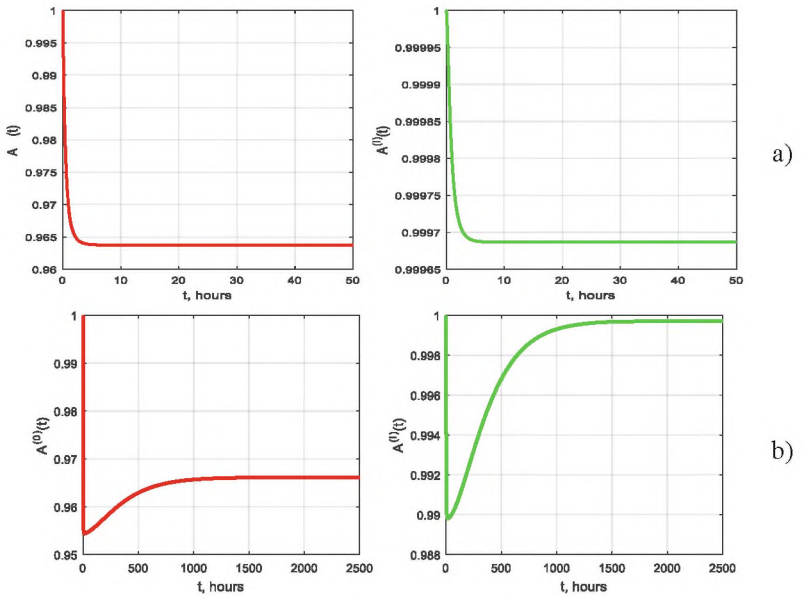

Fig. 5. Results of availability simulations of two-zone CPSS for different levels of degradation: a) model M_{PSS0}, b) model M_{PSSm}

In further analysis of the results, it is necessary to take into account the following groups of values of the resulting indicators for two levels of availability degradation:

a) for zero degradation level $A^{(0)}_{Mpssm}$
   - availability function minimum value $A^{(0)}_{Mpssm}min = 0.9544$;
   - availability function value in stationary mode $A^{(0)}_{Mpssm}const = 0.9661$;

- time interval for the transition of the availability function to the stationary mode $T^{(0)}_{Mpssm}$ = 3383,4 h.

b) for the first degradation level $A^{(I)}_{Mpssm}$

- availability function minimum value $A^{(I)}_{Mpssm}min$ = 0.9898;
- availability function value in stationary mode $A^{(I)}_{Mpssm}const$ = 0.9997;
- time interval for the transition of the availability function to the stationary mode $T^{(I)}_{Mpssm}const$ = 3328,3 h.

4 Conclusion

The article describes two models for assessing the availability of a two-zone physical security system, taking into account vandal and cyber attacks on objects of different zones.

In the M_{PSS0} model, the availability functions of different levels of degradation decrease to stationary values $A^{(0)}$ = 0,9638 and $A^{(I)}$ = 0.9997 during the first 10 h of operation.

In the M_{PSSm} model, the availability function decreases to stationary values $A^{(0)}const$ = 0.9661 and $A^{(I)}const$ = 0.9997 after 3300 h of operation. Thus, the increase in the availability function while eliminating software defects and vulnerabilities is 0.23% for a zero level of system degradation.

Further research should be directed to the studies of the impact of reducing the failure rate (and recovery) of HW and SW on the resulting indicators, as well as the development and research of both Markov and multi-fragment CPSS availability models, in which the assumption of high reliability of the cloud service is removed.

References

1. Waleed, A., Kharchenko, V., Uzun, D., Solovyov, O.: IoT-based physical security systems: structures and PSMECA analysis. In: 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), pp. 870–873. (2017). https://doi.org/10.1109/idaacs.2017.8095211
2. Zheng, Z., Trivedi, K., Wang, N., Qiu, K.: Markov regenerative models of webservers for their user-perceived availability and bottlenecks. IEEE Trans. Dependable Secure Comput. **17**, 92–105 (2020). https://doi.org/10.1109/TDSC.2017.2753803
3. Boano, C., Römer, K., Bloem, R., Witrisal, K., Baunach, M., Horn, M.: Dependability for the Internet of Things—from dependable networking in harsh environments to a holistic view on dependability. e & i Elektrotechnik und Informationstechnik. **133**, 304–309 (2016). https://doi.org/10.1007/s00502-016-0436-4
4. IEC 61508-1: 2010 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements. https://webstore.iec.ch/publication/5515. Accessed 21 Jan 2020
5. IEC 60050-192: 2015 International Electrotechnical Vocabulary (IEV) - Part 192: Dependability. https://webstore.iec.ch/publication/21886. Accessed 21 Jan 2020

6. IEC 61703: 2016 Mathematical expressions for reliability, availability, maintainability and maintenance support terms. https://webstore.iec.ch/publication/25646. Accessed 21 Jan 2020
7. Volochiy, S., Fedasyuk, D., Chopey, R.: Formalized development of the state transition graphs using the Erlang phase method. In: 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). (2017). https://doi.org/10.1109/idaacs.2017.8095255
8. Kharchenko, V., Butenko, V., Odarushchenko, O., Sklyar, V.: Multifragmentation markov modeling of a reactor trip system. J. Nuclear Eng. Radiation Sci. **1**, 031005 (2015). https://doi.org/10.1115/1.4029342
9. Trivedi, K., Bobbio, A., Muppala, J.: Non-homogeneous continuous-time markov chains. Reliabil. Avail. Eng. 489–508 (2017). https://doi.org/10.1017/9781316163047.018
10. Liu, B., Chang, X., Han, Z., Trivedi, K., Rodríguez, R.: Model-based sensitivity analysis of IaaS cloud availability. Fut. Gener. Comput. Syst. **83**, 1–13 (2018). https://doi.org/10.1016/j.future.2017.12.062
11. Kharchenko, V., Ponochovnyi, Y., Abdulmunem, A., Andrashov, A.: Availability models and maintenance strategies for smart building automation systems considering attacks on component vulnerabilities. Adv. Dependab. Eng. Complex Syst. 186–195 (2017). https://doi.org/10.1007/978-3-319-59415-6_18
12. Bobalo, Y., Horbatyi, I., Kiselychnyk, M., Medynsky, I., Melen, M.: Semi-Markov reliability model of functioning of wireless telecommunication system with complex control system. Math. Model. Comput. **6**, 192–210 (2019). https://doi.org/10.23939/mmc2019.02.192
13. Iglin, S. grTheory - Graph Theory Toolbox – File Exchange – MATLAB Central. https://www.mathworks.com/matlabcentral/fileexchange/4266-grtheory-graph-theory-toolbox. Accessed 21 Jan 2020
14. Kharchenko, V., Ponochovnyi, Y., Boyarchuk, A.: Availability assessment of information and control systems with online software update and verification. Inf. Commun. Technol. Educ., Res. Ind. Appl. 300–324 (2014). https://doi.org/10.1007/978-3-319-13206-8_15
15. Yakovyna, V., Seniv, M., Lytvyn, V., Symets, I.: Kolmogorov-chapman differential equation systems software module for reliable design automation. Sci. Bull. UNFU. **29**, 141–146 (2019). https://doi.org/10.15421/40290528
16. Solve stiff differential equations and DAEs – variableorder method – MATLAB ode15s. https://www.mathworks.com/help/matlab/ref/ode15s.html. Accessed 21 Jan 2020