computing@computingonline.net
www.computingonline.net

Print ISSN 1727-6209
On-line ISSN 2312-5381
International Journal of Computing

RESEARCH OF THE ATTACKS SPREAD MODEL ON THE SMART OFFICE'S ROUTER

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

[1)] Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "KhAI", Ukraine, 61000, Kharkiv, 17, Chkalova Str, m.kolisnyk@csn.khai.edu, https://csn.khai.edu/en
[2)] Department of Automation and Computer-Integrated Technologies, Educational and Scientific Institute of Energy and Computer Technologies, Kharkiv Petro Vasylenko National Technical University of Agriculture, Ukraine, 61052, Kharkiv, 12, Christmas Str, 19

Paper history:
Received 18 May 2020
Received in revised form 19 October 2020
Accepted 17 October 2020
Available online 30 December 2020

Keywords:
cybersecurity;
DDoS-attacks;
router;
IoT;
reliability.

Abstract: Currently, the number of DDoS attacks on various institutions has increased, so research on this issue is necessary and relevant. One of the devices that is targeted first is the router. This paper is devoted to the study of the spread of DDoS attacks on the router's subsystems of the Smart Office system. This paper analyzes and solves the problem of optimizing the search for the minimum propagation path of an attack on router subsystems using a mathematical tool – graph theory. The goal of this paper is to determine the most vulnerable router's subsystems to the effects of DDoS attacks.

1. INTRODUCTION

A growing number of different devices using the technology of machine-to-machine (M2M) interaction are being connected to the Internet. As part of this technological solution, a number of specialized devices are used that collect telemetric information. A key feature of such systems is their industrial orientation and the need for human participation in management decision-making. This aspect greatly limits the use of M2M technologies and led to the improvement of the concept and the emergence of the concept of "Internet of things (IoT)". The IoT is understood to be connected to a computer network: robotic manufacturing facilities, smart medical equipment, power supply networks and countless industrial control systems (turbines, valves, servo drives, etc.), cars, televisions, surveillance cameras, etc. There are various models of interaction of Internet-connected devices: Thing-Thing, Thing-User and Thing-Web Object [1]. Connecting Smart Things to a single network provides critical qualitative changes for the development of human activity, and the main part of the connected objects will be a variety of specialized devices that include a microcontroller with various expansion cards – a data transmission module, a memory module, and measurement tools (sensors) and means of identification. To control the device, processing and transmitting data on the controller, a real-time operating system is used, which is responsible for collecting and initial processing of data to minimize traffic [2].

Smart offices are a small part of the IoT. The increase in the number of devices connected to the IoT leads to an increase in the possibility of man-made risks and a sharp decline in the security of critical systems. Since a number of such facilities and IoT systems have already been attacked and considerable damage has been caused, ensuring their protection is coming to the fore [1-3]. DDoS (Distributed Denial of Service)-attack is a series of malicious actions that a hacker makes trying to block users from accessing the service. Such an attack can be carried out in relation to almost anything: servers, devices, services, networks, applications, and even specific transactions within

This paper has been submitted for the Open Special Issue on Green Mobile Computing and IoT Systems. Assessment, Modeling, Assurance.

applications. During this process, the hacker sends malicious data or requests from several different systems to the target resource. Typically, such attacks overwhelm a resource with requests for data so much that it simply does not withstand the load. As a result, it stops working due to an oversupply of requests. The losses that this attack will entail may be minimal – the resource will simply not work for a while. But sometimes this can lead to global negative consequences, especially if interruptions in the work of the service greatly harm its users. The impact of DDoS-attacks on the infrastructure of a smart office leads to an increase in energy consumption by infrastructure components. Sending by the attackers of a huge number of service requests does not allow the smart office subsystem to switch to low power modes. The most frequently vulnerable to attacks are routers. Therefore, it is advisable to consider which nodes of the router will be more susceptible to attack, and to offer recommendations for protecting them from such effects.

1.1 WORK RELATED ANALYSIS

In [4-6], a research of security problems in IoT and a classification of possible cyber attacks at each level of the IoT architecture was done. It also addresses issues with traditional security solutions, such as cryptographic solutions, authentication mechanisms, and key management in IoT. In [7, 8], a classification is presented based on analysis and comparison of the serious consequences of attacks, a study of security, security problems, and various types of active and passive attacks on IoT. In [9], vulnerabilities and threats in the IoT environment and protection methods were considered. A classification of security risks of a particular architecture level, as well as security risks, depending on the type of use of the IoT concept, is proposed. The paper [10] examined various types of attacks on the router, the principles of creating and maintaining an automatic log for network and security management. The authors of the reviewed sources assessed the reliability and security of network devices, applied graph theory and Dijkstra's algorithm for network models, not including router functioning models. The scientific novelty of this article is that a new approach is applied to the well-known Dijkstra's algorithm – to determine the most vulnerable subsystem of the router, determining the optimal route of DDoS-attack on it.

1.2 THE GOAL OF THE PAPER

The number of DDoS-attacks to various institutions has increased, so research on this problem is necessary and relevant. One of the devices that is attacked first is a router. This work is devoted to the study of the spread of DDoS attacks on the router subsystems of the smart office system, for which it is proposed to use Dijkstra's algorithm to detect the router subsystems most vulnerable to attacks in order to develop in the future recommendations to improve the cybersecurity and reliability of these subsystems.

The purpose of the paper is to determine the most vulnerable subsystems to the effects of DDoS attacks on router.

2. GENERAL INFORMATION

2.1 ANALYSIS OF THE ATTACKS STATISTICS ON THE IOT SYSTEM INFRASTRUCTURE USING BOTNETS

To implement the Internet of things in all industries, in particular, the smart office, it is necessary to develop new ways to protect network equipment from various attacks and analyze the most vulnerable components. Developers need to ensure an adequate level of cybersecurity for any IoT system, where it is of great importance. IoT devices work around the clock and attackers can use them at any time to perform malicious activity. Additional functionality, the ability to manage security should be provided at the design stage of IoT devices [11, 12].

Software vulnerabilities can arise not only during the creation of software code, but also due to errors in the configuration of gateways and servers, due to frequent reprogramming, with each change or modification of products that become more diverse, and sometimes even done for individual orders. Compatibility with the existing production and management systems at the enterprise means, inter alia, interaction with outdated software products with much less stringent requirements for cybersecurity. Over the past two years, there have been serious attacks on IoT devices using botnets Mirai, Torii, VPNFilter, Hide N Seek (HNS) [11-15]. These botnets change the mechanism of action, becoming more and more sophisticated over time.

The Mirai botnet uses a connection to the victim computers using a brute force attack (brute force) attack on Telnet servers, using more than 60 factory credentials for the BusyBox software. Then each infected device blocks itself from additional bots, the botnet sends the victim's IP address and credentials to a special centralized service ScanListen.26, while the new victim then helps to attract new bots, creating a self-replicating model [13].

The TORII botnet software code affects x86_64, x86, ARM, MIPS, Motorola 68k, SuperH, PPC processors, as well as their variants, and allows for remote control and data stealing [14, 15]. The

program uses five different commands to deliver a botnet, either via HTTP or via an attacker's FTP resource, and Tor tunnels were used to deliver malicious code.

The BrickerBot botnet implements Permanent Denial of Service (PDoS) attacks – these are fast-moving bot attacks that are gaining popularity and are intended to make equipment stop working [16].

The Hide 'N Seek botnet (HNS) attacks not only routers, DVRs, but also vulnerable DB solutions (Apache OrientDB and CouchDB), as well as AVTECH webcams, Cisco Linksys RCE, TP-Link RCE, Netgear RCE, ASUS, D-Link, Huawei, MikroTik, QNAP, Ubiquiti, Uplevel, ZTE; JAWS / 1.0 Web server [17–19].

The Hajime botnet is a sophisticated, flexible, thoughtful, reliable and innovative IoT botnet that can self-update and provide its booth partners with enhanced capabilities quite effectively and quickly. The attack is carried out by scanning the Internet to detect and infect new victims through the open ports of TCP 23 (Telnet) and TCP 5358 (WSDAPI), using the brute force method to log into the system and gain control over the devices. Also, a botnet can remove malicious software from a device that wants to infect, while protecting it from future infections, controlling its connection with Telnet [20].

The VPNFilter botnet attack affects network devices for the home or small office, as well as a number of network storage systems. Network devices of such manufacturers as ASUS, D-Link, Huawei, Ubiquiti, UPVEL and ZTE, Linksys, MikroTik, Netgear and TP-Link [19-21] were subject to attacks.

The Gafgyt botnet affects IoT devices, including Huawei devices, GPON and D-Link devices, vulnerabilities CVE-2018-10562 and CVE-2018-10561 in Dasan routers.

The analysis of attacks performed using IoT botnets, showed, that attacks most often affect IoT network routers.

The cybersecurity of the IoT is enhanced by ensuring the security of communication systems, monitoring network interactions, controlling and protecting devices. IoT systems use significantly enhanced security measures – secure and robust system architectures, specialized chipsets, modern types of encryption and authentication, threat detection systems, etc.

Communication channels must be secured; encryption and authentication technologies are used to ensure that devices know if they can trust the remote system.

Protecting IoT devices is ensuring cybersecurity and software integrity. All critical devices, whether sensors, controllers, or something else, must be configured to run only signed code. Devices must be protected at subsequent stages, after the code has been launched.

Some attacks will be able to overcome any measures taken, no matter how well everything is protected, so it is crucial to have security analytics capabilities in IoT. Most IoT devices are “closed systems”. Therefore, the protection functions should be initially built into the IoT devices so that they are safe in their architecture. Security in the manufacture of the device at the factory is the best way to ensure the protection of the Internet of things, such as encryption, authentication, integrity checks, intrusion prevention and the possibility of secure updates.

To ensure the security of the IoT hardware and software, protection programs can use an extension of the hardware functions. Many chip makers have already embedded security features in hardware. It is also assumed that when using servers and routers, appropriate security policies will be configured.

Regardless of whether the device is connected to any other device or data is exchanged with a remote service, for example, a cloud-based one, the connection must always be secure. For many IoT applications, absolute data confidentiality is required; this requirement can be met using certificates and TLS/DTLS protocols.

2.2 THREATS IN IOT DEVICES

IoT devices face many threats, including malicious code that can spread through proven connections, exploiting vulnerabilities or configuration errors. In such attacks, several software vulnerabilities are often exploited, including [4–10]: failure to use code signature checks and secure downloads; poorly implemented validation models that can be circumvented. Attackers often use these flaws to install software for data collection, file transfer capabilities for extracting confidential information from the system, and sometimes even for command & control (C&C) infrastructure to manipulate system behavior.

Some attackers exploit vulnerabilities to install malware directly into the memory of already running IoT systems. And sometimes this type of infection is chosen, in which the malware disappears after the device is rebooted, but it manages to cause enormous damage. This works because some IoT systems and many industrial systems almost never reboot. In this case, it is difficult for the security department to detect the vulnerability used in the system and investigate the origin of the attack. Sometimes such attacks occur through an IT network connected to an industrial network or to an IoT network, in other cases an attack occurs via the Internet or through direct physical access to the

device. In this way, you can identify threats that use a mutated code or adapt their encryption scheme by simply separating high-risk files from secure files, quickly and accurately detecting malware, despite all their tricks. The combination of technologies used will depend on the specific situation, but the above tools can be combined to protect devices, even in environments with limited computing resources [2].

Increasing the flow of processed data in the smart office system leads to the development of more powerful routers and the improvement of routing protocols and network operation principles. In the construction of modern networks, in addition to the traditional infrastructural level of data transmission, containing routing and switching equipment, a control level is distinguished. Separating the functions of transmission and management allows you to virtualize the network infrastructure and significantly increase the centralization of resource management, implementing the technology of software-defined networks (Software Defined Network), designed to work in conditions of dynamic changes. This approach already finds its use in the data center when building cloud services and is rapidly gaining popularity in corporate networks and networks of providers. The applied value of the Internet is a number of specialized services implemented on its basis – DNS, e-mail, file transfer (FTP), World Wide Web, streaming media, etc. The services provided are in continuous development, transforming society and sociologizing interaction within the network. Most applications use a user-service interaction model and serve as a reflection of the emerging information society.

Today, IoT is interested in many business executives. They are exploring ways to use this technology and the benefits it can give to the company. Application of IoT can be found in almost any industry. For example, in the manufacturing sector, IoT systems can be used to predict equipment failures (predictive analytics). This allows you to optimize the frequency of maintenance and minimize downtime. In the health sector, IoT technologies can provide more accurate monitoring of health outcomes, which helps improve patient outcomes.

In 2016, the Mirai botnet was attacked, which disabled many websites (Twitter, Shopify, NetIX, etc.). The attack was successful due to the vulnerability of outdated IoT device firmware [22].

Currently, Mirai is not lost, there are several options on the network. Network security experts have discovered an interesting version of the Mirai, with extensive features. He was found after analyzing a powerful DDoS-attack lasting 54 hours. Apparently, now the botnet has become more powerful than ever.

A special feature of Mirai is hacking smart devices, including cameras, thermostats, etc., and then using these devices as bots for DDoS attacks. The first version of Mirai included about 400-500 thousand connected devices. Per second, the botnet target received about 30,000 HTTP requests. In February 2017, an attack was made on one of the educational institutions in the USA. The duration of the attack was more than 54 hours. This was significantly different from the usual Mirai opening hours; previously, the duration of the attacks was about 24 hours and no more. Mirai botnet, by selecting combinations of default usernames and passwords, hacked a large number of cameras and routers, which were later used for the most powerful DDoS attack on the UK Postal Office, Deutsche Telekom, TalkTalk, KCOM and Eircom. At the same time, the “bootforce” of IoT devices was carried out using Telnet, and routers were hacked through port 7547 using the TR-064 and TR-069 protocols [23]. The longest attack in the second quarter of 2018 lasted 258 hours (almost 11 days), in the last quarter the maximum attack duration was 297 hours (12.4 days) [24].

It is worth noting that now Mirai consists of new devices that have been cracked relatively recently. All elements of the botnet carried out an attack on the target using HTTP flood. About 10.000 IoT devices participated in this attack, including cameras, routers and other devices. Their manufacturers have not yet fixed software vulnerabilities that were discovered during the work of the first version of Mirai, so it is not surprising that the work of Mirai was again possible. Its latest version includes 30-user agent alternatives, a step forward compared to 5 for the original botnet. A greater number of user agents allow Mirai to successfully counteract most of the security measures taken by information security specialists. The spread over IP is quite large. Approximately 18% of botnet elements are located in the United States, 11% in Israel, and 11% in Taiwan [25].

More than 2 million attacks via SSH and Telnet were committed to server bait deployed by cybersecurity experts during June 2018. Malicious scripts from the USA and Russia are most active. The top five countries, from whose territory the majority of attacks occur, also include the United Kingdom, France and the Netherlands.

The sources of the malicious script were uploaded to the network, after which new versions of the program were created based on the original code. The most famous of them, the Wicked and Satori botnets, have been repeatedly observed in attacks on the IoT devices [26].

The first botnet IoTroop (aka Reaper), built on the basis of Mirai, was discovered in October 2017.

Malicious software spreads through various vulnerabilities in D-Link, TP-Link, Avtech, Netgear, MikroTik, Linksys, Synology devices.

In January 2018, a series of DDoS attacks were launched against financial institutions in the Netherlands, affecting such large companies as ABN Amro and Rabobank. Recorded Future analysts reported that these attacks were one of the first recorded applications of the IoTroop botnet.

According to the calculations of Recorded Future, the power of attacks at peak times reached 30 Gbit/s, and the attackers used amplification through DNS. This is not the most powerful attack. In March 2018, attacks of 1.7 TB/s were recorded. During the first malicious campaign, the botnet comprised 80% of the MikroTik routers, and the remaining 20% of the devices were a mix of vulnerable Apache and IIS servers, as well as various smart Ubiquity, GoAhead, Linksys, TP-Link, Dahua, Cisco and ZyXEL devices [26, 27].

In June – September 2018, it was reported that a new IoT-botnet Hakai appeared, whose victims now are mainly D-Link, Huawei and Realtek routers. This bot was based on Qbot source codes (Gafgyt, Bashlite, Lizkebab, Torlus or LizardStresser), which spread over the network several years ago. In July 2018, Hakai began to evolve, hacking and infecting all new devices. This was an exploit for the CVE-2017-17215 vulnerability affecting Huawei HG532 routers. In August, Hakai exploited vulnerability in D-Link routers that support the HNAP protocol, as well as attacking Realtek routers [26].

In September, two more new versions of this malicious program, Kenjiro and Izuku, appeared on the network [26, 27].

As can be seen from the analysis of the spread of DDoS attacks on network subsystems in recent years, one of their main directions is a router. Therefore, it is relevant to analyze the impact of attacks on routers to further ensure the security of network routers.

2.3 MODELING TO FIND THE MINIMAL PATH TO THE ROUTER'S COMPONENT IF ATTACK SPREADS

The object of research in the paper was selected Smart Office (SO). In previous papers [28-30], the availability of SO considered and a study was conducted with the use of firewalls, servers, and routers in the context of DDoS-attacks and threat patching using a mathematical apparatus – Markov models.

This paper analyzes and solves the optimization problem of finding the minimum propagation path for an attack router, using a mathematical tool – graph theory.

A graph is a set of objects. In our task, these are the critical components (subsystems) of the router. To solve problems with such a set, you need to designate each object from this set as vertices of the graph.

Task setting: It is necessary to determine the path for a possible attack on the router subsystem in order to lead to the failure of the router in the shortest possible time.

Let us build a graph that shows the paths of possible attack propagation. A graph is a set of objects. In our task, these are critical components (subsystems) of the router. To solve problems with such a set, each object from this set must be designated as the vertices of the graph. The values of the transition times are taken as average from various sources [26, 27].

To search for the shortest time of transition from state to state, you can use several algorithms. The best known are the traveling salesman problem, the Dijkstra algorithm, the Bellman-Ford algorithm. To determine the shortest path to which the attack on the router may be oriented to bring it to a faulty state, the Dijkstra model was chosen. This algorithm iterates through all the vertices of the graph and assigns labels to them, which are the known minimum distance from the top of the source to a specific vertex.

Dijkstra's algorithm solves the problem of the shortest paths from one vertex for a directed graph. The result of the shortest path search algorithm should be a sequence of edges connecting the specified two vertices and having the shortest length among all such sequences. The algorithm works only for graphs without edges of negative weight. The structure scheme of router includes: PFC hardware special-cases limiter, Control-plane policing software, PFC hardware, PFC software, router's ROM, router's RAM, cores of Data Plane, Control Plane Interface, power supply unit of the router, Control Plane Interface, Data Plane. The values of transition times are taken from the average of various sources [10, 28-30].

The graph has 14 states: start of DDoS-attack (0); failure of PFC hardware special-cases limiter (1); failure of Control-plane policing software (2); failure of PFC hardware (3); failure of PFC hardware and software (4); failure of router's ROM (5); failure of router's RAM (6); failure of the one core of Data Plane (7); fault of the Control Plane Interface (8); failure of power supply unit of the router (9); failure of the Control Plane Interface (10); fault of the router (11); failure of all cores of Data Plane (12); failure of the router (13) (Fig. 1).

A graph is given, the states of which reflect the states of a router's failure or fault due to an attack. The purpose of the algorithm is to find the shortest

attack time for disabling the router subsystems. Suppose you want to find the shortest distance from the 0th vertex to all the others. Circles denote vertices that reflect the failure or fault of the router subsystem (RAM, processor, etc.), and the lines indicate the propagation paths of attacks between them (graph edges). The circles indicate the numbers of the vertices, above the edges their weight is indicated – the time of the impact of the attack until the result is obtained (failure or fault of any router device).

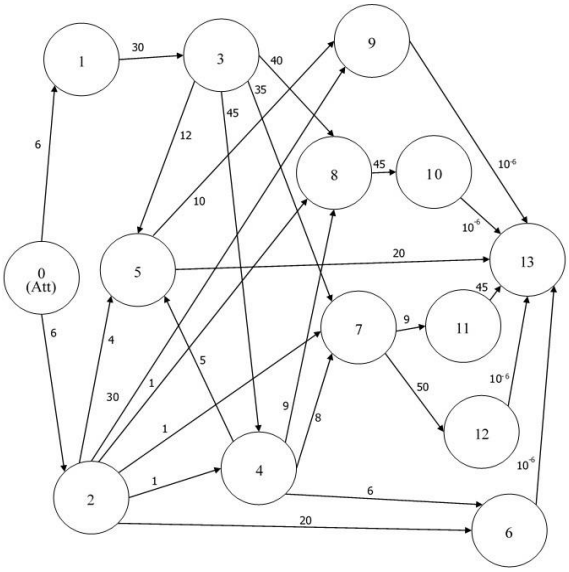

Figure 1 – Graph of the attack spread

This graph can be represented as a matrix (Fig. 2). A square matrix is used to store the weights of the graph. In the row and column headers are the values of the vertices of the graph. And the weights of the arcs of the graph (the exposure time of an attack to transition a router to another state) are placed in the internal cells of the table. The graph does not contain loops, so zero values are contained on the main diagonal of the matrix.

We will take the initial vertex 0 (the beginning of the attack) and will look for the shortest routes from vertex 0 to vertex 13.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	0	6	6	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	30	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	1	4	20	1	1	10	0	0	0	0
3	0	0	0	0	45	12	0	35	40	0	0	0	0	0
4	0	0	0	0	0	5	6	8	9	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	10	0	0	0	20
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0,000001
7	0	0	0	0	0	0	0	0	0	0	0	9	50	0
8	0	0	0	0	0	0	0	0	0	0	45	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0,000001
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0,000001
11	0	0	0	0	0	0	0	0	0	0	0	0	0	45
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0,000001
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 2 – Matrix of the attack spread

2.4 SIMULATION RESULTS

The simulation results are shown in Table 1. For example, it has been selected (Fig. 3), which step by step allows you to determine the duration of the attack and the transition to the next step. The graph weighting factors are defined as the time characteristics – duration of the attack (in hours) of the transition from one state of the graph to another state. They were taken according to the average statistical values given, for example, on the CERT website and in various reports on attacks on microprocessor systems. In accordance with Table 1, the first step is 0 state – 2 system state. The attack lasted 6 hours, led to failure of PFC hardware special-cases limiter by matching policy (2). A small value of the weight on the edge of the graph indicates that it takes very little time to transfer from one state of the graph to another, for example, if the RAM fails (6 is the state of the graph), the router immediately fails (13 is the state of the graph).

Table 1. Simulation results

Step	Start of step	End of step	Time, h	Accumulation of time, h
1	0	2	6	6
2	2	4	1	7
3	4	6	6	13
4	6	13	0,000001	13,000001

In accordance with Table 1, the first step is 0 state – 2 system state. The attack lasted 6 hours, led to the failure of the PFC hardware special-cases limiter by matching policy (2). The second step is from 2 states to failure of PFC hardware and software (4). According to Dijkstra's algorithm while minimizing the attack time to 13 states (failure of the router), the total number of steps is 4, the total attack time 13,000001 hour.

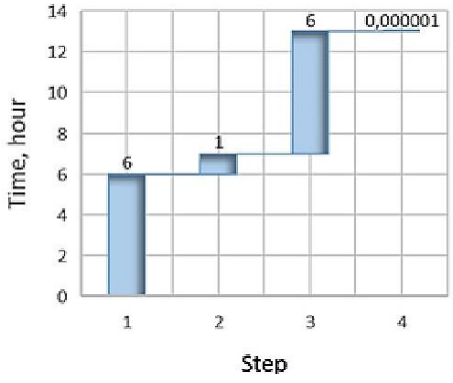

Figure 3 – A cascading diagram of the attack spread from 0 state to 13

If the target of the attack is the state of failure of power supply unit of the router (9) (Table 2) – the attack goal is achieved in 2 steps (Table 2, Fig. 4).

The first step lasts 6 hours and leads to the failure of the PFC hardware special-cases limiter by matching policy (2). In the second step, the attack lasts 10 hours and leads to the failure of the power supply unit (9). The total time of disabling the device is 16 hours.

Table 2. Simulation results

Step	Start of step	End of step	Time, h	Accumulation of time, h
1	0	2	6	6
2	2	9	10	16

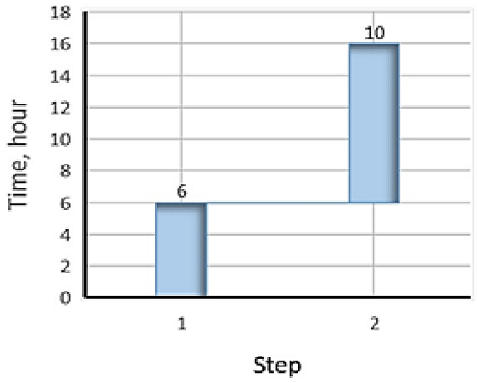

Figure 4 – A cascading diagram of the attack spread from 0 state to 11

If the target of the attack is the fault of the router (11), it is achieved in 3 steps (Table 3). The first step lasts 6 hours and leads to the failure of the PFC hardware special-cases limiter by matching policy (2) (Fig. 5). The second step to failure of the one core of Data Plane (7) lasts 1 hour. The third step to the final goal lasts 9 hours. Attack time equals to 16 hours.

Table 3. Simulation results

Step	Start of step	End of step	Time, h	Accumulation of time, h
1	0	2	6	6
2	2	7	1	7
3	7	11	9	16

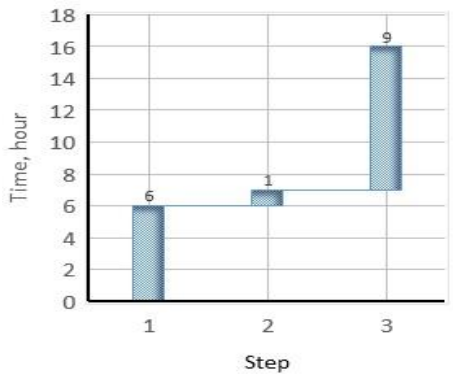

Figure 5 – A cascading diagram of the attack spread from 0 state to 11

3. CONCLUSIONS

A new approach is applied to determining the most critical subsystem inside the router when exposed to an attack – using the well-known Dijkstra algorithm for this purpose, which was previously actively used to solve network problems – when finding the optimal path between network devices, but not for solving problems inside the device. The results obtained in the article make it possible to identify the router subsystems most vulnerable to DDoS attacks. Using the average initial data on the attack time on the hardware and software subsystems of the router, a simulation was carried out using Dijkstra's algorithm to find the shortest attack path inside the router. Analysis of the simulation results showed that control level control software, and the router's RAM are most vulnerable to a DDoS attack, and leads to a failure of the router. That is, it is necessary to take measures to protect the data of the router subsystems from the effects of DDoS attacks.

Thus, when creating a cyber protection system for the Smart Office system, it is necessary to increase the security of the router, and, above all, to ensure it at the stage of development, production and operation of its subsystems.

Thanks to the conducted research, it became possible to identify the most vulnerable subsystems and develop recommendations for ensuring and improving the reliability and cybersecurity of the hardware and software of the router in SO.

ACKNOWLEDGEMENT

This research is supported by the project STARC (Methodology of SusTAinable Development and InfoRmation Technologies of Green COmputing and Communication) funded by the Ministry of Education and Science of Ukraine and Horizon 2020 project ECHO (European network of Cybersecurity centres and competence Hub for innovation and Operations H2020-SU-ICT-2018-2020, 2019-2023).

4. REFERENCES

[1] *Rise of the Machines: Transforming Cybersecurity Strategy for the Age of IoT.* A Technical Report from Forescout Research Labs. Device Visibility and Control, 2019, 33 p. [Online]. Available at: https://www.forescout.com/company/resources/iot-research-report-transforming-cybersecurity-strategy-for-the-age-of-iot/.

[2] *Good Practices for Security of Internet of Things in the Context of Smart Manufacturing*, 2018, 118 p. [Online]. Available at: https://www.enisa.europa.eu.

[3] J. Reo, *What Motivates DDoS Attackers*? Jan. 2016. [Online]. Available at: https://www.corero.com/blog/690-what-motivates-ddos-attackers.html.

[4] I. Ali, S. Sabir, Z. Ullah, "Internet of things security, device authentication and access control: A review," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 14, issue 8, pp. 456-466, August 2016.

[5] O. El Mouaatamid, M. Lahmer, M. Belkasmi, "Internet of things security: Layered classification of attacks and possible countermeasure," *Electronic Journal of Information Technology (e-TI)*, vol. 9, pp. 24-37, 2016. [Online]. Available at: https://www.researchgate.net/publication/321905085_Internet_of_Things_Security_Layered_classification_of_attacks_and_possible_Counterrmeasures.

[6] I. Andrea, G. C. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," *Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC)*, Larnaca, Cyprus, July 6-9, 2015, pp. 180-187.

[7] I. Butun, Member, P. Osterberg, "Security of the internet of things: Vulnerabilities, attacks and countermeasures," *Journal of IEEE Communications Surveys & Tutorials*, pp. 1-24, 2019.

[8] M. El-Hajj, A. Fadlallah, M. Chamoun, A. Serhrouchni, "A survey of internet of things (IoT) authentication schemes," *Sensors*, vol. 19, issue 5, p. 43, 2019.

[9] I. Cvitić, M. Vujić, S. Husnjak, "Classification of security risks in the IoT environment," *Proceedings of the 26th DAAAM International Symposium*, Vienna, Austria, October, 2015, pp. 731-740.

[10] J. Sanders, *Why Router-based Attacks could be the Next Big Trend in Cybersecurity*, April 2018, [Online]. Available at: https://www.techrepublic.com/article/why-router-based-attacks-could-be-the-next-big-trend-in-cybersecurity/.

[11] IBM Institute for Business Value, *Electronics Industrial IoT cybersecurity. As strong as its weakest link*, 2018, 24 p. [Online]. Available at: https://www.ibm.com/downloads/cas/NYQDYE5X//.

[12] Cisco Annual Information Security Report, 2018, 68 p. [Online]. Available at: https://www.cisco.com/c/dam/global/ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf.

[13] *IoT-botnet Hide and Seek Infects Android Devices Through Debugging Feature*, Sept. 2018. [Online]. Available at: https://www.securitylab. ru/news/495709.php.

[14] A. Wang, A. Mohaisen, S. Chen, "An adversary-centric behavior modeling of DDoS attacks," *Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, Atlanta, GA, USA, July 17, 2017, pp. 1126-1136.

[15] A. Wang, W. Chang, S. Chen, A. Mohaisen, "A data-driven study of DDoS attacks and their dynamics," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, issue 8, p. 14, August, 2015.

[16] L. O'Donnell, *Mirai, Gafgyt Botnets Return to Target Infamous Apach*, [Online]. Available at: https://threatpost.com/mirai-gafgyt-botnets-return-to-target-infamous-apache-struts-sonicwall-flaws/137309/.

[17] C. Osborne, *Mirai, Gafgyt IoT Botnets Stab Systems with Apache Struts, SonicWall Exploits. The IoT Botnets are Back with a New Arsenal Containing a Vast Array of Vulnerabilities*, September 2018. [Online]. Available at: https://www.zdnet.com/article/mirai-gafgyt-iot-botnets-stab-systems-with-apache-struts-sonicwall-exploits/.

[18] Patch Now: New Mirai, Gafgyt Variants Target 16 Flaws Via Multi-Exploits, September 2018, Available at: https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/patch-now-new-mirai-gafgyt-variants-target-16-flaws-via-multi-exploits.

[19] 2018 Data Breach Investigations Report, 8 p., [Online]. Available at: https://www.verizonenterprise.com/resources/cмreports/rp_DBIR_2018_Report_execsummary_en_xg.pdf.

[20] H. Boyes, B. Hallaq, J. Cunningham, T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Computers in Industry*, vol. 101, pp. 1-12, 2018. https://doi.org/10.1016/j.compind.2018.04.015

[21] The Foundation of Well-Being: How to Secure IoT Systems, May 2018, [Online]. Available at: https://security-news.today/osnova-blagopoluchiya-kak-obezopasit-iot-sistemy/.

[22] B. Dickson, IoT Botnets might be the Cybersecurity Industry's Next Big Worry, 2017, [Online]. Available at: https://www.iotsecurityfoundation.org/iot-botnets-might-be-the-cybersecurity-industrys-next-big-worry//.

[23] K. E. Skouby, R. Tadayoni, S. Tweneboah-Koduah, "Cyber Security Threats to IoT Applications and Service Domains," Wireless Pers Commun 95, Springer Science+Business Media, New York, 2017, pp. 169-185.

[24] A. Rodríguez-Mota, P. J. Escamilla-Ambrosio, J. R. C. Nurse, "Towards IoT cybersecurity modeling: From malware analysis data to IoT system representation," *Proceedings of the 2016 8th IEEE Latin-American Conference on Communications (LATINCOM)*, Medellin, Colombia, November 15-17, 2016, pp. 1-6.

[25] R. H. Weber, E. Studer, "Cybersecurity in the Internet of Things: Legal aspects," *Journal Computer Law & Security Review*, vol. 32, issue 5, pp. 715-728, Oct. 2016. [Online]. Available at: https://www.sciencedirect.com/science/article/pii/S0267364916301169.

[26] C. Cimpanu, *New Hakai IoT botnet takes aim at D-Link, Huawei, and Realtek routers*, September 2018, [Online]. Available at: https://www.zdnet.com/article/new-hakai-iot-botnet-takes-aim-at-d-link-huawei-and-realtek-routers/.

[27] Symantec. Executive Summary 2018 Internet Security Threat Report, vol. 23, March 2018, 89 p.

[28] M. Kolisnyk, V. Kharchenko, I. Piskachova, "Markov model of the smart business center wired network considering attacks on software and hardware components," *International Journal of Computers and Communications*, vol. 10, pp. 113-119, 2017.

[29] M. Kolisnyk, V. Kharchenko, I. Piskachova, "Markov model of the Smart Business Center wired network considering attacks on software and hardware components," *International Journal of Computers and Communications*, vol. 10, pp. 113-119, 2016.

[30] M. Kolisnyk, V. Kharchenko, I. Piskachova, "The research of the smart office availability model considering patches on the router firewall software," *Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kiev, Ukraine, May 24-27, 2018, pp. 169-174.

Maryna Kolisnyk, *Doctor of Philosophy (Ph.D.), Associate professor of Dept. of Computer Systems, Networks and Cybersecurity, Faculty of Radioelectronics, Computer Systems and Infocommunications at National Aerospace University "Kharkiv Aviation Institute", Ukraine.*

Research areas: dependability, reliability, cybersecurity of IoT based and WSN systems.

Vyacheslav Kharchenko, *Doctor of Sciences, Professor of Dept. of Computer Systems, Networks and Cybersecurity, Faculty of Radioelectronics, Computer Systems and Infocommunications at National Aerospace University "Kharkiv Aviation Institute", Ukraine.*

Research areas: dependability, cybersecurity, resilience, safety, reliability of critical infrastructure systems.

Iryna Piskachova*, Doctor of Philosophy (Ph.D.), Senior Researcher, an Assistant Professor at Dept. of Automation and Computer-Integrated Technologies, Educational and Scientific Institute of Energy and Computer Technologies at Kharkiv Petro Vasylenko National Technical University of Agriculture, Ukraine.*

Research areas: computer science.