# Patching the Firewall Software to Improve the Availability and Security: Markov Models for Internet of Things Based Smart Business Center

Maryna Kolisnyk [1], Iryna Piskachova [2], Vyacheslav Kharchenko [3]

[1] Department of Automation and Control in Technical Systems, National Technical University "KPI", Kharkiv, Ukraine
kolisnyk.maryna.al@gmail.com
[2] Department of Computer Science and Control Systems, Ukrainian State University of the Railway Transport, Kharkiv, Ukraine
[3] Department of Computer Systems, Networks and Cyber Security, National Aerospace University "KhAI" Kharkiv, Ukraine
v_s_kharchenko@csn.khai.edu

**Abstract.** The paper considers the tasks and solutions for availability assessing and securing the Internet of Things (IoT), in particular, the Smart Business Center (SBC) with wired communication networks. The goal of this paper is to develop and research of SBC availability models, taking into account the changes in power consumption modes in operating systems, denial-of-services (DDoS) attacks, patching for firewalls depending on the presence of software vulnerabilities, considering reliability of system components such as a server and a router. Comparison of several models of the IoT system availability has been made and recommendations have been formulated regarding the policy of patching.

**Keywords:** IoT; a Markov model; DDoS attack; patch on the firewall software; security; availability.

## 1 Introduction

At the present time various intelligent solutions are being actively introduced into Internet of Things (IoT). It is a paradigm that includes the ubiquitous presence of various things/objects in the environment that use wireless and wired networks to transmit data, and a unique addressing scheme allows them to interact with each other and other things/objects to create new applications/services to achieve certain purposes [1].

IoT consists of a large number of different types of devices connected to network devices and networks based on various technologies. IoT systems can be affected by a large number of attacks that adversely affect their proper functioning. Most often, attacks are implemented with the help of software vulnerabilities of devices connected to the IoT network and network devices that connect the sensors to the Internet. Also,

the impact of attacks is often directed to servers that act as control devices that store data collected from sensors, as well as control and monitoring programs. The occurrence of fails and failures of components of the IoT system can also lead to unstable and unreliable operation of IoT. Therefore, protecting the security of IoT components and ensuring their high reliability is a very important task, one of the ways to solve this is to timely patch the vulnerabilities of IoT components. The paper considers how the availability of the IoT system, in particular, the smart business center (SBC), is affected by the installation of patches on the vulnerability of the firewall as a separate network device and server firewall.

The main features of IoT [1, 2]: the interconnection of things (privacy protection, semantic consistency between physical and related virtual things), dynamic changes in device states (connected and/or disconnected things, their location and speed, network scale change with change number of devices).

Standards for IoT was proposed for wired also wireless networks, such as: IEEE 802.3 Ethernet, IEEE 802.11Wi-Fi, IEEE 802.15 Bluetooth, IEEE 802.15.4 ZigBee, Z-Wave, LoRa, 3GPP LTE-A, IEEE 802.16 WiMAX, 2G GSM, 5G [3-5]. IoT devices require protection of confidentiality, integrity and availability of information [1-5]. To ensure the security of the IoT system, can to use [2-11]: restrict network access and connectivity; secure logging, secure password management to ensure user privacy, control and restrict access to the source code of the program (registration procedures should be supported by selecting, implementing and using appropriate authentication methods, closing confidential information in the logs, protecting against various types of attacks); encryption methods; control and protection against physical unauthorized access, registered and protected system user and administrative/operational actions, exceptions, errors and events of information security; the removal of vulnerabilities of hardware and software, and the use of rules to regulate the installation of software by users; secure networks and network services; compliance with the security requirements of information systems, including Web applications and transactions, the use of group access policies. On system components IoT, such as routers, servers, it is necessary to install special antispyware and antivirus programs, firewalls.

Analysis of attack statistics conducted by NIST and CERT [12,13] indicates that there may be vulnerabilities in IoT systems through which attackers perform DDoS attacks. Producers of network equipment and servers used in the construction of IoT systems, after detecting of vulnerability, suggest installing an updated version of the software on the device firewall, which fixes the identified vulnerabilities.

Currently, there are methods of protecting against cyber-attacks, which can also be used to protect against Denial of Service (DDoS) attacks on components of IoT systems [13,14]: Hybrid DDoS Protection; Detection based on behavior; Creation a signature in real time; Plan for responding to emergencies in cybersecurity.

When different types of DDoS attacks are impacted, different methods and mathematical models exist to assess the IoT functioning availability [15-21]. To assess the reliability and the security of IoT systems, mathematical models are often used: Markov chains; semi-Markov chains; hidden Markov models; neural networks; Petri nets;

models of the inhomogeneous Poisson process. In this paper, the mathematical apparatus of Markov chains is applied.

## 2 Goal of the Research

As an object of research, a system based on IoT - a Smart Business Center (SBC) is used. The availability function (AC) is an indicator that is used to assess reliability and security. The goal of the paper is the development and investigation of Markov models of the functioning of SBC subsystems that take into account the different power modes of the operating systems (OS) of the server and router and the impact of DDoS attacks on SBC systems with application of the possible patches to the vulnerabilities of the firewall software and without them.

## 3 Markov Models of SBC Subsystems

The structure of the SBC network includes devices: a router with Ethernet ports, a softswitch, a firewall, a power network, a server with management software, an IP camera, sensors, cables [22, 23]. In the OS of the server and the router there are several power consumption modes of operation [15, 18-21].

When creating SBC, it is advisable to take into account the security, reliability of software and hardware subsystems, the choice of energy saving modes [37,38]. The improved Markov model (Fig. 1) based on the Markov model proposed in [37], describes the SO states considering reliability of SBC software and hardware, attacks on the system and the various power consumption modes of the server and the router. The graph of the Markov model states shown in Fig. 1. This model is an extended in comparing with the model, given in [22] and have differences from the it as takes into account corrected transitions to the states of power consumption modes of the server and the router (from state 2 to 3, 4, 5 and from state 14 to 13, 15, 16). Timely installation of a patch on the firewall software vulnerabilities can reduce or stop the impact of DDoS attacks, which primarily impact the server firewall, router and firewall (as a separate network device) SBC. Figures 2-4 shows the restructured Markov models of SBC states when patches are installed on the firewall software vulnerabilities of the router, server, SBC firewall. The proposed improved Markov model (Fig. 1), in contrast to the model given in [22], takes into account the change in the SO states and the transitions from the state to state when the patch was installed on the server firewall (state 9), on the router firewall (state 14), on the firewall of the SO (state 10).

For the developed model, the following assumptions were chosen [13, 14]:

- the flow of failures that occurs in the SBC system is a process without aftereffects, each time in the future the system's behavior depends only on the state of the system at this time and does not depend on how the system has passed to this state. The flow of failures and failures of both software and hardware is the simplest and obeys the law of exponential distribution. The failures flow in the SBC system has the Markov property;
- the structure of the network include the reservation of the server and router, time of transition to the reserve in the event of a failure of the main device is minimal;

- the number of DDoS attacks and the number of primary defects in the software are constant;
- the monitoring and diagnostics tools are in good working order and determine the technical state of the system with a high degree of authenticity.

Figures 2-4 shows Markov models with a rebuilt structure that change the number of transitions on the graph in case the patch is installed either on the firewall or on the server firewall.

For each rebuilt model (different options for patching or lack of patching on the vulnerability of firewalls), the system of differential linear Kolmogorov-Chapman equations was presented and researched, the AC value calculated and analyzed if normalization conditions:

$$\sum_{i=1}^{22} Pi(t) = 1; P1(0) = 1. \quad (1)$$

The AC is an important indicator of the reliability of SBC when exposed to various types of DDoS attacks, so AC was chosen as the SBC availability indicator, which is defined as the sum of the probabilities of the system staying in well-operating states.

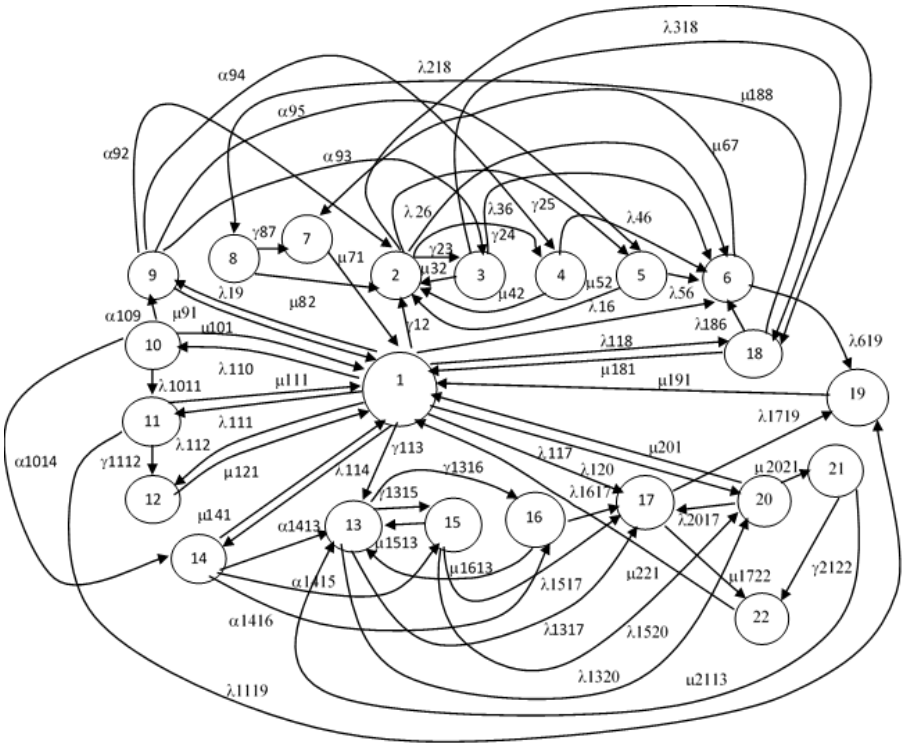


**Fig. 1.** A graph of a Markov model of SBC systems states

For the model shown in Fig. 1, the AC is determined from the equation:

$$AC=P1(t)+P2(t)+P3(t)+P4(t)+P5(t)+P12(t)+P13(t)+P15(t)+P16(t)+P21(t). \quad (2)$$

Pi(t) – probabilities of SBC components states.

The notation for the transition rates in Fig. 2-4 correspond to the notations adopted in [13]. In Fig. 2-4 shown the Markov model of subsystems SBC states when installing patches on the software: the server firewall (Fig. 2); firewall as a separate network device (Fig. 3) and the firewall of the server and the router (Fig. 4).

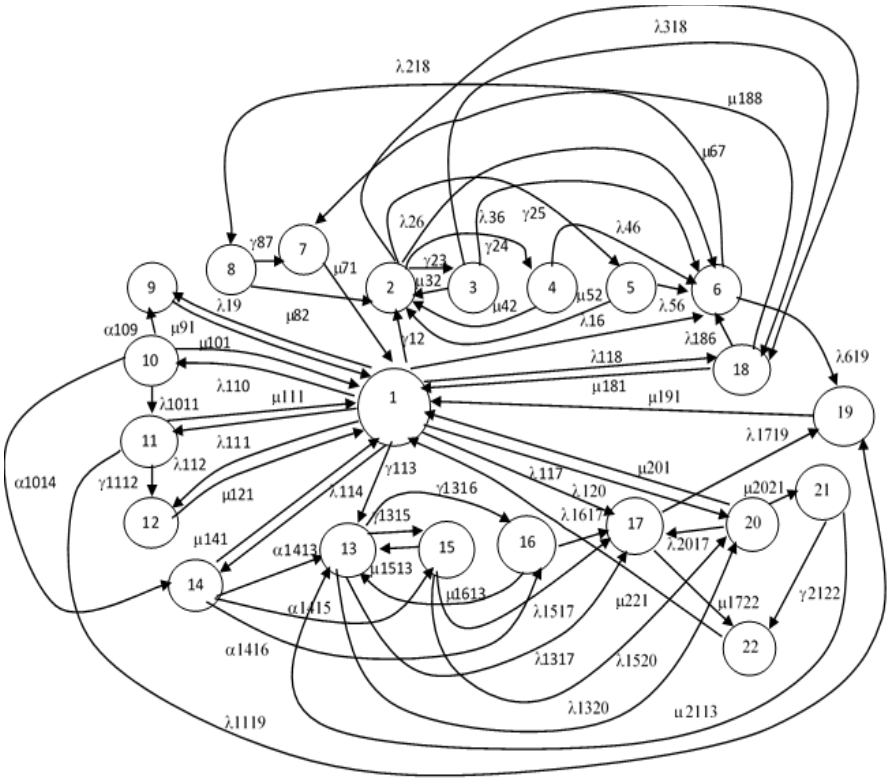


**Fig. 2.** A graph of a Markov model of SBC systems states when installed patches on the server firewall

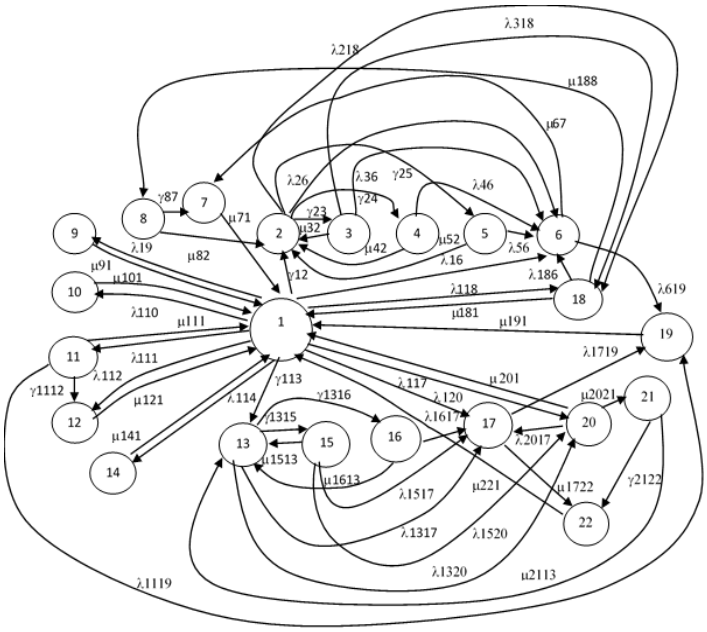


**Fig. 3.** A graph of a Markov model of SBC systems functioning when installed patches on the firewall and the server firewall

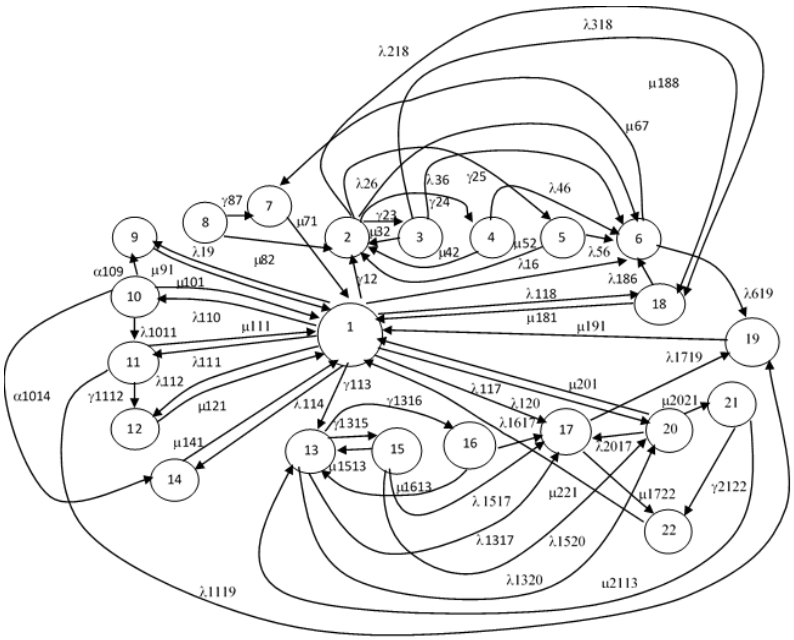


**Fig. 4.** A graph of a Markov model of SBC systems functioning when installed patches on the router firewall and server firewall

## 4 Simulation Results

Basing on the analysis of statistical data, an indicator of the AC can be found. The graphical dependencies of the system AC on the transition rates to different states (λij - failure rates, αij - attack rates, γij - transition rates in different modes power consumption of the router and server, where i = 1...22, j = 1...22) have been received for the various technical states of the SBC components shown in Fig. 5-10.

The analysis of the IoT - SBC system availability was performed taking into account component reliability, recovery rates and various power modes of the server and router, DDoS attacks on the router and server, and removal of vulnerabilities in the firewall software.

In the values of failure rates, factors influencing the reliability of the IoT subsystems during operation (climatic factors, load, vibrations) are taken into account. Initial data for the calculation of AC, the values of which are based on the analysis of statistical data, are: $\lambda 1317=5{,}7\cdot10^{-4}$ 1/h; $\lambda 1517=1\cdot10^{-5}$ 1/h; $\lambda 1617=1\cdot10^{-6}$ 1/h; $\lambda 218=1\cdot10^{-5}$ 1/h; $\lambda 318=1\cdot10^{-5}$ 1/h; $\lambda 1320=1\cdot10^{-6}$ 1/h; $\lambda 1520=1\cdot10^{-6}$ 1/h; $\lambda 2017=1{,}14\cdot10^{-3}$ 1/h; $\lambda 120=1\cdot10^{-6}$ 1/h; μ67=60 1/h; μ141=0,125 1/h; μ111=0,5 1/h; μ32=40 1/h; μ42=30 1/h; μ52=30 1/h; μ1513=50 1/h; μ1613=60 1/h; μ71=0,02 1/h; μ87=2 1/h; μ81=30 1/h; μ101=1 1/h; μ121=5 1/h; μ181=1 1/h; μ191=0,02 1/h; μ91=1 1/h; μ171=1 1/h; μ188=60 1/h; μ61=0,02 1/h; μ2021=60 1/h; μ221=20 1/h; μ211=30 1/h; μ1722=60 1/h; μ201=40 1/h; μ2113= 20 1/h.

The graphical dependencies (Figures 5-10) shows the change in the AC values from the change in the transition rates from one state to another in the Markov models with fixes for software vulnerabilities: the server firewall (AC 9); firewall (AC 10); the firewall of the server and the router (AC 9_14) and without patches (AC).

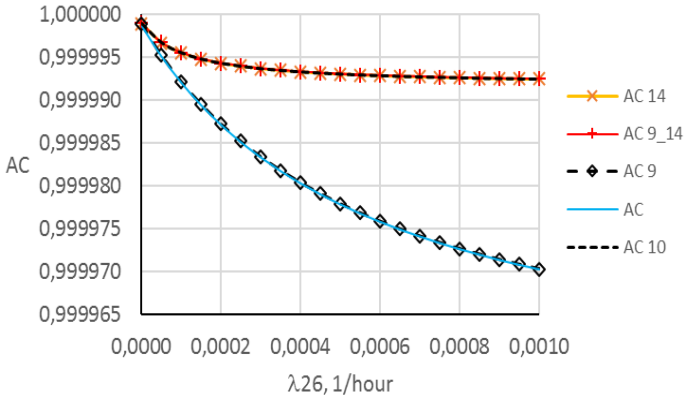


**Fig. 5.** Graphics of AC SBC dependence on the transition rate λ26 from active-power state of the server 2 to a state of the server failure 6 for models with patches on vulnerabilities of: router firewall (AC 14); server firewall (AC 9); firewall (AC 10); server and router firewall (AC 9_14) and without patches (AC) if λ26 change values in range $0...1\cdot10^{-3}$ 1/h

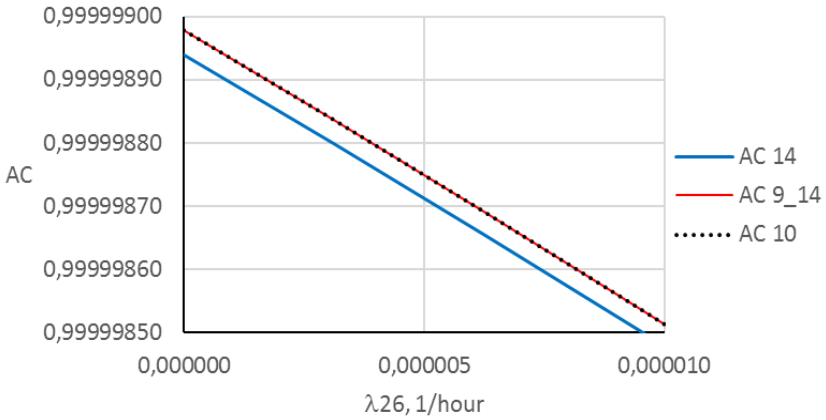


**Fig. 6.** Graphics of AC SBC dependence on the transition rate λ26 from active-power state of the server 2 to a state of the server failure 6 for models with patches on vulnerabilities of: server firewall (AC 9) and router firewall (AC 14) and without patches (AC) if λ26 change values in range $0...1 \cdot 10^{-5}$ 1/h

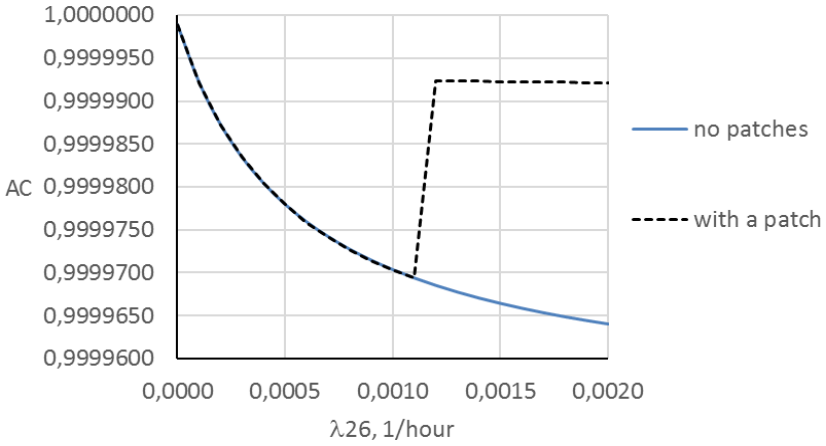


**Fig. 7.** Graphics of AC SBC dependence on the transition rate λ26 from active-power state of the server 2 to a state of the server failure 6 for models with patches on vulnerabilities of: firewall (AC 10) and server and router firewall (AC 9_14) if λ26 change values in range $0...2 \cdot 10^{-3}$ 1/h

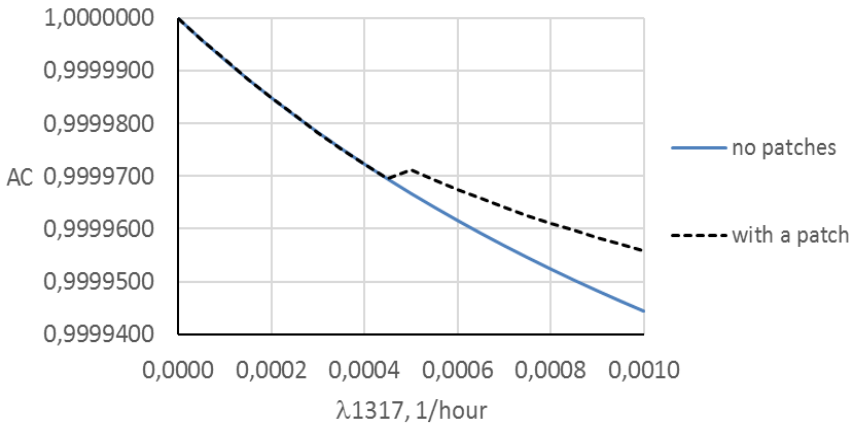


**Fig. 8.** Graphics of AC SBC dependence on the transition rate λ1317 from active-power state of the router 13 to a state of the router failure 17 for models with and without patches on firewall if λ1317 change values in range $0...1 \cdot 10^{-3}$ 1/h

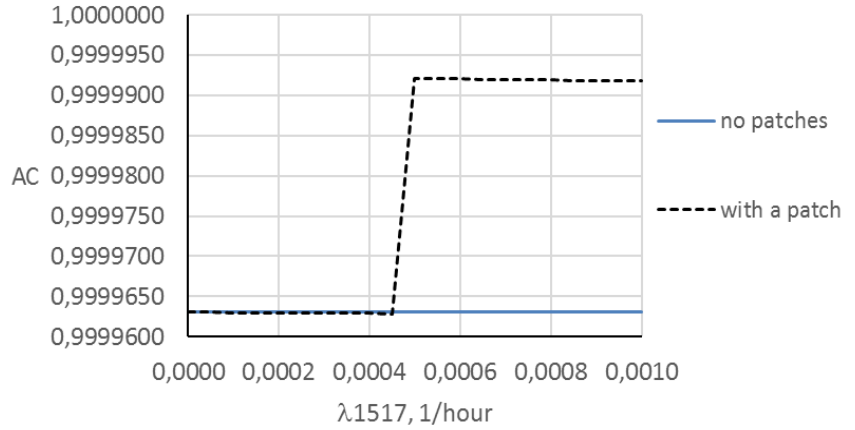


**Fig. 9.** Graphics of AC SBC dependence on the transition rate λ1517 from low-power state of the router 15 to a state of the router 17 for models with and without patches on firewall if λ1517 change values in range $0...1 \cdot 10^{-3}$ 1/h

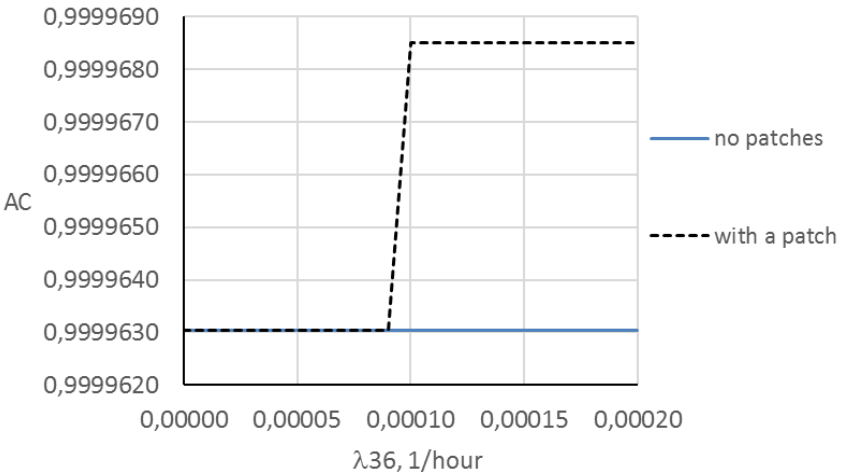


**Fig. 10.** Graphics of AC SBC dependence on the transition rate λ36 from not active-power state of the server 3 to a state of the server failure 6 for models with patches on vulnerabilities of firewall (AC 10) and without patches if λ36 change values in range $0...2 \cdot 10^{-4}$ 1/h

At the software maintenance stage, vulnerabilities can be detected in it, and the manufacturer suggests fixing the patches. If patches on firewall software vulnerabilities are installed, the impact of attacks on the SBC firewall, server or router stops, and the proposed model (Figure 1) is rebuilt (Figures 2-4). When DDoS attacks affect the SBC server and router, the power consumption of these devices increases, because they can't switch to a low-power mode, because they constantly process requests for data transmission and processing.

Figure 5 shows the graph of AC SBC from λ26 - the transition rate from a good-working state in the active mode (2) to the server failure state (6) without patches in the attack conditions (AC) and patches on vulnerabilities of the firewall software of the router (14), router and server simultaneously (9 and 14), server (9), firewall at SBC (10) input. As can be seen from the figure, with increasing λ26, installing a patch on the firewall software of the server at $\lambda 26 = 1 \cdot 10^{-3}$ 1/hour gives the value of AC = 0.99997 and slightly affecting the availability of the system, since with the selected source data it differs from the system's AC without patches on $10^{-9}$. At the same time, when the patches are installed on the vulnerabilities of the firewall software, the firewall server and the router, the firewall of the router (states 10, 9_14, 14) the system readiness is increased and at $\lambda 26 = 1 \cdot 10^{-3}$ 1/h is AC = 0.999925. On Fig. 6 shown the graph of AC dependency, taking into account patching, on the vulnerability of the firewall software, the server firewall and the router, the router's firewall with a higher sampling rate than Fig. 5. Analysis of graphs (Fig. 5, Fig. 6) showed that the greatest increase in AC occurs when patching the vulnerabilities of the router and the server simultaneously (9_14) or the vulnerabilities of the entire system's firewall (10).

The research data are valid for a given set of input data, which must be periodically refined.

The developed models allow to take into account the change in the transition rates from one state to another state under attack conditions and the installation of patches for various vulnerabilities (Fig. 7-10). The calculations took into account the average statistical data from several sources [24,25] - the critical number of data packets for DDoS attacks, which leads to possible fails and failures of various SBC devices or failure of the entire system. The beginning of the attack can't always be determined. An indirect sign of the beginning of the attack can serve as an increase in the requests flow to a critical level. Under the influence of an attack, an increase in the transitions rates from one state to another leads to a decrease in the value of AC. After installing the patch, when the critical level of the transitions rates is reached, AC increases. According to the average statistical data, critical values were adopted for the rates of transitions under attack conditions: $\lambda 36 \leq 1 \cdot 10^{-4}$ 1/h, $\lambda 26 \leq 1.2 \cdot 10^{-3}$ 1/h, $\lambda 1317 \leq 5 \cdot 10^{-4}$ 1/h, $\lambda 1517 \leq 1 \cdot 10^{-5}$ 1/h. When specifying conditions for determining attacks based on later statistics and installing patches, can get updated graphs of the AC dependence on the system transitions rates from one state to another.

The graphical dependences shown in Fig. 7-10, reflect the change in the value of AC, when the transition rates $\lambda 26$, $\lambda 1517$, $\lambda 36$ change values in the range $0...2 \cdot 10^{-4}$ 1/h in two cases: when the model does not take into account the installation of a patch on the vulnerabilities of the firewall software and when in the model it is considered that fixing the vulnerabilities of the firewall software will be immediately as soon as the attack shows itself. The use of patches on software vulnerabilities of devices after detection of the attack process immediately significantly increases the value of AC SBC: AC ($\lambda 26$) to about 0.9999925, AC ($\lambda 1317$) to about 0.99997, AC ($\lambda 1517$) to about 0.99999, AC ($\lambda 36$) to about 0.99990.

## 5 Conclusions and the Future Work

The research showed that the IoT system, even with the required high AC value, is highly dependent on the correct failure-free operation of the firewalls.

Analysis of the graphical dependencies obtained for the developed models, taking into account the rearrangement in case of appearance and installation of the patch on the vulnerability of the firewall software, showed that AC SBC is most sensitive to patching the firewall software of the router and the network firewall. When the patch is set, the AC remains high (0.9999925), even with a transition rate to a failure state of 0.001 1/h.

The hypothesis is confirmed that the establishment of the patch significantly increases the AC value even at clearly high values of the transition rates to the failure state.

Further research can be aimed at clarifying the time of attacks on SBC components, so that the firewall software vulnerabilities is closed by the patch in a timely manner to prevent the failure of SBC components.

The practical importance of the results allows to assess the SBC availability and to develop recommendations to reduce the vulnerability of its software from the impact of DDoS attacks, as well as reduce its power consumption.

## 6 Acknowledgements

This research is supported by the STARC project ("Methodology of sustainable development technologies and information technologies for green computing and communications"), funded by the Department of Education and Science of Ukraine. In addition, the authors, thanks to the colleagues in the Erasmus + ALIOT project (573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP) for discussion during the development of MSc and courses PhD, dedicated to the research and evaluation of the reliability and security of IoT systems.

## References

1. Internet of Things. IoT Governance, Privacy and Security Issues. European Research Cluster on the Internet of Things. January, 2015. 128 p. Available at: https://www.researchgate.net/publication/275540220_IoT_Governance_Privacy_and_Security_Issues.
2. ISO/IEC JTC 1. Preliminary Report 2014. Internet of Things (IoT). 13 p. Available at: https:\\www.iso.org, https:\\iec.ch.
3. Roberto Minerva, Abyi Biru, Domenico Rotondi. Towards a definition of the Internet of Things (IoT). IEEE Internet of Things. Issue 1 – Published 13 MAY 2015. Telecom Italia S.p.A. 86 p.
4. IEC. IoT 2020: Smart and secure IoT platform. White paper. http://www.iec.ch/whitepaper/pdf/iecWP-loT2020-LR.pdf. 193 p.
5. Architecture and Protocols for the Internet of Things: A Case Study/ Angelo P. Castellani, Nicola Bui, Paolo Casari, Michele Rossi, Zach Shelby, Michele Zorzi. 679-683 p. Available at: https:\\www.ieeexplore.ieee.org/document/5470520/.
6. Andrei Babulevich. The Importance of Quality Assurance Testing for the Internet of Things/ Andrei Babulevich, Ron Mader, Dan Myers, Sudha Sundaresan/Ayla Networks. 12 p. Available at: https:\\www.aylanetworks.com.
7. Ovidiu Vermesan, Peter Friess. Internet of Things – From Research and Innovation to Market Deployment/ River Publishers Series in Communication. 2014. 451 p.
8. ISO/IEC 27002:2013. Information technology — Security techniques — Code of practice for information security controls. Available at: http://www.iso27001security.com/html/27002.html.
9. IERC-AC4-SemanticInteroperabilityManifiesto-V1. IoT Semantic Interoperability: Research Challenges, Best Practices, Solutions and Next Steps - IERC AC4 Manifesto - "Present and Future". IERC AC4 2012 – 2014. 99 p.
10. ISO/IEC. Study Report on IoT Reference Architectures/Frameworks. August 2014. 76 P.
11. Masanobu Katagi, Shiho Moriai. Lightweight Cryptography for the Internet of Things. Sony Corporation. 2012. Available at: https://www.researchgate.net/ publication/267246530_Lightweight_Cryptography_for_the_Internet_of_Things.
12. NIST initiatives in IoT. 31.10.2017. Available at: https://www.nist.gov/ itl/appliedcybersecurity/nist-initiatives-iot.
13. NIST Special Publication 800-183 Networks of 'Things'. Jeffrey Voas. Computer Security Division Information Technology Laboratory. Available free of charge from: http://dx.doi.org/10.6028/NIST.SP.800183. July 2016. 30 p.

14. Threat Advisories and Attack Reports. RDoS Attacks: DDoS For Ransom Blooms in the Spring. ERT Threat Alert Cyber Ransom Blooms in the Spring May 3, 2017. 4 p. Available at: https://security.radware.com/ddos-threats-attacks/cyber-ransom-spring2017/. 05.03.2017.
15. Internet Architecture Board (IAB). RFC 7452 “Architectural Considerations in Smart Object Networking”. https://www.rfceditor.org/pdfrfc/rfc7452.txt.pdf.
16. Device Power States. Microsoft. https://docs.microsoft.com/enus/windows-hardware/drivers/kernel/device-power-states.
17. Seh Kwa, Debra T. Cohen — INTEL corporation. PCI Express Architecture Power Management. White Paper - November 8, 2002. 15 p. https://www.intel.com.br/content/dam/doc/white-paper/pci-expressarchitecture-power-management-rev-1-1-paper.pdf.
18. Device power management. Microsoft Hardware Dev Center. https://docs.microsoft.com/en-us/windows-hardware/drivers/ bringup/device-power-management.
19. Advanced Configuration and Power Interface. Specification Revision 5.1. Hewlett-Packard Corporation, Intel Corporation, Microsoft Corporation, Phoenix Technologies Ltd., Toshiba Corporation. July, 2014. 958 p. http://www.acpi.info/DOWNLOADS/ACPIspec50.pdf.
20. Industrial Enterprise and IoT Security Threats: Forecast for 2018 Kaspersky Lab ICS CERT. Available at: https://icscert.kaspersky.com/media /KL_ICS_CERT _Predictions2018_ICS_IoT_EN_30112017.pdf. 8 p.
21. Common Internet of Things devices may expose consumers to cyber exploitation. October 17, 2017. Alert Number I-101717a-PSA. Available at: https://www.fbi.gov/contact-us/field, https://www.ic3.gov/media/2017/171017-1.aspx, https://www.uscert.gov/ncas/current-activity/2017/10/17/IC3-Issues-Alert-IoT-Devices.
22. A Markov model of IoT system availability considering DDoS attacks and energy modes of server and router. Maryna Kolisnyk, Vyacheslav Kharchenko, Iryna Piskachova, Nikolaos Bardis. ICTERI 2017. 14 p. http://ceur-ws.org/Vol-1844/10000699.pdf.
23. Reliability and Security Issues for IoT-Based Smart Business Center: Architecture and Markov Model. Kharchenko Vyacheslav, Kolisnyk Maryna, Piskachova Iryna. IEEE; Computer of science, MCSI 2016, Greece, Chania, 2016. Paper ID: 4564699.