DDoS Attack, a Threat to IoT Devices in the High-Speed Networks—An Overview

Pravir Chitre and Srinivasan Sriramulu

1 Introduction

Communication technology and the speed of communication over the network have been growing ever since communication technology and Internet have been invented. With the increasing speed and developments in the communication technology, new and new means of automation are being invented/developed. Among the latest development is the Internet of things, which is becoming more popular with the advancements in the network communication technology. The quest for more and more speed has given rise to the Wi-Fi-6, 5G mobile network, and high speed communication technology. World is now going for smart cities with the advent of this new technology i.e. Internet of things. The smart cities are bringing in the mission-critical applications as a part of automation that is using high-speed communication technologies in implementation of Automation Techniques as a part of smart city projects.

The next generation technologies are simplifying up-gradation and management of the high-speed network devices by implementing the new concept like software defined network (SDN), which in turn is providing additional techniques like network function virtualization (NFV) and network slicing (NS). Though these are some of the powerful features, the misuse of these features has also been designed by the miscreants.

The security threat to the SDN controller has been long identified, and the problem of securing the SDN controller is already being addressed. But with the use of Smart devices which are being developed with the inbuilt support of IoT technology, the

P. Chitre (✉) · S. Sriramulu
Galgotias University, Greater Noida, UP, India
e-mail: pravir.chitre_phd19@galgotiasuniversity.edu.in

S. Sriramulu
e-mail: s.srinivasan@galgotiasuniversity.edu.in

P. Chitre
Bhai Parmanand DSEU Shakarpur Campus II, Galgotias University, Delhi, India

J. K. Mandal et al. (eds.), *Proceedings of International Conference on Network Security and Blockchain Technology*, Lecture Notes in Networks and Systems 738,
https://doi.org/10.1007/978-981-99-4433-0_18

networks and SDN controllers are now facing new security threats. One of the major security threats has been identified in which the IoT devices are used to initiate the IoT-DDoS attack by the attackers without the knowledge of IoT device users by turning the IoT device as zombie or reflector. This is specially evident since the network servers faced DDoS attack where the innocent IoT end devices were used to initiate the DDoS attack using the Mirai Botnet [20]. In this paper, security threat due to poorly configured end point IoT devices is discussed. Also the measures that may help mitigate such security threats have been discussed.

2 Background

The high speed in the network communications is being achieved using the 5G mobile technology and the sixth generation Wi-Fi technology, as these are the vehicles in terms of achieving high speed in network communication. The 5G, or fifth generation, mobile phone system, and the sixth generation Wi-Fi, or Wi-Fi-6, which is also known as the IEEE 802.11ax standard, will coexist as these are complementary technologies. The 5G mobile technology is also enabling higher density and capacity for network devices. With the implementation of Wi-Fi-6, the data communication rates are increasing as Wi-Fi-6 offers Wi-Fi connectivity with the devices at much higher data transfer rate. This is also adding up to the increased data consumption [19]. While 5G is the preferred option for the outdoor network, Wi-Fi-6 is still the preferred indoor access network. With 5G and Wi-Fi-6 in place, data communication is advancing in terms of speed, latency, and device density [2, 7]. The next generation hardware is using the new technologies like:

- ***Software Defined Network (SDN)***: Software defined networking (SDN) is a networking architecture that makes networks more flexible and manageable. SDN centralizes management by decoupling the control plane from the data forwarding task in discrete networking devices. SDN uses software-based controllers or application programming interfaces (APIs) to direct traffic on a network in order to communicate with the underlying hardware infrastructure. The network control plane is physically separated from the forwarding plane, and a control plane is capable of controlling several devices [4].
- ***Network Function Virtualization (NFV)***: Network function virtualization (NFV) is a technology where the physical hardware devices like switches, routers, firewalls, load balancers, and others are replaced with software-based virtual devices which are highly scalable and are implemented using the technologies like virtual machines, thus forming a virtual network [5]. By implementing software solutions, NFV increases scalability and agility by allowing service providers to instantly deploy new network services and applications without the need for additional hardware resources [3].
- ***Network Slicing (NS)***: Network slicing is the process of dividing a single network connection into many virtual connections that deliver various amounts of resources

to different types of traffic using network virtualization. The network slice is a logically segregated, self-contained, independent, and secure portion of the network that targets distinct services with varying speed, latency, and reliability needs [6].

High-speed networks are being deployed using technologies like SDN, NFV for a variety of applications that will support the next generation smart city. As smart cities are growing, new technology like IoT is being used to automate the mission-critical and high risk applications. Together with activities that require quick responses, such as self-driving cars, automation is being used in applications like numerous crucial services including distribution of water and electrical supplies and traffic control, and others [1, 24]. The IoT devices are entering the households with the use of smart and IoT-enabled devices.

This implementation of applications that are mission-critical and response-sensitive is producing new security issues, and these challenges are driving the need for a higher level of security protection. For instance: If a smart city that makes use of 5G services for essential services like supplying the city with electricity or water and has a security system flaw due to which a hacker succeeds in getting the access of control of these essential services, then they might be able to tamper the services or even shut down these services, which could have devastating effects on the smart city [1, 24].

Major Security Threats

In the era of 5G and high-speed networks when the new concepts like, i.e., Internet of things (IoT) are gaining popularity and the new projects like smart city and implementation of mission-critical applications are being executed, the security threats on the next generation network are getting higher and higher. This is because with IoT and smart city like applications, lots of small devices are getting installed for controlling various gadgets and appliances. These devices are designed for low battery consumption and are being implemented with SDN-based application. Due to their small size and low-power consumption, these devices' designs provide new vulnerabilities and can be readily compromised by hackers who then use them as weapons to launch various forms of attacks on mission-critical applications and other targets. The most popular of the attacks/vulnerability is denial of service and/or distributed denial of service attack. As per "DDoS Attack Statistics, Facts and Figures For 2022" from Web portal PixelPrivacy [8–10], DDoS attack is one of the most popular online weapon that is used by the hackers. As mentioned in Web portal pixelprivacy, "Cisco estimates that the total number of distributed denial of service attacks will double from the 7.9 million attacks experienced in 2018 to 15.4 million attacks in 2022" [8]. This security threat has already been experienced by the world with the DDoS attack on the Security Blog of Brian Krebs on September 20, 2016 [20, 26] which was initiated by weaponizing the CCTV cameras and other IoT devices. More such attacks are being faced by the world.

Denial of Service (DoS) and Distributed Denial of Service (DDoS)

DoS attacks have the potential to deplete an opponent's network resources. DoS is a type of security attack that reduces a network's availability. A DoS attack can be

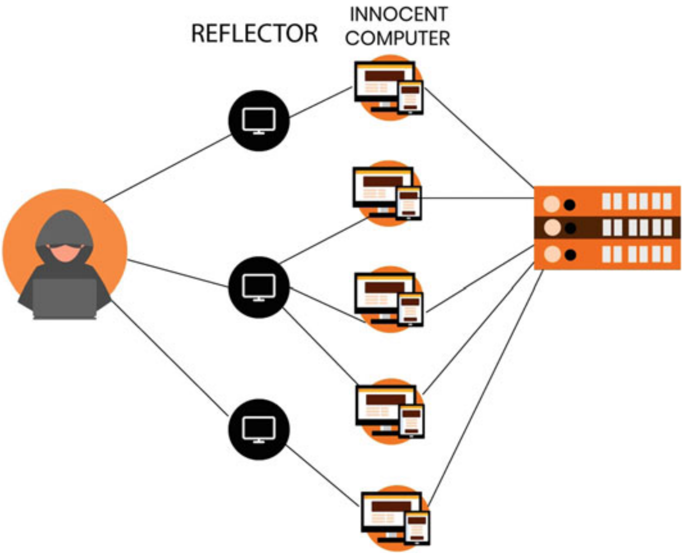

Fig. 1 Attacker is using innocent machines to perform a DDoS assault on the victim system [11]

launched using jamming or flooding so that the target is overloaded with requests and the service's or resource's usage is severely compromised. It is possible to identify and mitigate the attack when there is a single attacker which is DoS attack. But when the similar type of attack is carried out using multiple resources, then the attack is called as DDoS attack. In such an attack it is difficult to identify the attacker and to mitigate the attack. In case of DDoS attack, attacker rather than directly attacking, identifies and uses the weak devices to launch the attack. Attacker uses the remote handlers like Botnets, reflectors and controls the devices remotely to initiate and manage the attack on the target system/device/network/resource. A DDoS model is shown in Fig. 1.

The prevention of DoS or DDoS attacks is not possible. The only solution is to identify and detect these attacks. If these attacks can be detected, then these attacks may be stopped or prevented. The best defense toward the DDoS attack is to detect the attack, as soon as possible and to mitigate it. Sooner the attack can be detected, earlier it can be mitigated and lesser the damage due to the attack.

DoS and DDoS attacks have recently become a serious concern to many Websites and could pose a big threat to operators as the deployment of large number of devices in 5G wireless networks has been increasing. These connected devices are normally designed to be smaller in size, and to manage with the smaller size, these devices may be designed to be either less secured or with the advent of SDN, devices and are secured and controlled by the SDN controller. Attacker can gain control of the SDN controller, thereby gaining the control and access to the controlled devices. The attacker can use these devices to launch the attack and hides itself, behind these smaller devices. A DoS/DDoS assault can be categorized as either a device/user

DoS/DDoS attack or a network infrastructure DoS attack, depending on the attacker's target. DoS attacks can target the battery, memory, disc, CPU, radio, actuators, and sensors in devices [1, 24].

DDoS attacks are, according to Norton, "*one of the most powerful weapons on the internet*". Denial of service attacks can strike at any time, affecting any aspect of a Website's operations or resources, and resulting in major service disruptions and financial losses. DDoS assaults used to be a source of amusement, but research suggests that they're increasingly being used by hackers to make money or to cause disruption for political reasons [9].

Why there is increase in DDoS attacks

As it has been observed that there in explosive growth of DDoS attacks in the world of Internet and Web. DDoS attacks can be considered to be asymmetrical warfare. Hackers can more easily build the firepower needed for a DDoS assault, thanks to millions of vulnerable IoT devices. Manufacturers of IoT devices who are looking to cut costs, frequently overlook security features. This omission causes broad harm and stymies IoT growth in the long run. Once an IoT device is installed, it is challenging to upgrade its security [12, 13].

Types of DDoS attacks

DDoS assaults can be divided into three categories: volume-based, protocol-based, and application-layer attacks. SYN attacks are the most prevalent attacks among the many varieties (about 94% of all types of DDoS Attacks) [14]. Other common DDoS attacks includes ICMP (Ping) Flood, UDP Flood, etc. Earlier, it was the trend of DDoS attacks that would last for long time. As per the analysis done by Kaspersky, the longest known DDoS attack was of about 509 hours [9].

3 Discussion

Security Challenges in SDN

The networking technology known as software defined network (SDN) offers innovation in 5G networks and the next generation of network hardware. The primary cause of security challenges is SDN. In older technology, the hardware was in charge of controlling the network; hardware upgrades could not be made simply by updating the firmware. In case of any technological changes required in the network or the network devices, the only solution was to replace the old devices with devices supporting the new technology.

With SDN, majority of technological up-gradations are possible simply by software configuration or software up-gradation, and the need for replacement of existing hardware which may be a costly affair, that may not be required. The network devices can be remotely controlled and managed by software, thanks to the innovative SDN technology. Moreover, the network controller contains centralized network intelligence.

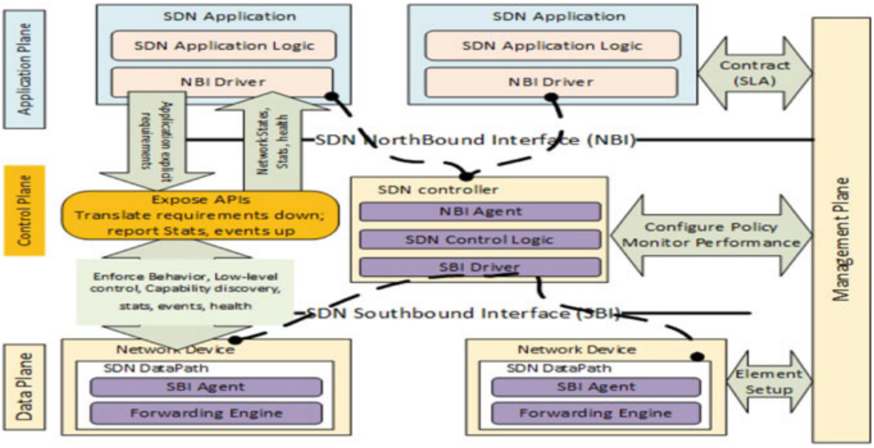

Fig. 2 SDN reference architecture [15]

Applications based on SDN are used to implement the network functionalities of next generation network hardware (including 5G and high speed network). As a result, designing and establishing network architecture as required is simple. It is still simpler for an attacker or hacker to begin an attack because they must concentrate on the primary network controller [24]. A hacker or attacker can send malicious code to the network controller, where it will start to wreak havoc on the entire network. So, keeping such malicious code out of the system becomes essential for safeguarding the Network.

The availability of open APIs in network equipment is one of the key security vulnerabilities that applications might provide to the network that can alter or change network behavior. The majority of 5G features will be developed as applications depending on how quickly they can be supplied, updated, and modified. NFV will make application-based services possible and introduce them into the networking domains [24]. Hence, safeguarding the network from anomalies brought on by applications will be crucial. Figure 2 illustrates how the control plane in SDN functions as a centralized decision-making unit. The controller may be heavily targeted for network intrusion or malicious operations due to its crucial role. In this case, it is important to keep in mind that since the hacker or attacker will attempt to assault the SDN Controller's core control plane, it will be easier to mitigate the attack there.

Distributed Denial of Service Attack in SDN

In recent years, a DDoS assault has been one of the most serious security concerns to the SDN network. In addition to preventing authorized users from using and accessing network resources, it has the power to fully destroy the network. As a result, defending the SDN network against DDoS attacks is critical [16, 17].

In order to establish zombie host groups that meet their attack needs, attackers hack many hosts and unite them. These zombie hosts bombard the target with an enormous number of useless data packets, consuming a lot of its bandwidth and

CPU resources, in the process. The target host will become unresponsive and unable to process real data packets when it receives much more data packets than it can handle. DDoS attacks are favored by attackers because they are easy to carry out. The switch receives attack packets and matches each one with a flow entry when the controller is assaulted. The flow table entry in the flow table cannot be matched because the attack packet is invalid. The packet is wrapped by the switch and sent as a packet-in message to the controller. The controller then decides on the direction of the data packet. Attackers flood the controller with attack packets, causing packet-in messages to continuously flow in and use up a lot of the controller's resources. The controller is therefore unable to process legitimate traffic data and becomes inefficient, or gets flawed. This demonstrates that the security issues associated with SDN should not be overlooked [16, 17].

Use of IoT devices as remote devices to Launch attack

The attacker and hacker have been using the attack on SDN controller as it is deduced that the attack will be very much destructive for the services which the said SDN has been in use. Most of the SDN implementations have now understood the need for securing controller. Since the SDN controllers are secured, there is no way to target the SDN controller. The hackers have been trying to use some different techniques for the attack. They seem to have found the possible loop hole in the end IoT devices. Hackers/attackers are trying to use the vulnerabilities [12] of the IoT devices, which are the part of network that is controlled by SDN controllers-based network. This is evident from the Mirai Botnet attack on the Security Blog of Brian Krebs that happened on September 20, 2016 and in Dyn DDoS attack that happened on October 21, 2016 [22, 23, 26]. Most of these IoT devices have following vulnerabilities:

- Most of these devices are small in size and are designed to consume less power. So, these devices are designed with scaled downed version of embedded operating system as a part of firmware so that it can run with the limited resources.
- These devices have hard coded password that is not been set. Thus, the devices have weak authentication mechanism.
- Devices comes with insecure Telnet support, so it is easy to install a Malware.
- The traffic between the controller and the device is normally not encrypted.
- As reported by the authority on video surveillance IPVM [25], CCTV can be a soft target.
- Open JTAG interface in the chip that gives physical access to the chip. (JTAG is a special interface added to the chip. With the help of these pins the test probe can be connected to the chip) [18]. It is used to inspect chip interconnects and printed circuit boards (PCBs). To determine how a chip responds to different commands, hackers use JTAG and debugging tools.

The Mirai botnet is a worm that would replicate by itself. It would infect and attack the vulnerable IoT devices. It is called as botnet as the infected devices would be then controlled by the remote command and control server. These server would tell the infected device to target which site. This would be possible as these bots would have replication module and the attacking modules. Later, lots of similar bots surfaced

Table 1 Some of the incidences of Mirai like attacks [22]

Date	Target	Type of attack
20 September 2016	Website of Computer security journalist Brian Krebs using Mirai and BASHLITE, a malware	DDoS attack
March 2018	A new variant of Mirai named "OMG", target vulnerable IoT devices	Truned IoT devices into Proxy Servers
May to June 2018	A Mirai variant "Wicked" targetting Netgear Routers and CCTV DVRs	Locate vulnerable IoT devices
July 2018	13 variants of Mirai detected to target Android devices	Target vulnerable IoT devices
21 October 2016	Multiple major DDoS attack on DNS service provider DYN using IoT devices	DDoS attack

and have been used for attacking the target network by the attacker [21]. Some of the popular attacks using the IoT devices is listed in Table 1.

Security Solution in SDN

A global perspective of the network is provided by the logically centralized control plane of SDN, which also makes it possible to configure network components in real-time. The SDN architecture makes network forensics, security policy changes, and security service insertion possible by supporting extremely proactive and reactive security monitoring, traffic analysis, and reaction systems.

By continuously collecting and accumulating data from network resources, states, and flows, SDN enables quick threat identification. With adjustments to the flow table, the SDN design offers traffic redirection for data analysis, policy change, and reconfiguring the network. SDNs' programmability makes it possible to change security policies on the fly without needing to individually configure each piece of hardware. Mis-configurations and policy conflicts across numerous networks are less likely as a result of this automation. Due to the network's high visibility, standardized network security standards may be established. As a result, security services like firewalls and intrusion detection systems (IDS) may be applied to specific traffic in line with generally recognized security standards.

The above measures may be enough so as to secure the SDN controller and the network, but in view of the new challenges those are added due to the vulnerabilities of IoT devices, which are used by hackers and attackers to launch their attacks on to the target victim network resources, the above measures may not be enough for securing the network from vulnerabilities due to vulnerable IoT devices.

Possible Solution to IoT-DDoS Security Threats

There have been research in the area of IoT-DDoS, and some of the solution have been proposed include the use of edge computing [26]. In this paper, the authors have proposed to implement a Show Net at the edge devices and also to implement

Shadow Server to detect and mitigate the IoT-DDoS attack. While in another paper [27], the authors have proposed to implement flow guard at the edge devices, an edge defense mechanism to detect the IoT-DDoS attacks. But in both the solutions, such mechanism has to be implemented in each edge device. This can be herculean task as the IoT devices may be located geographically apart and implementing such edge mechanism may not be possible in big network.

Following care may be taken to secure the IoT devices:

1. For your IoT devices, choose a strong operating system along with powerful development tools like *Windriver* Helix or *VMware Liota*. They also make it easier to apply security upgrades.
2. Implement more stringent authentication measures. A strong and unique password must be created by users, or default passwords should be updated. To protect IoT devices, public key authentication could be used.
3. The telnet support may be disabled on the device and a strong password with strong authentication mechanism may be followed, may be by using public key encryption, by enabling SSH instead of Telnet.
4. Verify that the correct control server is being used by the devices. This can be done by guarding the IP addresses of the control servers and limiting access to them. A reliable control server should be used to validate IoT firmware changes. Also by implementing the defense mechanism at the Edge devices.
5. To prevent hackers from accessing your IoT devices, make sure the JTAG interface is encrypted.
6. Ensure the security of both your own servers and the IoT control servers against such assaults. A number of services are provided, including an advanced threat solution that provides traffic visibility, security information, and situational awareness across the whole network. Better threat identification and incident response are made possible by real-time insights, visualization, and forensics.

4 Conclusion

The 5G network, 6G network, and high-speed wireless network are the future. But need for speed brings various risks. Biggest risk that is troubling the connected world is the threat of various cybersecurity attacks. As has been discussed, the next generation network will employ a number of technologies, including software defined networking, network function virtualization, and network slicing. Additionally, the use of connected devices for the Internet of things will expose the network to security risks like DDoS attacks. These new generation networks must be protected from these risks by law. Since now the techniques are being developed to secure such SDN controllers. It is the need of hour to secure the networks and network resources by securing the end point devices from being misused for launching attacks like DDoS attack and other type of attacks. One of the security mechanisms that may be considered is implementation of edge computing in the edge devices, but this technique is in nascent stage and security measure which are required to be developed, so that the world can enjoy the speed of life that will take us to the future.

Acknowledgements The authors would like to express sincere gratitude to the guide and mentor Dr. Srinivasan Sriramulu for his sincere efforts and all his support. The author would also like to thank Dr. Sampath Kumar, Dr. Naresh Kumar and all the Faculty members of Galgotias University for their support and guidance without which this paper would never have happened.

References

1. Fang D, Qian Y, Hu R (2018) Security for 5G mobile wireless networks. IEEE Access 6:4850–4874
2. Mantas G, Komninos N, Rodriguez J, Logota E, Marques H (2015) Security for 5G communications. In: Fundamentals of 5G mobile networks, pp 207–220
3. A smart city solution with 5G mMTC technology. https://www.gigabyte.com/Solutions/mmtc#:~:text=Example%20applications%20can%20include%20waste,charging%20stations%20for%20electric%20vehicles
4. Software defined network. In: Software-defined networking. Cisco. https://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html
5. What is NFV? In: Red Hat—we make open source technologies for the enterprise. https://www.redhat.com/en/topics/virtualization/what-is-nfv
6. 5G network slicing. https://www.ericsson.com/en/network-slicing
7. 5G phase I release 15 documentation released by 3GPP and TSG. https://www.3gpp.org/release-15
8. DDoS attack statistics, facts and figures for 2022. https://pixelprivacy.com/resources/ddos-attack-statistics-report/
9. DDoS attack statistics and facts for 2018–2022. https://www.comparitech.com/blog/information-security/ddos-statistics-facts/
10. 32 remarkable DDoS statistics for 2022. https://www.softactivity.com/ideas/ddos-statistics/
11. What is a DDoS attack? How to prevent DDoS attacks? https://www.testbytes.net/blog/ddos-attack/
12. Puri D. DDoS attacks using IoT devices follow The Manchurian Candidate model. https://www.networkworld.com/article/3128372/ddos-attacks-using-iot-devices-follow-the-manchurian-candidate-model.html
13. Galov N. 39 Jaw-dropping DDoS statistics to keep in mind for 2022. https://webtribunal.net/blog/ddos-statistics/
14. DDoS attacks. https://www.imperva.com/learn/ddos/ddos-attacks/
15. Hakiri A, Berthou P (2015) Leveraging SDN for the 5G networks: trends, prospects and challenges. CoRR. abs/1506.02876. http://arxiv.org/abs/1506.02876
16. Fan C, Kaliyamurthy N, Chen S, Jiang H, Zhou Y, Campbell C (2022) Detection of DDoS attacks in software defined networking using entropy. Appl Sci 12. https://www.mdpi.com/2076-3417/12/1/370
17. Mahrach S, Haqiq A (2020) DDoS flooding attack mitigation in software defined networks. Int J Adv Comput Sci Appl 11
18. JTAG. https://www.jtag.com/jtag-interface/
19. Why India's 5G users are experiencing high data consumption, choppy connectivity. https://www.techcircle.in/2022/11/11/why-india-s-5g-users-are-experiencing-high-data-usage-choppy-connectivity
20. Heightened DDoS threat posed by Mirai and other Botnets. https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets

21. Inside the infamous Mirai IoT Botnet: a retrospective analysis. https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/
22. Mirai (malware). https://en.wikipedia.org/wiki/Mirai_(malware)%23:%7E:text%3DThe%20Mirai%20botnet%20was%20first,Krebs%27%20website%2C%20an%20attack%20on
23. How IoT is making DDoS attacks more dangerous? https://insights2techinfo.com/how-iot-is-making-ddos-attacks-more-dangerous/
24. Chitre P, Sriramulu S (2023) Analysis and evaluation of security and privacy threats in high speed communication network. In: Gupta D, Khanna A, Bhattacharyya S, Hassanien AE, Anand S, Jaiswal A(eds) International conference on innovative computing and communications. Lecture notes in networks and systems, vol 471. Springer, Singapore. https://doi.org/10.1007/978-981-19-2535-1_39
25. The authority on physical security technology. https://ipvm.com/about?from=quick-links
26. Bhardwaj K, Miranda JC, Gavrilovska A (2018) Towards IoT-DDoS prevention using edge computing. In: USENIX workshop on hot topics in edge computing
27. Jia Y, Zhong F, Alrawais A, Gong B, Cheng X (2020) FlowGuard: an intelligent edge defense mechanism against IoT DDoS attacks. IEEE Internet Things J 7(10):9552–9562. https://doi.org/10.1109/JIOT.2020.2993782