ANALYSIS OF THE IoT IMPACT ON VOLUME OF DDoS ATTACKS

Dragan Peraković, Marko Periša, Ivan Cvitić
Faculty of Transport and Traffic Sciences, University of Zagreb,
dragan.perakovic@fpz.hr, marko.perisa@fpz.hr, ivan.cvitic@fpz.hr

Abstract: *Availability of information and services, along with integrity and confidentiality presents a critical parameter in security in information and communication systems. Activities focused on denial of network communication availability are current from the beginning of global communication network development and they demand continuous development of protection methods. Significant challenge is the emergence of the Internet of Things (IoT) concept which will significantly increase the number of connected devices. That kind of environment is possible to use for generation of DDoS attacks. The paper investigates the effect of a significant increase in the number of connected devices in the IoT concept on increase of the number and volume of DDoS attacks.*

Keywords: *denial of service attack; system availability; network resources flood; network security;*

1. Introduction

Need for information and communication systems (ICS) protection derives from sudden increase in dependence on information and communication technologies in support of a wide range of activities in the private and business environment. Access to Internet based services, such as e-mail and web, has become an indispensable segment of everyday life to private customers. The variety of services range from simple information search up to purchasing and financial transactions. Pervasive use of information and communication technologies is also visible from an organizational perspective. Example of that is e-mail which is considered a primary way of communication, also online transactions and e-business in general that increases organizational commercial activities.

Emergence and actualization of the Internet of Things (IoT) concept resulted in connecting a large number of different devices to provide new services and automation of many processes in the industry, household, transportation and many other sectors. Disadvantages of that kind of devices are primarily reflected in the impossibility of implementation of protection methods what makes them vulnerable to numerous attacks. Other than possibility to attack the devices, their inadequate protection provides

opportunities for exploitation of these devices to generate attacks directed against third parties.

Denial of service availability is growing security problem because of the process simplicity. Devices in IoT environment become potential generators of illegitimate traffic with a goal to create a deliberate congestion in the communications network. The assumption is that the emergence and growth of the IoT devices number affects their more frequent use in creating botnets used in distributed denial of service (DDoS) attacks. Hypothesis will seek to prove by analysing DDoS attacks recorded in the period from 2013 to 2015 (ten quarters).

1.1 Previous research

Implementation of DoS compared to other types of attacks is extremely simple in terms of the required knowledge and software tools. Thus, the number of DoS attacks and its instances is constantly increasing, which requires continuous research of problem area in order to define the updated taxonomy of current attacks that will serve as a basis for development of protection methods of its specific instance. The importance of research of mentioned problem area proves a large number of scientific papers dealing with specific issues, and some of the works will be shown below.

Development of IoT concept and increase in wireless sensor networks (WSN) application and other wireless communication technology is resulting in an increased risk of DDoS attacks in this segment of the network infrastructure. Taxonomy of DoS attacks directed towards WSN networks is presented in paper [1]. The paper includes the means of identification of attacker, its ability, and the object of attack, used vulnerability and the results of attack. Paper [2] assumes that a detailed taxonomy can help in distinguishing different types of attacks as well as a better understanding of these classes of attacks. The paper shows the current classification of DoS attacks and protection methods, and proposes a new classification scheme of new features attacks. Based on the proposed classification of DoS attacks a new classification of protection methods was formed. Paper [3] identifies botnet computer network as often used threat in a number of attacks on the ICS. Given that the current methods of detection of botnets targeting specific protocols and structures for control and management (C&C) of such networks, hypothesis of the paper is the inefficiency of such methods in the case of changes in the structure and management and control techniques. Paper gives classification of botnet detection methods in two categories: honeypot systems and intrusion detection systems.

Wireless technology that has great potential in increasing the quality of health services, Wireless Body Area Networks (WBAN), participates in the collection and transfer of high sensitivity data and thus requires a high level of security infrastructure for the storage, transmission and processing. Given the limited resources of processing and storage, in [4] has been noticed the existence of threats to the availability of data in such networks, and as a threat to the highest risk identified as a DDoS attack that directly affects the availability of data users (patients). The purpose of the paper was to identify the types of DDoS attacks which represent the highest level of threat and identify methods of protection for these types of attacks. Research has shown that the greatest threat of DDoS attacks is TCP SYN flooding, given that 85% of DDoS attacks using the TCP protocol.

Research conducted so far has proven that devices in the IoT environment can be utilized in generating DDoS attacks. Considering the large increase in the number of devices in the IoT environment, the goal of this paper is to explore the impact of such changes on the growth of the DDoS attacks volume by analysing the used protocols. The purpose of the research is to provide a foundation for the development of new and adaptation of existing mechanisms to protect the new vectors of attack.

1.2 Research methodology

This paper synthesized and analysed statistical data on protocols used in the generation of DDoS attacks. The data used in the analysis were collected from the company Prolexic whose primary activity is protection against DDoS attacks and are publicly available on the official website of the company. Analysed data is collected by the company Prolexic quarterly through hardware solutions for protection against DDoS attacks implemented in different geographical locations and in different environments (medical facilities, government institutions, IT companies, banking systems, etc.). The data are analysed only of one company because of methodological consistency of data collection. Comparison of data collected from different companies would have been impossible because of the large difference in the number of devices, environments within which data was collected, geographic locations, etc.

Analysed data was collected in period from first quarter of 2013 until first quarter of 2015 (ten consecutive quarters) because of rapid increase of traffic volume used in DDoS attacks in the same time period.

2. Overview of IoT concept

IoT concept is connecting objects from the environment into the global network based on IP protocol, which makes it a prerequisite for the development of smart environment in large scale. The development of this concept is influenced by previous development of certain areas of engineering sciences such as connecting devices in motion, wireless sensor networks, processing large amounts of data, IPv6 standards and others. There were created the preconditions for the development of IoT concept by linking developed, independent, technical areas through an intermediary program layer [5].

IoT can be viewed as a further development of M2M (Machine-to-machine) communication. M2M communication supports data transmission between machines and automated means of information transfers and orders without human intervention [6]. In order to meet the requirements of various industries, companies, institutions and other organizations the layered IoT functional model was designed and shown in Figure 1.

Functional model contains two transversal functionality groups that are required by each of the seven longitudinal groups.

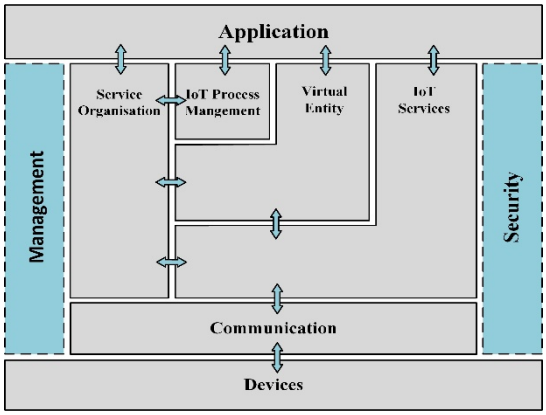


Figure 1. *IoT functional model [6]*

Main interactions between the functional groups are depicted with arrows. Since the transversal functional groups (management and security) interface with most of the other functional groups, their interactions with them are not explicitly depicted [7].

3. Attacks directed at the service availability

Congestion in the communication node affects the quality of service (QoS) as an important element of providing any form of service. According to [10], QoS is defined in several ways and according to recommendation of the ITU-T E.800 (International Telecommunication Union) it is "joint effect of the performance service that determines the level of satisfaction of users of the service." From the aspect of service providers, QoS is expected condition of service quality offered to the user defined in the basic parameters such as bandwidth, packet loss, latency / delay and jitter [8].

Intentionally causing traffic congestion in the network by generating large amounts of illegitimate network traffic has had a negative impact on the QoS (a direct impact on one or more parameters that determine it) and can impair Service Level Agreement (SLA) established between the end user and the service provider [9].

Denial of service attacks, implies a general class of attacks aimed at the availability of information and communication (IC) services and resources. As the purpose of each IC service is to provide requested information, DoS can be defined as an attack aimed at preventing access to the data [10]. Availability, as one of three key principles of ICS security, is referred in the availability of the required information to legitimate users within the required time and under given conditions. If that is not fulfilled then its primary function is meaningless, and the system is unable to meet the requirements set by the end-users [11]. According to the method of distribution DoS attacks can be divided into two categories, denial of services with a single source (SDoS) and distributed denial of service (DDoS) [12]. Source of SDoS attack is one computer or device on the network. In DDoS attacks multiple devices are coordinated for the purpose of routing large volumes of illegitimate traffic to attack target.

Reason for the appearance of DDoS attack methods is to increase the speed of processing packets within the router and end devices (e.g. server) causing one device in the network often not been able to generate a sufficient traffic volume to create

congestion in the network. Other reason is to camouflage real attack source by applying a large number of mostly geographically dislocated, attack generating devices. An additional reason for the application of DDoS attacks is a high probability of creating congestion in unwanted network segment using the SDoS attack methods.

4. Analysis of DDoS attack trends

Denial of service attacks represent a growing problem therefore it is necessary to research and analyze trends of applied protocols and traffic volume and bandwidth of attacks with the aim of timely response to future attacks.

Distribution of DDoS attack methods based on application layer protocols is shown in Figure 2. The data is presented on a quarterly basis for the period from Q1 2013 to Q1 2015. From the visible data application of the GET method of attack based on the HTTP protocol is the most common. Decrease of 10.63% is visible in transition from Q4 2013 (19.91%) to Q1 2014 (29.9%). From Q4 2013 to Q1 2015 use of application layer protocols for the realization of DDoS attacks have consistently fallen. The highest incidence was recorded in Q2 2013 (25.29%) while in Q1 2015 amounted to (9.32%) as a total decline of 15.97%.

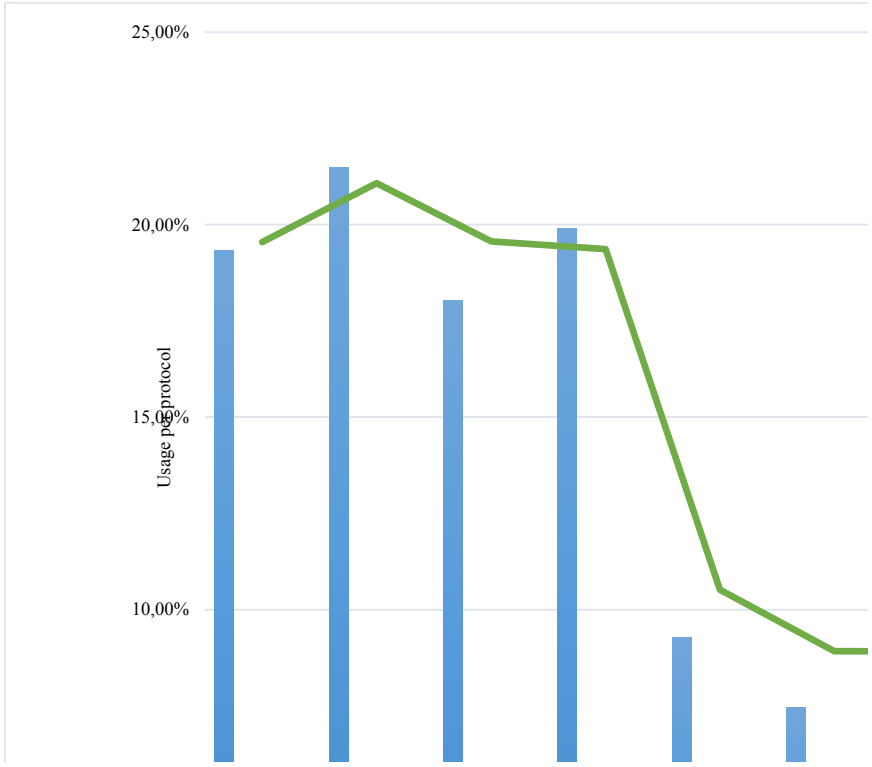
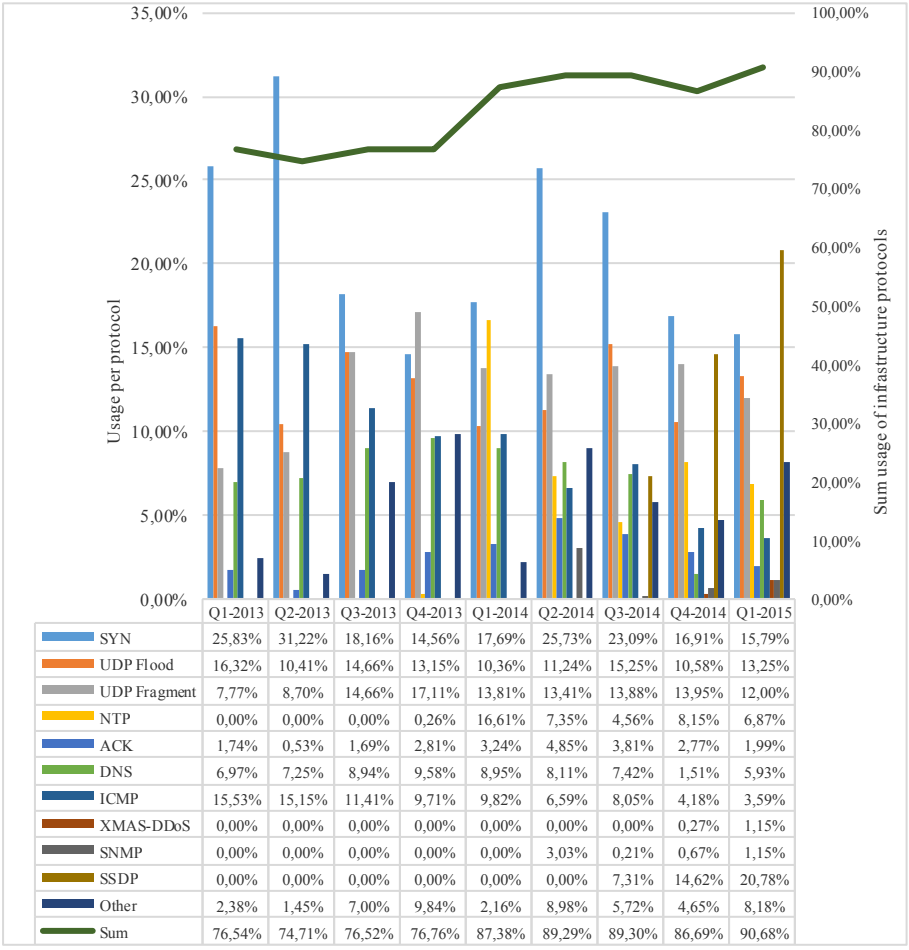


Figure 2. *Frequency of application layer protocol used in conducting DDoS attacks period Q1-2013 - Q1-2015 [13-21]*

Distribution of infrastructure layer (OSI network and transport layer) for the realization of DDoS attacks is shown in Figure 3. For the entire analyzed period of time

we can see continued growth. The overall increase from Q1 2013 to Q1 2015, a summary of all protocols, is 14.14%. In Q1 2015, 90.68% of all recorded DDoS attacks used infrastructure layer protocols. The primary protocol used for the implementation of DDoS attacks from Q1 2013 to Q4 2014 was the TCP SYN.



	Q1-2013	Q2-2013	Q3-2013	Q4-2013	Q1-2014	Q2-2014	Q3-2014	Q4-2014	Q1-2015
SYN	25,83%	31,22%	18,16%	14,56%	17,69%	25,73%	23,09%	16,91%	15,79%
UDP Flood	16,32%	10,41%	14,66%	13,15%	10,36%	11,24%	15,25%	10,58%	13,25%
UDP Fragment	7,77%	8,70%	14,66%	17,11%	13,81%	13,41%	13,88%	13,95%	12,00%
NTP	0,00%	0,00%	0,00%	0,26%	16,61%	7,35%	4,56%	8,15%	6,87%
ACK	1,74%	0,53%	1,69%	2,81%	3,24%	4,85%	3,81%	2,77%	1,99%
DNS	6,97%	7,25%	8,94%	9,58%	8,95%	8,11%	7,42%	1,51%	5,93%
ICMP	15,53%	15,15%	11,41%	9,71%	9,82%	6,59%	8,05%	4,18%	3,59%
XMAS-DDoS	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,27%	1,15%
SNMP	0,00%	0,00%	0,00%	0,00%	0,00%	3,03%	0,21%	0,67%	1,15%
SSDP	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	7,31%	14,62%	20,78%
Other	2,38%	1,45%	7,00%	9,84%	2,16%	8,98%	5,72%	4,65%	8,18%
Sum	76,54%	74,71%	76,52%	76,76%	87,38%	89,29%	89,30%	86,69%	90,68%

Figure 3. *Frequency of infrastructure layer protocols used in DDoS attacks in the period Q1-2013 - Q1-2015 [13-21]*

From Q3 - 2014 a growth of application SSDP protocol (7.31%) is seen, and in Q1 2015 usage of the same protocol was increased by 13.47% and amounted to 20.78%, which is 4.99% more than the TCP SYN.

5. Discussion

SSDP whit the share of 20.78% represents the most common protocol in the conducting of the infrastructure layer DDoS attacks. SSDP protocol is used to detect

Universal Plug and Play (UPnP) devices. UPnP is a set of network protocols that allow detection and connection of network devices without user intervention [22]. A large proportion of attacks based on the SSDP protocol is the result of development and progressive implementation of the M2M and its upgrade, the IoT concept. These concepts are based on connecting a large number of devices that are communicating with each other, and use the SSDP protocol.

Figure 4 shows the extent of DDoS attacks in the period from 2002 to 2014. In the last two years exponential growth of the attack volume is seen (measured in Gbps). Compared to the year 2012 the volume of DDoS attacks in 2013 increased by 475%, and in 2014 for 615%. The result is the increasing availability of online services that offer the service botnets usable in conducting DDoS attacks, a growing number of connected devices that are potential agents in botnet networks which allows generating larger amounts of network traffic and finally the use of new protocols in the realization of attack (e.g. SSDP) and reduced levels of protection in certain devices (eg. the IoT devices).

According to [23], shown in Figure 4, the accelerated growth of the connected devices number based on the IoT concept is predicted. Currently in the world there are approximately 5 billion of these devices, and interpolation growth trend indicates a potential 25 billion connected devices by 2020. The same figure is shown that the increase in the number of connected devices is followed by an increase in DDoS attacks bandwidth. The sharp rise in the number of devices connected through the IoT concept offers the possibility of forming a botnet network that is able to generate significantly greater amount of illegitimate traffic than in previous years.

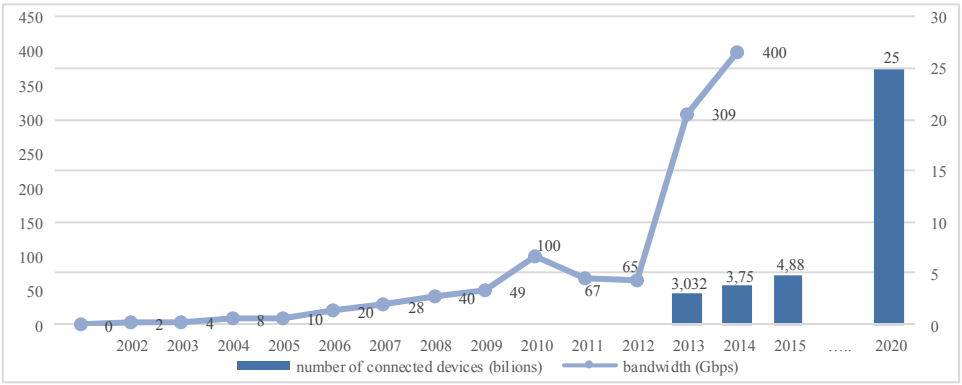


Figure 4. *The ratio of increase in the number of connected devices and DDoS attack bandwidth [23], [24]*

Although IoT concept provides a number of features and the foundations for the development and delivery of new services, devices used in this concept contain significant limitations compared to traditional terminal devices (PC, notebook computers), such as reduced storage capacity, processing, physical size and power consumption (increase of the device autonomy). As a result of various limitations standard protection methods are often not applicable in such an environment that exposes devices to an additional risk of presumed threats [22]. The growing number of these

devices and the low level of protection implemented allows them to be easily join in the botnet network devices, which are ultimately reflected on the scope of DDoS attacks in terms of traffic volume (pps) and used bandwidth (bps).

6. Conclusion

Security is an essential element for achieving the work of information and communication system in a predictable way. To information communication system was able to achieve its basic functions and meet the demands placed before him by the end users need to maintain the required level of the basic factors of safety or the availability, confidentiality and integrity. On the availability of the communications network congestion that may occur due to the stochastic nature of network traffic. The impact on the availability and has deliberately generating network traffic by illegitimate users with the purpose of intentionally inducing congestion in a particular segment of the communications network, with a view of the negative impact on service availability.

Goal of this paper is to analyze the attacks focused on the availability of services based on flooding network resources. We analyzed the trends of these attacks to the quarterly data collected during the period from 2013 to the first quarter of 2015. The analysis shows the increasing representation of attacks based on the infrastructure layer (OSI network and transport layer) as compared to those based on the application layer. Increasing trend of attacks on infrastructure layer contributes to the rapid growth of devices based on the concept of IoT who are potential participants in the generation of illegitimate network traffic. Proof of this is the increase in the proportion attacks through SSDP protocol whose application is necessary in a number of IoT supported devices. Given the predictions on the future size of these devices can be concluded that the proportion of such attacks continues to have growth.

Although new methods and ways of protection against DDoS attacks are continuously researched, the analysis conducted in this paper suggests a further and more intense need to explore new, and adapting existing methods to protect the upcoming types of attacks caused by dynamic changes and the development of communication technologies.

Future research will be focused on the analysis of the possibilities of using SSDP and other protocols in IoT environment in conducting DDoS attacks on the infrastructure layer. In addition to exploring the possibilities of developing new methods of protection aimed at protocols IoT environment as a result of a significant increase in DDoS attacks that are generated through the SSDP protocol.

References

[1] A. D. Wood and J. A. Stankovic, “A taxonomy for denial-of-service attacks in wireless sensor networks,” Handb. Sens. Networks Compact Wirel. Wired Sens. Syst., pp. 739–763, 2004.

[2] S. Ramanauskaite and A. Cenys, “Taxonomy of DoS attacks and their countermeasures,” Cent. Eur. J. Comput. Sci., vol. 1, pp. 355–366, 2011.

[3] H. R. Zeidanloo, M. J. Zadeh, Shooshtari, P. V. Amoli, M. Safari, and M. Zamani, "A taxonomy of Botnet detection techniques," in 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT 2010), 2010, pp. 158–162.
[4] R. Latif, H. Abbas, and S. Assar, "Distributed Denial of Service (DDoS) Attack in Cloud- Assisted Wireless Body Area Networks: A Systematic Literature Review," J. Med. Syst., vol. 38, pp. 128–140, 2014.
[5] A. Antonić, M. Marjanović, K. Pripužić, and I. P. Žarko, "A mobile crowd sensing ecosystem enabled by CUPUS: Cloud-based publish/subscribe middleware for the Internet of Things," Futur. Gener. Comput. Syst., vol. 1, pp. 1–16, 2015.
[6] D. Peraković, S. Husnjak, and I. Cvitić, "IoT infrastructure as a basis for new information services in the ITS environment," in 22nd Telecommunication forum (TELFOR 2014), 2014, pp. 39–42.
[7] R. M. Cardoso, N. Mastelari, and M. F. Bassora, "Internet of Things Architecture in the Context of Intelligent Transportation System – A Case Study Towards a Web-based Application Deployment," in 22nd International Congress of Mechanical Engineering (COBEM 2013), 2013, pp. 7751–7760.
[8] Š. Mrvelj, "Dynamic allocation of capacity of the Internet node according the service demands", Ph.D. dissertation, Faculty of Transport and Traffic Sciences, University of Zagreb, Zagreb, Croatia, 2008.
[9] S. Fowler, S. Zeadally, and N. Chilamkurti, "Impact of Denial of Service Solutions on Network Quality of Service", Secur. Commun. Networks, vol. 4, no. 10, pp. 1089–1103, 2011.
[10] Imperva, "Hacker Intelligence Initiative Overview," Redwood City, USA, 2012.
[11] M. Ciampa, "Guide to Network Fundamentals." Course Technology, Boston, 2012.
[12] A. Hussain, J. Heidemann, and C. Papadopoulos, "A Framework for Classifying Denial of Service Attacks," in Applications technologies architectures and protocols for computer communications (SIGCOMM 03), 2003, pp. 99–110.
[13] Prolexic, "Prolexic Quarterly Global DDoS Attack Report (Q1-2013)." Prolexic Technologies, Inc., 2014.
[14] Prolexic, "Prolexic Quarterly Global DDoS Attack Report (Q2-2013)." Prolexic Technologies, Inc., 2013.
[15] Prolexic, "Prolexic Quarterly Global DDoS Attack Report (Q3-2013)." Prolexic Technologies, Inc., 2014.
[16] Prolexic, "Prolexic Quarterly Global DDoS Attack Report (Q4-2013)." Prolexic Technologies, Inc., 2014.
[17] Prolexic, "Prolexic Attack Report (Q1-2014)." Prolexic Technologies, Inc., 2014.
[18] Akamai Technologies, "Faster Forward to the Latest Global Broadband Trends (Q2-2014)," Massachusetts, USA, 2014.
[19] Akamai Technologies Inc., "Akamai's State of the Internet - Security (Q3-2014)," 2014.
[20] Akamai Technologies Inc., "Akamai's State of the Internet - Security (Q4-2014)," 2014.
[21] Akamai Technologies, "Faster Forward to the Latest Global Broadband Trends (Q1-2015)," Massachusetts, USA, 2015.

[22] M. Chowdhury and F. Kader, “Security Issues in Wireless Sensor Networks : A Survey,” Int. J. Futur. Gener. Commun. Netw., vol. 6, pp. 97–116, 2013.
[23] P. Middelton, P. Kjeldsen, and J. Tully, “Forecast: The Internet of Things, Worldwide, 2013,” 2013. [Online]. Available: https://www.gartner.com/doc/2625419/forecast-internet-things-worldwide-.
[24] Arbor Networks, “Worldwide Infrastructure Security Report,” Burlington, USA, 2015.

Sažetak: *Dostupnost informacija i usluga, uz integritet i celovitost predstavlja ključan parametar bezbednosti informaciono komunikacionog sistema. Aktivnosti usmerene prema uskraćivanju dostupnosti mrežne komunikacije aktuelne su od početaka razvoja globalne komunikacione mreže i zahtevaju kontinuirani razvoj metoda zaštite. Značajan izazov predstavlja pojava koncepta Internet of Things (IoT) kojim će se značajno povećati broj povezanih uređaja. Takvo okruženje moguće je iskoristiti u svrhu generisanja DDoS napada. Radom je istražen uticaj značajnoga rasta broja povezanih uređaja u konceptu IoT na povećanje broja i obima DDoS napada.*

Ključne reči: *napad uskračivanja usluge; dostupnost sistema; plavljenje mrežnih resursa; mrežna bezbednost;*

ANALIZA UTICAJA KONCEPTA IoT NA PORAST OBIMA DDoS NAPADA

Dragan Peraković, Marko Periša, Ivan Cvitić