A Markov Model of IoT System Availability Considering DDos Attacks and Energy Modes of Server and Router

Maryna Kolisnyk[1], Vyacheslav Kharchenko [2], Iryna Piskachova[3], Nikolaos Bardis[4]

[1] Department of Automation and Control in Technical Systems, National Technical University "KPI", Kharkiv, Ukraine
kolisnyk.maryna.al@ukr.net
[2] Department of Computer Systems and Networks National Aerospace University "KhAI" Kharkiv, Ukraine
v_s_kharchenko@csn.khai.edu
[3] Department of Computer Science and Control Systems, Ukrainian State University of the Railway Transport, Kharkiv, Ukraine
ipiskacheva@gmail.com
[4] Department of Mathematics & Engineering Sciences Hellenic Military Academy Athens - Vari - 16673, Greece

Abstract. Internet of things (IoT) gets more spread, and large number of smart things are connect to the Internet. In this regard, increases energy consumption. The devices of the IoT can be affected by special attacks on the power supply system, DDos attacks, spy attacks. The purpose of research is to develop and research an availability model of IoT systems considering energy modes and cyber attacks. The analysis of main subsystems of the IoT system such as the smart business center (SBC) in terms of availability, security and energy saving was provided. Main research issues of the paper are analysis of the possible types of attacks on IoT infrastructure, assessment of its availability factor, development and research of a Markov model of SBC availability taking into account DDoS attacks on the server and the router and the diversification of energy supply systems and energy modes.

Keywords: IoT, DDoS and DoS attacks, Availability, Energy mode.

1 Introduction

1.1 Motivation and Work Related Analysis

The paper discusses the Internet of Things (IoT), a concept that includes the ubiquitous presence of various elements / objects that use a wireless or wired network and a unique addressing scheme and interacts to create new applications / services to achieve the specified goals [1,2].

This wired and wireless sensor systems, which transmit information from one device to another (M2M solutions, applications to process data from sensors, mobile

electronic devices, and cloud infrastructure). IoT extends the scope of the Internet by people working at the computer in the direction of the autonomous intelligent smart devices connected to the Internet for remote monitoring and diagnosis [3-5].
IoT networks consist of components such as: data processing centers (datacenters) or stand-alone servers, routers, switches, sensors, communication lines. Network devices are able to receive and transmit information; can interact with other objects or be independent; may have different levels of access to its settings, depending on the security level, etc. [1-4]. The number of devices connected to the IoT, is growing every day [5-7]. It may be smart sophisticated industrial complexes, smart transport, smart lighting systems of cities, car parks, hospitals smart, smart buildings.

For business IoT provides significant advantages in terms of automation, energy efficiency, asset tracking and inventory management, dispatch and location, security, personal tracking and power savings. Energy efficiency in this case is essential to bring the full potential of IoT to life. Most of the sensors and cameras that make up the IoT network, has power from batteries, which must operate for several years without any maintenance or replacement. To operate for extended periods only from a single battery charge, the device should consume minimal power. Also IoT devices may have the power of the energy derived from an external sources such as solar panels, wind turbines, diesel generators, heat pumps, natural gas, the use of which leads to a lower consumption of electrical energy [5-7].

1.2 Goal and Structure

The increasing complexity and importance of IoT has led to an increase in the number of DoS- (Denial of Service), DDoS- (Distributed DoS) attacks on the IoT management system, the use of IoT devices for malicious purposes. All of these unauthorized influences lead to failures and failures of the critical systems that are part of the IoT. Therefore, studies aimed at improving the reliability of the system in the context of successful DoS and DDoS attacks are topical. The article examines the statistics of DoS and DDoS attacks in the world, developed the Markov model of IoT research, taking into account the impact of attacks on the server, router and IoT power supply system. We investigate the effect of successful attacks on the availability factor of the IoT system.

Due to the increased complexity of IoT there were two issues that require quick solutions: 1) increasing the number of DoS- and DDoS- attacks on IoT systems and data center servers; 2) increasing in power consumption in the case of successful attacks. Nowadays in the code 80% of the web-resources was discovered average risk level vulnerability Cross-Site Scripting (XSS), which allows attacker to implement in the user's browser arbitrary HTML-tags, including JavaScript language scripts, and other languages, and get the value of the identifier of attacked session, and perform other illegal actions, such as phishing attacks. Nearly 47% of web sites also contain the vulnerability associated with the lack of protection against the selection of credentials (Brute Force). Now is the large number of vulnerability of TCP connections and spurious resets (RSTs), sent with forged IP source addresses (spoofing) [8-10].

An example is using of protocols causing reflection when an attacker sending a TCP SYN packet to a well-known server with a spoofed source address; the resulting TCP SYN ACK packet will be sent to the spoofed source address. The DDoS attack prevents normal use of the computer or network by valid users. A new form of attack is a class known as the Non-Reflection DDoS attack. This new technique uses very large numbers of devices typically classified as "Things" in the terminology of the IoT, that can be harnessed from all areas of the Internet and for large number of networks. This massive number of devices that successfully generate attacks on throughput rates on the order of one Terabit-per-second (Tbps) or more [11].

The devices which are used to attack: DVRs, IP Cameras, CCTV, NVR, DVR devices (video surveillance); satellite antenna; network devices (such as routers, access points, WiMAX, cable and ADSL-modems, etc.); NAS (Network Attached Storage) with Internet access, video monitors, game consoles. Affected Internet devices are used for: preparation of an attack on any Internet destinations and Internet services such as HTTP, SMTP and network scanning. Vulnerable devices are then become infected with malicious software that turns them into "bots," forcing them to obey to a central control server that can be used as a staging ground for launching powerful DDoS attacks designed to knock Web sites offline. The most attacked protocols were SSH (57%) and Telnet (42%) [12**].** Is being created and use unauthorized SSH tunnel, although IoT devices must to be protected from this type of access by the implementation of secure shell commands in a web-interface without any user administrator privileges [13].

Malware-based botnets like Mirai, XOR and BillGates continues to expand on botnet-based attacks but is also being used in DDoS-For-Hire and extortion campaigns [14]. Attack vectors: SYN, UDP fragment, PUSH, TCP, DNS and UDP floods [15]. In addition to the simple flood-attacks, widespread in the last few years the application level attacks DDoS flooding attack at Application-level (Level 7 of the OSI model), aimed at ending the provision of legitimate services to the user and exhaustion of the server resources like CPU, memory, disk/database bandwidth, sockets, input/output bandwidth. DDoS is accomplished by sending large amounts of otherwise legitimate requests to a network-aware application. It can be sending a large amount of requests to a web server, for increase the load the server process. The goal of this type of attack is to prevent other users to access the service by forcing the server to fulfill an excessive number of transactions. The network itself may still be usable, but since the web-server process cannot respond to the users, access to service is denied [16].

The fight against these attacks is more difficult, as the system firewall and Image Packaging System (IPS) regard such attacks as legitimate traffic, taking into account the construction of a full TCP 3-way handshake. Also DDoS-attacks in 2016 aimed at disabling of Load balancer mechanism of known companies-developers routers, using the vulnerability in their software or features of balancing algorithms. The fight against these attacks more difficult, as the system firewall and IPS regard such attacks as legitimate traffic, taking into account the construction of a full TCP 3-way handshake [17].

Attacks on IoT are the massive DDoS campaigns, which were tied to an IoT malware strain known as Mirai, is capable of launching multiple types of DDoS attacks, including SYN-flooding, UDP (User Datagram Protocol) flooding, Valve Source Engine query-flooding, GRE (Generic Routing Encapsulation) flooding, ACK-

flooding (including a variant intended to defeat intelligent DDoS mitigation systems, or IDMSes), pseudo-random DNS label-prepending attacks (also known as DNS "Water Torture" attacks), HTTP GET attacks, HTTP POST attacks, and HTTP HEAD attacks [18].

In September 2016 attackers organized DDoS attack with capacity of 620 Gbps on site of journalist Brian Krebs, then on hosting provider OVH, follow a trend to exploit a 12-year-old vulnerability in OpenSSH to take control of thousands of poorly protected and vulnerable IoT devices being used for malicious purposes and generated 1.2 Tbps malicious traffic, which was primarily masked TCP and UDP traffic over port 53, using mechanism TCP/ACK, TCP/ACK+PSH, TCP/SYN [17-20]. Mirai exploits a version of Linux known as BusyBox, which is used in various IoT devices, botnet numbered 145607 IP wireless cameras, DVRs and home routers as proxies for malicious traffic [21].

The domain name system (DNS) DDoS attacks caused problems for Dyn and intermittently disrupted websites such as Netflix, Amazon, Twitter, Reddit and others. As a result, the target systems responds slowly or are completely crashed [22,23]. Statistics of DDoS attacks in 2015-2016 is shown in the table 1.

Table 1. Statistics of DDoS attacks

Date	Name of Botnet	Number of attacks	Using mechanisms
May 2015	MIT	30 DDoS	SYN flood
December 2015	BillGates Botnet	6 DDoS	SYN and DNS Floods, ICMP flood, TCP flood, UDP flood, SYN flood, HTTP Flood (Layer7), DNS query-of-reflection flood
January 2016-March 2016	BillGates Botnet	19 DDoS	GET –flood
March 2016	BillGates Botnet	4 DDoS	TFTP reflection
August 2013 - April 2016	MIT	74 DDoS	SYN and DNS Floods, ICMP flood, TCP flood, UDP flood, SYN flood, HTTP Flood (Layer7)
April 2016	BillGates Botnet	10 DDoS	TFTP Reflection
June 2016	XOR	6 DDoS	UDP Flood, UDP Fragment, SYN and DNS Flood, SSH brute force attempts for root login credentials (previously it was reported that infection methods include a vulnerability in ElasticSearch Java VM)
August 2016	Kaiten/STD / Mirai	6 DDoS	Brute-force of Telnet and SSH ports
September 2016	Mirai/Gafgyt (known under the name Lizkebab, BASHLITE, Bash0day,	2 DDoS	Masked TCP and UDP, TCP/ACK, TCP/ACK+PSH, TCP/SYN

	Bashdoor and Torlus) DDoS		
October 2016	Mirai	2 DDoS	Vulnerabilities in NTP and DNS, SYN, UDP fragment, PUSH, TCP, DNS and UDP floods, GRE flood
November 2016	Mirai	5 DDoS on banks	TCP/ACK, TCP/ACK+PSH, TCP/SYN

After gaining access to the network, the attacker can:

- make the process of the invasion transparent for the personnel serving the information system for the purpose of theft of more information from the servers.
- send invalid data to applications or network services, which causes abnormal termination or behavior of the applications or services.
- flood a traffic of computer or the entire network until a shutdown occurs because of the overload. To block traffic, which results in a loss of access to network resources by authorized users [24].

Investigation of DDoS-attack statistics showed that they have different principles of implementation. Even small data packets, which are formed in large number during attacks, can lead to catastrophic failures. Therefore, it is necessary to consider all possible consequences of attacks, their effect on system failure and increase in power consumption by the system under the influence of DDoS attacks.

Goals of the paper are:

- research of IoT based Smart Business Center (SBC) availability considering DoS and DDoS-attacks and determining of the most vulnerable subsystems of SBC;
- develop a mathematical model to assess availability taking into account security and energy modes issues.

2 Analysis of SBC Power Consumption Issues

2.1 Requirements to SBC

To IoT for office solutions (SBC) are presented such basic requirements:

a) in order to save energy in SBC may to perform the installation of temperature control automatic systems, connection to the mobile network of intelligent systems Smart Metering accounting (electricity, gas and water), which allows you to make decisions on the use of certain energy modes in the office, as well as to save staff time through the use of remote water consumption data collection, electricity, gas, etc.

b) the possibility of using the various sensors and control units. It is necessary not just to automate certain functions (control of lighting, heating, ventilation and air conditioning - HVAC, etc.), but to integrate virtually any SBC equipment into a single system, works on the algorithm which will set the installer and designer SBC;

c) a complete feedback, which will allow to operate virtually all systems SBC, analyze the situation, make conclusions and to be able to control the SBC without

external intervention (without pressing the control panel button), but only upon the occurrence of an event (for example should be provided, the emergence of the human in the corridor include of lighting, on-off ventilation and air conditioning system, power source switching to an alternative power supply, etc.);

d) SBC system should give staff full control over their offices and to provide protection against emerging new threats and threats due to the fact that new computer technologies with connection to the internet allow attackers to connect to the system. IoT architecture of any system consists of five levels: the intellectual level of the connection, the data information at the connection level, the cybernetic level, cognitive level, the configuration level. Malicious attacks on impact and vulnerability components of IoT devices, software, and a database (DB) can be applied to each of these levels. The aim of intruders can be stored data, video and audio recording, shutdown of hardware and software components of IoT, industrial espionage. List of types of malicious actions performed by the attacker: illegal use of user accounts; physical theft of office equipment and data carriers; theft software; run the executable code for the damage to the systems, for the destruction or corruption of data; modification data; identity theft; execution of actions that do not allow users to access network services and resources; execution of actions that reduce network resources and bandwidth. The basis of any SBC system - is the server on which the control software is stored. The largest number of DoS - and DDoS – attacks direct to servers. Some types of attacks aimed at disabling the router and the switch, resulting in a malfunction of computers, tablets, smart phones and a variety of IoT devices connected to the system, as well as the basic components SBC system - sensors [8]. Also on the supply system can be carried out special attacks;

f) increase the number of computers and servers resulting in significant power consumption, it is necessary to provide greater flexibility and adaptability of the infrastructure of power facilities.

2.2 Methods to Reduce the SBC Power Consumption

To reduce the load on the power supply can to use a variety of methods, including:

- active implementation of alternative energy sources. Alternative energy helps to improve the economic situation in the country and contribute to environmental improvement. Appropriate use of renewable or locally generated energy in SBC: solar, wind, hydro, geothermal, fuel cell, heat pumps, incorporating liquid cooling in a data center environment will reduce the consumption of electric energy [5];

- using a virtualization to reduce the number of computers and servers. Using this method can reduce the number of servers, which will decrease the load on the power supply and reduce the release of thermal energy;

- using of energy-efficient chips at designing UBTS management systems. For example, a prototype energy-efficient Wi-Fi-chip Rockchip RKi6000, reducing the consumption of IoT-devices by 85% was introduced in early 2016, to BT4.0 LE level. One of the advantages of the chip - technology of adaptive dynamic power management. Ultra-low consumption and can be achieved in the operating mode, and a standby mode [6];

- using, whenever possible, the low-speed, but reliable data transmission. The use of traditional cellular technology in this area is too expensive, it can use a network of Low-Power Wide-area Network - energy-efficient network of long-range - wireless small data volume transmission technology over long distances, providing environment data collection from sensors, meters and sensors [7];

- with sleep mode, these devices may not work for a while. According to the [25], there are mode power network equipment, which is used when creating IoT: Active - sending packages with high power consumption. Normal Idle (N_IDLE) - no packets (less energy). Low-Power Idle (LP_IDLE) - no packets, less energy-intensive. Power consumption is reduced by turning off unused circuitry during LP_IDLE (part of the PHY, MAC, interconnects, memory, CPU), and only the necessary circuits (for example, clock recovery, alarm) should be included;

- using of standby mode. This mode is implemented in servers, workstations, in some models of routers. In standby mode, the power consumption of each individual device IoT is minimal, and power consumption increases when attacks to the server and network equipment are successful.

The operation system of server has the following modes of reduced energy consumption [26]:

S1 (Power On Suspend, POS, Doze) - Power Saving mode, which turns off the monitor, hard drive, but the central processing unit (CPU) and RAM (memory modules) power is applied, reduced the frequency of the system bus. CPU cache is cleared, the CPU does not perform the instructions from the generator CPU.

S2 (Standby Mode) - reduced power consumption mode. In this mode, the monitor and the hard drive disable. From the CPU turns off the power supply. They stop clocks (continue to operate only those devices that are necessary for memory). Power is supplied only to the system memory (it contains information about the system status).

S3 (Suspend to RAM, STR, Suspend) - Standby. With this power saving mode, power is supplied only to the RAM (it stores information about the system status). All other PC components are disabled.

S4 (Suspend to Disk, STD, Suspend to Hard Drive, S4-Hibernation) - a deep sleep. With this power saving mode, the current state of the system is written to the hard drive, the power to all components of the PC is turned off.

3 A Markov Model of SBC Availability

3.1 Development of the Model

Based on the analysis of standard solutions for the implementation of IoT system is proposed the wired architecture of the network SBC. Using for IoT SBC Internet wire network devices are: router with Ethernet-ports and wireless access ability, softswitch the second layer, firewall, power block, server with control software, IP-camera, sensors, cables [27,28]. The system can operate as a standalone or with Internet connection. Assumptions for the developed model are the following:

- the flow of hardware system failures obeys the Poisson distribution law;

- there is reserve of the server and the router;

- failures caused by software design faults of SBC subsystems obeys Poisson distribution, as on the results of monitoring and diagnostics, testing corrected secondary error (the result of the accumulation of the effects of primary errors and defects, software backdoors) to fix a malfunction or failure of the software, remove of impacts on software vulnerabilities, DoS - and DDoS - attacks, the number of primary defects in the software permanently;

- the process, which occurs in the system, it is a process without aftereffect, every time in the future behavior of the system depends only on the state of the system at this time and does not depend on how the system arrived at that state. Therefore, the process has the Markov property. The mode of the server when software system shutdown and startup cycles in this model S4 is absent, because in this mode it is impossible to manage the server remotely.

A Markov model of SBC subsystems functioning represented on fig.1, considering DDoS attacks and energy modes of server and router, which has the following condition: Good-working state (1); The server is fully used with high power consumption state (2); The server is fully used, the hardware, that are not used, can enter the low-power mode S1 (3); Sleep mode of the server with low power consumption, a computer can wake up from a keyboard input, a LAN network or USB device S2 (4); Server appears off, power consumption is reduced to the lowest level S3 (5); Server failure (6); Switching to the backup server device after the server failure (7); Restarting the server software after the software fault (8); Successful DDoS-attack on the server after the firewall failure (9); Firewall software or hardware failure (10); Attack on the power supply system after the firewall failure, that lead the failure of general power system of IoT system (11); Technical condition of switch from the general power system after its failure on the alternative energy sources (solar, diesel generator, wind turbine) (12); Router Status Active - sending packages with high power consumption (13); DDoS- successful attack on the router (14); Good-working state of the router without transmitting packets - Normal Idle (15); Good-working state of the router without packet transmission Low-Power Idle (16); Router software or hardware failure (17); Server software or hardware fault (18); Router hardware or software fail (20); Switching to the backup router device after the router failure (21); Restarting the router software after the router software fault (22).

A system of linear differential equations of the Kolmogorov-Chapmen composed and solved in the paper with the initial conditions:

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

An important indicator of dependability SBC under the influence of different kinds of DDoS attacks is the availability factor. As an index of reliability SBC we choose availability function AC(t), that is defined as the sum of the probabilities of staying the system in an up-states. Availability function AC(t) is determined from equation:

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

Pi(t) – probability of good condition SBC components.

Solving the system of Kolmogorov-Chapmen equations, we can get the value of the availability function components and SBC network after successful DDoS attacks and with considering energy modes of the server and the router. It follows that service availability, service continuity, cyber security, data integrity, resilience and high dependability of software and hardware should be inherent in IoT networks.

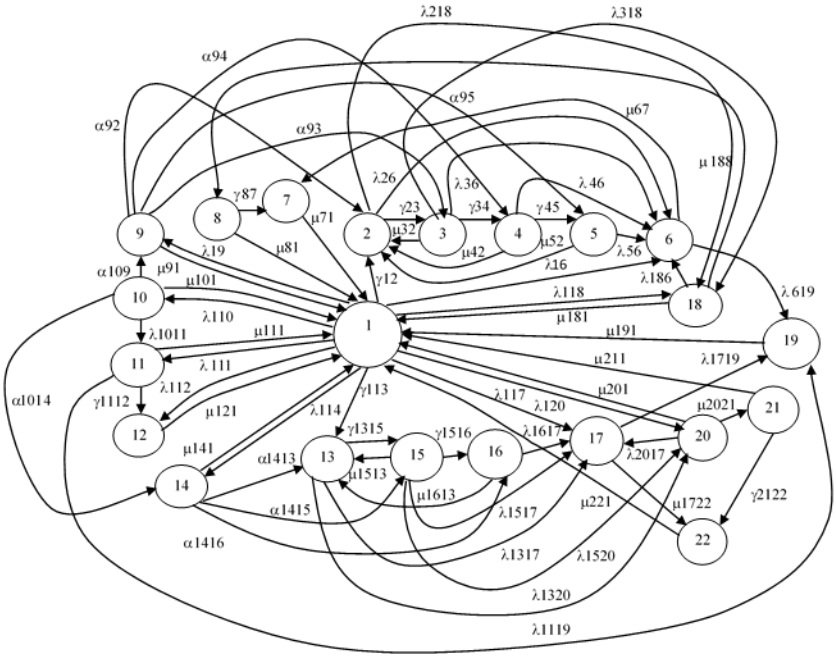

Fig. 1. A Markov model of functioning general subsystems of SBC

3.2 Simulation Results

On the basis of the analysis of statistical data we assess the main indicators of dependability and built a graph shown in Fig. 2-7. As an example, we give graphical dependencies for different technical states of the server. We constructed the dependence of the system availability function (we denote it AC) from the transitions rates to different states (λij, αij, γij, where i = $\overline{\mathbf{1},\mathbf{22}}$, j = $\overline{\mathbf{1},\mathbf{22}}$), which depend on events occurrence time. Figures 2-7 shows the changing of availability function AC from changing the transitions rates from one state to another in the Markov's model.

The analysis of the Markov's model simulation results shows decreases the value of SBC availability function AC with increase of:

- the transition rate λ218 from an active-power mode of the server 2 to a state of the server fail 18 (fig. 6),

- the transition rate λ1317 from active-power mode of the router 13 to a state of the router failure 17 (fig. 2),

- the transition rate λ26 from server's active-power mode 2 to a state of the server failure 6 and the transition rate λ36 from server's low-power mode 3 to a state of the server failure 6 (fig. 4, fig.5).

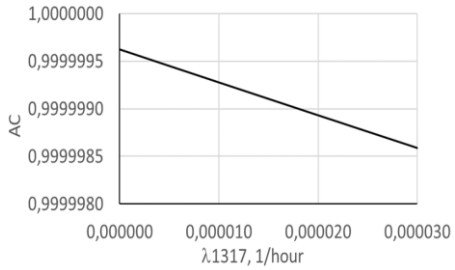

Fig. 2. Graph of dependence of SBC AC on the transition rate λ1317 from active-power state of the router 13 to a state of the router failure 17

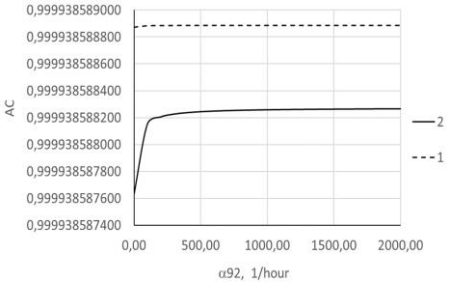

Fig. 3. Graph of dependence of SBC AC on the transition rate α92 from the state of successful DDoS-attack on the server after the firewall failure 9 to state of active-power state of the server 2

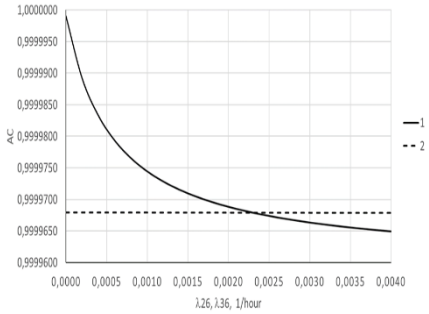

Fig. 4. Graph of dependence of SBC AC on the transition rate λ26 from active-power state of the server 2 to a state of the server failure 6 and the transition rate λ36 from server's low-power mode 3 to a state of the server failure 6 if γ12=30 1/hour; μ61=0,02083 1/hour; μ67=60 1/hour; μ71=20 1/hour

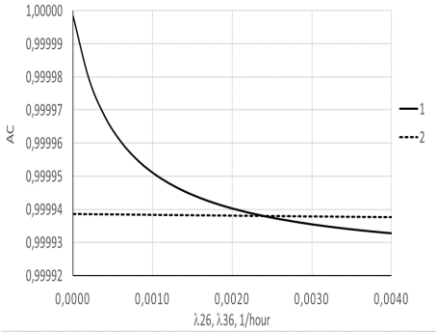

Fig. 5. Graph of dependence of SBC AC on the transition rate λ26 from active-power state of the server 2 to a state of the server failure 6 and the transition rate λ36 from server's low-power mode 3 to a state of the server failure 6 if γ12=100000 1/hour; μ61=20 1/hour; μ67=1000 1/hour; μ71=50 1/hour

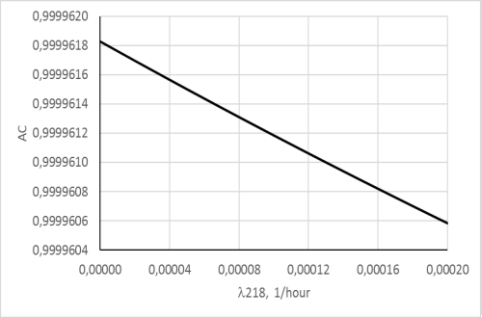

Fig. 6. Graph of dependence of SBC AC on the transition rate λ218 from active-power state of the server 2 to a state of the server fail 18

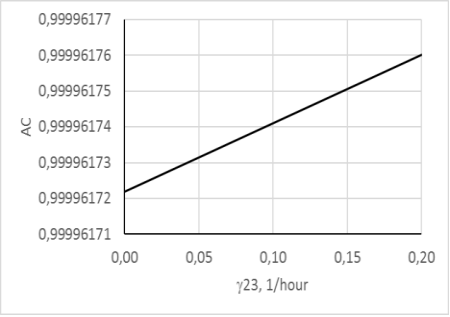

Fig. 7. Graph of dependence of SBC AC on transition rate γ23 from active-power state of the server 2 to a state of the low-power mode of the server 3

Increase the transition rate from a good state of a server with full power consumption 2 to a server failure state 6 (λ26); from a good state of a server with a reduced power consumption 3, to the server's failure state 6 (λ36) results to AC decrease. With an increase of the transition rate from a good state 1 to a state with full power consumption 2 (γ12), increase the nominal value of AC(t). Moreover, at a high intensity of the transition from the defective state of the server 6 to the working state 1 (μ61), and also to the reconfiguration state 7 (μ67), a smoother change in the availability function is observed than values of μ61, μ67 are low. Moreover, at a high transition rate from the server failure state 6 to the working state 1 (μ61), and also to the reconfiguration state 7 (μ67), a smoother change in the availability function is observed than at low values of μ61, μ67. With the transitions rates γ12=30 1/hour; μ61=0,02083 1/hour; μ67=60 1/hour; μ71=20 1/hour (fig. 4) – the value of AC with λ26=0,004 1/hour is about equal to 0,9999340. If γ12=100000 1/hour; μ61=20 1/hour; μ67=1000 1/hour; μ71=50 1/hour (fig. 5) availability function value with λ26=0,004 1/hour is equal to 0,9999650.

Therefore, it is necessary to choose such values of SBC parameters at which the availability factor of the proposed system for any changes in parameters taking into account the power consumption modes and under states of DOS and DDoS attacks will not change significantly.

Reducing the availability function when increasing the transition rate from a good state with a high power consumption of the server into a software fail mode occurs due to the impact of external influences (Dos- and DDoS-attacks), and because of internal causes associated with defects in the software and/or hardware of the server (fig. 6).

The initial value of the AC is less than 1 when the transition rate from state 9 to state 2 (α92) changes (by the Dos- and DDos-attacks influence on the state of the server with high power consumption if there is a vulnerability in the server firewall), because the AC is influenced both by external influences (attack), and internal causes (defects of software and/or hardware). With the increase in the attack flow to the server through the firewall vulnerability, it is perceived as a simple increase in the flow of data to the server, which leads to the server's transition into a good state of high energy consumption. With a further increase in α92, the change in AC ceases. Fig. 3 shows

how the AC varies depending on $\alpha 92$ for different values of the transition rate of the system from good state 1 to the vulnerability state of the server firewall 9. Analysis of the dependences for $\lambda 19$ = 0.000001 1/hour (line 1) and $\lambda 19$ = 0.001 1/hour (line 2) showed that an increase in the value of $\lambda 19$ leads to a decrease in the AC.

Besides, increasing of the transition rate from active-power mode of the server to a state of the low-power mode of the server $\gamma 23$ (fig. 7) insignificantly increase the AC function. Behavior of the availability function AC ($\gamma 23$) (fig. 7) is justified by the fact that when switching from an active mode of operation of a server with full power consumption to a low power consumption mode, the AC increases depending on the transition rate ($\gamma 23$) by reducing the load on the power supply equipment increases its availability.

Under the influence of DDoS attacks, the server, which is in one of the energy-saving modes, will switch to the mode of increased power consumption.

The practical significance of the results is the following. They allow to assess the availability factor and to develop recommendations for the design SBC for reduce the vulnerability of the system from DoS- of DDoS-attacks, as well as reducing SBC energy consumption.

4 Conclusion and the Future Work

The paper consider and research the process of SBC functioning under the influence of external factors affecting its reliability, safety and energy modes.

New approach to building SBC is proposed taking into account the functioning of the power supply system with different power consumption modes of the server and router operating system.

To assess the reliability SBC have been proposed a model that takes into account successful DDoS attacks, failures and malfunctions hardware and software of various components of SBC; energy modes of the SBC system, the rate of which is based on the analysis of statistical data of firewall functioning; failure of IoT devices management systems, following an attack impact to the router software, power supply systems, servers, etc.

Was researched and analyzed the function availability of IoT system – SBC, taking into account the reliability of components, rate of restoration, and different kinds of energy modes of server and router operation system, DDoS attacks on the router and the server. The Markov model of SBC availability was developed and investigated based on the analysis of hardware failures, software components, communication lines, router, firewall, special attacks on the SBC power system, DDoS attacks on the router and the server, attacks using components IoT infrastructure.

Studies have shown that the definition of the beginning of attacks is difficult, especially if there are vulnerabilities, program bookmarks, hardware bookmarks, hardware failures or software errors in firewalls.

References

1. O. Vermesan, p. Friess, P. Guillemin, et.al. Internet of things – from research and innovation to market deployment. river publishers series in communication, 2014. Available at: http://www.internet-of-things-research.eu/ pdf / IERC_Cluster_Book_2014_Ch.3_SRIA_WEB.pdf (access date: 3.08.2016). 141 p
2. Internet of Things and its future. Available at: http://www.huawei.com/ilink/en/about-huawei/newsroom/press-release/HW_080993?dInID=23407&relatedID=19881& relatedName= HW_076569&dInDocName=HW_076557 (access date: 3.08.2016).
3. Matat D. Internet rechey I tehnotrendi yak oznaki evolyutsIYi suspIlstva. Osvita Ukrayini. Available at: http://pedpresa.ua/136666-internet-rechej-i-tehnotrendy-yak-oznaky-evolyutsiyi-suspilstva.html (access date: 3.08.2016).
4. Cisco IoT System Brochure Cisco IoT System Deploy. Accelerate. Innovate. 2015. http://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/brochure-c02-734481.pdf. (access date: 3.08.2016). 52 p.
5. Energy-saving technologies. 2016. http://cetus.org.ua/ energosberegaushie-tehnologii.html (access date: 03.11.2016).
6. Rockchip RKI6000 smart home products unveiled at mwc 2016. http://chinagadgetsreviews. com/rockchip-rki6000-smart-home-products-unveiled-at-mwc-2016.html. (access date: 03.11.2016).
7. Prohorov, A. NB-IoT: narrow band – wide perspectives. www.it-weekly.ru/analytics/tech/83261.html. (access date: 03.11.2016).
8. Defending TCP Against Spoofing Attacks, https://tools.ietf.org/html/rfc4953/
9. Kaspersky security bulletin 2015. Kaspersky-Security-Bulletin- 2015_FINAL_EN.pdf, https://securelist.com/files/2015/12/ Kaspersky-Security-Bulletin-2015_FINAL_EN.pdf. (accepted at 3.08.2016). 85 p.
10. Internet Security Threat Report VOLUME 21, APRIL 2016. Symantec. Available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21- 2016-en.pdf. 81 p.
11. Electricity Information sharing and analysis center. Internet of Things DDoS White Paper, http://media.wix.com/ugd/416668_9d3598f6f4c649ad9eff6f17d00f30a2.pdf (access date: 24.10.2016).
12. Who is Anna-Senpai, the Mirai Worm Author? https://krebsonsecurity.com/tag/bashlight. (access date: 01.10.2016).
13. SSHowDowN – Exploit von internet. Ezra Caltum & Ory Segal, Akamai Threat Research. Verцffentlichungsdatum: https://www.akamai.com/de/de/our-thinking/threat-advisories/sshowdown-exploitation-of-iot-devices-for-launching-mass-scale-attack-campaigns.jsp (access date: 11.10.16).
14. Kaiten/STD router DDoS Malware, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/kaiten-std-router-ddos-malware-threat-advisory.pdf. (access date: 01.10.16).
15. Attack Spotlight: 363 Gbps DDoS Attack. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-363-gbps-ddos-attack-threat-advisory.pdf. (access date: 25.07.16).
16. Risk & Repeat: Breaking down the latest Mirai IoT botnet attacks, http://searchnetworking.techtarget.com/tip/80211-Security-Attacks-and-risks.
17. Andrey Goldshtein. DDoS-attacks: mechanisms of creation and variants of security, http://www.itsec.ru/articles2/Oborandteh/ddosataki-mehanizmi-sozdaniya-i-varianti-zashiti.

18. Peter Loshin, http://searchsecurity.techtarget.com/news/450401962/Details-emerging-on-Dyn-DNS-DDoS-attack-Mirai-IoT-botnet (access date: 28.10.2016).
19. Rob Wright. Risk & Repeat: Rapid7 tackles IoT threats, vulnerabilities, http://searchsecurity.techtarget.com/podcast/Risk-Repeat-Breaking-down-the-latest-Mirai-IoT-botnet-attacks (access date: 03.11.2016).
20. Rob Wright. Risk & Repeat: DNS DDoS attacks raise concerns over IoT devices, http://searchsecurity.techtarget.com/podcast/Risk-Repeat-DNS-DDoS-attacks-raise-concerns-over-IoT-devices (access date: 28.10.2016).
21. Rob Wright. Risk & Repeat: Breaking down the latest Mirai IoT botnet attacks, http://searchsecurity.techtarget.com/podcast/Risk-Repeat-IoT-attacks-on-the-rise (access date: 03.11.2016).
22. DDoS Attacks: Trends show a stronger threat in 2015, http://www.calyptix.com/top-threats/ddos-attacks-trends-show-stronger-threat-in-2015/ ((access date: 02.2015).
23. How DDoS Detection and Mitigation Can Fight Advanced Targeted Attacks, https://www.sans.org/reading-room/whitepapers/analyst/ddos-detection-mitigation-fight-advanced-targeted-attacks-35000/ September, 2013. A SANS Whitepaper Written by John Pescatore.
24. Common Types of Network Attacks, https://technet.microsoft.com/en-us/library/cc959354.aspx/.
25. https://standards.ieee.org/findstds/standard/802.3az-2010.html.
26. System Sleeping States.https://msdn.microsoft.com/en-us/library/windows/hardware/ff564575(v=vs.85).aspx.
27. 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.
28. Markov Model of the Smart Business Center Wired Network Considering Attacks on Software and Hardware Components. Vyacheslav Kharchenko, Maryna Kolisnyk, Iryna Piskachova, Nikolaos Bardis. International journal of computers and communications ISSN: 2074-1294, Volume 10, 2016, P. 113-119. //http://www.naun.org/cms.action?id=11961.