applied sciences

MDPI

Article

A Study on Improving M2M Network Security through Abnormal Traffic Control

Seongsoo Cho [1] and Bhanu Shrestha [2,*]

[1] School of Computer Science and Engineering, Soongsil University, Seoul 07027, Korea
[2] Department of Electronics Engineering, Kwangwoon University, Seoul 01897, Korea
* Correspondence: bnu@kwa.ac.kr; Tel.: +82-2-940-8626

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

Keywords: M2M; IoT security; DDoS; network filters

check for updates

Citation: Cho, S.; Shrestha, B. A Study on Improving M2M Network Security through Abnormal Traffic Control. *Appl. Sci.* **2022**, *12*, 10836. https://doi.org/10.3390/app122110836

Academic Editors: Eui-Nam Huh and Dimitris Mourtzis

Received: 19 August 2022
Accepted: 22 October 2022
Published: 26 October 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The future of the internet is evolving through the convergence with existing infrastructure and the Internet of Things (IoTs), such as a sensor, while simultaneously accommodating the communication speed and the increase of various access terminals to meet the rapidly increasing demands of users. In addition, this is the era of the 4th Industrial Revolution which 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 the Internet of Things (IoT) [1–4]. The machine-to-machine (M2M) intelligent network is emerging as an ICT infrastructure for future telecommunication convergence enabling intelligent communication services between people, and this 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 from a remote object through a combination of communication and ICT technology [5–8].

The M2M intelligent network is intangible, and enables existing specific technologies to be seen through the internet when things are used in the form of objects, and services. As compared to laptops and mobile devices connected to the internet, which is determined by the number of individual users, M2M intelligent networks can solve social issues, prevent disasters through u-City, u-Health, u-Saving, CO2 reduction, and so on. It is an intelligent environment where users and smart home appliance and devices transmit and receive information and data in real time through converging ICT. The M2M intelligent network is the idea of applying IT to very important problems, unlike the existing internet, such as disaster prevention. Most people prefer wireless rather than wired, and M2M intelligent networks are mostly for wireless use as well. In order to solve this problem, M2M intelligent networks need the procedures to acquire empirical data about the M2M intelligent network's information security, security field, and data reliability [3,9,10]. In the

case of the IoT, we can also use the heuristic recommendation technique exploiting swarm intelligence and in the same environment, a distributed clustering algorithm that builds an information system as well [10,11].

Security is a core technology that must be provided for intelligent network generalization and new service creation. The increase in the number of devices connected to the network means an increase in the 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 facilities. 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 concerns 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].

Presently, in the DRDoS attack method using Network Time Protocol (NTP), an IoT device that receives information about the time makes a request to the server, and the server calculates the time. When an attack is made by altering the IP requested by the NTP server to a DRDoS victim, the victim will receive a response at an unsolicited time. NTP uses port 123 at both ends of the client and server, and it is possible to use NTP servers such as numerous Zombie PCs and IoT devices to deplete the victim's network bandwidth during a DRDoS attack. Because the victim simply sends packets from the NTP server, an attacker may mistake it for an NTP server on the surface.

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

The entire paper is organized with introduction, background of the M2M network, implementation of the security filter and the conclusion.

2. M2M Intelligent Network Background

The M2M intelligent network environment is shown in Figure 1, which evolved into a concept that interacts with all the data in the real and virtual world by being applied to a network structure beyond wireless communication [14,15]. The 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 including objects and services. In the era of the M2M intelligent network, the privacy issue caused by data exchange of various devices, as well as the vulnerability in numerous industries such as automobiles and medical care, may threaten life [6,16].

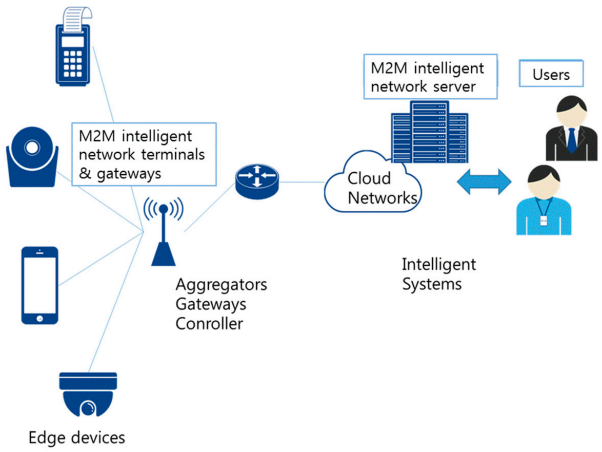


Figure 1. Configuration of the M2M intelligent network environment.

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 wide range of attacks targeting all industries and areas of life will increase the chances of malicious hackers pursuing a wide range of targets, from manufacturing to power grids, automobiles, medical devices, and home appliances. There may be a situation in which personal medical information is leaked by a hacker, and national infrastructures, such as networks, power systems and traffic signals, could be brought to a complete stop, or rendered uncontrollable [6,17,18].

In 2009, computer programmer John Matherly launched Shodan, a computer search engine with a graphical user interface that identifies internet-facing devices [19]. In particular, the emergence of a Shodan site that can detect M2M intelligent networks to locate its connection to the network increases the security threats [6,20–22]. As shown in Table 1, Shodan has detected the connected devices and collected the data more than 40 networks, such as servers, web cams, IP CCTV, network printers, and routers [19,22,23].

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		

Shodan retrieves OpenSSL patch version information from M2M intelligent networks and through the heartbleed of this version, it is confirmed that the system is defenseless from information stealing/attacking and service denying/attacking etc. [24–26]. The ability to identify devices that monitor and control critical infrastructure assets has raised major security concerns. A CNN article [27] claims that Shodan is "the scariest search engine on the internet". 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 [28].

A type of network attack that can occur in the M2M intelligent network environment is a Distributed Reflection Denial of Service (DRDoS) attack, which is more advanced than the DDoS attack [29,30]. GitHub.com posted an official engineering blog post on 1 March 2018, explaining the background of a DDoS attack that occurred on February 28th. In a report dated 1 January, the US ZDNet reported that a massive 1.1Tbps of DDoS attacks on GitHub.com targeting one of the world's largest service providers [31–35]. According to GitHub, a large DDoS attack occurred with over a thousand automated systems, including tens of thousands of unique endpoints.

The size of DDoS attacks is expected to grow further. In the case of M2M intelligent networks, it is difficult to cope with device security patches, which are not smooth, and it is hard to know if a device is infected.

Here, malicious code variants continue to make it more difficult to respond. Distributed Reflector Denial of Service (DRDoS) uses the vulnerability of Simple Service Discovery Protocol (SSDP), and is a highly likely form of attack in M2M intelligent network environments as shown in Figure 2.

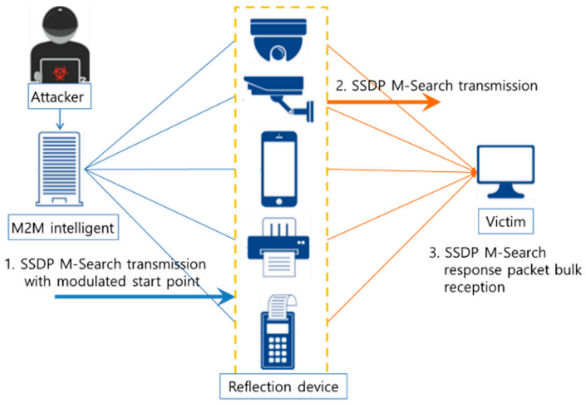


Figure 2. DRDoS attack using M2M intelligent network.

3. Implementation of 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 [33]. 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 a "filter to control the allow/block, IP Network Address Translation (NAT) and NAT to control routing, and RAW, which controls connection tracking for sessions and manages the modification and marking of communication packets". The role of the table and the function of the chain are the same as shown in Table 2.

Table 2. Iptables table and chain based on Linux.

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

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 which is a part of Linux network stack, specifically part of the firewall subsystem.

When a new kind of packet arrives, it generates a conntrack and finally records whether the packet is allowed/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 an 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. If you want to create a session with an unauthorized access during the network communication process, it is helpful 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 3, TCP prepares flags according to the situation.

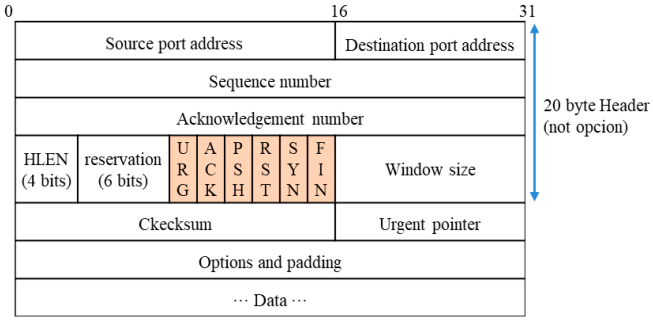
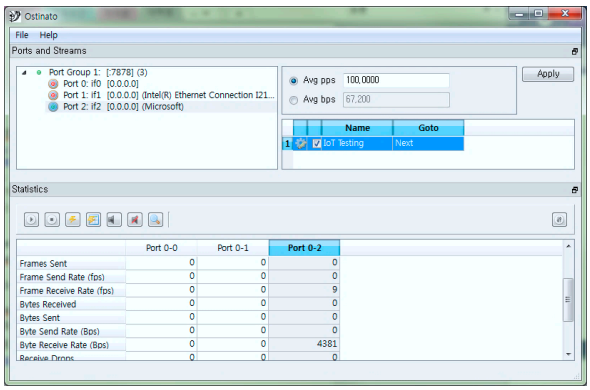


Figure 3. TCP header and control flag structure.

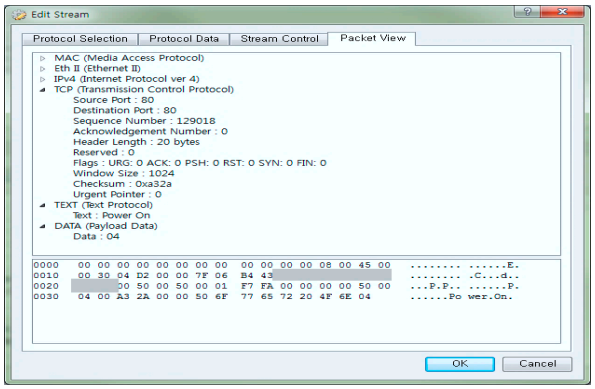
4. Experiment Results

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 purposes 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 [33]. In addition, simulation of DoS and DDoS attacks that can occur in the M2M intelligent network environment is possible by defining packet transmission.

In order to verify the improved security filter, data packets are generated by Ostinato environment settings as shown in Figure 4, assuming an abnormal packet triggering state of an 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 4. Ostinato settings environment (**a**) set up packet transmission and, (**b**) generate packets.

The Iptables environment for implementing the security filter is built into 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 5, 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
```

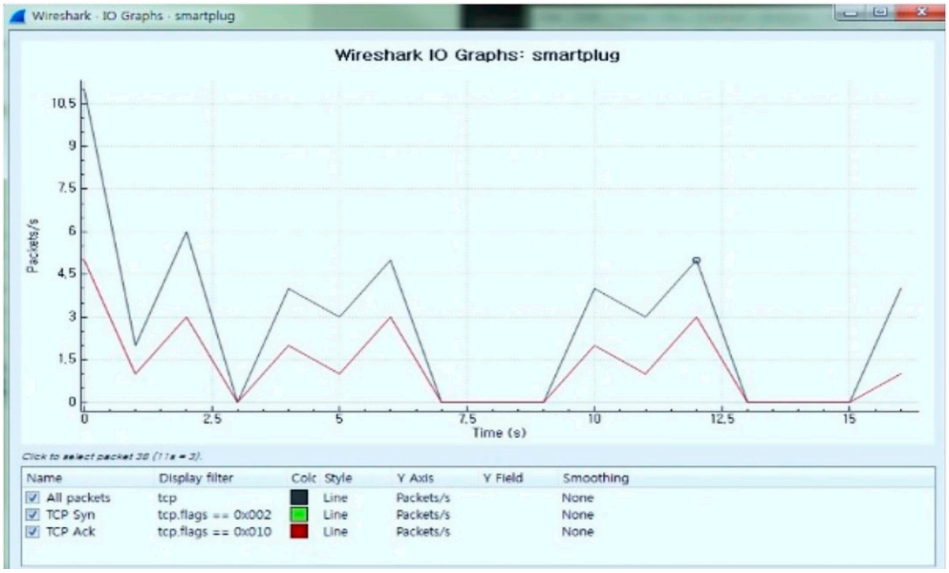
Figure 5. Iptables in internet environment.

The security filter implementation is shown in Figure 5, which is explained 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, when it is confirmed that the ICMP packet is not used, block all ICMP that can be used for attacks such as DDoS and DoS. Finally, the most important security filter setting in the actual M2M intelligent network environment applies the thresholds shown in the actual filters to the M2M intelligent network devices 'TCP Syn 5/s, TCP Ack 25/s, UDP 5/s'. The threshold level is also used to confirm that there is no communication problem in the applied setting. Experiments were conducted in an M2M intelligent network environment and abnormal traffic was generated using Ostinato. We compared the device response in terms of speed and network stability before and after applying the filter. First, it was confirmed whether the use of each M2M intelligent network device was normal when the network security was applied. Second, in the case of an M2M intelligent network device DDoS attack, we verified the resource status of the damage system before and after security filter implementation in case of DDoS attack to an external system. Finally, in the case of M2M intelligent network equipment, an M2M intelligent network device was used 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 setting for normal service or the threshold value, and this is shown in Figure 6. The black line indicates total traffic, red indicates TCP Ack traffic, and green indicates TCP Syn traffic. Figure 6a shows the M2M intelligent network device air cleaner filter operation function time was 0.800/0.900 milliseconds, and Figure 6b shows the M2M intelligent network device 220v plugin which was 2000/2200 milliseconds. In a general application environment, it was difficult to sense these numerical results. Next, we tested a scenario where a DDoS attack was performed from outside on a M2M intelligent network device. In the case of DDoS attack to the external system, the resource status of the damage system before and after the security filter was verified. Using Ostinato, the TCP Syn packet was maintained at 100 pps for about 5 s as shown in Figure 7. 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 6. Experiments on M2M intelligent network device packet and operation (**a**) Air Cleaner, (**b**) 220v Plugin.

Finally, we measured the response speed of M2M intelligent network devices before and after the network security filter was applied by sending packets from the external network to the M2M intelligent network device. Similar results to the communication session of the M2M intelligent network device were found. When testing 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 s at 100 pps. The orange line in Figure 8 shows the Syn and Rst Flag generated that stops after 10 s.

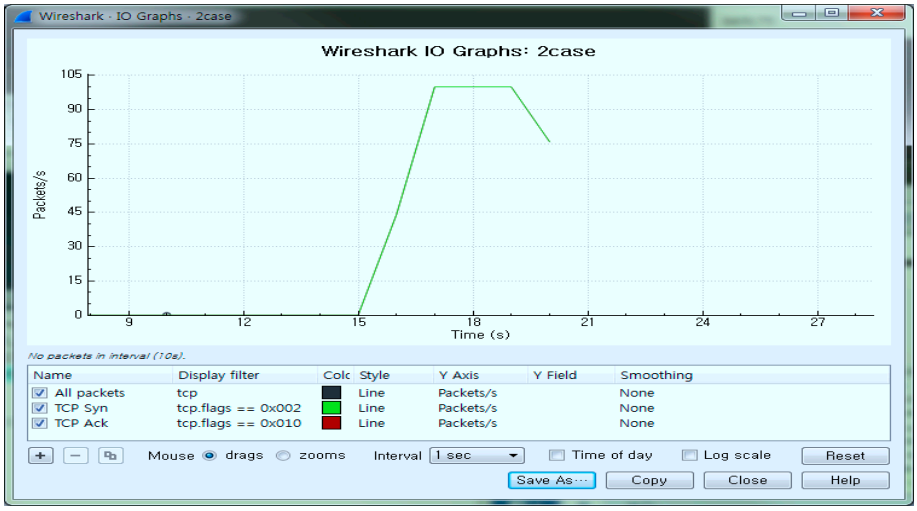


Figure 7. Packet with modulated source from M2M intelligent network device.

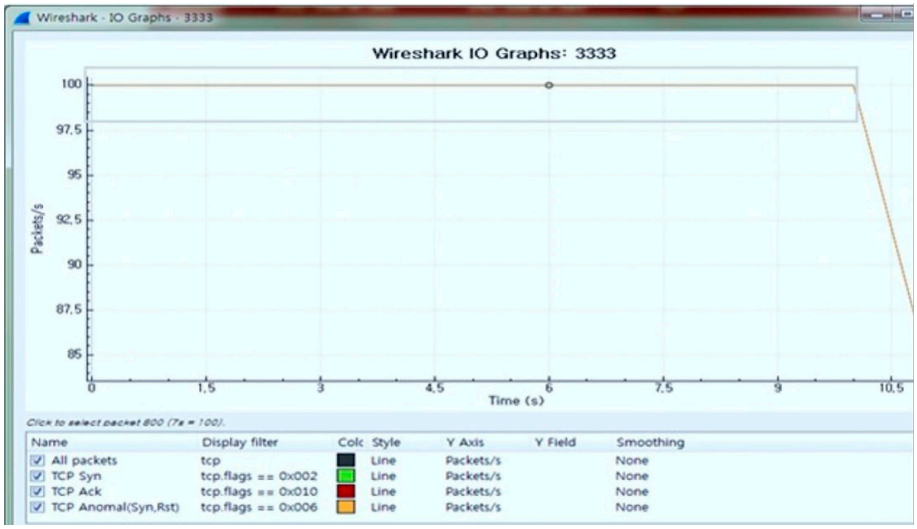


Figure 8. Packet transmission that does not match TCP Flag combination.

In the experimental results of the packet sent to the M2M intelligent network devices (a) and (b), when the network security filter was not applied, the response time was (a) 4000 milliseconds and (b) 6000 milliseconds, as shown in Figure 8. After applying the network security filter, it was confirmed that the time required for the M2M intelligent network device (a) was 1000 milliseconds and (b) was 3000 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 3. When the usual security filter is applied, a response delay time of about 10% occurs, which shows an improvement in the response speed of about 50% or more compared with the application of the security filter in the case of abnormal packet generation as shown in Table 4. 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.

Table 3. 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	2000 millisecond
Applying Security Filters	0.900 millisecond	2200 millisecond

Table 4. Device response time when security filter is applied after abnormal packet input.

	Experiment (a) Air Cleaner	Experiment (b) 220v Plugin
Security filter not used	4000~4500 millisecond	6000 millisecond
Applying Security Filters	1000~1500 millisecond	3000 millisecond

5. Conclusions

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 the M2M intelligent network environment. 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 the intelligent network environment. Security in the M2M intelligent network environment is based on the study of the security enhancement of the device itself. However, due to environmental factors (such as low-capacity hardware) and the installation of security programs (such as antivirus, or OS patches, which can cause problems characteristic of M2M intelligent network devices), it is difficult to strengthen the network 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 the damage of third-party DDoS attack damage due to an M2M intelligent network device.

Experimental results show that the delay of less than 10% depends on the characteristics of the device when the security filter is applied, and that the response speed of the device improves by 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 increase in the delay time through the tuning of the system and the operating system in which the security filter is installed. M2M intelligent network environments may find it 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 with a small Linux device (such as Raspberry), can be applied to various locations and environments. Among the three security factors, 'confidentiality, integrity, and availability', the 'availability' can be increased when we utilize the proposed security filters.

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 in the future.

Author Contributions: Conceptualization, S.C.; methodology, S.C. and B.S.; software, S.C.; validation, S.C. and B.S.; formal analysis, S.C. and B.S.; investigation, S.C.; resources, S.C.; data curation, S.C.; writing—original draft preparation, S.C.; writing—review and editing, B.S.; visualization, S.C.; supervision, B.S.; project administration, S.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Acknowledgments: This research was supported by the Mid-Career Researcher program through the National Research Foundation of Korea (NRF) funded by the MSIT (Ministry of Science and ICT) under Grant 2020R1A2C2014336.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Fadlullah, Z.M.; Fouda, M.M.; Kato, N.; Takeuchi, A.; Iwasaki, N.; Nozaki, Y. Toward intelligent machine-to-machine communications in smart grid. *IEEE Comm. Mag.* **2011**, *49*, 60–65. [CrossRef]
2. Chen, M. Towards smart city: M2M communications with software agent intelligence. *Multimed. Tools Appl.* **2013**, *67*, 167–178. [CrossRef]
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*, 122–140. [CrossRef]
4. Jow, J.; Xiao, Y.; Han, W. A survey of intrusion detection systems in smart grid. *Int. J. Sens. Netw.* **2017**, *23*, 170–186. [CrossRef]
5. Elhattab, K.; Abouelmehdi, K.; Elmoutaouakkil, A. Internet of Things (IoT) for Smart City, Agriculture and Healthcare. *J. Theory Appl. Inform. Technol* **2022**, *100*, 4.
6. Porter, M.E.; Heppelmann, J.E. How smart, connected products are transforming competition. *Harv. Bus. Rev.* **2014**, *92*, 64–88.
7. Ansar, M.H.; Vakili, V.T. Detection of clone node attack in mobile wireless sensor network with optimised cost function. *Int. J. Sens. Netw.* **2017**, *24*, 149–159. [CrossRef]
8. Eom, Y.H.; Cho, S.; Kim, R.Y.C.; Jeon, B. Design and Implementation of a Speed-reactive Connected Mobile Virtual Fence System with Context-aware Computing. *J. Eng. Technol.* **2018**, *7*, 307–321.
9. Sujatha, R.; VijayaRagavan, N.; Suganya, K.S. IOT: To enhance automatic accident notification using M2M technologies. *Int. J. Sens. Netw.* **2015**, *6*, 1–4.
10. Byun, E.Y.; Son, H.S.; Jeon, B.; Kim, R.Y.C. Reusability Strategy Based on Dynamic Reusability Object Oriented Metrics. *J. Eng. Technol.* **2018**, *6*, 365–377.
11. Forestiero, A. Heuristic recommendation technique in Internet of Things featuring swarm intelligence approach. *Expert Syst. Appl.* **2022**, *187*, 115904. [CrossRef]
12. Forestiero, A.; Giuseppe, P. Agents-based algorithm for a distributed information system in Internet of Things. *IEEE Internet Things J.* **2021**, *8*, 16548–16558. [CrossRef]
13. Bandyopadhyay, D.; Sen, J. Internet of things: Applications and challenges in technology and standardization. *Wirel Pers Commun.* **2011**, *58*, 49–69. [CrossRef]
14. Cho, S.; Yi, J.H.; Shrestha, B.; Seo, C. Multipath routing technique for responding to sniffing attacks in wireless multimedia sensor network environment. *Int. J. Sens. Netw.* **2017**, *24*, 200–207. [CrossRef]
15. 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*, 112–121. [CrossRef]
16. Wang, Y.; Shi, H.; Cui, L. EasiSec: A SoC security coprocessor based on fingerprint–based key management for WSN. *Int. J. Sens. Netw.* **2013**, *13*, 85–93. [CrossRef]
17. Sadeghi, A.R.; Wachsmann, C.; Waidner, M. Security and privacy challenges in industrial internet of things. In Proceedings of the 52nd ACM/EDAC/IEEE DAC, California, CA, USA, 8–12 June 2015; pp. 1–6.
18. Appari, A.; Johnson, M.E. Information security and privacy in healthcare: Current state of research. *Int. J. Internet Enterp. Manag.* **2010**, *6*, 279–314. [CrossRef]
19. Wu, S.; Jiang, Y.; Luo, H.; Zhang, J.; Yin, S.; Kaynak, O. An integrated data-driven scheme for the defense of typical cyber–physical attacks. *Reliab. Eng. Syst. Saf.* **2022**, *220*, 108257. [CrossRef]
20. SHODAN the Computer Search Engine. Available online: https://www.shodan.io/ (accessed on 10 August 2022).
21. Cyber Search Engine Shodan Exposes Industrial Control Systems to New Risks. Available online: https://www.washingtonpost.com/investigations/cyber-search-engine-exposes-vulnerabili-ties/2012/06/03/gJQAIK9KCV_story.html (accessed on 10 August 2022).
22. Genge, B.; Enăchescu, C. ShoVAT: Shodan-based vulnerability assessment tool for Internet-facing services. *Secur. Commun. Netw.* **2016**, *9*, 2696–2714. [CrossRef]
23. Furrer, F.J. Cyber-Physical Systems. In *Safety and Security of Cyber-Physical Systems*; Springer Vieweg: Wiesbaden, Germany, 2022; pp. 9–76.
24. Bodenheim, R.; Butts, J.; Dunlap, S.; Mullins, B. Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices. *Int. J. Crit. Infrastruct. Prot.* **2014**, *7*, 114–123. [CrossRef]
25. Ball, T.; Zorn, B. Teach foundational language principles. *Commun. ACM* **2015**, *58*, 30–31. [CrossRef]
26. Wang, J.; Zhao, M.; Zeng, Q.; Wu, D.; Liu, P. Risk assessment of buffer "Heartbleed" over-read vulnerabilities. In Proceedings of the 45th Annual IEEE/IFIP International Conference on DSN, Rio de Janeiro, Brazil, 22–25 June 2015; pp. 555–562.
27. Tundis, A.; Modo Nga, E.M.; Mühlhäuser, M. An exploratory analysis on the impact of Shodan scanning tool on the network attacks. In Proceedings of the 16th International Conference on Availability, Reliability and Security, Vienna, Austria, 17–20 August 2021; pp. 1–10.
28. Shodan: The Scariest Search Engine on the Internet. Available online: https://money.cnn.com/2013/04/08/technology/security/shodan/index.html (accessed on 10 August 2022).
29. The Open Web Application Security Project. Available online: https://www.owasp.org (accessed on 10 August 2022).
30. Hongsong, C.; Zhongchuan, F.; Dongyan, Z. Security and trust research in M2M system. In Proceedings of the IEEE International Conference on ICVES, Beijing, China, 10–12 July 2011; pp. 286–290.

31. Markowsky, L.; Markowsky, G. Scanning for vulnerable devices in the Internet of Things. In Proceedings of the 8th International Conference on IEEE, IDAACS, Warsaw, Poland, 24–26 September 2015; pp. 463–467.
32. February 28th DDoS Incident Report. Available online: https://githubengineering.com/ddos-incident-report (accessed on 10 August 2022).
33. Kührer, M.; Hupperich, T.; Rossow, C.; Holz, T. Exit from Hell? Reducing the Impact of Amplification DDoS Attacks. In Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, 11–13 August 2014; pp. 111–125.
34. Ali, A.; Shah, G.A.; Farooq, M.O.; Ghani, U. Technologies and challenges in developing machine-to-machine applications: A survey. *J. Netw. Comput. Appl.* **2017**, *83*, 124–139. [CrossRef]
35. Network Traffic Generator and Analyzer. Available online: https://ostinato.org (accessed on 10 August 2022).