Journal of Engineering Technology

Volume 8, Issue 2, July 2019, PP. 1-16

RESEARCH ARTICLE -ENGINEERNG TECHNOLOGY

A Study on Improving M2M Internet Network Security through Abnormal Traffic Control

Seongsoo Cho[1], Young-Sik Kim[1]*, and Changho Seo[2]*

[1]Department of Information and Communication Engineering, Chosun University, Gwangju 61452, Republic of Korea
[2]Department of Applied Mathematics, Kongju National University, Kongju 32588, Republic of Korea
*Corresponding Author

Abstract: Machine-to-machine (M2M) intelligent network devices are exposed to vulnerable networks and there is always existed a security threats. The devices are composed of low-capacity hardware by their nature and exposed to various security threats such as worms, viruses and distributed denial of service (DDoS) flooding attacks due to lack of security or vaccine program installed in personal computer environment. In this paper, we proposed a network filter that improves the security of M2M intelligent network by configuring the network security filter in a specific form that can be adapted to M2M intelligent network. In this work we proposed a behavior-based filter to match the characteristics of M2M intelligent devices and control abnormal traffic in the M2M intelligent network. The proposed filter increases user convenience and decreases unnecessary data loss. Experimental results show that when the security filter is applied the response speed of the device improved more than 50% in abnormal traffic environment with the cost of less than 10% delay depending upon the characteristics of the device.

Keywords: M2M, IoT security, DDoS, network filters.

1 Introduction

The future of the Internet is evolving through convergence with existing infrastructure and Internet of Things (IoTs), such as sensor, while simultaneously accommodating the communication speed and the increase of various access terminals to meet the rapidly increasing demand of the users. The 4th Industrial Revolution, which is currently under development, is a combination of ultra-intelligent computing technologies that utilize artificial intelligence and big data, ultra-connectivity information and communication technologies that utilize mobile and 5G technology to broaden various Internet of Things (IoT) [1-4]. Machine-to-machine (M2M) intelligent network is emerging as an ICT infrastructure for future telecommunication convergence that enables intelligent communication services between people and the intelligent communication between them should be achieved safely and conveniently anytime and anywhere in real time. In a narrow sense, M2M intelligent network means, communication between machines and terminals used by humans. In a broad sense, it means a solution that can confirm information of a remote object through a combination of communication and ICT technology [5-8].

M2M intelligent network does not mean a part of technology, and existing specific technologies can be seen through the Internet when things are used in the form of things, objects, and services.

Compared to laptops and mobile devices connected to the Internet, which are determined by the number of individual users, M2M intelligent network can solve social issues, prevent disasters through u-City, u-Health, u-Saving, CO2 reduction, and so on. It means intelligent environment where users and home appliance smart devices transmit and receive information and data in real time by converging ICT. M2M intelligent network has the idea of applying IT to a very important problem unlike the existing Internet, such as disaster prevention. M2M intelligent network is mostly used for wireless, but people prefer wired to wireless rather than wireless. In order to solve this problem, M2M intelligent network needs the receiving procedures to acquire empirical data about the M2M intelligent network's information security, security field, and data reliability [9-11].

Security is a core technology that must be provided for intelligent network generalization and new service creation. The increase of number of devices connected to the network means the increase of number of attackable targets and an expansion of threats in the devices. Security applications are indispensable for Internet devices and communication technologies, especially those that apply to healthcare and industrial facility controls. If these services are infringed, it could cause economic damage and even damage to people. In addition, the fact that the surrounding objects are connected to the network means an increase in the range of concern about personal information leakage or privacy invasion, and it is obvious that the level of infringement will be so large that it cannot be compared with the current level [12-13].

In this paper, we designed a service access control system using security filters and an efficient management method for network services for objects, and proposed an implementation of a secure availability network to provide intelligent network. The security filter proposed in this paper identifies and controls unusual packets that may occur inside or outside of the Internet appliance to allow stable service of the Internet appliance.

2 M2M intelligent network background

Through the M2M intelligent network, an intelligent and active relationship is created that can control, sense, exchange and process key components, and this has evolved into a service form. The M2M intelligent network concept refers to the M2M intelligent network environment as shown in Figure 1, which evolved into a concept that interacts with all the data in real and virtual world by being applied to network structure beyond wireless communication [14-15]. M2M intelligent network is a network environment of object space that forms intelligent relationships such as sensing, networking, information exchange and processing without any user intervention between distributed elements such as human, object, and service. In the era of M2M intelligent network, the privacy issue caused by data exchange of various devices, as well as vulnerability in numerous industries such as automobiles and medical care, may threaten life [16-17].

The biggest issue of security arising is the migration through numerous data routes. In the case of embedded smart devices that have been in use for a long time, structural defects and cyber-attacks using security vulnerabilities can cause enormous confusion and issues in the market environment and major infrastructure. The wider range of attacks targeting all industries and areas of life will increase the chances of malicious hackers targeting a wide range of industries, from manufacturing to power grids, automobiles, medical devices, home appliances and home appliances. There may be a situation in which personal medical information is leaked to the outsiders by a hacker, complete stop or uncontrollable of national infrastructures, such as networks, a power system and a traffic signal among others [18-20].

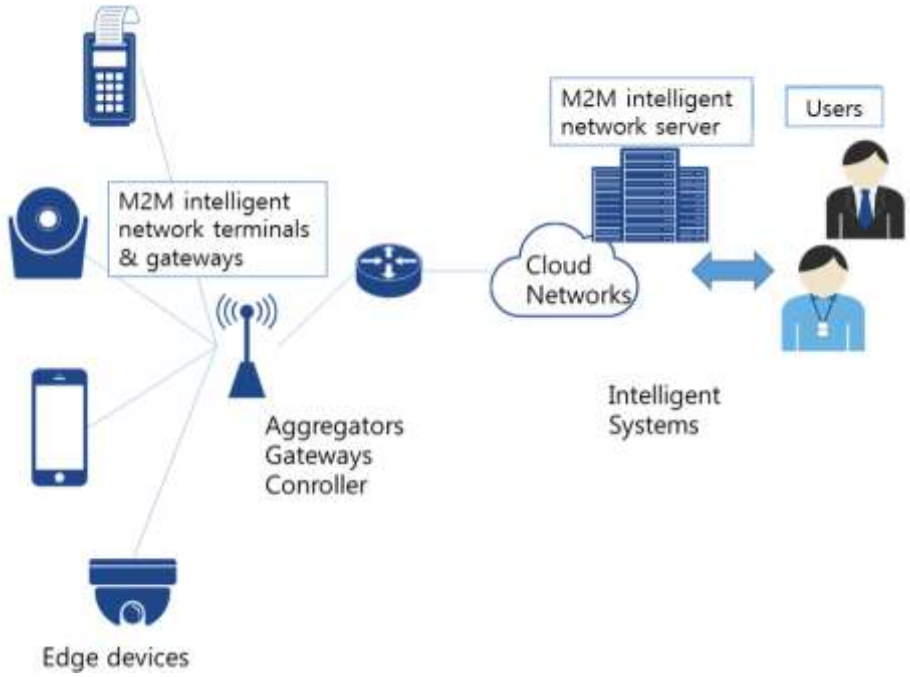


Figure. 1. Configuration of the M2M intelligent network environment.

In 2009, computer programmer John Matherly launched Shodan, a computer search engine with a graphical user interface that identifies Internet-facing devices [21]. In particular, the emergence of a Shodan site that can detect M2M intelligent networks to locate its connection to the network and it increases the security threats [22-23]. As shown in the Table 1, Shodan has detected the connected devices and collected the data more than 40 networks, such as Server, Webcam, IP CCTV, Network Printer, and Router [21, 24-25].

Table 1. Shodan documented service interrogation filters.

Port	Service	Port	Service	Port	Service
21	FTP	465	SMTP	5632	PC Anywhere
22	SSH	623	IPMI	5900	VNC
23	Telnet	993	IMAP+SSL	6379	Redis
25	SMTP	995	POP3+SSL	7777	Oracle
53	DNS	1023	Telnet	8000	Qconn
80	HTTP	1434	MS-SQL	8080	HTTP
81	HTTP	1900	UPnP	8129	Snapstream
110	POP3	2323	Telnet	8443	HTTPS
119	NNTP	3306	MySQL	9200	ElasticSearch
137	NetBIOS	3389	RDP	11211	MemCache
143	IMAP	5000	Synology	27017	MongoDB
161	SNMP	5001	Synology	28017	MongoDB Web
443	HTTPS	5432	PostgreSQL		
445	SMB	5560	racle		

As shown in Figure 2, Shodan retrieves OpenSSL patch version information of M2M intelligent network and through the heartbleed of this version, it is confirmed that the system is defenceless on information stealing /attacking and service denying/attacking etc [26-28]. The ability to identify

devices that monitor and control critical infrastructure assets has raised major security concerns. A CNN article [29] claims that Shodan is "The scariest search engine on the Internet".

Figure. 2. Shodan search engine with M2M intelligent network.

The Open Web Application Security Project (OWASP) announced the top ten critical web application security risks. The ten largest vulnerabilities can be viewed as security vulnerability items that underpin the Internet security threats of industry-specific objects such as lack of encryption, weak physical security of object Internet devices, and leakage of personal information [30].

The type of network attack that can occur in the M2M intelligent network environment is one more advanced Distributed Reflection Denial of Service (DDoS) attack than the DDoS attack [31-32]. GitHub.com has posted an official engineering blog post on March 01, 2018, explaining the background of a DDoS attack that occurred on February 28th. In a report dated January 1, the US ZDNet reported that DDoS attacks targeting GitHub.com have surpassed 1.1Tbps DDoS attacks, which had been the largest ever occurred before [33]. According to GitHub, a large DDoS attack occurred with over a thousand automated systems, including tens of thousands of unique endpoints. Figure 3 shows that a memcached amplification attack or a "Memcached UDP Reflection" attack, in which somebody is generating 1.35 Tbps traffic at the maximum point through 126.9 million packets per second. Memcached servers are servers that store caches to reduce the load on large data stores, such as disk storage or databases (DBs). Since it is not normally exposed to the Internet, there is no separate authentication process. However, there was a memcached server set to be exposed to the Internet, and the attacker seemed to have exploited it and made a massive attack using the memcached server as a reflector.

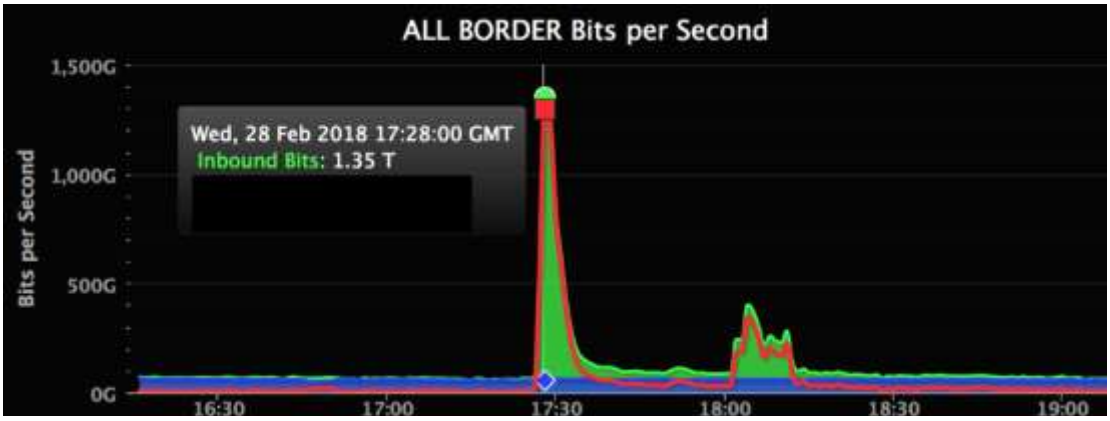


Figure. 3. DDoS attack traffic that caused malfunction at GitHub.com at the end of February 2018 [33].

The size of the DDoS attack is expected to grow further. In case of M2M intelligent network, it is difficult to cope with device security patch, which is not smooth, and it is hard to know if device is infected. Here, malicious code variants continue to make it more difficult to respond. This is Distributed Reflector Denial of Service (DRDoS) using vulnerability of Simple Service Discovery Protocol (SSDP), which is highly likely to attack in M2M intelligent network environment as shown in Figure 4.

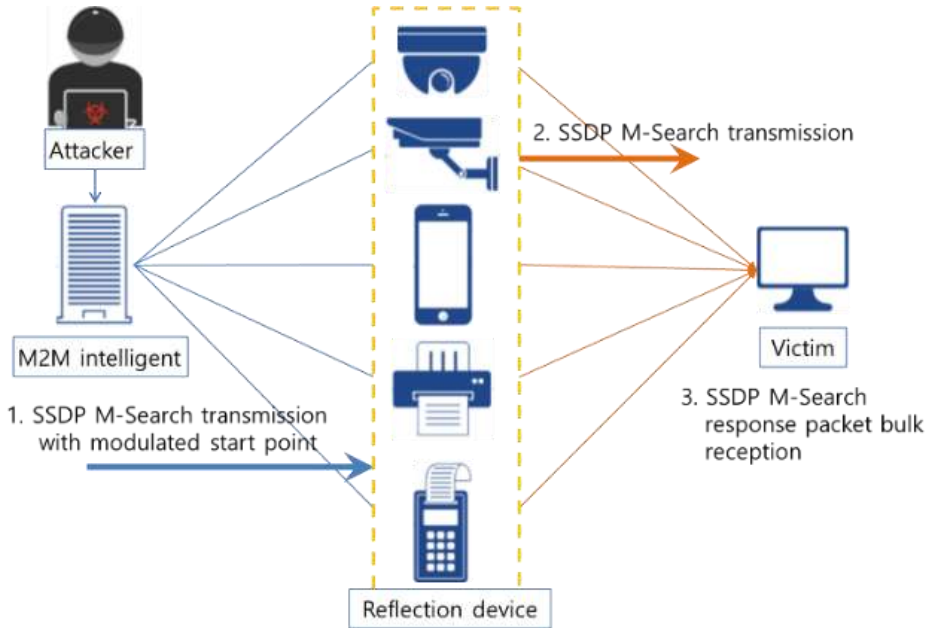


Figure. 4. DRDoS attack using M2M intelligent network.

The attacker scans the SSDP service externally using his M2M intelligent device to attack the victim and prepares the victim for the attack. The attacker modifies IP from the originating IP of the M-Search request packet in the form as shown Figure 5 through the M2M intelligent device to the victim and sends a request to the M2M intelligent devices.

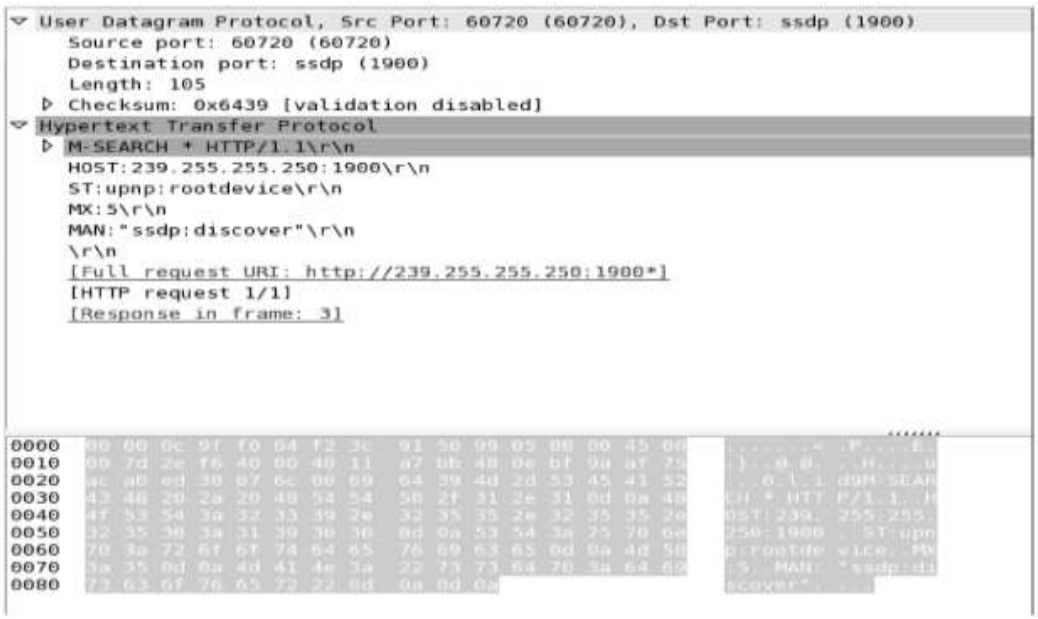


Figure. 5. M-Search request packet.

The M2M intelligent device that receives the M-Search request transmits a response packet containing more data than the request packet as shown in Figure 6. Since the size of the response packet is large compared to the request packet, the SSDP protocol attempts DRDoS using a large response packet to the victim, and the victim cannot use the normal service [34].

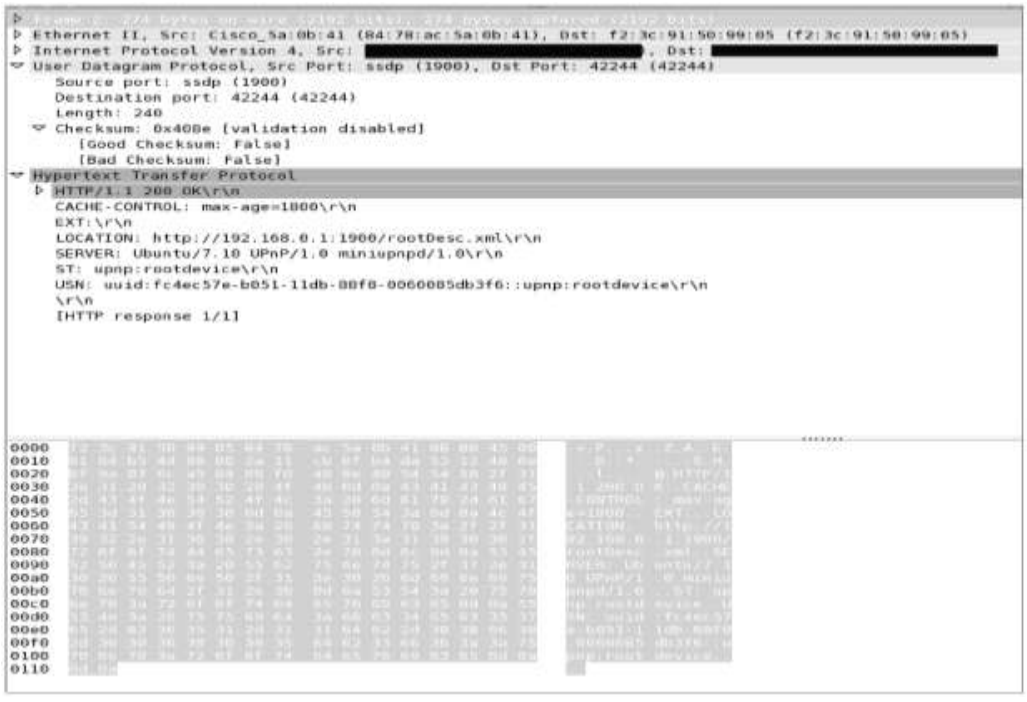


Figure. 6. M-Search response packet.

3 Implement M2M intelligent security filter

Linux and embedded Windows, which are the foundations of M2M intelligent devices, are vulnerable to network attacks if they are not secured or properly updated on the device [35]. The proposed security filter is based on Linux's iptables. It has a behavior-based filter to match the characteristics of M2M intelligent devices. Iptables consist of four tables that supports "filter to control the allow / block, IP Network Address Translation (NAT) and NAT to control routing, RAW which controls connection tracking for sessions, manage to modify and marking communication packet". The role of the table and the function of the chain are the same as shown in Table 2.

The iptables used in the proposed security filter is intended to control abnormal traffic in the M2M intelligent network environment using the following options. The first is the ability to manage and check the state of the session with the conntrack option.

Table 2. Iptables table and chain.

Chain	Table			
	Filter	IP NAT	Raw	manage
INPUT	○			○
FORWARD	○			○
OUTPUT	○	○	○	○
PREROUTING		○		○
POSTROUTING		○	○	○

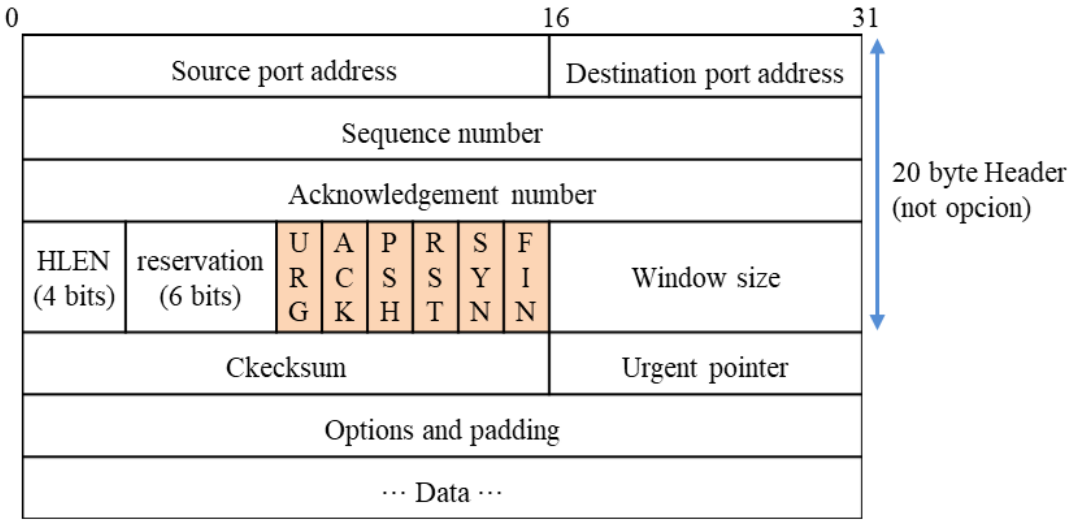


Figure.7. TCP header and control flag structure.

When a new kind of packet arrives, it generates a conntrack and finally records whether the packet is allowed or blocked. If the packet is allowed, it can be considered as safe, and it is safe to continue accepting packets at least for that session. However, since the firewall for packet filters allows each rule to be applied to the entire packet, it is checked continuously even if the packet is allowed once. Since this operation is unnecessary waste of resources, if the same connection is allowed, conntrack leaves a record of the session through conntrack and allows matching packets without checking rules. The second invalid option provides control over abnormal session creation. Once a session is created with an unauthorized access during the network communication process, it

helps to obtain the availability by the advance control through the option. The third option to TCP-flags is to provide control for each flag in TCP. As shown in Figure 7, TCP prepares flags according to the situation.

TCP a connection-oriented protocol, basically connects sessions through 3-way handshake as shown in Figure 8 and terminates the session through 4-way handshake as shown in Figure 9. Through the 4-way handshake of Figure 9, it is possible to organize garbage sessions that are not used for communication that may remain in the user and server due to the normal session termination.

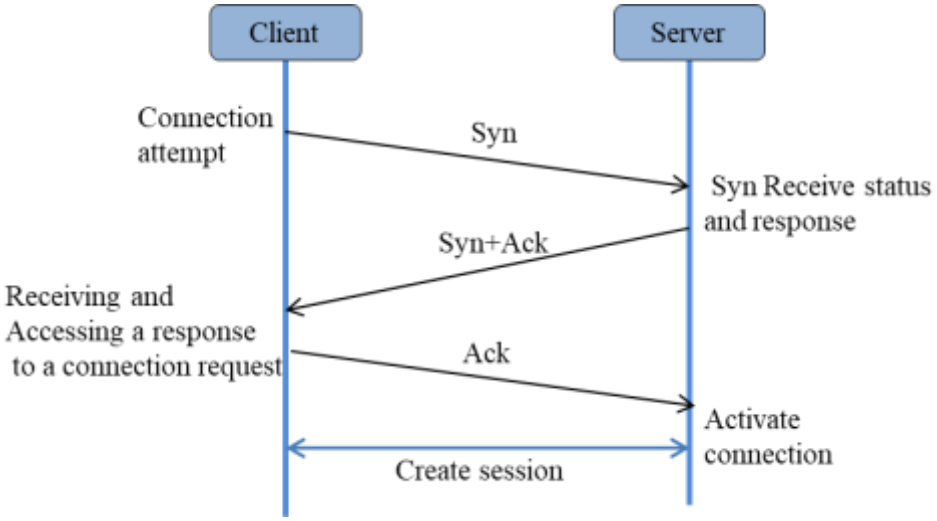


Figure.8. TCP 3-way handshake process.

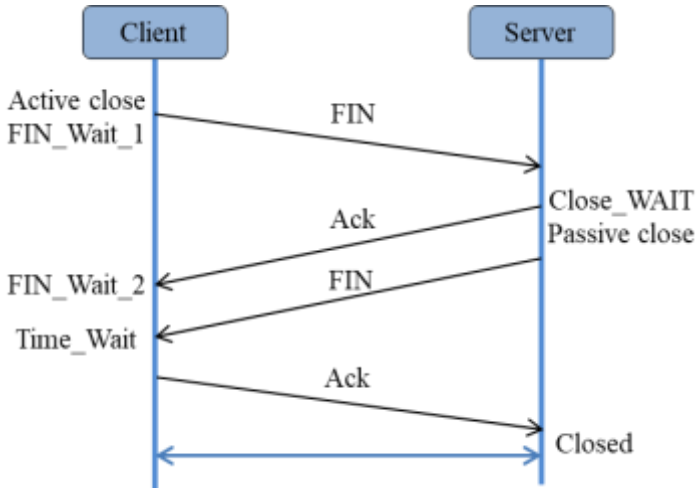


Figure.9. TCP 4-way handshake process.

The goal of the proposed security filter is to enhance the security by controlling the combination of flags that do not correspond to the normal TCP communication process. The combinations of flags are controlled by the following TCP-flags function ‘ACK / URG’, ‘ACK / FIN’, ‘FIN / SYN / RST / PSH / ACK / URG’, ‘FIN / SYN’ , ‘SYN / FIN’, ‘FIN / RST’, ‘FIN / PSH / URG’, ‘SYN / FIN / PSH / URG’ and ‘SYN / RST / ACK / FIN / URG’.

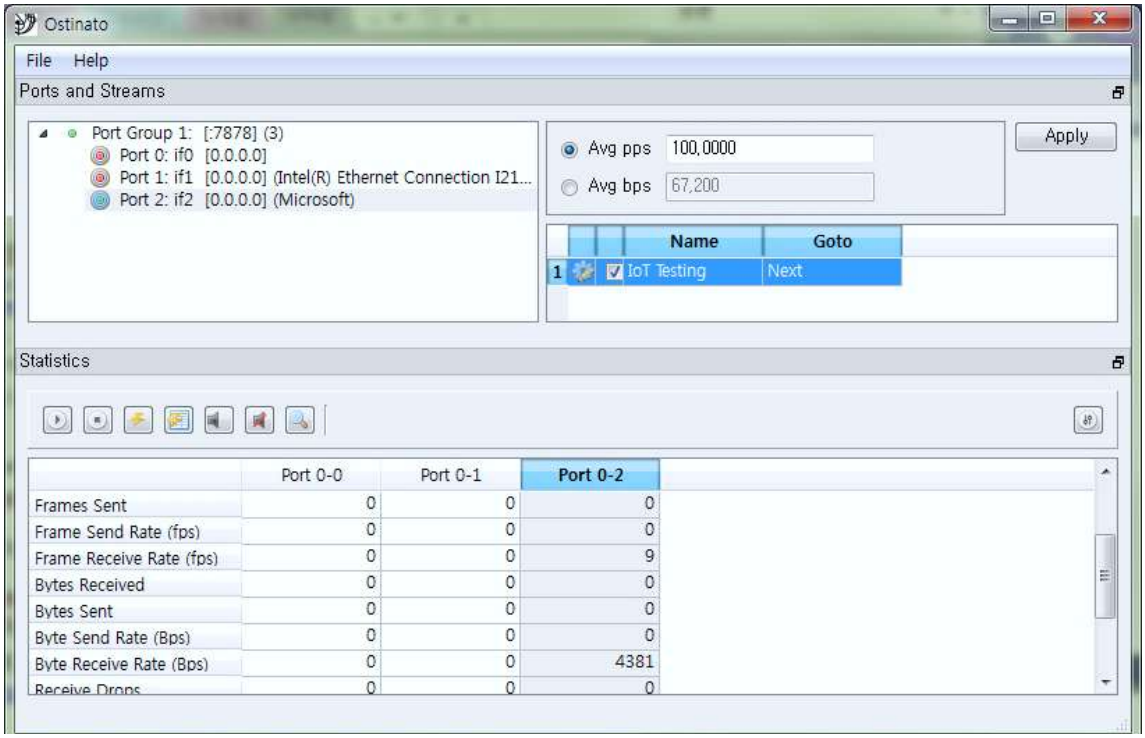
4 Experiment results

The Ostinato environment for security filter verification is a cross-platform based program that can generate IPv4-based packets and operates on Windows, BSD, MAC OS, and so on. Ostinato can analyze network traffic for GUI-based API network test automation. It is developed for non-commercial purpose and is being used as a research program. It supports various standard protocols including TCP, UDP, ICMPv4, ICMPv6 (6over4, 4over6, 4over4, 6over6) TCP / UDP / IP-in-IP, 'Ethernet / 802.3 / LLC SNAP, VLAN , IGMP, MLD and any text based protocol (HTTP, SIP, RTSP, NNTP etc.)' and detailed modifications are possible [36]. In addition, simulation of DoS and DDoS attacks that can occur in the M2M intelligent network environment is possible by defining packet transmission. Table 3 is a list of software that the user can generate and simulate arbitrary packets. Ostinato can be used for testing purposes with the General Public License (GPLv3).

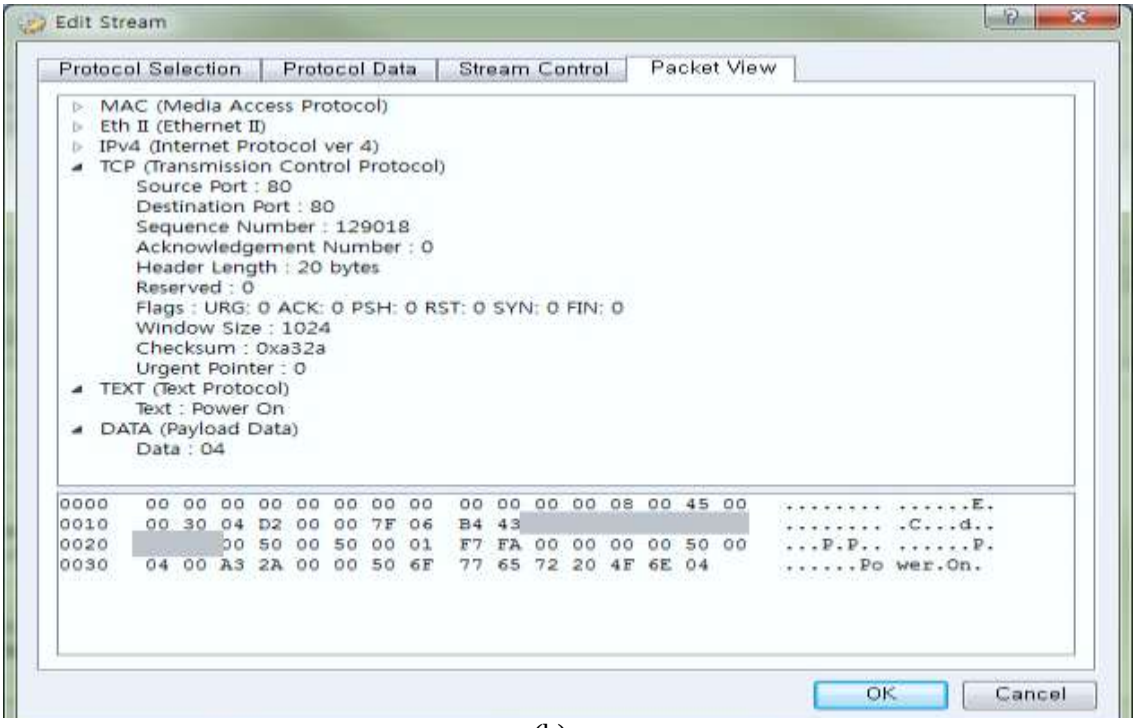
Table 3. Iptables table and chain.

Program	Producer	Operating system	Control
AnetTest	Anton aka kronos256	Windows / Unix	CLI
Bit-Twist	ayeowch aka det_re	Windows / Linux/BSD	CLI
Cat Karat packet builder	Valery Diomin, Yakov Tetruashvili	Windows	GUI
Colasoft Packet Builder	Colasoft	Windows	GUI
Nemesis	Jeff Nathan	Windows / Unix	CLI
Ostinato	pstavirs	Windows / Linux / BSD / MacOSX	GUI
Pktgen	Linux Foundation	Linux	CLI
packETH	Miha Jemec aka jemcek	Linux / Windows	GUI
pierf	Pieter Blommaert	Windows (Cygwin) / Linux	CLI
Scapy	Philippe BIONDI	Linux / Unix / Windows	CLI
targa3	Mixter	Linux, Unix	CLI

In order to verify the improved security filter, data packets are generated by Ostinato environment setting as shown in Figure 10, assuming abnormal packet triggering state of M2M intelligent network device. We set up about 100 pps for testing on low capacity lines. We set the source IP as the actual IP of the object Internet device and the destination of the packet as the test PC.



(a)



(b)

Figure.10. Ostinato settings; (a) set up packet transmission through Ostinato, (b) generate packets through Ostinato.

The Iptables environment for implementing the security filter built in the environment, where Centos and two network cards are installed to handle the inbound/outbound traffic separately. Iptables is implemented as a security filter in the Internet environment using the control options as shown in Figure 11, and devices other than the object Internet are to be used through exception processing.

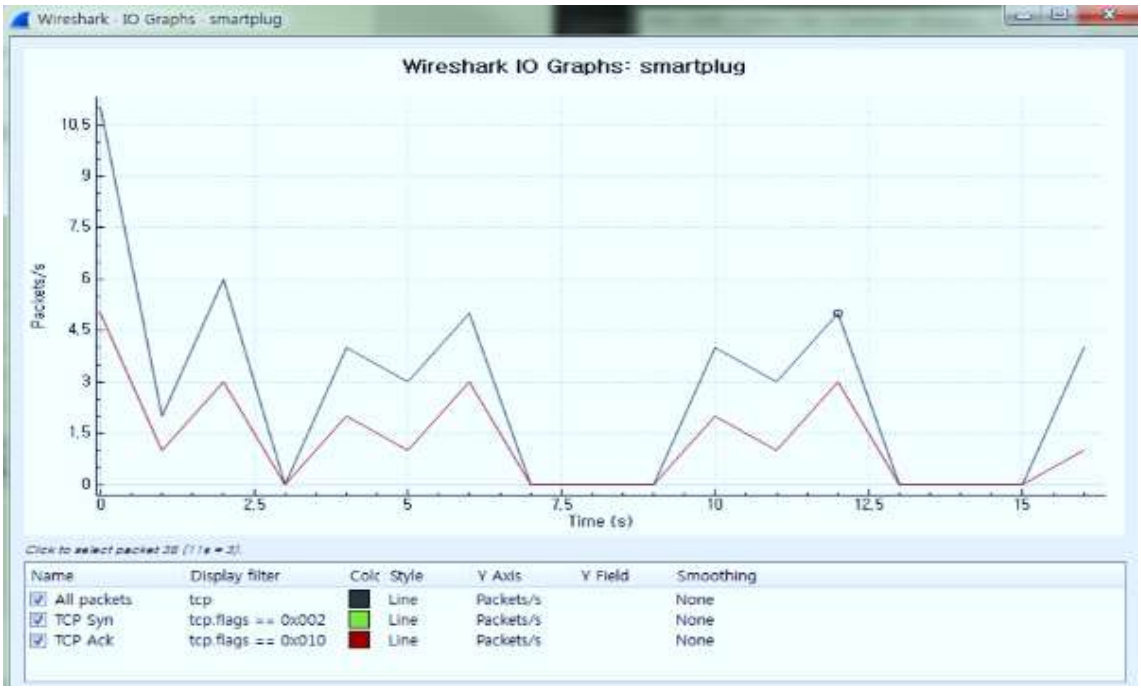
```
#/sbin/iptables -t mangle -A PREROUTING -p tcp --tcp-flags FIN,SYN FIN,SYN -j DROP
#/sbin/iptables -t mangle -A PREROUTING -p tcp --tcp-flags SYN,RST SYN,RST -j DROP
#/sbin/iptables -t mangle -A PREROUTING -p tcp --tcp-flags SYN,FIN SYN,FIN -j DROP
#/sbin/iptables -t mangle -A PREROUTING -p tcp --tcp-flags FIN,RST FIN,RST -j DROP
#/sbin/iptables -t mangle -A PREROUTING -p tcp --tcp-flags FIN,ACK FIN -j DROP
#/sbin/iptables -t mangle -A PREROUTING -p tcp --tcp-flags ALL ALL -j DROP
#/sbin/iptables -t mangle -A PREROUTING -p tcp --tcp-flags ALL NONE -j DROP
#/sbin/iptables -t mangle -A PREROUTING -p tcp --tcp-flags ALL FIN,PSH,URG -j DROP
#/sbin/iptables -t mangle -A PREROUTING -p tcp --tcp-flags ALL SYN,FIN,PSH,URG -j DROP
#/sbin/iptables -t mangle -A PREROUTING -p tcp --tcp-flags ALL SYN,RST,ACK,FIN,URG -j DROP
#/sbin/iptables -t mangle -A PREROUTING -p icmp -j DROP
#/sbin/iptables -t mangle -A PREROUTING -f -j DROP
```

Figure.11. Iptables in internet environment.

The security filter implementation is shown in Figure 11, which explains as follows: Firstly, abnormal packets that do not fit the IP communication scheme, do not meet the TCP Flag combination condition, and fragmented packets are blocked. Secondly, M2M intelligent network devices in test environments, which is confirmed that the ICMP packet is not used, and it blocks all ICMP that can be used for attacks such as DDoS and DoS. Finally, it is the most important security filter setting in the actual M2M intelligent network environment. The thresholds shown in the actual filters are applied to the M2M intelligent network devices 'TCP Syn 5 / s, TCP Ack 25 / s, UDP 5 / s' the threshold level is also used the value confirmed that there is no communication problem in applied setting. Experiments were conducted in an M2M intelligent network environment and generated abnormal traffic using Ostinato. We compared the device response in terms of speed and network stability before and after applying the filter. First, confirm whether the use of each M2M intelligent network device is normal when the network security is applied. Second, in case of M2M intelligent network device DDoS attack, we verified the resource status of damage system before and after security filter implementation in case of DDoS attack to external system. Finally, in the case of M2M intelligent network equipment, M2M intelligent network device to measure the response speed of internet devices.

Experimental results show that after the application of the network security filter, the traffic that was generated during the control process of the object Internet device did not exceed the traffic set to the normal service and the threshold value and this is shown in Figure 12. Black line indicates total traffic, red indicates TCP Ack traffic, and green indicates TCP Syn traffic. In the Figure 12 (a) M2M intelligent network device air cleaner filter operation function time is 0.800 / 0.900 millisecond, (b) M2M intelligent network device 220v plugin is 2,000 / 2,200 millisecond. In general application environment, it was difficult to sense these numerical results. Second, M2M intelligent network device is a scenario where DDoS attack was performed outside. In case of DDoS attack to the external system, the resource status of damage system before and after security filter was verified. Using Ostinato, the TCP Syn packet was maintained at 100 pps for about 5 seconds as shown in Figure 13. If the attacker was actually a large number of M2M intelligent network devices, it proved that the network security filters can prevent situations that can cause fatal damage to third parties.

(a)



(b)

Figure.12. M2M intelligent network device packet and operation; Experiments (a) Air Cleaner, (b) 220v Plugin.

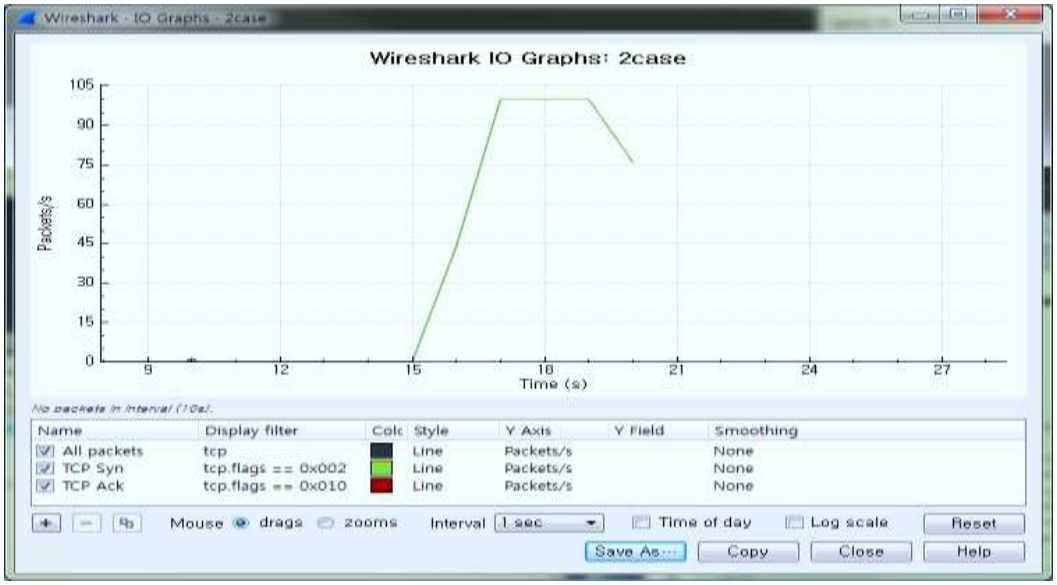


Figure.13. Packet with modulated source from M2M intelligent network device.

Finally, we measured the response speed of M2M intelligent network devices before and after the network security filter by sending packets from the external network to the M2M intelligent network device, similar results found to the communication session of the M2M intelligent network device. In order to test the Syn and Rst Flag packets that do not fit the TCP Flag combination with the same IP as the session that had been communicated with the management system by the M2M intelligent network device, it lasted for about 10 seconds at 100pps. The orange line in Figure 14 shows the Syn and Rst Flag generated that stops after 10 seconds.

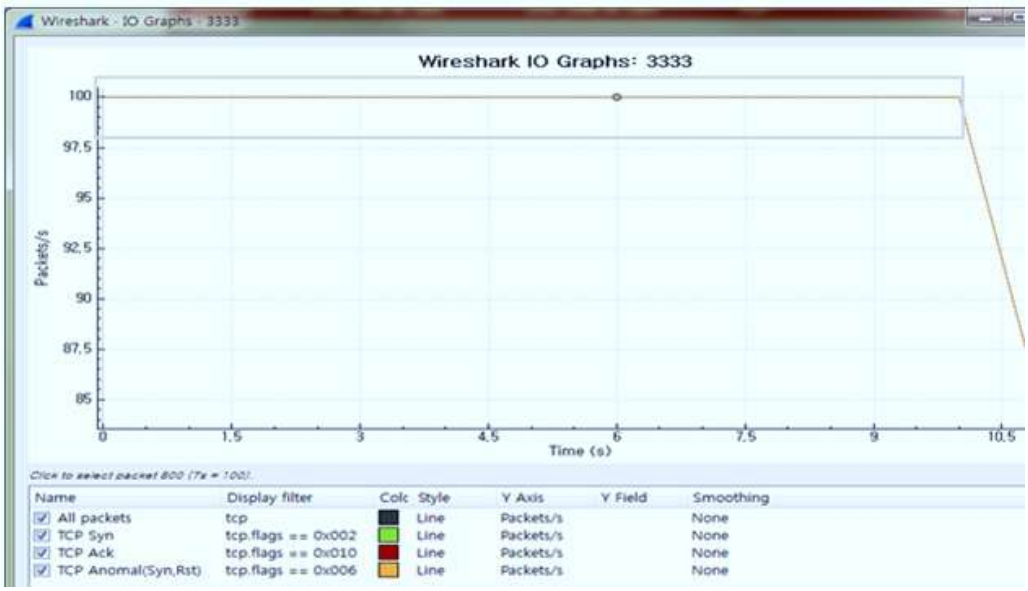


Figure.14. Packet transmission that does not match TCP Flag combination.

In experiment result, the packet in M2M intelligent network device (a) and (b) in case of not applying network security filter, (a) has 4,000 milliseconds and (b) has 6,000 milliseconds, as shown in Figure 14. After applying the network security filter, it is confirmed that the time required for the M2M intelligent network device (a) is 1,000 milliseconds and (b) is 3,000 milliseconds.

Experimental results show that the response speed is improved due to the abnormal traffic control in the network environment used by the Internet devices after applying the network security filter. The

comparison of the delay time when the security filter is applied when there is no abnormal traffic is shown in Table 4.

Table 4. Device response time when security filter is applied in normal state.

	Experiment (a) Air Cleaner	Experiment (b) 220v Plugin
Security filter not used	0.800 millisecond	2,000 millisecond
Applying Security Filters	0.900 millisecond	2,200 millisecond

When the usual security filter is applied, response delay time of about 10% occurs, which shows improvement of response speed of about 50% or more by application of security filter in case of abnormal packet generation as shown in Table 5.

Table 5. Device response time when security filter is applied after abnormal packet input.

	Experiment (a) Air Cleaner	Experiment (b) 220v Plugin
Security filter not used	4,000~4,500 millisecond	6,000 millisecond
Applying Security Filters	1,000~1,500 millisecond	3,000 millisecond

By controlling abnormal packets, the security and response of M2M intelligent network devices can be improved and the third victim of DDoS can also be prevented. In addition to M2M intelligent network devices used for the study, it is necessary to verify the packet specificity of more devices and to have more accurate policy tuning methods.

5 Conclusion

In this paper, we proposed a security filter that improves the security and response speed of M2M intelligent network devices through abnormal traffic control in M2M intelligent network environment. Based on this, we confirmed the possibility of securing the availability and security of the network used by M2M intelligent network devices by simulating the network packet simulator Ostinato in M2M intelligent network environment.

Security in the M2M intelligent network environment is based on the study of security enhancement of the device itself. However, due to environmental factors such as 'low capacity hardware, installation of security program such as vaccine, OS patch problem' characteristic of M2M intelligent network device, it is difficult to strengthen the security. The security filter proposed in this study can improve the security of the device and the network efficiency by controlling the abnormal traffic generated in the M2M intelligent network environment, we confirmed that it is possible to prevent third DDoS attack damage due to M2M intelligent network device.

The experiment results show that depending on the characteristics of the device, when the proposed security filter is applied, delay incurs less than 10% and the response speed of the device improves more than 50% when abnormal traffic occurs. The latency that occurs when applying the security filter is a value that the general user does not feel, but it is necessary to compensate for the improvement of the delay time through tuning of the system and the operating system in which the security filter is installed. Actually, M2M intelligent network environment may be difficult to construct a security filter on the same server as the experimental environment of this work. The application of the security filter in this work to a small Linux device such as Raspberry, can be

applied to various locations and environments, when the proposed method is applied to the network. When the proposed method is applied to the network, among the three security factors 'Confidentiality, Integrity, and Availability', it is expected that the availability due to the security filter can be increased.

Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (Ministry of Science and ICT) (No. NRF-2017R1A2B2010588).

References

[1] Fadlullah. ZM, Fouda. MM, Kato. N, Takeuchi. A, Iwasaki. N, Nozaki. Y, "Toward intelligent machine-to-machine communications in smart grid", *IEEE Comm. Mag.*, 2011; 49 (4):60-65.
[2] Chen. M, "Towards smart city: M2M communications with software agent intelligence", *Multimed Tools Appl.*, 2013; 67 (14):167-178.
[3] Atzori. L, Iera. A, Morabito. G, "Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm", *Ad Hoc Net.*, 2017; 56 (1):122-140.
[4] Jow. J, Xiao. Y, Han. W, "A survey of intrusion detection systems in smart grid", *IJSNet.*, 2017; 23 (3):170-186.
[5] Friess. P, Internet of Things-Global Technological and Societal Trends from Smart Environments and Spaces to Green ICT, Vermesan. O, Friess. P, River Publishers: Aalborg, Denmark, 2011.
[6] Porter. ME, Heppelmann. JE, "How smart, connected products are transforming competition", Harv Bus Rev, 2014; 92 (11):64-88.
[7] Ansari. MH, Vakili. VT, "Detection of clone node attack in mobile wireless sensor network with optimised cost function", *IJSNet*, 2017;24 (3):149-159.
[8] Eom. YH, Cho. S, Kim. RYC, Jeon. B, "Design and Implementation of a Speed-reactive Connected Mobile Virtual Fence System with Context-aware Computing", Journal of Engineering Technology, 2018, 7(Special Issue, Oct): 307-321.
[9] Atzori. L, Iera. A, Morabito. G, "Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm", Ad Hoc Net., 2017; 56 (1):122-140.
[10] Sujatha. R, VijayaRagavan. N, Suganya. KS, "IOT: To enhance automatic accident notification using M2M technologies", IJSER, 2015; 6 (3): 1-4.
[11] Byun. EY, Son. HS, Jeon. B, Kim. RYC, "Reusability Strategy Based on Dynamic Reusability Object Oriented Metrics", Journal of Engineering Technology, 2018;6(1):365-377.
[12] Bandyopadhyay. D, Sen. J, "Internet of things: Applications and challenges in technology and standardization", Wirel Pers Commun, 2011; 58 (1): 49-69.
[13] Cho. S, Yi. JH, Shrestha. B, Seo. C, "Multipath routing technique for responding to sniffing attacks in wireless multimedia sensor network environment", IJSNet., 2017;24 (3):200-207.
[14] Jin. J, Gubbi. J, Marusic. S, Palaniswami. M, "An information framework for creating a smart city through internet of things", IEEE Internet Things J., 2014;1 (2):112-121.
[15] Porter. ME, Heppelmann. JE. "How smart, connected products are transforming competition", Harv Bus Rev., 2014; 92 (11):64-88.
[16] Wang. Y, Shi. H, Cui. L, "EasiSec: a SoC security coprocessor based on fingerprint–based key management for WSN", International Journal of Sensor Networks, IJSNet., 2013;13 (2):85-93.

[17] Sadeghi. AR, Wachsmann. C, Waidner. M, "Security and privacy challenges in industrial internet of things", Proceedings of the 52nd ACM/EDAC/IEEE DAC, California, USA, June. 8-12, 2015; 1-6.

[18] Appari. A, Johnson. ME, "Information security and privacy in healthcare: current state of research", IJIEM, 2010;6 (4):279-314.

[19] Porter. ME, Heppelmann. JE, "How smart, connected products are transforming competition", Harv Bus Rev, 2014;92 (11): 64-88.

[20] Loukas. G, "Cyber-physical attacks: A growing invisible threat", Stover T. River Publishers: MA, USA, 2015.

[21] SHODAN the computer search engine, Available online: URL https://www.shodan.io/ (accessed on 01-11-2018)

[22] Cyber search engine Shodan exposes industrial control systems to new risks, Available online: URL https:// www. washingtonpost.com/investigations/cyber-search-engine-exposes-vulnerabilities/ 2012/06/03/gJQAIK9KC V_story.html (accessed on 03-11-2018)

[23] Genge. B, Enăchescu. C, "ShoVAT: Shodan- based vulnerability assessment tool for Internet- facing services", Secur Commun Netw., 2016;9 (15): 2696-2714.

[24] Bodenheim. RC, :Impact of the Shodan computer search engine on internet-facing industrial control system devices", MS. Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, March, 2014.

[25] Bodenheim. R, Butts. J, Dunlap. S, Mullins. B, "Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices", IJCIP, 2014;7 (2):114-123.

[26] Ball. T, Zorn. B, "Teach foundational language principles", Commun. of the ACM, 2015; 58 (5):30-31.

[27] Wang. J, Zhao. M, Zeng. Q, Wu. D, Liu. P, "Risk assessment of buffer "Heartbleed" over-read vulnerabilities", Proceedings of the 45th Annual IEEE/IFIP International Conference on DSN, Rio de Janeiro, Brazil, June 22-25, 2015; 555-562.

[28] U.S. Department of Homeland Security, Analysis of Shodan Computer Search Engine, Technical Report CSAR-10-025-01, Washington, DC, 2010.

[29] Shodan: The Scariest Search Engine on the Internet, Available online: URL https://money. cnn.com/2013/04/08/ technology/security/shodan/index.html (accessed on 10-11-2018).

[30] The Open Web Application Security Project, Available online: URL https://www.owasp.org (accessed on 12-10-2018).

[31] Hongsong. C, Zhongchuan. F, Dongyan. Z, "Security and trust research in M2M system", Proceedings of the IEEE International Conference on ICVES, Beijing, China, Jul. 10-12, 2011; 286-290.

[32] Markowsky. L, Markowsky. G, "Scanning for vulnerable devices in the Internet of Things", Proceedings of the 8th International Conference on IEEE, IDAACS, Warsaw, Poland, September 24-26, 2015; 463-467.

[33] February 28th DDoS Incident Report, Available online: URL https://githubengineering.com/ ddos-incident-report (accessed on 12-6-2018).

[34] Kührer. M, Hupperich. T, Rossow. C, Holz. T. "Exit from Hell? Reducing the Impact of Amplification DDoS Attacks", Proceedings of the 23rd USENIX Security Symposium, CA, USA, Aug. 11-13, 2014; 111-125.

[35] Ali. A, Shah. GA, Farooq. MO, Ghani. U, "Technologies and challenges in developing machine-to-machine applications: A survey", J Netw Comput Appl, 2017;83 (1):124-139.

[36] Network Traffic Generator and Analyzer, Available online: URL https://ostinato.org (accessed on 12-5-2018).