Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY
Vol. 10. No. 4, December 2022 – Special Issue on Cryptography & Security Mechanisms

Article Citation Format
Kpieleh, F. (2022): A Review of Ddos Attack Detection in Iot Networks. Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology.
Vol. 10, No. 2. Pp 43-54
DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V10N4P6

A Review of Ddos Attack Detection in Iot Networks

Kpieleh Ferdinand
School of Technology
Ghana Institute of Management & Public Administration
GreenHills, Accra, Ghana
E-mail: ferdinand_kpieleh@yahoo.com
Phone: +233502024517

ABSTRACT

The security risks and vulnerabilities associated with these resource-constrained Internet of Things (IoT) devices grow as their usability rises. Distributed Denial of Service is one of the main dangers to Internet of Things devices (DDoS). Continuous monitoring, early detection, and adaptive decision-making are necessary for IoT device security to be robust and effective. With software-defined networking (SDN), these issues can be solved, giving IoT devices the chance to manage DDoS threats in an efficient manner. This study suggests a unique SDN-based secure IoT framework that uses IP Payload Analysis and session IP counters to identify IoT device vulnerabilities and malicious traffic sent by IoT devices. The proposed methods can readily identify the DDoS attack in the SD-IoT network by analyzing several metrics, even with high traffic volumes, thanks to the DDoS attack detection module of the framework. By creating a lot of traffic from a compromised node, which is later identified and alerted, these tactics are tested on an SDN controller. The results and comparison analysis show that the suggested framework effectively and accurately detects DDoS attacks in their early stages, with a detection rate ranging from 98% to 100% and a low false-positive rate.

Keywords; IoT networks, DDoS, DDoS attacks, DDoS Detection and IoT security

1. INTRODUCTION

The purpose of this paper is to review distributed denial of service attacks detection in IoT networks. DDoS is defined as a process by which an attacker prevents authorized users from accessing a computer system, network, service, or other information technology (IT) resource. In this type of attack, the attacker often floods a web server, system, or network with traffic, making it difficult or impossible for other users to use them, thereby draining the victim's resources.(Ferguson & Loshin, 2011).

Internet of Things (IoT) on the other hand, is defined as a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.(Gillis, 2022).

A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an Internet Protocol (IP) address and is able to transfer data over a network. Increasingly, organizations in a variety of industries are using IoT to operate more efficiently, better understand customers to deliver enhanced customer service, improve decision-making and increase the value of the business. This technology may have potential benefits for people with disabilities and the elderly as it allows for greater levels of independence and quality of life at a reasonable cost. IoT network systems implement appropriate security mechanisms such as encryption, data backup, user authentication and application, and integrity protection of data processed and stored within the system.

In theory, IoT systems are fully protected with all necessary security mechanisms. However, the situation is not so simple. Like other computer network systems, IoT is vulnerable to various cyber-attacks. Recent attacks against IoT networks show that IoT network cybersecurity remains a major problem. With the development of IoT networks, cyber-attacks against such systems, especially distributed denial-of-service (DDoS) attacks have increased significantly, affecting many IoT networks and causing catastrophic losses. I'm here. Intrusion detection system "IDS" One of the cyber-attack detection technologies.

Real-world data is typically huge, which can degrade IDS performance, resulting in feature selection (FS) requirements to reduce data dimensionality and improve IDS system performance. DDoS attacks are one of the attacks that have caused devastating losses in IoT networks. Figure 1 shows how to implement a DDoS attack. First, the hacker selects her IoT devices such as DDoS masters (bots), computers, laptops, etc. This he exploits vulnerabilities in IoT devices to compromise these devices. Attackers then use this DDoS bot to further compromise numerous systems (sometimes thousands) on the network such as laptops, computers, CCTV, etc. known as Zombie Her Bot. An attacker directs these zombie bots through a DDoS master to send multiple flood attacks to a target system, resulting in a denial of service to legitimate users of the system. These types of cyber-attacks are attractive to hackers because they can be easily implemented to disable large and popular websites. DDoS attacks therefore wreak havoc on servers and devices on the Internet, creating a situation in which legitimate users of the system are unable to access resources and services.

Recently, DDoS attacks have targeted various IoT networks. On October 21, 2016, Dyn Server, the company that manages much of America's Internet's domain name system infrastructure, was hit by his DDoS attack using a new weapon called the Mirai botnet. His top websites affected by this attack were Amazon, Netflix, PayPal, Spotify, and Twitter in Europe and the US. Another incident of DDoS attacks against IoT networks was documented in April 2017, when a new IoT botnet called Persirai was discovered, sharing Mirai's code base and implementing over 1000 different models of Internet protocols (IP) cameras were targeted. Discovered by Trend Micro cybersecurity researchers, the attack affected 122,069 IP cameras worldwide.

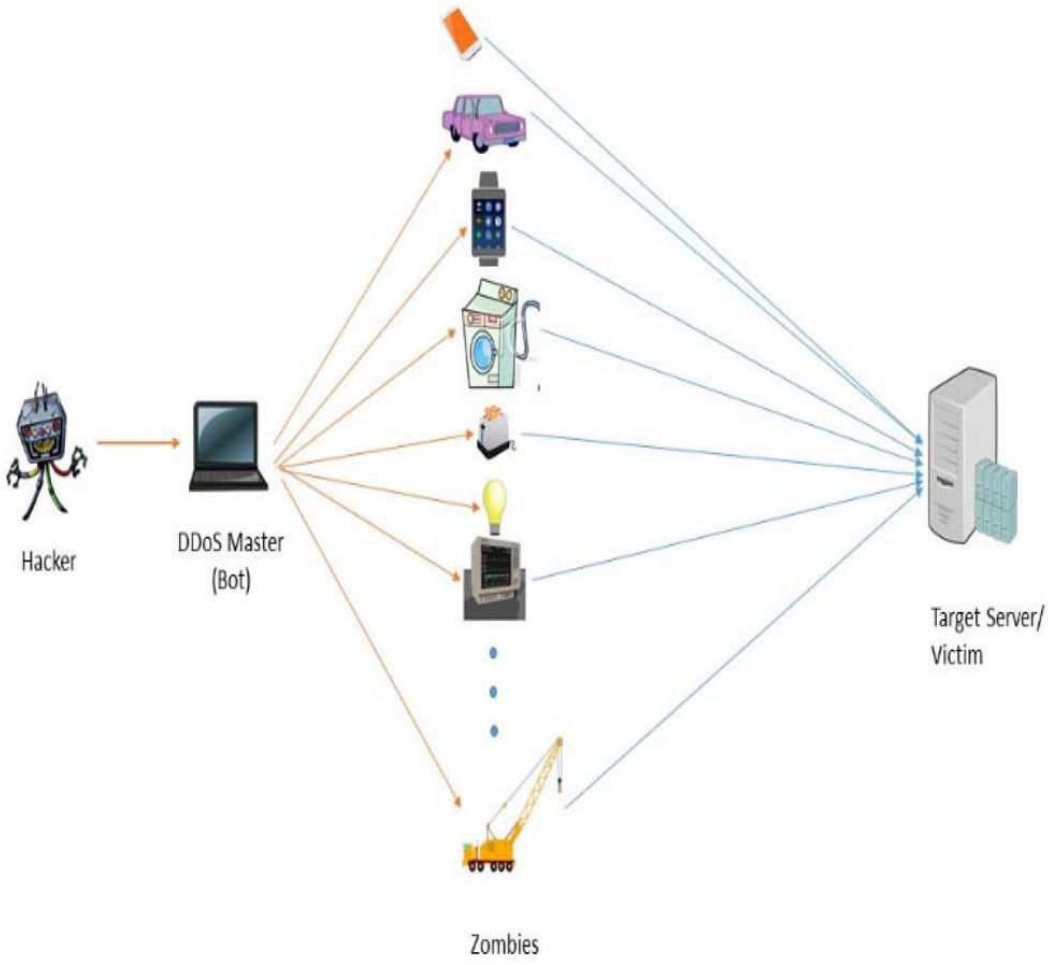

Fig 1 DDoS Attack Implementation
(Džaferović et al., 2019; Roopak et al., 2020)

The motivation for this work is that IoT systems are currently being overwhelmed, as mentioned earlier in some examples of recent DDoS attacks like the Mirai DDoS attack against Dyn servers. The performance and efficiency of an IDS to detect such cyberattacks depends on the performance of the classifiers used to distinguish between normal and attack data. Real-time network measurements are typically huge and pose a significant challenge for classifiers. Therefore, we need to select appropriate features from the raw data so that we can improve the performance and complexity of our attack detection classifier. It is very important for IDS to exploit FS methods suitable for DDoS attacks. A key issue is choosing the key features that are most relevant to attack detection using learning algorithms. A DDoS assault is one of the main problems experienced by and through IoT devices. These devices are the target of the attackers' DDoS attack. The development of countermeasure methods for the detection and prevention of DDoS assaults utilizing SDN is the primary driving force behind this research project.

In this study, we will simulate various methods for detecting a DDoS assault, such as a counter for IP packets in a single session technique and an examination of historical data of IoT networks in terms of bandwidth and power consumption by the IoT devices. In the test simulation model, we will simulate the scenarios of DDoS attack creation (flooding and reflecting) and its detection mechanisms in addition to implementing the suggested algorithms on the SDNWISE controller. Furthermore, the framework's primary functionality is dependent on counter values, making it useful in detecting zero-day assaults. This article's remaining sections are organized as follows: section 2 elaborates on literature review, section 3 discuss the methodology used in the paper, section 4 shows the research gaps that are left behind by other writers and the last section 5 illustrates the conclusion and future direction.

2. LITERATURE REVIEW

The number of threats to IoT infrastructures has increased as a result of the quick development of Internet-based services and applications. As security solutions have advanced in the past, there are numerous strong solutions from the literature that are worth discussing. In order to address network-wide problems with flexibility, management, adaptation, and keeping a constant quality of service for future Internet development, SDN is a dependable and strong strategy. The SDN strategy seeks to divide a network's functionality into three layers, which reduces network management time and expands network security options. Deployment of the new paradigm is challenging despite the fact that it is equally susceptible to DDoS attacks. The SDN-based layered architecture was thoroughly explored by Singh and Behal, who also gave information on the network's benefits in the face of a DDoS assault and the related drawbacks that make them prone to new DDoS attacks rather than the traditional type of DDoS attacks. Since sensitive information can be intercepted by resource-constrained IoT devices, there will be a rise in the requirement for information security as more devices are connected to the Internet.

Al-Hayajneh et al. looked into how SDN may be combined with IoTs to increase overall security in the IoT ecosystem. Their tests and implementations show that IoT devices that can only use HTTP due to resource limitations can nevertheless be secured without requiring any device modification. In their study, Kim et al. presented a simplistic security architecture for IoT SODA that secures the IoT gateway and uses dynamic access control and other security services to safeguard the network's critical data. In order to limit assaults through its security features, SODA is implemented on IoT devices using SDN and virtual network functions (VNFs) through NFV. A system that logs the power of IoT nodes over time was put out by Fiore et al. If one node uses more power than another, the traffic on that particular host is monitored.

They were able to identify some of the hosts hosting malicious applications as a result. No evidence of involvement in an attack, however, was discovered. As is typical, each host or node on the network behaves differently from the others, and each node delivers a unique form of packet at a unique interval of time. This reasoning was used as a signature to determine whether any node was hacked and had been the source of the assault. Blockchain and SDN were used by Hameed et al. to offer a scalable approach for managing keys and trust for IoT devices. SDN introduces a number of additional protection methods, some of which are based on the detection of bots, malware, port monitoring, etc., enabling efficient attack detection and mitigation.

Numerous scholars have discussed various assault detection and defensive mechanisms. In their survey study, Vishwakarma and Jain analyze DDoS attack defense strategies for both traditional and Internet of Things (IoT) networks. They also divided these security systems into ways for detecting, preventing, and mitigating the DDoS attack. The writers also cover the well-known IoT malware and botnet, which target servers and infect IoT devices before launching DDoS attacks via the servers. Additionally, a thorough comparative analysis of various defense strategies is covered in this article to assist readers better grasp the problems and challenges related to DDoS assaults in IoT contexts.

In their paper, Silva et al. established a clear taxonomy to identify and evaluate DDoS attack mitigation solutions while considering SDN technologies in IoT contexts. Zçelik et al. talked about using SDN and fog technology to identify DDoS attacks in IoT networks. SDN and fog computing, which primarily offer features, such as network control and local services, are used to identify and mitigate the DDoS attack, which is carried out by a large number of IoT devices that have been infected with the Mirai botnet. Reams suggested three methods for identifying an IoT DDoS assault. The detection method relies on automata learning to create a plan for stopping DDoS attacks. Each network layer has set thresholds, and learning automata assist in identifying these packets so that the packages are rejected.

Needham also offers a different DDoS mitigation strategy, monitoring 6LoWPAN network traffic with IDS probes (in the promiscuous mode). It uses a signature-based IDS detection technique to find the attack. The introduction of a detection system for IPv6 over low-power wireless personal area networks (6LoWPAN) is based on the detection of DDoS through examining the power and energy required by nodes to identify the attack. In a research report, it is predicted that the methods and SDN framework model will make it easier to handle IoT process integration. The framework combines software-defined security and storage into a single software-based control mechanism. According to the study, it is advised to ban the devices on their home network using SDN on a dynamic basis.

This model detects and isolates the traffic of devices with known vulnerabilities, such as Philips Hue lights. Lim et al. have introduced an application that focuses on the concept of DDoS blocking. The main concept behind this research was to exploit SDN's advantages to stop DDoS attacks. The researchers' described application utilizes the POX SDN controller. The application's main job was to analyze traffic, spot malicious hosts, distinguish between good hosts, and direct the latter to the proper server hosting service. In this instance, the solution can only be helpful for Web server attack prevention because it is specifically intended for Web servers.

A DDoS attack detection technique was introduced by Akilarasu and Shalinie. The approach primarily filters packets based on the source's signature and maliciousness, which is recognized in sources that are blacklisted. Models-based for the purpose of detecting DDoS attacks, Manets are also suggested. Based on the sender of the delayed packets, the models identify the malicious source. The model's single attribute check foundation makes it ineffective for identifying the attack. Yi and colleagues created a method to stop DDoS flood attacks. The interaction between the neighboring nodes' communication is crucial to this method. The criteria are based on the adjacent node's traffic estimation. Every node has a threshold for talking with its neighbors, and each node calculates and tracks the neighbor's node's communication rate.

The source nodes record the id of the malicious nodes and stop traffic from those nodes when the communication rate exceeds the threshold. The problem with this approach is that the IoT node's power and energy are crucial, therefore processing on a node by itself will exhaust the nodes and use more energy. Researchers from and have presented their work on traffic anomaly identification. Although the investigation revealed a number of distinct anomaly symptoms, the researchers have concentrated on the volume of traffic because it appears to be the primary DDoS assault concern. They cause the port 80 traffic to rise and change its destination. Other ports and traffic types may still be included in detection on a given port-based traffic. The infrastructure of the IoT network is becoming vulnerable to security threats on a regular basis. It is challenging to rely on and enforce traditional security standards in IoT networks due to the scarce resources available and the large number of connected devices. In order to stop network attacks, hostile IoT devices, and/or malicious Internet-connected devices from carrying out such attacks on the IoT network architecture, Karmakar et al. [39] concentrated on creating a workable security solution.

The software-defined perimeter (SDP) paradigm, which aims to restrict network access and connections between permitted parts through a software-controlled architecture, is a good example of how their suggested security architecture compares. SDN has been used to develop a virtualization architecture that provides separation between the control and data planes. Communication between IoT devices is virtualized using overlays that mimic logical connections across a physical network, separating the ability to restrict access from the transmission of data. They have also shown how their suggested security architecture may help with detecting malicious IoT devices and flows as well as defending the IoT network infrastructure from DDoS attacks like the Mirai botnet attack.

A basic system, the HADEC Hadoop-based live DDoS detection framework, was also described by authors in their works [40] and [41]. This framework uses a counter-based method to identify DDoS attacks. With the use of MapReduce, the algorithm recognizes the four flooding-based DDoS assaults, including TCP-SYN, HTTP-Get, UDP, and ICMP. It quickly analyzes and detects with efficiency. This architecture resolves issues that conventional systems have with scalability, memory efficiency, and process complexity. Similar to this, Bhayo et al. [42] provide a counter-based strategy for DDoS attack detection known as the Counter Based DDoS Attack Detection (C-DAD) framework.

The control plan and the data plan are the foundation of C-DAD. The SD-IoT network's scalability is also provided, allowing for the enhancement of the resources at the control plan in the SDNWISE controller. In contrast, this research is based solely on the control plan, meaning there is no load on the data plan. Using semi supervised machine learning approaches for attack detection, Ravi and Shalinie introduced the learning-driven detection and mitigation (LEADEM) mechanism. In comparison to cutting-edge solutions, the LEADEM demonstrated greater accuracy; yet, it performed best against known or practiced attacks. Our suggested approach works well against unskilled or zero-day attackers. The entropy-based DDoS attack detection technique employing the POX controller for SDN was covered in Swami et al. This approach is used for traditional networks and requires less time and overhead while detecting attacks. Our suggested architecture, however, is based on the SDNWISE controller and works with the Contiki OS, which was created especially for IoT networks. Ali et al. similarly revealed AI-based attack detection techniques that shield aircraft against DDoS.

The authors' primary attention was on the SDN-based avionics communication network for aircraft. The detection system divides malicious and legitimate communications using neural network-based techniques. Although the model performs well, it can still be enhanced by adding more feature sets and fine-tuning it with a slower learning rate. Different risks and DDoS attack-related vulnerabilities have an impact on the SDN. Different controller types are implemented in several languages, making it easier to select one for a given application. In this regard, Ahmed and Kim talked about the problems and various SDN DDoS attack mitigation strategies. These DDoS attacks and the methods used to mitigate them inspire us to solve challenges.

In their SDN-based detection module for IoT controllers, Augusto et al. apply machine learning to categorize the network traffic. It has a 96% attack detection rate, low false-alarm rates, and high precision above 93%, according to the data. To detect a zero-day attack or an unknown attack, similar methods can also be used to detect trained or known attacks. Aljuhani covered several DDoS assaults, their effects on company, and various DDoS attack classifications. Additionally, it demonstrates various machine learning techniques for detecting DDoS attacks and its automated protection system. The DDoS concerns with regard to machine learning and data sets for various networks, such as traditional, cloud, SDN, and IoT, are also summarized in this article. The authors also covered various DDoS assault classification techniques. The authors, however, addressed the inadequate DDoS attack detection techniques and largely concentrated on the DDoS attack defense strategies pertaining to various network conditions.

IoT devices are deployed in open space and have limitations in the form of resources and security. IoT devices in various applications are sensing and sharing sensitive information; hence, these devices can put private and confidential data at risk. While IoT device makers are incorporating additional security features into their products, network-level approaches to detect and prohibit unusual behavior are still needed [51]. Rizvi et al. [52] discussed vulnerabilities and security challenges to IoT networks in common domains such as healthcare, commerce, and smart home. IoT devices have vulnerabilities, including DoS, SQL injection, unencrypted services, myriad, and console access. Table III discusses the different security threats against vulnerabilities to IoT devices concerning the communication environment.

In this regard, this article highlights various flooding-based DDoS attacks, which are launched to exploit vulnerabilities against the most common threat to IoT. The DDoS attacks are classified into different types, including flooding-based attacks, reflecting based attacks, amplification-based, and reprogramming-based attacks. Moreover, we present different DDoS attacks for security analysis and enlist the most common flooding-based attack. The proposed framework focuses on detecting the flooding-based DDoS in the SD-IoT network.

One of the difficult challenges is identifying malicious packets on a given network's path. In the area of network security, SDN offers special characteristics for DDoS attack detection and mitigation. To identify and counteract DDoS attacks at edge networks, Yaegashi et al. presented a novel DDoS attack mitigation mechanism at the network edge. They gather the network traffic from SDN-enabled switches as opposed to more conventional methods like sampling-based at proprietary routers to obtain high accuracy.

Our suggested work is based on the detection approach for the SD-IoT network, however this work clearly solves the attack mitigation issue with the use of SDN at the edge network. Regardless of accuracy, threshold and counter-based DDoS systems strive for faster detection times and throughput. However, due to traffic that self-floods, these types of DDoS systems attain higher accuracy (either normal or abnormal). The accuracy and DDoS detection rate in our scenario range from 98% to 100%. The results of the experiment show that the attack may be identified as soon as it starts, with a high detection accuracy and a low false-positive rate.

3. METHODOLOGY

In Fig. 2, the methodology used in this investigation is depicted. Network data that has undergone DDoS attacks and without are gathered and normalized. The IDS and internet protocol are regarded as the most crucial defenses against the expanding number of network threats, but a lack of trustworthy test and validation datasets prevents them from performing consistently and accurately. In Fig. 2, the methodology used in this investigation is depicted. Network data that has undergone DDoS attacks and without are gathered and normalized. The developer of this dataset employed a B-Profile method to profile the abstract behavior of human interactions and generated naturalistic background traffic while retaining realistic background traffic as a key focus. The frame per second (FPS), secure shell, email, and hypertext transfer protocol (HTTP) secure protocols were used to build the abstract behavior of 25 users. This dataset, which includes various cyberattacks as well as no assaults, was gathered over the course of five days in 2017. We used data that was recorded on July 7, 2017, which includes both regular and DDoS attack data, to evaluate our work. This dataset includes 225,742 cases with both attack and regular data, 85 network flow features, label attributes, and label attributes.

This dataset is rather unbalanced, thus for this study, we changed the training dataset to be balanced in terms of both attack and normal data, reduced the number of instances to 81 characteristics, and divided the data into training and test data. The normalized data are then sent to the ELM classifier algorithm after being modified. The target property is normalized in the range of 0 to 1, while the features are normalized in the range of 1 to 1.

4. RESEARCH GAPS

The table below shows the various research conducted and the gaps identified

S/No	Reference Year	Comparison
1	Aljuhani et al. 2021	The DDoS attack classification, tools, and techniques are discussed. In addition, the paper also highlighted different DDoS attack defense approaches with various network environments. However, this is mostly discussed as a defense mechanism with respect to Machine Learning. Our proposed work overcame gaps and addressed DDoS detection in the SD-IoT network.
2	Yaegashi et al. 2021	Attack detection and mitigation of DDoS attack at edge network using SDN with high accuracy. However, this work focused only on addressing the mitigation issues and limited work-related towards detection approaches. Our proposed work is specifically based on a detection method for the SD-IoT network.
3	Ravi et al. 2020	The LEADEM uses a semi-supervised mechanism for attack detection and mitigation. However, it works best for known and trained attacks and has limitations on untrained or zero-day attacks.
4	Augusto et al. 2020	Software-Defined based detection module for IoT controller using machine learning approaches. It archives good accuracy; however, this work also has limitations on untrained or unknown attacks.
5	Bhayo et al. 2020	The DDoS attack detection method is based on counter-based values. It is also focused on the SD-IoT network and provides good results. Although this study is best for zero-day attack or unknown attacks detection, it has limitations on the size of network nodes.
6	Ali et al. 2019	AI-based detection method for aircraft to protect from DDoS attack having good performance. However, this study mostly focused on avionic communication and required improvement in feature sets and learning rates.
7	Jagdeep Singh et al. 2020	SDN-Based layer architecture which includes details on network advantages when comforted with DDoS attack and shortcoming that vulnerable new type of DDoS attack.
8	Abdullah et al. 2020	It investigates and integrates SDN with IoT, however, it has limitations only useful for devices which supports HTTP.
9	Mohammad A et al. 2020	SDN-based DDoS detection method which is using a filtering approach for attack detection based on source-IP address. However, this work has an issue with massive amounts of DDoS traffic.
10	Kallol Krishna et al. 2020	A practical security solution developed for preventing network attacks. They separate the access control from the transmission of data and IoT devices are virtualized using overlays that simulate the logical connection over physical. However, this work mostly focused on access control mechanisms to prevent IoT infrastructure from DDoS attacks.

S.No	Reference Year	Comparison
11	Vishwakarma et al. 2019	The defense mechanism discussed including its categorization such as detection, prevention, and mitigation. In addition, the authors also discuss famous IoT malware and Botnet which are used to launch DDoS attacks. Moreover, the comprehensive comparative analysis of different defense mechanisms helps to understand open challenges about DDoS attacks in IoT networks.
12	Anadiotis et al. 2018	Authors presented SDNWISE framework for IoT network. It provides the complete network topology information and communication services between IoT nodes. However, this framework has limited standard functionalities which are required for IoT networks. In this regard, we customized and integrated the framework with a security module that provides attack detection services to SD-IoT.
13	Yeonkeun Kim et al. 2019	The authors present the IoT gateway as a security services provider, it protects through dynamic access control using NFV to mitigate and secure the IoT network.
14	Hameed et al. 2018	Hadoop-based framework presented for DDoS detection using counter-based algorithms. However, this work has been proposed for traditional networks; it has limitations with respect to SD-IoT.
15	Ahmed et al. 2017	Different DDoS attack mitigation approaches are discussed that resolve the security of SDN. In this regard, this study motivates and provides a roadmap towards our problem.

5. CONCLUSION AND FUTURE DIRECTIONS

We attempted to solve the security concerns related to DDoS assaults that IoT devices experience through this research. It is crucial to offer solutions with the least amount of resource usage that can detect and stop DDoS attacks launched at or through IoT devices. Our suggested framework is a cutting-edge method for identifying DDoS attacks. Due to the solution's SDN deployment, we have a centralized controller with full network topology knowledge that can effectively manage IoT security threats.

IoT devices are susceptible to attacks because of the high computing power limits and low level of protection. We have overcome these difficulties by making use of SDN's features. On the COOJA simulator, we created an SD-IoT network model for this study. This model's nodes include some that are set up to send a lot of traffic to other nodes. By using IP Packet counter and Payload Detection techniques and looking through packet records, the detection mechanism is implemented on the SDNWISE controller.

It will be preferable to take countermeasures, such as disconnecting IoT devices from communication with other nodes to prevent a higher level of attack creation, as soon as suspect IoT traffic is detected. In addition to providing support for the IP spoofing detection technique, which is the subject of this research, the security of the framework can also be increased. In order to assess the simulated infrastructure, different attack scenarios and detection techniques were tested. By identifying vulnerable nodes and removing or limiting their communication on the network, this research can eventually broaden the framework for DDoS assault mitigation. Additionally, the scope of this study might be expanded to include several DDoS attacks on IoT-based, real-time enterprise networks.

REFERENCES

Akilarasu, G., & Shalinie, S. M. (2017). Wormhole-Free Routing and DoS Attack Defense in Wireless Mesh Networks. *Wireless Networks*, *23*(6), 1709–1718. https://doi.org/10.1007/s11276-016-1240-0

Al Hayajneh, A., Bhuiyan, M. Z. A., & McAndrew, I. (2020). Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN). *Computers*, *9*(1), 8. https://doi.org/10.3390/computers9010008

Chen, Y., Hwang, K., & Ku, W.-S. (2007). Collaborative Detection of DDoS Attacks over Multiple Network Domains. *IEEE Transactions on Parallel and Distributed Systems*, *18*(12), 1649–1662. https://doi.org/10.1109/TPDS.2007.1111

Dantas Silva, F. S., Silva, E., Neto, E. P., Lemos, M., Venancio Neto, A. J., & Esposito, F. (2020). A Taxonomy of DDoS Attack Mitigation Approaches Featured by SDN Technologies in IoT Scenarios. *Sensors*, *20*(11), 3078. https://doi.org/10.3390/s20113078

Devi, P., & Kannammal, A. (2016). An integrated intelligent paradigm to detect DDoS attack in mobile ad hoc networks. *International Journal of Embedded Systems*, *8*(1), 69. https://doi.org/10.1504/IJES.2016.073754

Džaferović, E., Sokol, A., Almisreb, A. A., & Mohd Norzeli, S. (2019). DoS and DDoS vulnerability of IoT: A review. *Sustainable Engineering and Innovation*, *1*(1), 43–48. https://doi.org/10.37868/sei.v1i1.36

Ferguson, K., & Loshin, P. (2011). *Denial-of-Service attack* (pp. 3–3). https://doi.org/10.1109/icccn.2006.286236

Fiore, U., Palmieri, F., Castiglione, A., & De Santis, A. (2013). Network anomaly detection with the restricted Boltzmann machine. *Neurocomputing*, *122*, 13–23. https://doi.org/10.1016/j.neucom.2012.11.050

Gillis, A. (2022). *What is IoT (Internet of Things) and How Does it Work? - Definition from TechTarget.com*. TechTarget. https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

Hameed, S. (2018). SDN Based Collaborative Scheme for Mitigation of DDoS Attacks. *Future Internet*, *10*(3), 23. https://doi.org/10.3390/fi10030023

Hameed, S., & Khan, H. A. (2017). Leveraging SDN for collaborative DDoS mitigation. *2017 International Conference on Networked Systems (NetSys)*, 1–6. https://doi.org/10.1109/NetSys.2017.7903962

Hameed, S., Shah, S. A., Saeed, Q. S., Siddiqui, S., Ali, I., Vedeshin, A., & Draheim, D. (2021). A Scalable Key and Trust Management Solution for IoT Sensors Using SDN and Blockchain Technology. *IEEE Sensors Journal*, *21*(6), 8716–8733. https://doi.org/10.1109/JSEN.2021.3052009

Kim, Y., Nam, J., Park, T., Scott-Hayward, S., & Shin, S. (2019). SODA: A software-defined security framework for IoT environments. *Computer Networks*, *163*, 106889. https://doi.org/10.1016/j.comnet.2019.106889

Lim, S., Ha, J., Kim, H., Kim, Y., & Yang, S. (2014). A SDN-oriented DDoS blocking scheme for botnet-based attacks. *2014 Sixth International Conference on Ubiquitous and Future Networks (ICUFN)*, 63–68. https://doi.org/10.1109/ICUFN.2014.6876752

Manikopoulos, C., & Papavassiliou, S. (2002). Network intrusion and fault detection: a statistical anomaly approach. *IEEE Communications Magazine*, *40*(10), 76–82. https://doi.org/10.1109/MCOM.2002.1039860