INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

SDN-Based Security for Smart Devices Against Denial of Service Attacks

R Sherine Jenny[1]*, **N Sugirtham**[1]

1 Department of Electronics and Communication Engineering Dr.Mahalingam College of Engineering and Technology (An autonomous Institution affiliated to Anna University), Pollachi, Chennai, India

OPEN ACCESS

Received: 28-09-2022

Accepted: 21-12-2022

Published: 20-01-2023

Citation: Jenny RS, Sugirtham N (2023) SDN-Based Security for Smart Devices Against Denial of Service Attacks. Indian Journal of Science and Technology 16(3): 181-189. https://doi.org/10.17485/IJST/v16i3.1960

* **Corresponding author**.

sjenny98@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: To achieve a reliable IoT environment by mitigating the DoS attack. **Methods:** The study focuses on building a firewall on an Open Flow-based Software Defined Networking (SDN) controller to secure a network. We chose the POX controller, which is based on the Python programming language, from among various controllers. Furthermore, a detailed analysis of denial of service attacks against IoT devices has been carried out using Wireshark. **Findings:** SDN design allows networks to actively monitor traffic and diagnose threats, making network management easier. DoS & DDoS attack is simulated for IoT application which resulted in the loss of packets. **Novelty:** When compared to the traditional firewall where the internal traffic cannot be seen and filtered, SDN based firewall can filter the packet based on the policy defined. Here the experiment is carried out using open-source software.SDN security was built into the architecture to ensure the availability, integrity, and privacy of all connected resources and information. SDN-based Firewall is used as a solution against the denial of service attack. Through simulation, we have found and analyzed an efficient unsupervised method for detecting DDoS.

Keywords: Network Attack; Smart Devices; Security; Firewall; Software Defined Network

1 Introduction

The IoT framework of objects, humans, and services allows us to 'connect the unconnected', and access information at any time and from any location using any device. IoT is an excellent platform for devices to interact across network infrastructure remotely. The Internet of Things (IoT) has brought together hardware and software to create a smarter world. Over the past few years, it has received tremendous support [(1)]. IoT enables remote control of devices and machinery across a network that connects the physical world and computers. It has brought advancements to different aspects of human life by changing real-world objects into virtual or intelligent items. Additionally, it makes new services possible that will enhance daily life, commerce, and transportation. IoT has greater transparency and deals with automation and analytics with artificial intelligence, sensor, networking, electronics, cloud messaging, etc. This consists of networked smart gadgets that collect and distribute data from their environment. Despite the fact that users can connect with IoT devices, these

machines operate autonomously. Artificial intelligence (AI) and machine learning are used in the Internet of Things (IoT) to help make data collection methods simpler and more dynamic. There are many practical applications of IoT like industrial automation, health care, home automation, banking, agriculture, smart city, etc., These applications place a positive impact on our day-to-day routine by making our life easier. However, the security and dependability of data transmission to and from IoT devices are quickly growing to be very serious issues [2]. According to several studies, IoT networks are vulnerable to a range of security problems, including eavesdropping, jamming, information leakage, privacy, and verification.

Several new research approaches have been proposed by many researchers that have a significant impact on the future of IoT security. One such technique is Software-Defined Networking (SDN) [3]. SDN emerged as a strategy for increasing network functionality while lowering costs, reducing hardware complexity, and enabling innovative research. A possible field of research in designing and implementing optimization-based algorithms for detecting DoS/DDoS is SDN but SDN itself is prone to DOS attacks [4]. DoS and DDoS assaults have an adverse effect on network performance since they deplete resources, disable or degrade network services, and prevent legitimate sites from contacting the SDN controller or sending packets across the network [5]. Resource management in SDNs is thought to be possible using rule placement. This involves assigning rules to OpenFlow switches to manage the few resources while taking into account suggested network configurations and regulations [5]. The authors of [5] declare that some systems use the communication channel to mitigate the effect of an attack on the network by managing the utilised bandwidth by switches and clients via scheduling algorithms. However DDoS attack prevention techniques try to prevent the attack from spreading to the network and are complex and costly. Machine learning techniques have also been used and detection is done using algorithms. The challenge with using such algorithms is that the algorithms used may require more resources and may produce overhead [6]. Authors of [7] have proposed a hybrid entropy-based intrusion detection mechanism. The algorithm is implemented in the controller taking into account its processing power. The algorithm proposed by the authors does not take into account DDoS and further, the proposed algorithm may increase resource utilization. The authors' suggested algorithm may not be appropriate for IoT, in our opinion.

Despite the fact that new algorithms are constantly being offered, it is uncertain whether or not these mitigations will work with IoT devices. With the development of network functions virtualization (NFV), hardware like firewalls, routers, and intrusion detection systems (IDS) may now be implemented virtually. Virtual machines (VMs), which run on top of the cloud infrastructure's real server, are used for the implementation [8]. Hence we experimented by implementing a firewall in SDN. Detection, traceback, and filtering of denial-of-service attacks are very common methods to defend Denial of service attacks. The traceback mechanism is being used in [9]. Authors of [8] are very firm that SDN can provide a secure solution against these kinds of attacks. We utilized the open-source Mininet application in this instance, which many academics have tried out [3,5]. Additionally in our work, Wireshark was used to analyze the packets that were recorded in this case, and we concluded that this strategy may be utilized to counteract a DoS attack.

2 Methodology

2.1 IoT Security Architecture

The Internet of Things lacks a widely accepted architecture. A framework for understanding important connections between entities in a given environment is provided by the IoT reference model. The reference model attempts to provide a common foundation for IoT architectures and IoT systems. The IoT reference model as shown in the Figure 1 contains five layers that include perception, transport, processing, application, and business layers.

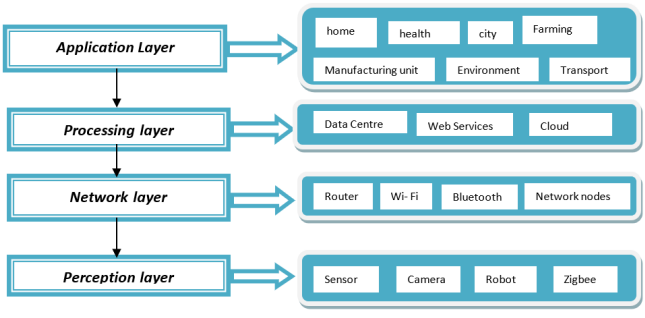

Fig 1. Layers of IoT reference model

The perception layer is made up of the physical components that have sensors for observing and gathering data about the environment. It finds specific physical characteristics or recognizes other intelligent objects nearby. The network layer is in charge of establishing connections between servers, other smart things, and network equipment. Prior to being delivered to a data center, where it is accessed by software applications, data must be analyzed and pre-processed. This is the responsibility of the processing layer. The user must receive application-specific services from the application layer. The transport layer transports the sensor data from the perception layer to the processing layer.

2.2 Why Security issues arise in IoT?

With enormous data creation and the exchange by IoT devices, security has become a vital issue these days. The critical characteristics for developing trust in IoT systems are data security and privacy.There are several reasons for security threats in IoT [(2)].

To list a few, lack of proper encryption,Insufficient privacy protection,Improper access control,extensive attack surface,obsolete software,Lack of proper physical security,User Interaction,absence of a reliable update method,Insecure data transfer, and storage, and Lack of User Knowledge & Awareness

Considering that the internet of things (IoT) connects billions of devices to the internet, it needs to be secured. Attackers penetrate the network by taking advantage of inadequately secured IoT devices because of the network's enlarged attack surface. To address the complicated issues in the approaching years, the IoT sector is anticipated to put a lot of emphasis on security. Industries, security-focused smart devices, and automatic network scanning for IoT devices are all expected to grow. The integration of IoT and artificial intelligence with the expanded function of data analytics will undoubtedly result in outstanding and more significant solutions.

2.3 Attacks in IoT devices

IoT is one of the most adaptable technologies that are available now. The growth rate of IoT is estimated and predicted to be 75 billion by 2025. The Growing internet facilities and connected devices have made IoT more scalable and versatile. More reliable guaranteed communication is an issue as standardization of IoT is still a question. However, this technology is under very great threat because of the characteristics that this technology possesses. The author of[(10)] claims that 70% of commonly deployed IoT devices are attackable. The threats are due to the connected devices, communication protocols, software, hardware involved, etc.,

The basic way of communication in IoT is wireless and hence vulnerable to eavesdropping. Side channel attack can gain the necessary content through leakage, during the execution of encrypted data. This is a very popular and dangerous perception layer attack. This may be a passive or active attack. Very common attacks that exploit IoT devices are spoofing, eavesdropping, Denial of service attack(DoS)/Distributed denial of service (DDoS), Replay attack, black hole, sinkhole, Sybil, Wormhole, etc [(11)] [(12)].

2.4 Denial of service

Denial of service attacks is considered to be a rising challenge to IoT devices. IoT devices are resource-limited/constrained devices, where memory, power, space, etc are limited. Denial of service attack gains attention in IoT application as, this attack focus on making the targeted device(Smart devices here) deny its service. The attacker bombards packets to the target and thereby depleting the network's capacity and hindering the activities of the victim. In addition, the legitimate request may not be serviced. The strategy of attack is shown in Figure 2 . A botnet, which is a global network of compromised computers, is where a DDoS attack is initiated. The botnet receives directives from the attacker. Fake traffic is sent to the target IP address by bots. Fake requests continue to pile up, eventually overwhelming the system. Finally, users can no longer access the server. Defending such an attack is a greater task. This attack is very common and can be easily implemented in IoT. This attack can be performed with a very less number of the node. One malicious node is enough to perform this attack successfully [(13)]. Attacks are becoming more frequent and more numerous every day. ICMP flood, Ping of death, UDP flood, and HTTP flood are very common DDoS attacks.

2.5 Types of attack

There are three basic categories used to classify denial of service attacks.

• Application layer Flood, where the attacker floods the network through a spoofed address. The attack's goal is to use up all of the targeted site's bandwidth. This is also said to be a layer 7 attack.

• Distributed Denial of service is the same as DoS, where the attacker is not a single node. Many to one strategy are followed here. This attack often uses Zombie machines.

• Unintended Denial of Service, as the name implies happens unknowingly, when someone post content and link to other websites. When it becomes popular and many visits the websites, the network gets crashed.

2.6 Security solutions against DoS

An incident response plan is a preventive step to ensure that staff members react promptly and effectively in the case of a DDoS attack. A clear step-by-step procedure for responding to an attack should be devised.For the purpose of thwarting any attack, firewalls and intrusion detection systems that scan network traffic are essential. Software that identifies and eliminates viruses and malware can be used. These are general solutions against an attack in a network but are not suitable for IoT devices. IoT devices lack virus protection because of their low power and memory.IoT devices are particularly susceptible to turning into bots and engaging in malicious activity on other networked devices since they lack virus and malware security. Since different vendors employ different architectures and protocols, the absence of a common design for the IoT network and devices has the biggest impact on security [12].

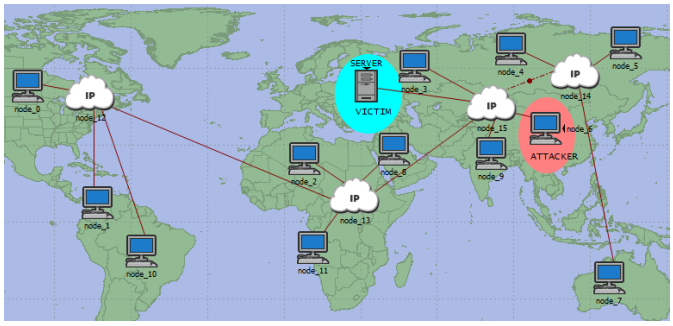

Fig 2. Strategy of DoS attack

The idea of network virtualization has lately evolved into SDN (software-defined networking).Through the use of a single location known as the controller, SDN controls the network by centralizing the routing and forwarding processes this can help the network operator and administrator adopt privacy over the entire network [14]. As per the authors of [14], within an IoT network, centralized monitoring offered by SDN can help detect and mitigate DDoS attacks.

2.7 Software defined networking (SDN and IoT)

The IoT architecture, applications, and security challenges were discussed in previous sections. SDN and its integration with IoT are discussed here. As discussed before, a Traditional network is not suitable for IoT devices. A more flexible and secure network infrastructure is needed to accommodate IoT operations. Figure 3 illustrates the structure of SDN and IoT. The SDN Controller connects with the IoT application through the ”Northbound API,” as indicated in the figure, which is a specific application programming interface. According to configuration rules, the northbound API analyses the network and takes action. The switches are communicated via the southbound API [3]. The IoT platform can use the debug tools provided by the SDN controller to increase security. IoT security issues can also be addressed by the idea of integrating modern firewalls or IDS/IPS solutions through an SDN controller or as a standalone entity within an SDN environment [15].

3 Result and Discussion

For the deployment of SDN, we used Mininet WiFi software. The routing protocol's data transmission is recorded using Wireshark which runs per the stated protocol after configuring the network using SDN. The data transmission commences after the protocol is announced. Figures 4 and 5 show a DoS and DDoS attack scenario created using mininet. hping3 command is used to perform the attack. Attacker stations execute the order to disable or stop a controller and smart device. Figure 6 depicts a simulation of an SDN network. The network is examined for connection. Wireshark is used to capture and examine packets. NOX is the name of the initial OpenFlow controller. It acts as a hub for network management. POX is an open-source development environment for software-defined networking (SDN) control applications, like OpenFlow SDN controllers. POX is used more commonly than NOX because it allows for quick prototyping and development.

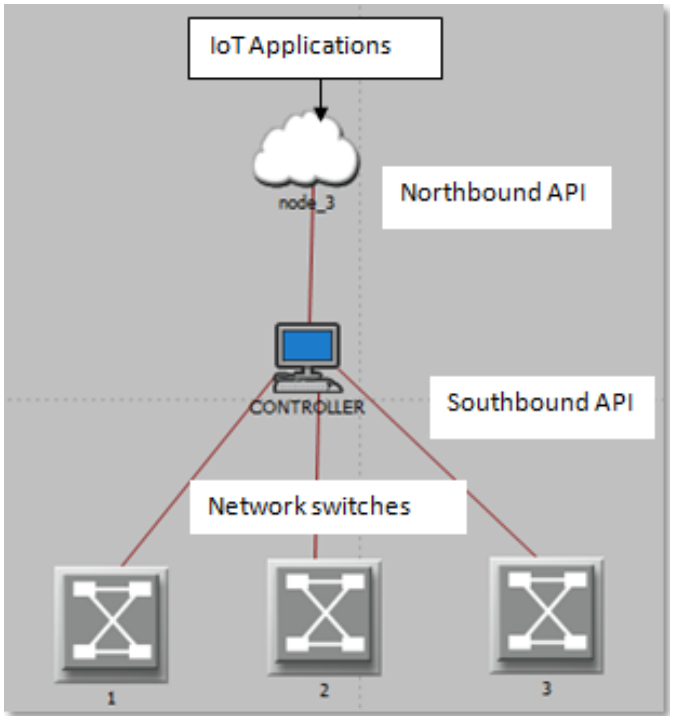

Fig 3. Structure of SDN and IoT

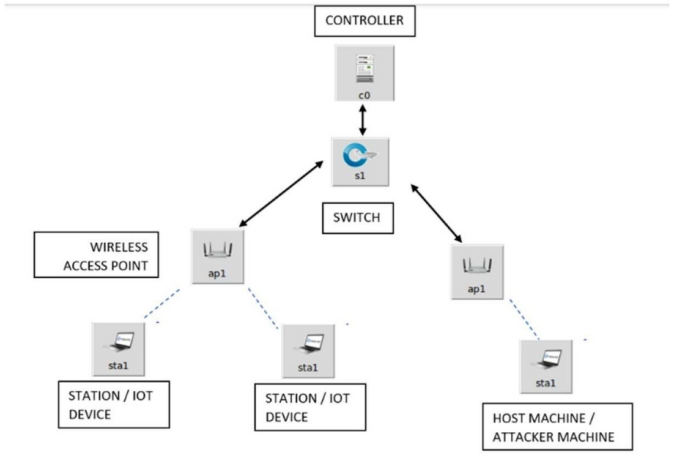

Fig 4. DoS Scenario

The pingall command, which sends a request to every node to check connectivity, is used to check for DoS, and it is recorded in Wireshark.

Figure 7 Represents packet capture while pinging to all nodes after designing SDN.

3.1 Firewall

A firewall is a device that blocks traffic coming its way and filters it in accordance with specified rules. For an SDN-based Firewall, the POX controller is used to establish our required policies or rules. The connection is checked after installing the firewall. The firewall considers the host as an unknown host based on the firewall configuration, Figure 8.

After installing a firewall, we kept pinging smart devices from the attacker machine and noticed that it was blocking the unknown host (the attacker machine) in accordance with the firewall rule setting as shown in Figure 9 . All the testing were

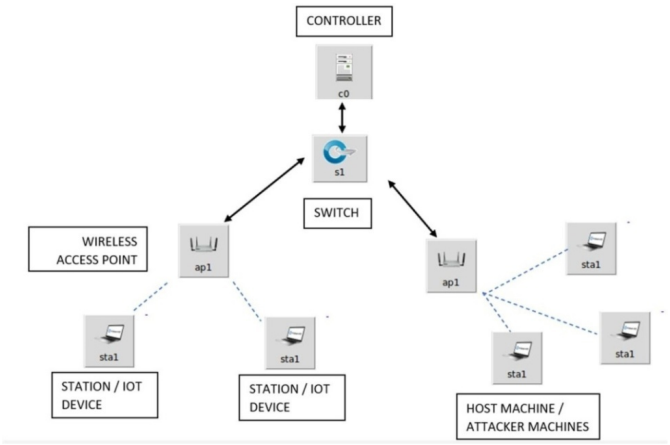

Fig 5. DDoS scenario

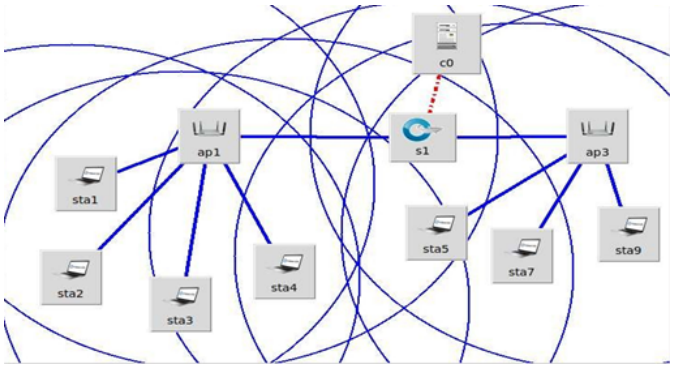

Fig 6. Simulation of SDN

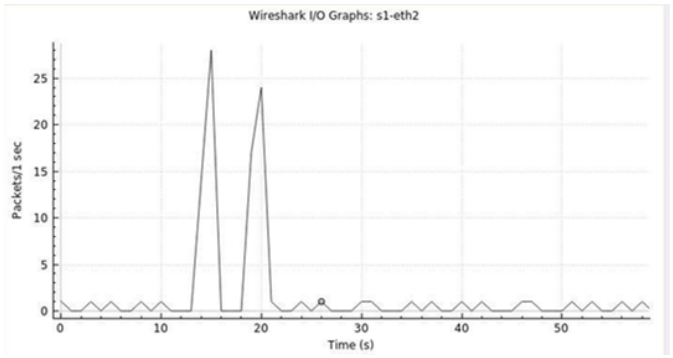

Fig 7. Packet capture

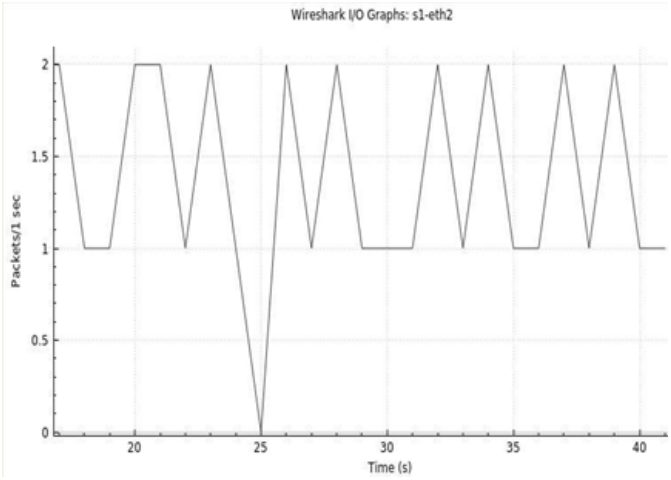

Fig 8. Attacker to Station Connection Graph after Firewall Installation

carried out in both DoS and DDoS attack scenario.

The attack is done using the command hping3 –faster -rand-source 10.0.0.1. As shown in Figure 10 , a single attacker machine attempted to deliver nearly 1000 packets but was blocked by a layer 2 firewall. This Wireshark traffic grab is from the controller.

Fig 9. Packet capture while attempt made to send 1000 packets

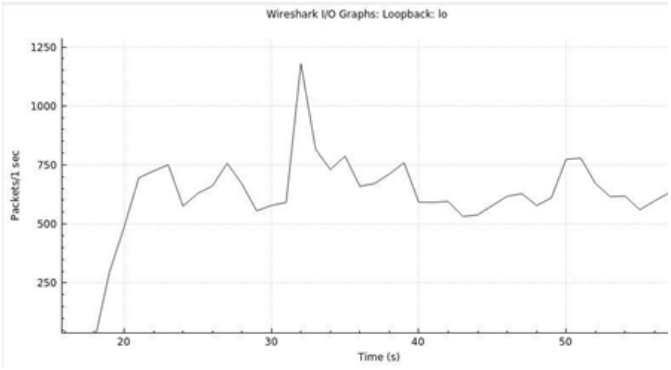

Fig 10. Packet capture while attempt made to send 1000 packets

In the DDoS attack, we added additional attacker machines (sta9, sta10, and sta8). The simulation demonstrates that the many attacker machines attempted to transmit more packets, but were blocked by the firewall. A section of the firewall program

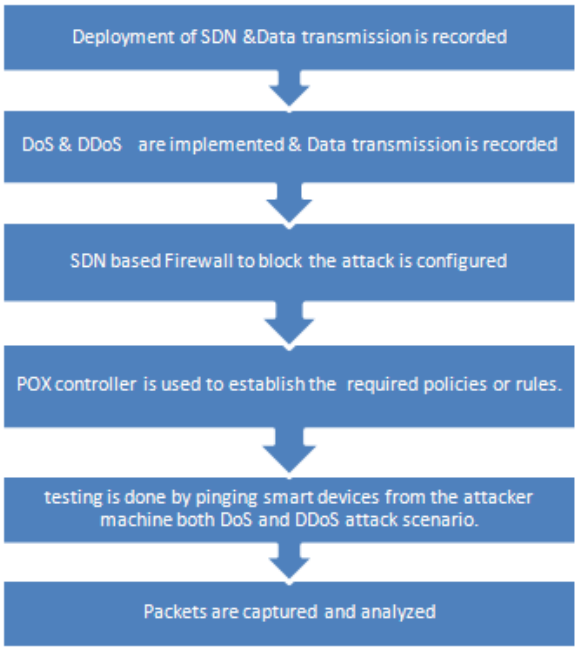

Fig 11. Flowchart of the proposed technique

utilized in the proposed work is shown. Figure 11 shows the overall structure of the proposed technique.

```
import core
import OpenFlow
import Ethernet Address
Frame rules
  Initialization
      block = Match rule 0
      block = Match rule 1
block = Match rule 2
      …….
      Check flow
```

4 Conclusion

A Secured scalable IoT platform to identify and reduce DoS and DDoS attacks in the IoT applications using Software Defined Network (SDN) was designed and experimented with. An in-depth study of DoS attacks in IoT was carried out. Since the traditional network is not suitable for IoT devices, SDN based Firewall can be used as a possible solution. DoS & DDoS attack is simulated for IoT application which resulted in the loss of packets. The network is managed and controlled using the SDN POX Python-based controller. The controller is responsible for managing, supervising, and regulating the actions of the forwarding devices. The SDN controller makes use of the Open Flow protocol and hence we suggest the SDN-based firewall as a solution against Denial of service attacks. Extensive research is been carried out on introducing a firewall in SDN as a mitigation to DoS attacks but to our knowledge, it is not been tested through wireshark. Wireshark was used to collect the packets, which were then analyzed before and after the firewall was installed.

The challenges that could be researched in the future are,

As it is difficult to provide a real-time defense against a denial of service attack in the Internet of Things, it necessitates developing novel intrusion detection techniques to ensure the security of associated systems and offered services. Approaches have to be proposed considering the effect of the mitigation techniques on the resources and, consequently the functionality of IoT devices. The most recent advancements in IoT security have also been reviewed here, along with some prospective future

research directions for increasing IoT security standards.

References

1) Jain S, Choudhari P, Srivastava A. The fundamentals of Internet of Things: Architectures, enabling technologies, and applications. Elsevier. 2021. Available from: https://doi.org/10.1016/B978-0-12-819664-9.00001-6.
2) Tawalbeh L, Muheidat F, Tawalbeh M, Quwaider M. IoT Privacy and Security: Challenges and Solutions. *Applied Sciences*. 2020;10(12):4102. Available from: https://doi.org/10.3390/APP10124102.
3) Hayajneh AA, Bhuiyan MZA, Mcandrew I. Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN). *Computers*. 2020;9(1):8. Available from: https://doi.org/10.3390/computers9010008.
4) A survey on DoS/DDoS mitigation techniques in SDNs: Classification, comparison, solutions, testing tools and dataset. 2022. Available from: https://doi.org/10.1016/j.compeleceng.2022.107706.
5) Eliyan LF, Pietro RD. DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. *Future Generation Computer Systems*. 2021;122:149–171. Available from: https://doi.org/10.1016/j.future.2021.03.011.
6) Alamri HA, Thayananthan V. Analysis of Machine Learning for Securing Software-Defined Networking. *Procedia Computer Science*. 2021;194:229–236. Available from: https://doi.org/10.1016/j.procs.2021.10.078.
7) Abdelazim NM, Fahmy SF, Sobh MA, Eldin AMB. A hybrid entropy-based DoS attacks detection system for software defined networks (SDN): A proposed trust mechanism. *Egyptian Informatics Journal*. 2021;22(1):85–90. Available from: https://doi.org/10.1016/j.eij.2020.04.005.
8) Singh J, Behal S. Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions. *Computer Science Review*. 2020;37:100279. Available from: https://doi.org/10.1016/j.cosrev.2020.100279.
9) Chen W, Xiao S, Liu L, Jiang X, Tang Z. A DDoS attacks traceback scheme for SDN-based smart city. *Computers & Electrical Engineering*. 2020;81:106503. Available from: https://doi.org/10.1016/j.compeleceng.2019.106503.
10) Rawlinson K. Internet of Things Behavioral-Economic Security Design, Actors & Cyber War. 2014. Available from: https://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/ReferencesPapers.aspx?ReferenceID=2024873.
11) Abosata N, Al-Rubaye S, Inalhan G, Emmanouilidis C. Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications. *Sensors*. 2021;21(11):3654. Available from: https://doi.org/10.3390/s21113654.
12) Al-Hadhrami Y, Hussain FK. DDoS attacks in IoT networks: a comprehensive systematic literature review. *World Wide Web*. 2021;24(3):971–1001. Available from: https://doi.org/10.1007/s11280-020-00855-2.
13) Ison S, Budd L, Magdi S, Mahmoud YX. Distributed denial-of-service attacks. *Cloud Control Systems*. 2020;p. 51–76. Available from: https://doi.org/10.1016/b978-0-12-818701-2.00011-1.
14) Hameed S, Khan FI, Hameed B. Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review. *Journal of Computer Networks and Communications*. 2019;2019:1–14. Available from: https://doi.org/10.1155/2019/9629381.
15) Biševac S, Šarac M. SDN Approach in Development Iot Environments. *Proceedings of the International Scientific Conference - Sinteza 2022*. 2022;p. 449–456. Available from: https://doi.org/10.15308/Sinteza-2022-449-456.