e-Prime - Advances in Electrical Engineering, Electronics and Energy 8 (2024) 100543

Contents lists available at ScienceDirect

e-Prime - Advances in Electrical Engineering, Electronics and Energy

journal homepage: www.elsevier.com/locate/prime

A comprehensive survey on DDoS attacks detection & mitigation in SDN-IoT network

Chandrapal Singh, Ankit Kumar Jain *

National Institute of Technology Kurukshetra, India

ARTICLE INFO

Keywords:
Internet of Things
Software-defined networks
Distributed denial of service
Network security

ABSTRACT

The Internet of Things (IoT) has transformed our lives by introducing new services and enhancing productivity. However, the widespread adoption of IoT devices and communication units has posed challenges in network management. In response, there is a growing necessity to rethink and redesign IoT network control. Software-defined networking (SDN) has emerged as a promising solution, leveraging its programmability and centralized management capabilities. SDN can simplify network management, offer network abstraction, facilitate development, and efficiently handle the complexities of IoT networks. Despite these advantages, security concerns, particularly the threat of Distributed Denial of Service (DDoS) attacks, persist in the IoT landscape. This survey focuses on exploring the collaboration between SDN and IoT. It investigates various types of DDoS attacks and highlights different types of defense, detection, and mitigation methods employed to address DDoS threats in SDN-based IoT (SDN-IoT) networks.

1. Introduction

As a natural evolution of technology that bridges the digital and physical realms, the Internet of Things (IoT) has gained popularity across various domains, including smart health, smart cities, smart homes, smart grids, etc. [1,2]. The advent of IoT services has significantly impacted people's lives, particularly benefiting individuals with disabilities who can leverage people-centered solutions, like enhancing their independence and engagement in their communities [3]. Moreover, IoT technologies have found utility in hazardous environments such as mines, where self-driving tools help keep workers away from dangerous areas [4]. However, it is essential to acknowledge that the proliferation of IoT devices also contributes significantly to the growing impact of Distributed Denial of Service (DDoS) attacks. The interconnected nature of IoT devices poses challenges in terms of security, making them susceptible to exploitation in DDoS attacks.

An attacker orchestrates a DDoS attack by compromising a large number of devices, commonly referred to as botnets [1]. These botnets are then utilized to swiftly overwhelm network capacity, deplete resources, and consume bandwidth. The research community identified Denial of Service (DoS) attacks, aimed at preventing legitimate users from accessing specific network resources, as early as the 1980s [5]. Presently, DDoS attacks on the Internet can be executed in two primary ways [6].

The first approach involves the attacker sending malicious packets to a specific protocol or application with the intent of disrupting its normal operation. In a basic DoS attack, the targeted host or server rejects all user requests, utilizing all available bandwidth and rendering the service unreachable for subsequent requests. This occurs due to the influx of a substantial amount of data flooding the communication channel.

The second method entails purposefully inundating a server with spurious requests, leading to delays or the deletion of legitimate requests before completion. When such exploitation transpires within a distributed system, where data is transmitted between numerous network devices throughout the network without centralized management, a DDoS attack ensues [7].

As IoT devices continue to evolve, mitigating DDoS attacks becomes increasingly challenging. DDoS attacks on IoT networks differ from other IoT threats in several key aspects. These attacks often involve a multitude of compromised devices that can generate and send out a substantial volume of traffic. Fig. 1 presents statistical data from past years, showcasing significant DDoS attack incidents and indicating a rising trend in both the frequency and severity of these attacks [8]. The graphical representation highlights notable spikes each year, underscoring that attackers target diverse industries with high attack rates.

According to Kaspersky's research [9], DDoS attacks saw a notable

* Corresponding author.
E-mail address: ankitjain@nitkkr.ac.in (A.K. Jain).

https://doi.org/10.1016/j.prime.2024.100543
Received 27 January 2024; Received in revised form 11 March 2024; Accepted 7 April 2024
Available online 9 April 2024

23 % increase in the first quarter of 2021 compared to the same period in 2020. The financial services industry emerged as the primary target, constituting 25 % of all DDoS attacks during the first quarter of 2021 [9]. Over the span from 2021 to 2022, the average magnitude of DDoS attacks rose by 31.8 %, escalating from 3.3 Gbps to 4.3 Gbps. Additionally, multi-vector attacks, which inundate the victim with various attack vectors, surged by 28.6 % [10].

The COVID-19 outbreak is suspected to have contributed to an upswing in DDoS attacks targeting the healthcare industry. Nexusguard analysis indicated a staggering 542 % increase in DDoS attacks during the second quarter of 2020 compared to the first quarter of that year [10]. In the realm of IoT devices, Neustar reported that in 2020, these devices accounted for 15 % of all DDoS attacks, up from 10 % in 2019 [11]. Furthermore, Akamai Technologies recorded a substantial 62 % increase in DDoS attacks against IoT devices in 2022 compared to the previous year [12].

The increasing complexity of IoT devices presents substantial challenges in mitigating DDoS attacks. DDoS attacks on IoT networks exhibit distinct characteristics compared to other IoT threats, often involving numerous compromised devices capable of generating substantial traffic [13]. Botnets, controlled groups of compromised devices frequently utilized for DDoS attacks on IoT networks, add to the challenge. Detecting and mitigating botnets is complex due to their elusive nature and the variety of attacks they can execute.

When a device detects a DDoS attack, it initiates the removal of suspicious flows, inadvertently resulting in a denial of service for legitimate users. Detecting and mitigating botnets is particularly challenging due to their decentralized structure and ability to launch diverse forms of attacks [14]. IoT devices may connect and coordinate through SDN technology, enabling centralized network traffic control and administration. SDN has emerged as a robust option for addressing security concerns in IoT contexts, providing flexibility, stability, and increased security [7,15,16]. The combination of IoT with SDN has given rise to the concept of an SDN-IoT platform, amalgamating the advantages of both technologies.

One significant benefit of SDN is its dynamic management capabilities, enabling the rapid detection and mitigation of DDoS attacks by creating and applying mitigation rules across the entire network. Mitigation involves reducing the impact of an attack on a specific network. Organizations employ various methods to mitigate DDoS attacks, tailored to the unique needs of their networks [15,17]. Given the diverse requirements of different networks, it is crucial to analyze and correlate various mitigation approaches for successful DDoS attack prevention, as merely deleting suspicious flows near the victim's location is insufficient.

The primary objective of this research is to assess multiple DDoS attack mitigation solutions utilizing Software-Defined Networking (SDN) and determine the most effective solution tailored to specific network requirements. Various mitigation solutions leveraging SDN capabilities were selected and categorized based on prior research on DDoS attack mitigation in both traditional networks and SDN environments. Each mitigation method is implemented and evaluated within an SDN environment to gauge its impact on the network. The assessment considers several variables, including the effects on attack packets, legitimate packets, and overall network processing. Additionally, the research investigates the optimal deployment site for the mitigation approach to minimize any adverse effects on genuine communications. The aim is to identify and recommend the most suitable DDoS attack mitigation solution in an SDN context, considering its effectiveness and impact on network performance.

1.1. Background data and historical context

The first documented large-scale Distributed Denial of Service (DDoS) attack occurred in 1999 [18], during which several high-profile websites, including Yahoo!, eBay, and Amazon, were targeted in coordinated attacks. Since then, DDoS attacks have evolved in terms of complexity, scale, and impact, solidifying their position as one of the most significant cybersecurity threats.

Several noteworthy DDoS attacks have left a substantial impact on the online landscape, highlighting the destructive potential of these attacks:

- In September 2016, the Mirai Botnet was utilized in one of the most notorious DDoS attacks. Capable of controlling approximately 3 million Internet of Things (IoT) device bots, it successfully targeted prominent websites [19] including Netflix, CNN, Twitter, and Reddit. With a bandwidth strength of 1.2 Tbps, it caused widespread disruptions and marked one of the largest attacks of the year.

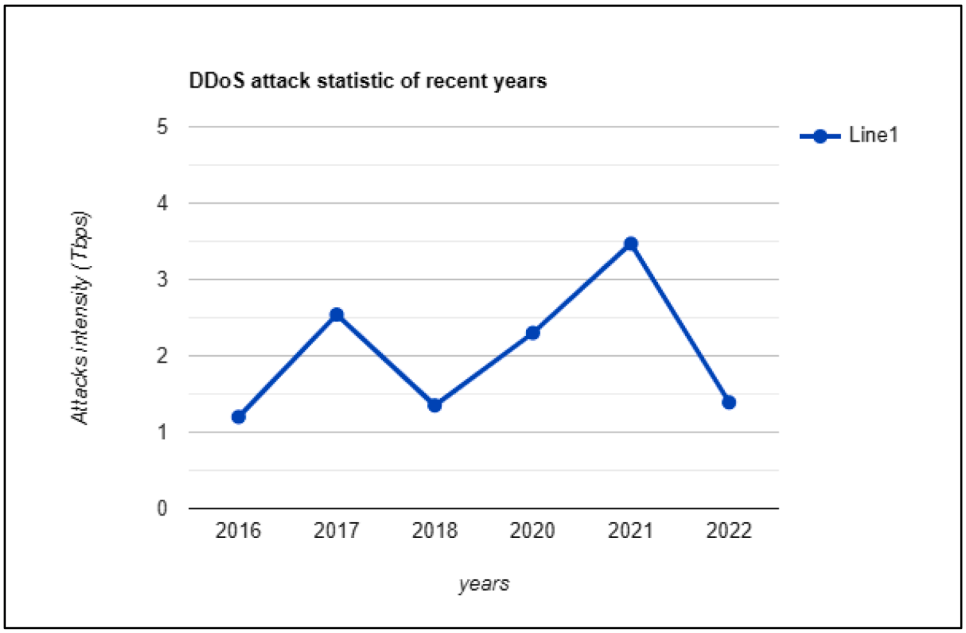

Fig. 1. Statistic of DDoS in IoT during 2016–23.

- In 2018, GitHub faced a massive DDoS attack, with peak traffic reaching 1.35 Tbps. To mitigate the attack, GitHub collaborated with DDoS mitigation provider Akamai Prolexic, resulting in a 10-minute platform outage [18].
- Amazon Web Services (AWS) encountered a significant DDoS attack in February 2020, reaching a volume of 2.3 Tbps. This attack surpassed other volumetric attacks by 44 %, highlighting the substantial scale of the threat [20].
- In September 2017, Google disclosed its successful defense against a 2.5 Tbps DDoS attack. This attack was the culmination of a six-month campaign that employed various techniques, retrospectively making it larger than previously mentioned attacks [21].
- Yandex, a Russian Internet giant, experienced a massive DDoS attempt in September 2021. The attack recorded an astonishing 21.8 million Requests Per Second (RPS) and spanned from August 7th to September 5th of that year [22].
- The most significant DDoS attacks ever observed by internet infrastructure organizations, such as Google Cloud and Cloudflare, were discovered in October 2023. The cloud service providers noted that these DDoS attacks were part of a larger scheme exploiting a zero-day vulnerability. Google stated that this was the largest DDoS assault "to date," reaching over 398 million requests per second (rps) at its peak [22].

These examples vividly illustrate the escalating scale and impact of DDoS attacks over time, emphasizing the critical need for robust defense mechanisms and continuous advancements in DDoS mitigation strategies. The ever-expanding threat landscape necessitates ongoing research and innovation to effectively combat and mitigate the disruptive effects of DDoS attacks. It underscores the importance of proactive measures and collaborative efforts within the cybersecurity community to stay ahead of evolving attack vectors and protect the resilience of online platforms and services.

The paper is structured into six distinct sections. The second section provides a historical context and background overview. Proceeding to the third section, various methods of executing Distributed Denial of Service (DDoS) attacks are examined. Section four outlines potential defensive measures against DDoS attacks. In the fifth section, a classification of numerous DDoS detection techniques is presented. Section 6 delves into mitigation strategies for DDoS attacks, detailing approaches such as blockage, controller relocation, and rate limiting. Finally, the concluding section summarizes the findings of the survey.

2. Technologies and architectures

These technologies and designs exemplify various DDoS attack strategies, each with its unique method of flooding or disrupting the target's networks, services, or resources. Enterprises and security specialists must comprehend these concepts to develop effective DDoS mitigation and prevention strategies.

2.1. DDoS attacks in IoT

In DDoS attacks, the attacker needs to remain anonymous to avoid detection by firewalls or other security systems at the target's location. To achieve this objective, attackers employ various intermediate technologies to carry out DDoS attacks. Fig. 2 depicts the architecture of a DDoS attack, wherein the attacker's host is shielded from direct interaction with the victim by multiple levels of compromised hosts, sometimes referred to as zombie hosts or botnets [23,13,24].

A botnet is a network of compromised computers, often called "Zombies," on which an attacker installs malicious software known as a bot. The primary goal of this strategy is to utilize the processing capacity of the compromised devices for various criminal operations. After installing the virus, the attacker gains remote control of these devices from different locations. The compromised workstations are then employed to send a large volume of spam emails, steal data, and potentially execute DDoS attacks.

Botnet-based networks are extensively utilized in these attacks [14], and the following botnet models serve as examples:

- **Agent-Handler model:** The Agent-Handler paradigm consists of clients, handlers, and agents, with handlers acting as intermediaries between the attacker or client and the agents. A crucial aspect of this paradigm is that the owners of the affected agent systems are often unaware that their systems have been infiltrated and are being used to launch DDoS attacks. Additionally, the attacker may interact with multiple handlers, installing handler software on compromised routers or network servers [14].

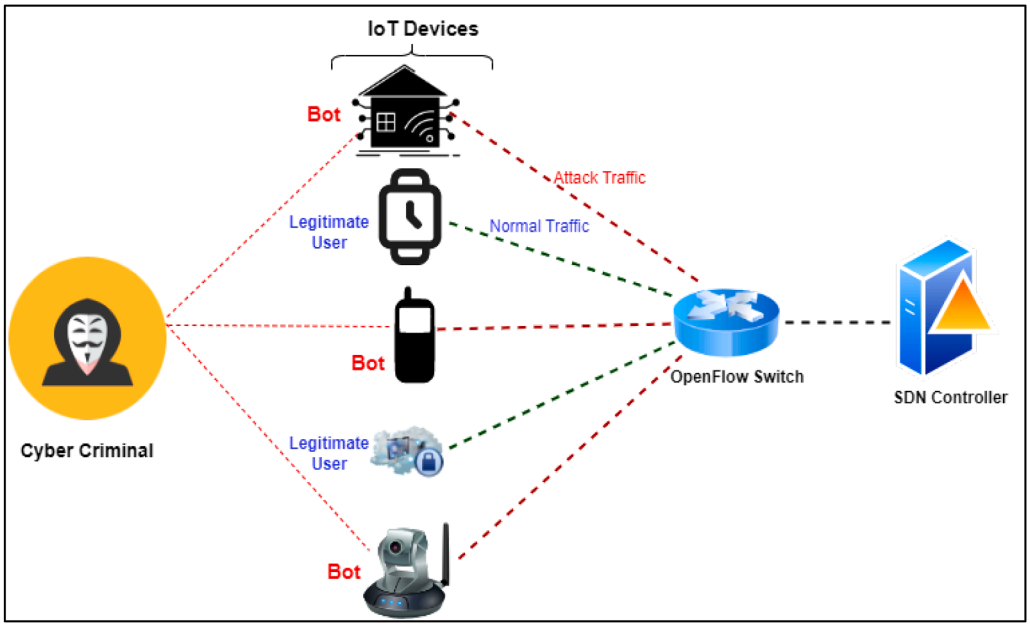

Fig. 2. Architecture of DDoS attack in SDN-IoT.

- **Internet Relay Chat (IRC) Model:** In the Internet Relay Chat paradigm, the client establishes connections with the agents via an IRC communication channel. This method aims to obfuscate the traceability of DDoS command packets, making tracking and identifying the source of the attack more challenging.
- **Web-based model:** This model involves submitting data to a website and offers various advantages over IRC. These benefits include simple deployment, reduced bandwidth requirements, the ability to support large botnets for dispersed load, traffic camouflage, resistance to filtering, and prevention of botnet hijacking.
- **AgoBot**: AgoBot is one of the most well-known bots, with over 600 variants discovered by antivirus vendor Sophos. Gaobot, Nortonbot, Phatbot, and Polybot are some of its versions [14].
- **SDBot:** With over 1800 variations, SDBot includes ping and UDP flooding features. SDBot's "SYN Flood Edition" executes Transmission Control Protocol (TCP) SYN flooding attacks. SDBot is primarily written in C++ and is intended for use on Windows computers.
- **RBot:** Similar to SDBot, RBot has over 1600 versions and is developed in C++ to target Windows computers.
- **SpyBot:** SpyBot is a program written in the C programming language that affects Windows computers.

2.2. SDN architecture

There are three planes in SDN: the Application plane, the Control plane, and the Data plane as shown in Fig. 3.

The application layer, situated at the top of the SDN architecture, plays a crucial role in managing business and security applications. This layer is responsible for executing essential software functions such as metering, routing, load balancing, intrusion detection systems, firewall deployment, and quality of service (QoS) mechanisms. Through the use of northbound APIs, the application layer establishes communication and integration with the lower layers of the SDN architecture, enabling seamless interaction with the rest of the system [16].

The control plane, positioned between the application and data planes, serves as the heart of SDN. It supervises the entire network, handling tasks such as packet forwarding, dropping, routing, and flow rule modifications through programmable interfaces [25,26]. While the controller is typically centralized, in distributed configurations, it interacts through eastbound and westbound APIs provided by Hyperflow [27] and Onix [28]. The control plane communicates with the data layer through the southbound API and the application layer via the northbound API. Lower-level devices such as switches, hubs, routers, and virtual switches like OpenvSwitch [29] constitute the data plane. The primary responsibility of this layer is to route packets based on the flow rules set within the physical device. The packet segment is sent to the controller for further processing and decision-making if no flow rules are identified in the flow table. SDN communication occurs through four interfaces, two of which facilitate plane-to-plane communication (southbound and northbound APIs), while the other two enable controller-to-controller communication (eastbound and westbound APIs).

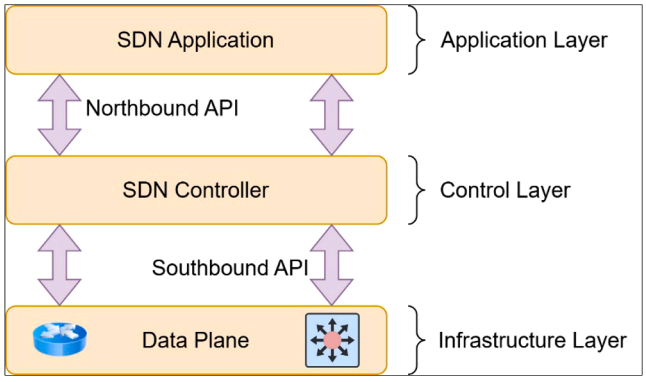

Fig. 3. Architecture of SDN.

Northbound APIs are employed to implement network regulations and to control network behavior. The controller informs application programs about network activity and resource availability using northbound APIs, connecting with the application plane. It is utilized by the application plane for activities such as latency computation, route selection, and security firewall configuration. Protocols like Procera and FML [15] utilize the Northbound interface.

Southbound APIs facilitate communication in the southward direction, enabling lower-level data plane devices, such as switches and routers, to communicate with the controller. The controller is responsible for managing flow rules, flow table entries, and altering the behavior of the switches. Protocols like OpenFlow [4] and Open Shortest Path First (OSPF) [7] are commonly used on the Southbound interface, with OpenFlow gaining widespread adoption due to standardization initiatives [6].

APIs for eastbound and westbound traffic enable the exchange of traffic between controllers. While SDN often employs a centralized approach with a single controller, in some cases, the controller network may be distributed, and communication between controllers occurs through eastbound and westbound APIs. Multiple controllers are employed to eliminate single points of failure, ensuring that if one controller fails, another can manage the traffic. Examples of interfaces using eastbound and westbound APIs include Google's Onix [28], Hyperflow [27], and ALTO [30]. These APIs play a crucial role in facilitating communication and coordination within the SDN architecture, enabling effective network control and administration.

2.3. Advantages of SDN over traditional networks

SDN offers significant benefits over conventional networks. The following are the advantages of SDN compared to traditional networks [31]:

- **Efficient Network Administration**: SDN allows network administrators to remotely modify network quality and transform network characteristics into programmable entities. Because network-wide modifications can be made promptly, this enables easy and dependable network management.
- **Network Programmability:** SDN enables centralized network administration, managing the entire network as a whole rather than separately controlling each network device. This programmability allows the creation of a distinct control layer that regulates the behavior of individual devices or the entire network. Programming can enhance traffic engineering skills, such as reducing network congestion.
- **Cost Savings**: Many SDN projects are open source, and free solutions like VMware NSX and Microsoft Hyper-V Virtualization are accessible. Compared to conventional networks, which require costly proprietary components, this lowers the cost of installing SDN.
- **SDN Service Expenses:** Because SDN eliminates the need for costly layer 3 components, capital expenses associated with network infrastructure are reduced.
- **Increased Security:** In today's digital environment, having strong security is critical. SDN allows for precise monitoring and tracking of all network devices, improving security and offering greater control over network access and rules.
- **Improved Reliability:** Automation is a critical component of SDN, allowing for dynamic network redirection and increased dependability. Network configurations can be changed on the fly, resulting in more efficient network operation and fewer interruptions.

2.4. SDN-IoT collaboration

The term "SDN-IoT collaboration" refers to the integration of technologies from the IoT and SDN. SDN is an architectural strategy that separates the control plane of the network from the data plane, enabling centralized administration and control of network devices. IoT, on the other hand, involves connecting numerous physical devices and things to the internet to facilitate data sharing and remote control [32].

Fig. 4 illustrates the collaboration between SDN & IoT, highlighting several advantages that enhance the capabilities of both technologies. The breakdown of their collaboration is as follows:

- **Enhanced Network Control:** SDN provides centralized management and programmability, enabling dynamic operation of network equipment. When paired with IoT devices, SDN can effectively handle different traffic patterns and meet the needs of IoT installations. Administrators can create and optimize network pathways, allocate bandwidth, and enforce security standards based on the unique requirements of IoT applications [33].
- **Efficient Resource Management:** IoT implementations may involve a large number of devices with varying communication needs. SDN's centralized control allows for effective resource allocation, ensuring that devices receive the necessary network resources. For example, SDN can prioritize essential IoT traffic over non-critical traffic, enhancing resource utilization and overall network performance.
- **Scalability and Adaptability:** With the anticipated tremendous growth of IoT networks, SDN's scalable design can support this expansion by providing a flexible infrastructure that adapts to changing network requirements. The separation of the control plane and data plane allows for network expansion by adding or removing devices without disrupting the entire network.
- **Security and Privacy:** IoT devices are often vulnerable to security attacks due to their low computing resources and lack of built-in security procedures. SDN can assist in addressing these challenges by establishing centralized security policies, implementing traffic monitoring, and detecting threats. It enables network administrators to enforce network-level security measures, offering improved protection against cyberattacks and unauthorized access to IoT devices [14].
- **Traffic Optimization and Quality of Service (QoS):** IoT applications exhibit varying traffic patterns, from real-time data streams to periodic or event-triggered transfers. SDN's programmability allows the use of intelligent traffic routing algorithms, traffic shaping, and QoS mechanisms to prioritize and optimize IoT traffic flows. This collaboration enables optimal network resource utilization and enhances the overall user experience.
- **Data Analytics and Insights:** IoT generates vast amounts of data, and SDN can help to capture, process, and analyze this data. SDN controllers can gather and aggregate data from IoT devices, providing administrators with valuable information for network optimization, anomaly detection, and decision-making processes.

3. Taxonomy of DDoS attacks in SDN-IoT network

DDoS attacks pose a serious concern, disrupting service availability and breaching a fundamental premise of service delivery. The intensity of DDoS attacks is influenced by various factors, including the type of attacks, the protocols or vulnerabilities exploited, the number of compromised attacker hosts, the involvement of unaffected hosts in the attack, the resource capacity at the victim's site, the defensive measures and network topology employed, and the resource capacity of the attacker's components [14]. DDoS attacks involve the intentional flooding of traffic or connection requests directed against a network, system, or

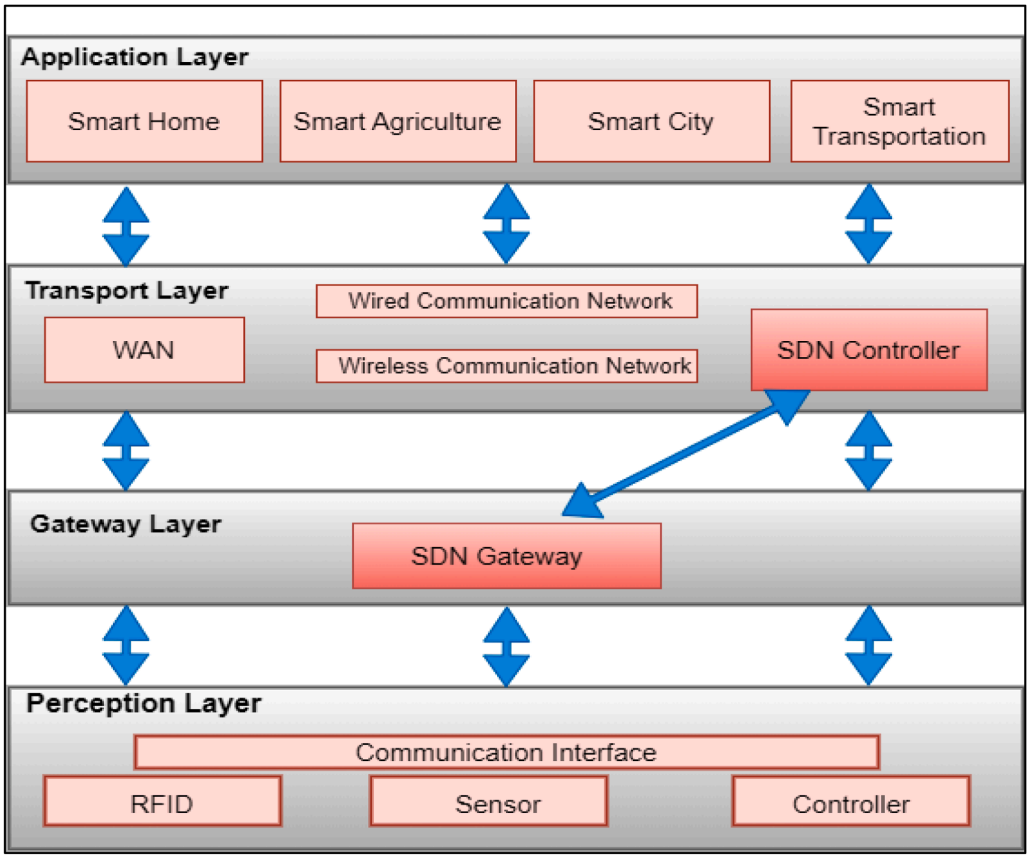

Fig. 4. Architecture of SDN-IoT network.

website. These attacks manifest in various forms, and the taxonomy of DDoS attacks is illustrated in Fig. 5.

- **Bandwidth Attack:** Bandwidth attack exploits vulnerabilities in a network's architecture intending to flood the network with data traffic. The primary objective is to overwhelm the network's existing bandwidth and other resources, disrupting regular network functioning. Attackers flood the network with an excessive amount of data packets, leading to congestion and hindering legitimate users' access to network services. Amplification is another strategy employed in DDoS attacks, where the attacker uses DNS or NTP services to make network queries to the target network, masking the sender's IP address as the victim's. The resulting DNS or NTP responses are significantly larger than the original queries, overwhelming the target network's resources [9,12,34,35].
- **Connectivity Attack:** Connectivity attack focuses on weaknesses in network protocols and services. The attacker inundates the victim with connection requests, depleting the system's resources. The goal is to overload the victim's operating system, including CPU, memory, and network stack, impairing its ability to process legitimate user requests.
- **Resource Exhaustion Attack:** Resource exhaustion attack aims to deplete critical resources, such as memory, CPU, or disk space, on the target. The attacker achieves this by making requests or performing activities that consume a large number of resources. The depletion of essential resources renders the target system or service inaccessible to authorized users [36,37].
- **Limitation Exploitation Attack:** Limitation exploitation attacks intentionally target limits or flaws in a system's design or configuration. The attacker capitalizes on these flaws to create interruptions or service outages. For instance, an attacker might exploit a server's restriction on the maximum number of concurrent connections, flooding it with connection requests and rendering it unable to service genuine users.
- **Process Disruption:** Process disruption attacks target specific processes or services running on the targeted system to exploit vulnerabilities. Attackers identify flaws in protocols, programs, or services and conduct a DDoS attack to take advantage of these flaws. This may cause the targeted processes to use excessive resources, become sluggish, or even crash, resulting in system interruptions [4].

3.1. Taxonomy of DDOS attacks on IoT layers

DDoS attacks may occur individually or concurrently across various levels, depending on the attacker's objectives and the vulnerabilities present in the IoT network. Therefore, Fig. 6 illustrates all the possible ways that IoT networks could be attacked at each level.

DDoS attacks are frequently launched using numerous bots, which are network nodes infiltrated and controlled by the attacker. Flooding is a common tactic employed in direct attacks, where many bots send repeated packets to the target. TCP SYN floods, UDP floods, ICMP floods, and HTTP floods are examples of such attacks [108–110].

TCP SYN flooding and other protocol exploitation attacks exploit vulnerabilities in the TCP connection setup process. The attacker sends TCP SYN packets to the victim's infrastructure without providing ACK answers, utilizing the victim's system resources [38]. Automated scripts may also be used to saturate the communication channel alongside the victim's infrastructure with TCP flags such as ACK, PUSH, RST, and FIN packets.

Ping of death and land attacks are two additional types of DDoS attacks. Ping-of-death attacks involve issuing Ping instructions with packet sizes larger than the maximum allowable size (65,536 bytes) to cause the target machine to crash. In land attacks, the attacker sends forged packets with the same sender and destination IP address, instructing the victim to transmit the packet to itself, resulting in an unending loop and the victim's computer crashing [38]. Furthermore, DDoS attacks may exploit zero-day vulnerabilities to infiltrate legitimate PCs and execute effective denial-of-service attacks [39].

3.1.1. Application-layer DDoS attacks

Attacks on the application layer [2] aim to compromise the security of IoT network infrastructure by exploiting vulnerabilities in programs or web servers through techniques such as HTTP (GET/POST) calls and other queries directed at system software like Windows, Apache, OpenBSD, and others. This results in a large number of lost packets, often measured in requests per second (Rps), reflecting the attack's frequency. These attacks present a greater detection and mitigation challenge since they generate traffic at a slower rate, and the requests they submit seem legitimate, initiating backend procedures that drain system resources. DNS service attacks, HTTP floods, and other related tactics are examples of such attacks.

These risks are similar to classic DoS/DDoS attacks. They broadcast HTTP GET and HTTP POST requests, which are large-volume application-layer queries, to a target. However, these dangers focus on the

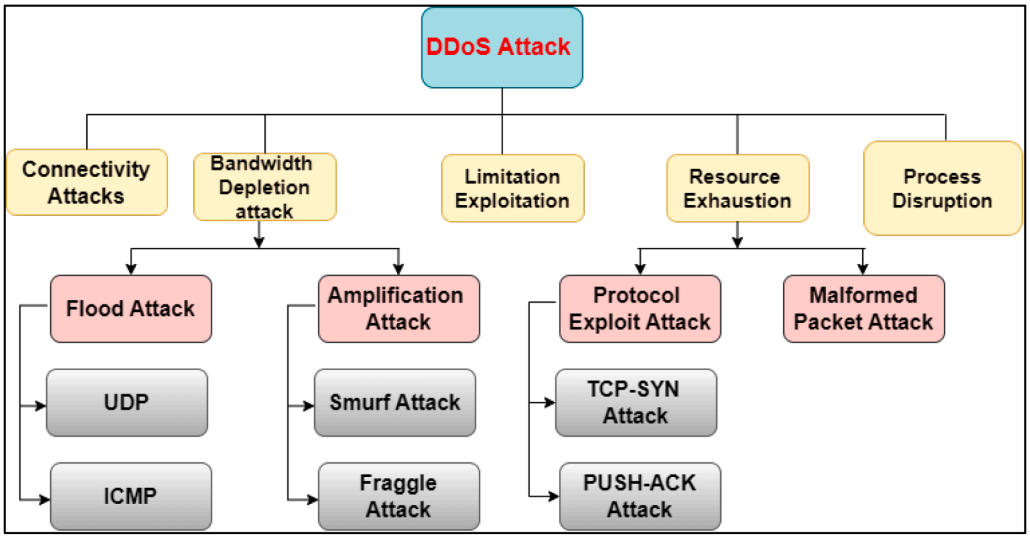

Fig. 5. Taxonomy of DDoS Attacks.

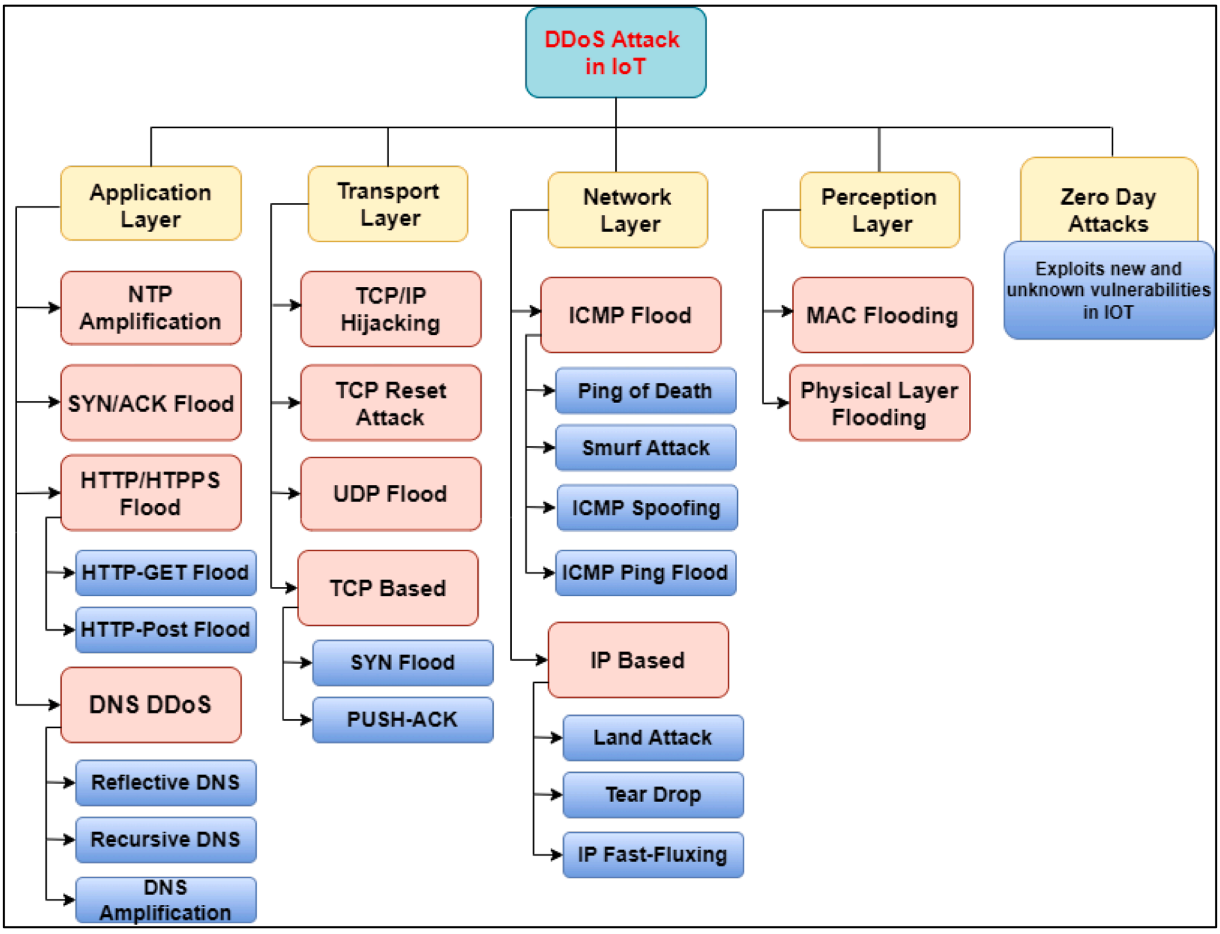

Fig. 6. Taxonomy of DDoS Attacks in IoT Layers.

server's resources and require less malicious traffic. The DoS GET attack targets a web server or application by mimicking valid HTTP GET requests. Multiple synchronized computers may be used in this attack to generate a large number of GET requests for a specific item from a targeted site, such as graphics. When the target is overwhelmed with incoming requests and responses, subsequent requests from valid traffic sources will experience denial-of-service. The issue of amplification is posed by distributed and rejected domain name servers (DrDNSBots used in a DrDNS attack send UDP-based queries to an open DNS server with a fictional IP address that has been changed to match the genuine source IP address of the intended target. Because UDP is a connectionless protocol, it is possible to receive very large replies from a short request. Additionally, since the true IP address is concealed, it turns into a reflection attack [6].

3.1.2. Transport layer DDoS attack

When a DDoS attack targets an IoT network's transport layer, it aims to overload the communication protocols used for data transfer. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are two protocols employed at the transport layer to facilitate reliable and efficient data flow between IoT devices. The objective of an attacker in a transport layer DDoS attack on an IoT network is to disrupt the normal flow of data or render the network inaccessible to authorized users. Here's how such an attack may unfold:

- **TCP SYN Flood Attack:** A prevalent form of transport layer DDoS attack is the TCP SYN flood attack. In a TCP connection, a three-way handshake transpires between the client and the server: SYN (synchronize), SYN-ACK (synchronize-acknowledge), and ACK (acknowledge). During an SYN flood attack, the attacker inundates the network with a substantial number of SYN requests but refrains from responding to the server's SYN-ACK. Consequently, the server remains in anticipation of the ACK, depleting its resources and hindering the establishment of valid connections.
- **UDP Flood Attack:** Another variant of transport layer DDoS attack is the UDP flood attack. In contrast to TCP, UDP is a connectionless protocol that does not necessitate a handshake. In a UDP flood attack, the attacker deluges the target's IP address with UDP packets, overwhelming the network's capacity and depleting its resources. Since UDP does not validate data or ensure its delivery to the intended receiver, a flood of packets can rapidly overload the network, causing congestion and disrupting communication between IoT devices [40].

3.1.3. Network layer DDoS attacks

Multiple devices, sensors, and actuators are interconnected in a typical IoT network to exchange data and interact with one another and other systems. A DDoS attack targets the network layer, responsible for routing and sending data packets across the network. It involves flooding the network infrastructure with a massive amount of malicious traffic, rendering the network and its connected devices inaccessible or significantly degrading their performance. A DDoS attack seeks to disrupt the IoT network's regular operation by overwhelming its resources and depleting its ability to respond to valid requests. To exploit vulnerabilities and undermine network availability, the attacker may target individual devices, gateways, or even the network infrastructure itself. DDoS attacks on IoT networks must be prevented by protecting IoT devices, installing network traffic monitoring and anomaly detection

procedures, and applying DDoS mitigation strategies to maintain network availability and integrity [41].

3.1.4. Perception layer DDoS attacks

DDoS attacks on the perception layer of an IoT network target the components responsible for sensing and collecting data from the physical environment. The attacker's goal is to disrupt data collection and transmission by overpowering or compromising these perception layer devices, thereby weakening the overall operation of the IoT network.

Protecting against DDoS attacks on the perception layer requires a multi-layered protection strategy. This involves enforcing strict access rules, regularly updating and patching the firmware and software of IoT devices, monitoring sensor data for abnormalities, and deploying anomaly detection tools. Encryption and authentication procedures may also be employed to secure the integrity and authenticity of data sent between perception layer devices and the network.

3.1.5. Zero day DDoS attack

This new terminology has just been suggested as one of the classifications to separate those unknown or unique DDoS attacks that make use of the service's vulnerabilities. The community of attackers now often uses this tactic [41].

4. Classification of DDoS defense mechanism in SDN-IoT networks

Extensive research has been conducted over the last two decades to identify and successfully mitigate DDoS attacks. Various mitigating techniques have been proposed, each with different deployment areas and times [42]. These location-based deployment options are classified into four categories:

i. Implementation of source-based defense in the perimeter routers or the source Autonomous System (AS) of the attack source.
ii. Destination-based routing implementation at the victim edge routers or victim AS level.
iii. Network-based defense, often implemented by Internet Service Providers (ISPs) and critical networks, is typically required to respond to attacks at the intermediate network level.
iv. Hybrid defense integrates methods at the source, destination, and network levels.

Source-based defenses aim to detect and mitigate attacks in their early stages, yet separating genuine from malicious DDoS traffic at the source level remains a challenging issue. On the other hand, destination-based defense measures are simpler and less expensive to develop, as they focus on the victim's vicinity. However, the attack traffic consumes resources along the channels leading to the victim before discovery. DDoS attacks are detected and mitigated at the AS or ISP levels, which are closer to the attack sources. Implementing these solutions increases network infrastructure storage and processing costs, potentially necessitating the use of additional DDoS prevention devices, such as middle boxes, for effective traffic handling. Furthermore, the identification of attacks becomes difficult due to a lack of aggregated traffic specifically intended for the victim.

Mitigating attacks in the internet core provides benefits by preventing attack traffic from reaching the victim's network, minimizing congestion in communication channels, and preserving the victim's computational and network resources. This method is particularly useful for mitigating network-wide effects [4].

The hybrid defense technique, which combines various defense measures to prevent DDoS attacks, is a more robust strategy. The hybrid strategy offers greater resilience by combining source, destination, and network-based strategies. Moreover, detection and mitigation can be more effectively carried out by installing defenses at the destination or network level and using mitigation strategies close to the attack sources. However, adopting a hybrid defense plan is challenging as it requires coordination and cooperation among multiple groups [42]. Establishing trust among stakeholders is crucial for the successful transmission of attack information, especially given the variety of service providers.

4.1. DDoS attack and honeypot defense in SDN

Unlike traditional designs, the SDN controller in Industrial Internet of Things (IIoT) environments offers centralized device management, providing enhanced flexibility in resource utilization and control [43]. However, SDN is susceptible to DDoS attacks, where a large number of packets with forged source addresses are injected into SDN servers. These packets, when unable to find a match in the switch's rule tables, are forwarded to the SDN controller. The influx of legitimate and spoofed packets exhausts the controller's resources, leading to exhaustion. Consequently, the SDN controller becomes unresponsive to legitimate data packets, potentially causing the entire SDN to fail. Exploiting this situation, hackers can compromise IIoT nodes and disrupt their normal operations.

To address these challenges, honeypots are employed to attract attackers, gather evidence, and conceal actual servers. By incorporating honeypots within authentic servers, an internal network is created, leveraging the honeypots' network port mapping to enhance the security of the genuine servers. Even if attackers breach the external "servers," they are unable to obtain critical information as they are inadvertently targeting the honeypots instead [44].

Several ways have been developed to effectively combat DDoS attacks and improve honeypot-based security measures. The IHoneycol method, developed by Zhan et al. [45], efficiently handles the issue of DDoS attacks. Jiang et al. [46] proposed the Collapsar architecture, which employs virtual machines to collect attacks and monitor high-interaction virtual honeypots inside a black hole. Honeypot back-propagation, a sophisticated hop-tracking approach described by Walfish et al. [47], allows accurate attack signature detection using a roaming honeypot strategy. Wang et al. [48] suggested a honeypot detection approach that detects attackers inside honeypot botnets to counteract botnet attacks. Hayatle et al. [49] provided a system that enables botmasters to accurately analyze the performance of hacked computers. These novel ideas help to build effective tactics for reducing DDoS attacks and improving honeypot detection and response capabilities in cybersecurity systems.

4.2. Moving target defense (MTD)

MTD [50] is a proactive cybersecurity approach that involves regularly modifying the configuration and behavior of a network to enhance ambiguity and complexity for attackers. As a result, the attackers' window of opportunity is narrowed, and the cost and effort needed for exploring and launching effective attacks are increased. SDN has various advantages for applying MTD approaches, including network programmability, centralized control, and a global view of the network [51]. These characteristics allow for the effective and flexible regulation of random host mutation, which is an important part of MTD.

In the IoT context, SDN-based honeypots play a critical role in fighting against DDoS attacks. Honeypots are meant to resemble IoT devices to attract intruders, enabling them to be accommodated and captured. Organizations can identify and mitigate several sorts of attacks by installing SDN-based honeypots, such as scanning-based attacks, SSH-based attacks, Telnet-based attacks, and SYN flood attacks. The combination of MTD and SDN-based honeypots is an effective way to improve IoT network security and limit the effects of DDoS attacks. The suggested methodology's usefulness has been proved by experimental data. Organizations may effectively identify and prevent many sorts of threats by using MTD approaches and exploiting the capabilities of SDN-based honeypots. This method not only improves IoT network security but also allows proactive defense measures, enabling

organizations to keep one step ahead of attackers. Organizations can successfully disrupt attackers' reconnaissance attempts and raise the cost and complexity of launching successful attacks by continually changing and developing network setups. Experimentation also indicated that suggested MTD and SDN-based honeypot methods can detect and neutralize scanning, SSH, Telnet, and SYN flood attacks [52].

4.3. Blockchain-based defense strategies

A blockchain is a type of distributed ledger technology that consists of an immutable and ever-growing chain of blocks. Each block includes digital data such as the preceding block's hash and a timestamp [53]. The blockchain's security is secured through cryptographic algorithms and smart contracts [33], which are self-executing programs. Smart contracts are critical to the security of blockchain-based systems, particularly communication between distributed servers and IoT devices. Smart contracts and decentralized apps (DApps) may be created on popular platforms like Ethereum, Bitcoin, and Pi. For example, Ethereum has a state-based approach in which data is kept in blocks, and transactions are confirmed by network nodes. Ethereum incorporates resource restrictions to avoid system overload and possible attacks. Once the barrier is reached, further resource consumption is disabled. This method prevents DDoS attacks by limiting the availability of resources.

Single-point failures may be reduced by incorporating Ethereum into an IoT network, known as an IoT-Ethereum network [23]. The network's smart contract keeps a list of authorized devices or nodes and checks service requests against this list before granting access. This method efficiently restricts resources and protects against DDoS attacks. Even if all nodes in the network request resources for a DDoS attack at the same time, Ethereum's resource limit feature disables services if the maximum limit is reached.

Blockchain technology's [36] openness and decentralized data storage contribute to its usefulness in reducing DDoS attacks. These characteristics make it difficult for attackers to breach the system. Organizations can strengthen their networks' resistance against DDoS attacks by exploiting blockchain's capabilities, while also ensuring transparency and rigorous data security.

4.4. Ensemble voting (EV)

EV combines the strength of many distinct classifiers, including SVM, Logistic Regression (LR), Random Forest (RF), KNN, Naive Bayes (NB), and others. The purpose of EV [54] is to create a single, robust model that outperforms any of the separate classifiers. During the creation of the ensemble voting model, the voting strategy is set to "Hard." In hard voting, each classifier in the ensemble votes for a single class. The final prediction is made based on the class that receives the most votes. This method relies on the collective decision-making of individual classifiers, with the majority vote serving as the decisive element for the ensemble's prediction.

On the other hand, in soft voting, each classifier delivers a probability value to each data point, indicating the chance that it belongs to a certain target class. To calculate the final prediction, these probability values are combined, often by average or weighted averaging. Soft voting considers the confidence ratings of the different classifiers, incorporating their probabilistic outputs to make a more informed decision.

Ensemble learning is used in combination with ensemble voting to improve the accuracy of anomaly detection, as detailed in [55]. Ensemble learning involves using multiple models to jointly generate predictions or judgments. The combination of ensemble voting and ensemble learning approaches aims to enhance the overall performance and reliability of anomaly detection. Within the ensemble learning framework, ensemble voting allows the model to leverage the diverse viewpoints and skills of individual classifiers. Each classifier contributes its expertise and knowledge to the ensemble, enhancing the model's ability to identify abnormalities in the data. By using ensemble voting, the model can mitigate the shortcomings or biases inherent in individual classifiers and reduce the risk of overfitting. The use of multiple classifiers enables a more robust and comprehensive data analysis, leading to improved anomaly detection performance.

4.5. Change point detection algorithm for DDoS

SDN provides advantages such as flexibility and reuse, but its centralization and plane separation raise security risks. Existing DDoS detection algorithms in SDN often ignore WSN computational and power constraints, leaving room for improvement.

Based on change point analysis [56], the goal of this research is to offer a lightweight and efficient DDoS detection approach for WSNs. This approach is suitable for WSNs due to its high detection rates and linear complexity. The detection method identifies and addresses irregularities in the data packet delivery rate. The detector's performance is assessed in software-defined WSNs with varying node counts and attack intensities. The findings show that as the attack strength increases, the detection rate approaches 100 %, and the nature of the attack can also be determined.

In addition, the paper discusses three kinds of security vulnerabilities in SDN networks: application plane attacks, control plane attacks, and data plane attacks. Control plane attacks are deemed high-impact and enticing because they influence network management. SDWSNs (software-defined wireless sensor networks) are vulnerable to comparable risks and vulnerabilities, with additional attacks exploiting resource constraints such as storage capacity, restricted bandwidth, and device processing power. A potentially weak connection between the SDN controller and the WSN is detected, demanding the adaptation or creation of security mechanisms intended for typical SDN networks to fit SDWSNs.

The research focuses on applying the change point approach to SDWSNs in two different attack scenarios: fake data flow forwarding (FDFF) and false neighbor information (FNI). Simulations use grid topologies with variable numbers of attackers. To monitor changes, the proposed DDoS attack detection method assesses network parameter mean values. Effective attack detection is enabled by monitoring either the data packet delivery rate or the control packet overhead, with different metrics performing better for different attack types. The detection rate grows with attack intensity and detects attacks within a few samples after their commencement [45].

4.6. DDoS attack defense in SDN-based cloud

The rise in DDoS attacks in cloud computing [57] settings can be attributed to several cloud-related factors. Features such as quick flexibility, usage-based pricing, extensive network access, on-demand self-service, and resource sharing enable attackers to exploit and target cloud customers' financial stability, leading to attacks such as Fraudulent Resource Consumption (FRC). The cloud's pricing mechanism, along with its quick flexibility, allows attackers to exploit excessive resources and compromise cloud clients' financial stability through DDoS attacks. Furthermore, due to the cloud's broad network access, attackers can use mobile devices as launch pads for DDoS attacks, taking advantage of high-speed internet technologies to overwhelm victims.

Botnets play an important role in DDoS attacks, and the cloud's on-demand self-service capabilities make it easy for attackers to construct enormous botnets. The presence of such large botnets increases the likelihood of DDoS attacks on cloud systems. Additionally, since the cloud architecture is multi-tenant, with several clients hosted on a single physical server, an attack on one customer might affect all customers using the same computer. The cloud's quick elasticity exacerbates the effects of DDoS attacks, distributing them to all cloud customers.

The integration of SDN with cloud computing brings both positive and negative consequences for cloud DDoS mitigation. SDN features that

can assist in DDoS attack detection and mitigation include the separation of the control plane from the data plane, a logically centralized controller, a global network perspective, network programmability, and software-based traffic analysis. SDN enables large-scale attack and defense testing in real-world settings, provides centralized network information for effective security rule generation, and supports the utilization of existing DDoS defense systems.

However, SDN is susceptible to various security issues, including flow table attacks, malicious applications, unauthorized access, configuration issues, and data leaks. The functional planes of the SDN architecture and their communication interfaces are vulnerable to DDoS attacks. Attackers may interrupt communication between SDN entities and the controller by targeting communication interfaces. Fake flows may overload the data plane switches' limited flow table space. The SDN controller, as the key decision-maker, is a prominent target for DDoS attackers. Third-party apps on the application plane pose a risk, as malicious or hacked apps can compromise the entire security of the SDN system [14]. Furthermore, Table 1 provides a brief overview of each defense mechanism's model, key points, and potential limitations.

5. Taxonomy of DDoS attack detection techniques in SDN-IoT network

The taxonomy divides detection methods into different groups based on the basic ideas behind them. First, anomaly-based methods analyze the patterns of network data to identify deviations from normal behavior. This allows the detection of new or unknown attacks. Second, data-mining methods utilize established patterns to match incoming data, enabling the recognition of known attack fingerprints. Third, statistical methods employ data analysis and modeling to identify unusual changes in traffic, which may indicate signs of DDoS attacks. Additionally, methods based on machine learning utilize algorithms that learn and adapt to changing threats, facilitating the recognition of new attack trends. Finally, hybrid methods combine more than one method to create a more comprehensive and accurate monitoring system, enhancing the resilience of SDN-IoT networks against DDoS attacks.

5.1. Anomaly-based detection

Anomaly-based detection systems establish a baseline using ML methods, statistical analysis, and behavioral modeling, as illustrated in Fig. 7. These systems examine new data to detect any unusual patterns, such as a sudden increase in network traffic, rapid changes in user access patterns, unexpected resource utilization, or other abnormal behaviors that could indicate an attack. By continuously learning and adapting to new patterns, these systems can identify emerging threats that may not exhibit clear signs [6].

- **Data Collection:** LEDEM collects and analyzes network traffic data, including flow records, packet headers, payload content, and other relevant information. This data is typically obtained from network devices, intrusion detection systems, or specialized sensors deployed across the network architecture.
- **Feature Extraction:** Various features are extracted from the collected data to represent different aspects of network traffic behavior. These features may include packet rates, packet sizes,

Table 1
A comparison of existing DDoS defense techniques in SDN-IoT Network.

Defense mechanism	Model	Key points	Vulnerabilities
Honeypot-based defense [58]	The use of a decoy system in conjunction with the IDS enables the redirection of attack traffic.	• When the likelihood of an attack increases, the honeypot is utilized to divert incoming attack traffic instead of directly reaching the main server. • By identifying any unfamiliar malware within the honeypot, valuable insights about the attack can be actively obtained, enabling future detection of similar attacks.	• Although the system is not suitable for real-time implementation, it can be utilized by connecting it to a central server through a microcontroller interface. • The system cannot effectively handle volumetric attacks that employ large botnets.
Mobile Edge Computing-based defense [59]	DDoS attack detection employs filters at the network's perimeter.	• A central controller is in charge of controlling and regulating all of the smart filters. • The filters may improve themselves and use self-organizing map filters to train autonomously.	• The central controller is susceptible to attacks, leading to the defense system's failure.
Blockchain-based Defense [60]	Smart contracts within the blockchain are self-executing programs.	• The gadgets used in this system are thought to be fully safe and unaffected under any circumstances.	• It is impractical to expect the gateway to stay unaffected during a DDoS attack. • The gateway is incapable of dealing with sophisticated botnet attacks.
SDN-based Defense [61]	The SDNi extension is utilized to address DDoS attacks across numerous SDN domains.	• By isolating and reconfiguring the targeted device, the attack is prevented from reaching network firewalls or other monitoring systems. • Congestion difficulties are reduced, and the attack is kept from escalating as a result of hostile IoT devices.	• The centralized control mechanism of the system poses a security threat. • The system's ability to detect newer types of attacks may be limited.
Machine learning-based defense mechanisms [62]	Supervised and unsupervised learning models and Neural network	• Capable of detecting attacks with a low amount of false positives. • Capable of detecting both traditional and IoT-based DDoS attacks using a variety of categorization techniques.	• The correctness of a dataset used to train the system to detect DDoS attacks in IoT has a direct influence on its dependability.
Hybrid IDPS [63,13]	The Intrusion Detection Prevention system utilizes a combination of Signature-based and Anomaly-based detection methodologies.	• The approach is capable of detecting both unknown attacks and DoS attacks. • Integrating the methodologies has resulted in a higher detection rate, leading to faster detection.	• The detection approach is more successful for detecting DoS attacks but is less effective for detecting DDoS attacks. • The anomaly-based detection technique occasionally produces more False Positives.
Deep Learning-Driven SDN-based Hybrid Mechanism [32]	Deep Learning models have been implemented on the SDN-enabled IoT network by the researchers.	• The SDN controller monitors and reports network anomalies. • Implementing deep learning models on the control plane allows for effective detection of DDoS and penetration attacks.	• Deploying the model over a large network becomes more challenging due to its hybridization, which adds complexity to the process. • The accuracy of Deep Learning models relies heavily on the dependability of the dataset utilized for training and testing purposes.

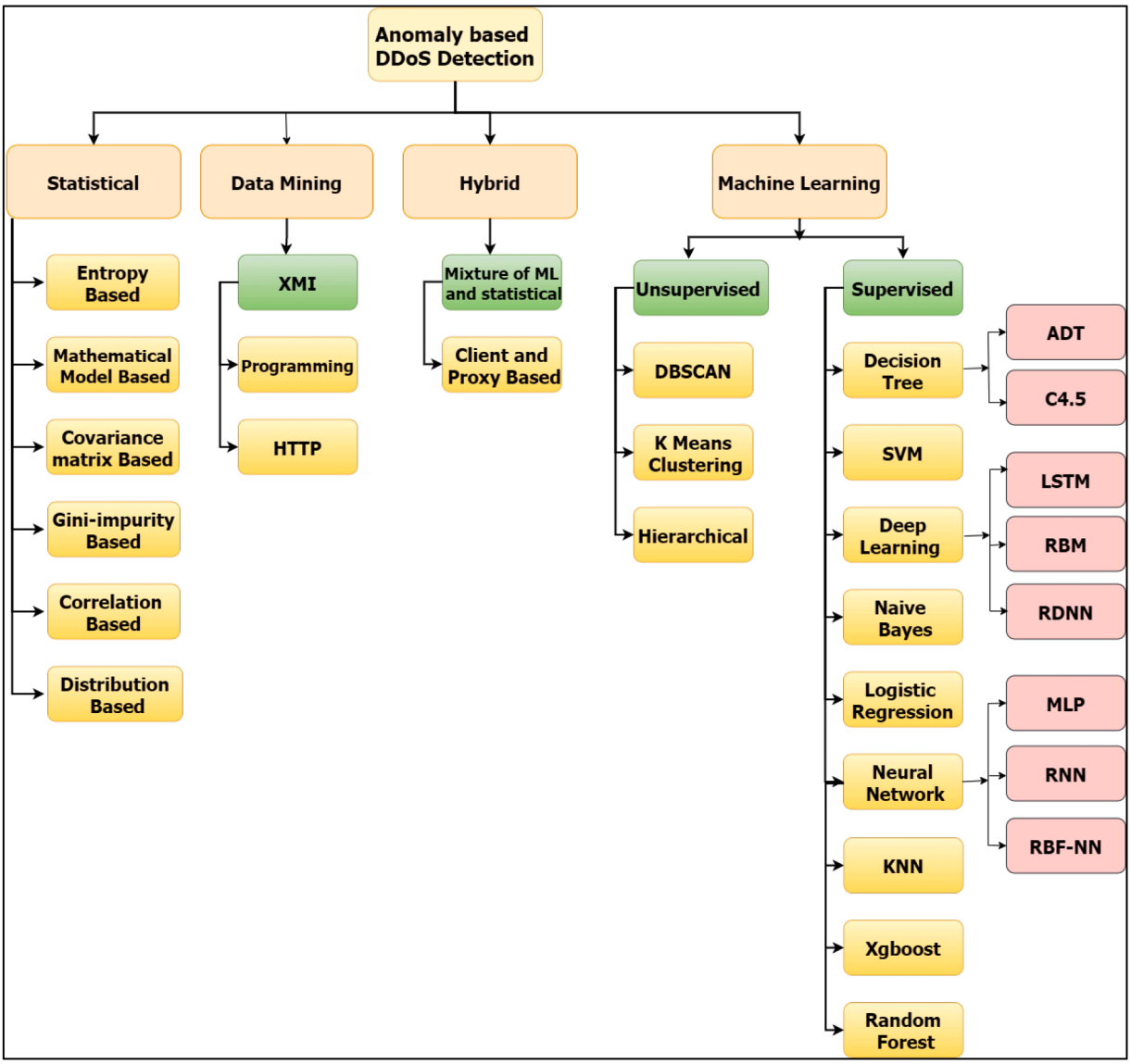

Fig. 7. Taxonomy of anomaly-based DDoS detection.

traffic distribution, protocol distribution, application-layer statistics, and other relevant elements.

- **Training Phase:** During the training phase, machine learning methods are applied to the collected data to build a model that replicates typical traffic behavior. This process involves preprocessing the data, identifying relevant features, and training the model using supervised, unsupervised, or semi-supervised learning approaches.
- **Anomaly Detection:** After training, the model is employed to identify anomalies in real-time network data. Deviations from normal behavior are flagged as potential DDoS attacks. Anomaly detection methods, such as statistical analysis, clustering algorithms, or neural networks, may be utilized for this purpose.

5.2. *Learning-driven detection and mitigation (LEDEM)*

LEDEM is a strategy that leverages machine learning and artificial intelligence approaches for the detection and mitigation of DDoS attacks. The primary focus of LEDEM is on continuous learning and adaptation to evolving attack patterns, thereby enhancing the effectiveness of DDoS defense mechanisms. The central concept of LEDEM involves the use of machine learning algorithms to analyze network traffic patterns, identify anomalies, and take proactive measures to neutralize attacks in real-time. When an anomaly is detected, LEDEM generates alerts or notifications to inform network administrators or security personnel about a suspected DDoS attack. These notifications typically include details about the identified anomaly, the impacted resources, and the severity of the attack.

It is crucial to understand that LEDEM is an adaptable and iterative method. The detection and mitigation systems within LEDEM continually learn and update their models based on fresh data and input. This adaptive nature enables them to respond to emerging attack strategies and changes in network conditions. LEDEM's adaptability allows it to provide effective and efficient DDoS defense while minimizing false positives and false negatives [33].

Table 2 provides a brief overview of different machine learning/deep learning detection techniques used for DDoS attack detection, including references, whether the experimental evaluation was conducted, the dataset used, remarks about the technique, features considered, performance achieved, and any additional remarks or considerations.

Table 2
A comparison of current ML/DL detection techniques in DDoS attacks.

Ref.	ML/DL	Exper.	Dataset	Features	Performance	Remark
[64] Hung	KNN, DT, NN	A real testbed	CAIDA 2007	IP and port address	Accu. =98 %	A minimally invasive defense approach is implemented with a monitor window period that offers flexibility.
[65] Sahoo	SVM, KNN, RF	Mininet	NSL-KDD	Not mentioned	Accu. =99 %	SVM produces the best result
[66] Seah	SVM, KNN, NB, DT, DA	VM	ISCX data	Packets count, byte count, and flow duration	Accu. =92 %	While ML/DL can serve as a classifier in SDN, the selection of appropriate characteristics for enhanced detection poses a significant challenge.
[67] Polat	SVM, KNN, NN, NB	VM	Self-generated	12 features	Accu. =98 %	The accuracy of detection can be enhanced by performing feature selection to filter out essential features before training.
[68] Dong	SKNN, NB, SVM	Mininet	Self-generated	Flow rate, speed, length, duration	Accu. =91 %	The performance of the basic KNN model can be significantly improved by incorporating a weighted value for the neighbors. Through simulations, the results demonstrate remarkable efficiency gains.
[69] Hussain	NB	Real testbed	NSL-KDD	25 features selected	Not mentioned	Within the ISP sector, the suggested DDoS mitigation approach has demonstrated tremendous potential and success.

6. Taxonomy of DDoS attack mitigation techniques in SDN-IoT network

SDN controllers dynamically implement mitigation policies across the entire network. The relevant literature on DDoS attack mitigation in SDN networks, including prior work [70] and conventional network DDoS mitigation systems, has been evaluated to identify these approaches. Consequently, the mitigation strategies have been categorized into four main groups: filtering, rate restriction, access control, and resource movement. Fig. 8 provides an overview of various mitigation approaches for SDN entities.

- **Filtering:** This method involves screening network traffic and eliminating suspicious connections. One approach is to identify the source of the attack and block all flows from that malicious source. However, attacks with faked source IP addresses make this strategy challenging. Another approach is aggressive aging, where a defined delay for flows in the flow table is set, deleting the flow when the timeout event occurs. This helps prevent expired or inactive flows from using resources for an extended period [70].
- **Dynamic Filtering:** This involves dynamically allocating network resources based on recognized attack patterns. It ensures that genuine traffic gets enough resources while limiting the impact of the attack by adjusting resource allocation, such as bandwidth, server capacity, or load balancing setups.
- **Rate Limiting:** Rate limiting is a technique for controlling the rate of transmission. It includes approaches like source rate limitation, granular rate limiting, and flow rate limiting. Source rate limitation aims to limit the number of packets transmitted from a suspected source at a certain time. Granular source limitation is based on the prior behavior of the sources. Flow rate restriction focuses on imposing rate limitations on a specific type of flow, enabling more precise control over the pace of communication for certain flows.
- **Access Control:** Access control involves limiting network users' communication and resource access. This can be done by creating a white-list and black-list of network hosts. Trusted users are on the white list, whereas questionable people are on the black list. However, establishing proactive access control based on these lists can be difficult, especially for Internet-connected networks.
- **Blacklisting/Whitelisting:** LEDEM may keep blacklists of known malicious IP addresses and whitelists of trustworthy IP addresses. By analyzing incoming traffic against these lists, LEDEM can either block or allow it, preventing known harmful sources from entering the network while allowing legal sources to join.
- **Migration:** This involves transferring suspected network traffic to a secure state for additional inspection. Flow migration diverts suspect network traffic to a secure middlebox for more in-depth analysis. Controller migration allows a proxy controller to take over the job of the original controller during a DDoS attack, protecting it from potential damage and allowing it to focus on managing and mitigating the attack while minimizing the risk of compromise or interruption [69].

Table 3 presents a comparison of various mitigation techniques employed in DDoS attacks, detailing the methods used, specific mitigation techniques applied, and the impact on legitimate users. Each technique comes with its own set of trade-offs, and the selection of a mitigation approach hinges on the specific requirements and priorities of the target system or network. Successful mitigation should aim for a delicate balance, minimizing the impact on legitimate users while effectively countering the DDoS attack.

6.1. Taxonomy of DDoS mitigation in SDN-IoT network

Collaborative (Cooperative) and non-collaborative (non-cooperative) techniques are two commonly employed approaches for mitigating

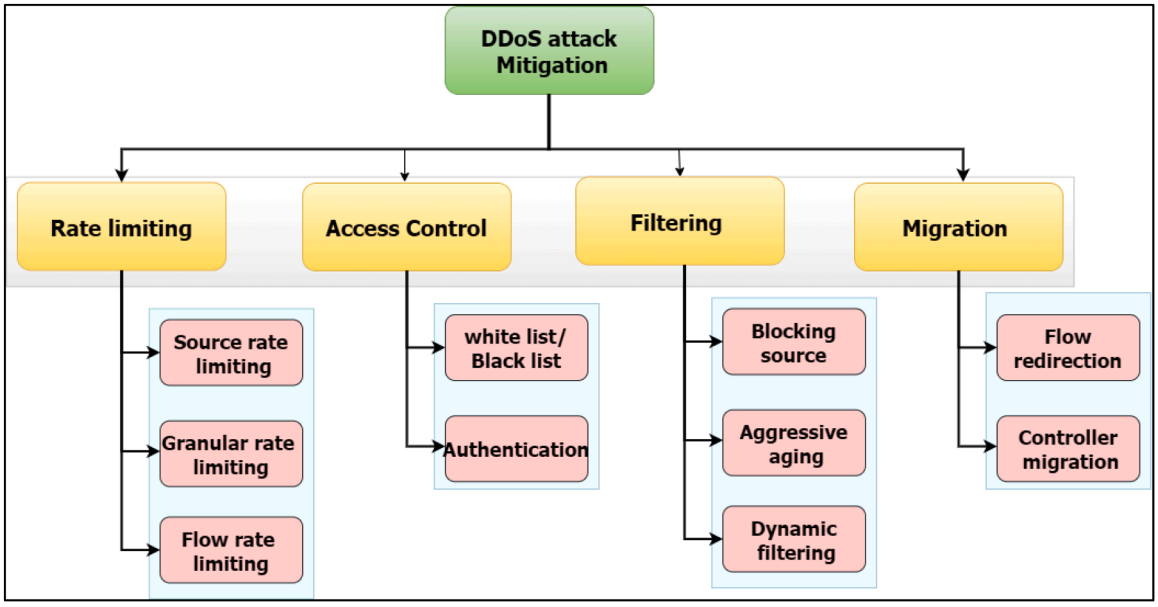

Fig. 8. Taxonomy of DDoS mitigation.

Table 3
A comparison of current mitigation techniques in DDoS attacks.

Techniques for detecting and mitigating DDoS attacks	Method	Technique for mitigation	Impact on legitimate users
FL-GUARD [71]	drop from a suspicious source	drop	high
New-flow attacks in SDN-based IoT [72]	suggested redirecting the suspicious flows to middle-boxes or secure applications	flow migration	low
SDN-based hybrid honeypot for attack capture [73]	Migrating attack flows to three different honeypots based on the level of severity	flow migration	low
Virtual IoT HoneyNets to mitigate cyberattacks in SDN/NFV-enabled IoT networks [74]	Policy-based packet filtering	filtering	high
An ML-based method using SDN Controller Framework [75]	drop the attack packet	drop	high
OrchSec [76]	Limiting the rate of suspicious flows	rate limiting	medium
OPERETTA [40]	Authentication/ access control	access control	low

DDoS attacks in SDN-IoT, as illustrated in Fig. 9. Both methods share the objective of defending against malicious attacks and ensuring the availability and reliability of network resources.

- **Collaborative DDoS Mitigation Techniques:** Collaborative techniques involve cooperation and coordination among multiple entities, such as network service providers, organizations, and security vendors. These techniques harness the collective power and resources of various stakeholders to effectively combat DDoS attacks.
- **Non-Collaborative DDoS Mitigation Techniques:** Non-collaborative techniques primarily focus on individual network defenses and do not rely on coordinated efforts with external entities. Typically implemented within an organization's infrastructure, these techniques aim to mitigate DDoS attacks without extensive external cooperation [61].

Here are some common Collaborative and non-collaborative DDoS mitigation techniques.

- **Pure SDN:** This approach relies solely on the capabilities of Software-Defined Networking (SDN) for DDoS mitigation. SDN separates the data plane (physical network devices) from the control plane (network intelligence and decision-making). This separation allows for programmatic control over the network, enabling the implementation of DDoS mitigation strategies. The techniques like filtering, rate limiting, and traceback are implemented via SDN controllers.
  - **Filtering:** SDN controllers can dynamically configure network switches to filter out malicious traffic based on pre-defined rules (e.g., source IP address, packet size).
  - **Rate Limiting:** The controller can limit the rate of incoming traffic from specific sources, preventing DDoS attacks that overwhelm the network with traffic.
  - **Traceback:** Some SDN controllers can analyze traffic patterns to identify the source of a DDoS attack, aiding in taking targeted mitigation actions.

  However, this approach has some limitations:
  - **Centralized Control Point:** A single point of failure exists – the SDN controller. If compromised, DDoS attacks can target the controller itself.
  - **Limited Edge Processing:** Pure SDN doesn't leverage resources closer to the edge of the network, potentially increasing latency for mitigation actions.
- **Hybrid SDN-Fog:** This approach combines the benefits of SDN with fog computing for DDoS mitigation. Fog computing distributes resources at the network edge (closer to IoT devices) to provide faster processing and decision-making capabilities. For implementing the hybrid SDN-Fog approach the following techniques are used:
  - **Leveraging SDN:** Techniques like filtering and rate limiting are still implemented by the SDN controller.
  - **Fog Nodes for Real-Time Analysis:** Fog nodes analyze traffic in real-time, enabling faster detection and mitigation of DDoS attacks closer to the source.

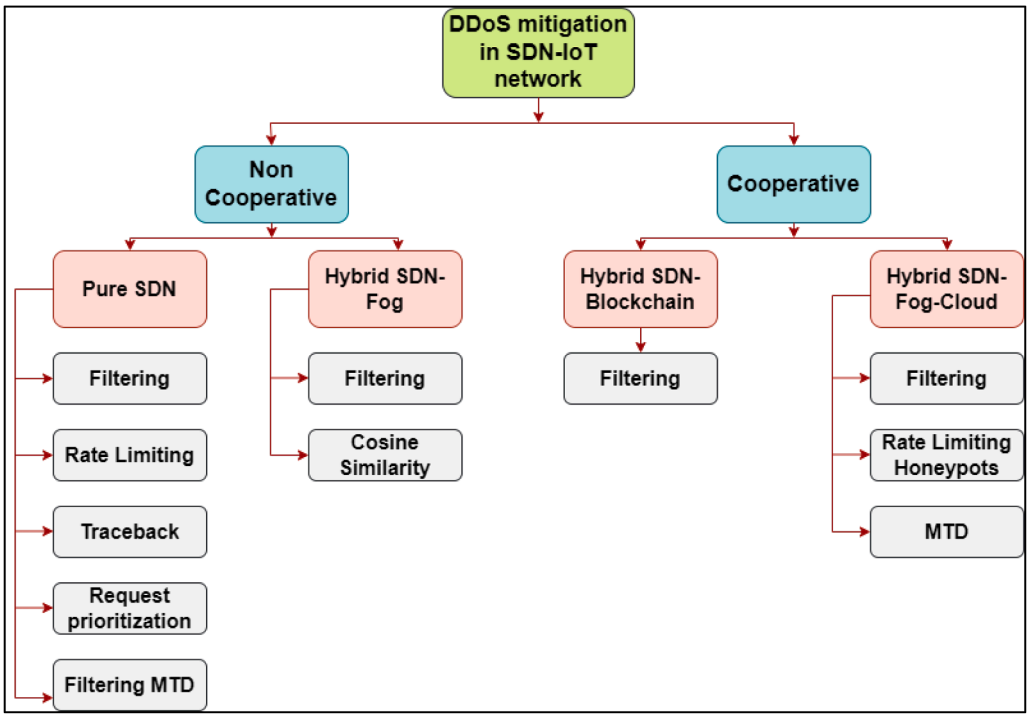

Fig. 9. Taxonomy of DDoS mitigation in SDN-IoT network.

- **Honeypots:** Fog nodes can be configured as honeypots to attract and identify DDoS attacks before they impact the core network.
- **Cosine Similarity:** Fog nodes can employ techniques like cosine similarity to compare traffic patterns and identify anomalies indicative of DDoS attacks.

This approach provides advantages like Faster Response and Reduced Latency, but it also has some limitations:

- **Fog Resource Constraints:** Fog nodes may have limited processing power and storage compared to the cloud, potentially hindering complex DDoS mitigation strategies.
- **Management Complexity:** Managing both SDN controllers and fog nodes can increase network complexity.

- **Hybrid SDN-Blockchain:** This approach integrates blockchain technology with SDN for a distributed and secure DDoS mitigation strategy. Blockchain's distributed ledger and immutability features help in filtering malicious traffic and coordinating mitigation efforts. Additionally, cosine similarity and MTD (Multi-tenant Detection) techniques are employed here.
  - **SDN for Traffic Control:** SDN controllers still manage network traffic flow based on policies stored on the blockchain.
  - **Blockchain-based Security Policies:** Security policies and attack signatures are stored on a tamper-proof blockchain ledger, ensuring trust and consistency across the network.
  - **MTD (Multi-tenant Detection):** Blockchain can help identify and mitigate multi-tenant DDoS attacks, where attackers leverage compromised resources within a network to launch attacks.
  - **Filtering MTD:** Leveraging blockchain data, network devices can filter out malicious traffic associated with multi-tenant attacks.

  The approach provides advantages like Increased Security and Distributed Mitigation strategies. However, the limitations associated with this approach are:
  - **Complexity:** Integrating and managing blockchain technology adds complexity to the network infrastructure.
  - **Scalability Concerns:** Scalability of blockchain-based solutions for large-scale networks is still under development.

- **Hybrid SDN-Fog-Cloud:** This approach leverages the strengths of all three: Software-Defined Networking (SDN), fog computing, and cloud computing for a comprehensive DDoS mitigation strategy. Similar to other hybrid approaches, the SDN controller plays a central role in network management and security policy enforcement. Fog computing resources are deployed closer to the edge of the network, near IoT devices. These fog nodes perform real-time traffic analysis, filtering, and mitigation techniques like rate limiting. They can also serve as honeypots to attract and identify DDoS attacks. The cloud acts as a centralized security hub, offering advanced DDoS mitigation capabilities. Fog nodes can communicate with the cloud for threat intelligence updates, attack signature sharing, and coordinated mitigation strategies. This offloads complex computations and large-scale filtering from the fog layer to the cloud's high-capacity resources.

  The approach provides some advantages:
  - **Layered Defense:** Combines real-time edge analytics with centralized cloud security, offering a multi-layered defense against DDoS attacks.
  - **Scalability:** Cloud resources provide scalability to handle large-scale DDoS attacks.
  - **Fast Response:** Fog nodes enable fast detection and mitigation at the network edge, minimizing latency impact.

It's important to note that, although collaborative techniques [77] offer the advantage of shared resources and intelligence, they necessitate coordination among various entities, which can be challenging. Conversely, non-collaborative techniques provide more control to individual organizations but may have limitations in handling large-scale or sophisticated DDoS attacks. Combining both approaches can formulate a comprehensive defense strategy against DDoS attacks, leveraging the strengths of each technique to enhance overall mitigation capabilities

7. Conclusion

The primary objective of a DDoS attack is to intentionally overload a

target system, causing degradation in its performance. To execute such an attack, the attacker installs malicious software, known as a bot, on multiple devices. By compromising these devices, the attacker gains remote control over them, utilizing their computational power for illicit purposes. Detecting and mitigating DDoS attacks pose significant challenges due to their complexity and evolving nature. In this paper, we conduct a comprehensive survey of DDoS attacks, considering various aspects. However, our research and proposed solutions specifically focus on the detection and mitigation of DDoS attacks. This means our work concentrates on developing methods and techniques to identify and alleviate the impact of DDoS attacks on targeted systems.

Narrowing our scope to detection and mitigation, the comprehensive survey specifically examines detecting DDoS attacks in SDN environments that incorporate IoT networks. The deployment of an SDN network enables centralized control and efficient management of security threats within IoT networks. Additionally, the method is well-suited for IoT networks as it demands minimal computational power. Furthermore, the proposed method goes beyond detection and includes mitigation capabilities, allowing for effective countermeasures against these disruptive attacks.

Despite numerous proposed approaches to protect users from DDoS attacks, the threat continues to persist, necessitating further emphasis on enhancing defense and mitigation solutions. It is essential to acknowledge that attackers constantly discover new methods to deceive users. Therefore, future work in the proposed survey should encompass the following areas of improvement: Enhanced Detection Techniques, Adaptive Mitigation Strategies, Collaborative Defense Mechanisms, Comprehensive Traffic Analysis, and Adaptive Network Infrastructure.

8. Research gaps and future scope

SDN offers a promising approach for managing IoT networks and addressing the complexities associated with network management in the context of DDoS attacks. However, DDoS attacks remain a significant threat to IoT networks, highlighting the need for robust detection and mitigation mechanisms. While the survey paper provides a comprehensive overview of DDoS attacks, focusing on detection and mitigation within SDN-based IoT networks, there are several areas where further research is needed:

- **Enhanced Detection Techniques:** The paper acknowledges the complexity and evolving nature of DDoS attacks. However, there is a need for more robust and advanced detection techniques that can accurately identify and differentiate between legitimate traffic and malicious activity in real-time. Future research can focus on developing more sophisticated detection algorithms capable of identifying new patterns and variations of DDoS attacks in SDN-IoT networks. Machine learning and artificial intelligence techniques can be employed to continuously adapt and improve detection accuracy.
- **Adaptive Mitigation Strategies:** The survey discusses mitigation capabilities within SDN environments, there is a gap in research regarding adaptive mitigation strategies that can dynamically respond to changing attack patterns and adjust mitigation measures accordingly. However, there is a need for dynamic and adaptive mitigation strategies that can respond to DDoS attacks in real-time. Future work can focus on developing self-learning algorithms or adaptive policies for mitigating DDoS attacks effectively while minimizing disruption to legitimate traffic.
- **Collaborative Defense Mechanisms:** Although the paper touches upon the collaboration between SDN and IoT for network security, there is room for exploring more collaborative defense mechanisms. Collaboration among network entities, such as IoT devices, SDN controllers, and cloud-based security services, can strengthen defense against DDoS attacks. Future work can investigate frameworks for sharing threat intelligence and coordinating defense mechanisms including IoT devices, SDN controllers, and security appliances to effectively detect and mitigate DDoS attacks collectively, leveraging their respective capabilities and intelligence across the entire network ecosystem.
- **Comprehensive Traffic Analysis:** While the survey discusses various aspects of DDoS attacks, including attack types and mitigation techniques, there is a need for more comprehensive traffic analysis methodologies. In-depth traffic analysis can provide valuable insights into the behavior of IoT devices and help distinguish between legitimate and malicious traffic. Future research should focus on developing techniques that provide deeper insights into network traffic behavior, enabling better detection and mitigation of sophisticated DDoS attacks tailored to exploit vulnerabilities in SDN-based IoT networks.
- **Adaptive Network Infrastructure:** The paper emphasizes the suitability of SDN for IoT networks due to its centralized control and minimal computational demands. However, there is a gap in research concerning the development of adaptive network infrastructures that can dynamically adjust network resources and configurations in response to DDoS attacks. The design and architecture of SDN-IoT networks can be optimized to enhance resilience against DDoS attacks. Future work can explore the integration of adaptive network infrastructure elements that can dynamically adjust resource allocation, reroute traffic, and isolate compromised devices to mitigate the impact of DDoS attacks effectively.

CRediT authorship contribution statement

Chandrapal Singh: Writing – original draft, Investigation, Conceptualization. **Ankit Kumar Jain:** Writing – review & editing, Validation, Formal analysis, Conceptualization.

Declaration of competing interest

We declare that we have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] P. Kumari, A.K. Jain, SDN-enabled IoT to combat the DDoS attacks, in: International Conference on Communication and Intelligent Systems, Springer Nature, Singapore, 2022, pp. 23–33.
[2] I. Farris, T. Taleb, Y. Khettab, J. Song, A survey on emerging SDN and NFV security mechanisms for IoT systems, IEEE Commun. Surveys Tuts. 21 (1) (2019) 812–837, 1st Quart.
[3] M. Du, K. Wang, An SDN-enabled pseudo-honeypot strategy for distributed denial of service attacks in industrial Internet of Things, IEEE Trans. Ind. Inf. 16 (1) (2020) 648–657. Jan.
[4] J. Mirkovic, P. Reiher, A taxonomy of DDoS attack and DDoS defence mechanisms, ACM SIGCOMM Comput. Commun. Rev. 34 (2) (2004) 39–53.
[5] A. Khanna, K. Sanmeet, Internet of things (IoT), applications and challenges: a comprehensive review, Wirel. Pers. Commun. 114 (2020) 1687–1762.
[6] J. Mirkovic, P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMM Comput. Commun. Rev. 34 (2) (2004) 39–53. April.
[7] M. Idhammad, K. Afdel, M. Belouch, Detection system of HTTP DDoS attacks in a cloud environment based on information theoretic entropy and random forest, Secur. Commun. Netw. 2018 (2018).
[8] Frolova, V., "8 Biggest DDoS attacks in history," 5 December 2021. [Online]. Available: https://news.cheapdeveloper.com/webmaster/articles/1517-8-biggest-DDoS-attacks-in-history.html. [Accessed 28 March 2023].
[9] https://securelist.com/kaspersky-DDoS-protection-q2-2022-report/103127/(Last accessed on 11 April 2023).
[10] DDoS Threat Landscape Report Q2 2022, Available at: https://www.nexusguard.com/threat-report-q3-2021/ (Last accessed on 11 April 2023).
[11] https://www.home.neustar/resources/reports/cyber-threats-and-trends-q2-2022 (Last accessed on 11 April 2023).

[12] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q2-2021-state-of-the-internet-security-report.pdf(Last accessed on 11 April 2023).
[13] P. Bhale, D.R. Chowdhury, S. Biswas, S. Nandi, OPTIMIST: lightweight and transparent IDS with optimum placement strategy to mitigate mixed-rate DDoS attacks in IoT networks, IEEE Internet Things J. (2023) 1.
[14] Alomari E., Manickam S., Gupta B.B., Karuppayah S., Alfaris R. Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art. arXiv preprint arXiv:1208.0403, 2012.
[15] J. Zheng, Q. Li, G. Gu, J. Cao, D.K.Y. Yau, J. Wu, Realtime DdoSdefense using cots sdn switches via adaptive correlation analysis, IEEE Trans. Inf. Forens. Secur. 13 (7) (2018) 1838–1853. July.
[16] T. Ubale, A.K. Jain, Taxonomy of DDoS attacks in software-defined networking environment, in: Futuristic Trends in Network and Communication Technologies: First International Conference, FTNCT 2018, Solan, India, Singapore, Springer, 2019, pp. 278–291. February 9–10, 2018, Revised Selected Papers 1.
[17] J. Singh, S. Behal, Detection and mitigation of DDoS attacks in SDN: a comprehensive review, research challenges and future directions, Comput. Sci. Rev. 37 (2020) 100279.
[18] Y. Jia, F. Zhong, A. Alrawais, B. Gong, X. Cheng, FlowGuard: an intelligent edge defense mechanism against IoT DDoS attacks, IEEE Internet Things J. 7 (10) (2020) 9552–9562.
[19] K.M. Prasad, A.R.M. Reddy, K.V. Rao, DoS and DDoS attacks: defense, detection and traceback mechanisms a survey, Glob. J. Comput. Sci. Technol. Netw. Web Secur. 14 (7) (2014) 15–32.
[20] Crane, C., "Re-hash: the largest DDoS attacks in history," 25 June 2020. https://www.thesslstore.com/blog/largest-DDoS-attack-in-history. [Accessed March 2023].
[21] Kovacs, E., "Google targeted in record-breaking 2.5 Tbps DDoS attack in 2017," 19 October 2020. [Online]. Available: https://www.securityweek.com/google-targeted-record-breaking-25-tbsp-DDoS-attack-2017. [Accessed 2023].
[22] A. Raza, Russian internet giant suffers largest DDoS attack in history, KoDDoS (2021), 17 September [Online]. Available: https://blog.koDDoS.net/russianinternet-giant-suffers-largest-DDoS-attack-in-history/.
[23] R.F. Hayat, S. Aurangzeb, M. Aleem, G. Srivastava, J.C. Lin, ML-DDoS: a blockchain-based multilevel DDoS mitigation mechanism for IoT environments, IEEE Trans. Eng. Manag. (2022) 1–14.
[24] S. Dong, K. Abbas, R. Jain, A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments, IEEE Access 7 (2019) 80813–80828.
[25] B. Wang, Y. Zheng, W. Lou, Y.T. Hou, DdoS attack protection in the era of cloud computing and software-defined networking, Comput. Netw. 81 (2015) 308–319.
[26] P. Kumari, A.K. Jain, A comprehensive study of DDoS attacks over IoT network and their countermeasures, Comput. Secur. (2023) 103096.
[27] L. Barki, A. Shidling, N. Meti, D.G. Narayan, M.M. Mulla, Detection of distributed denial of service attacks in software defined networks, in: 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2016, pp. 2576–2581. Sept.
[28] N. Meti, D.G. Narayan, V.P. Baligar, Detection of distributed denial of service attacks using machine learning algorithms in software defined networks, in: 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017, pp. 1366–1371. Sept.
[29] N. Ravi, S.M. Shalinie, Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture, IEEE Internet Things J. 7 (4) (2020) 3559–3570.
[30] J. Ashraf, S. Latif, Handling intrusion and DDoS attacks in software defined networks using machine learning techniques, in: 2014 National Software Engineering Conference, 2014, pp. 55–60. Nov.
[31] J.D. Gadze, A.A. Bamfo-Asante, J.O. Agyemang, H. Nunoo-Mensah, K.A.B. Opare, An investigation into the application of deep learning in the detection and mitigation of DDOS attack on SDN controllers, Technologies 9 (2021) 14.
[32] D. Javeed, T. Gao, M.T. Khan, I. Ahmad, A hybrid deep learning-driven SDN enabled mechanism for secure communication in Internet of Things (IoT), Sensors 21 (4884) (2021) 1–18. July.
[33] F.S.D. Silva, E. Silva, E.P. Neto, M. Lemos, A.J.V. Neto, F. Esposito, A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT scenarios, Sensors 20 (3078) (2020) 1–28. May.
[34] L. Breiman, J. Friedman, R. Olshen, C. Stone, Classification and Regression Trees, CRC Press, 1984.
[35] A. Saad, E. Taki, E. El-Araby, Comparative analysis of decision tree ID3 and C4.5, Int. J. Comput. Appl. 177 (43) (2017) 6–11.
[36] M. Singh, G.S. Aujla, A. Singh, N. Kumar, S. Garg, Deep-learning-based blockchain framework for secure software-defined industrial networks, IEEE Trans. Ind. Inform. 17 (2020) 606–616.
[37] N.M. Yungaicela-Naula, C. Vargas-Rosales, J.A. Pérez-Díaz, D.F. Carrera, A flexible SDN-based framework for slow-rate DDoS attack mitigation by using deep reinforcement learning, J. Netw. Comput. Appl. 205 (2022) 103444.
[38] A. Srivastava, B.B. Gupta, A. Tyagi, A. Sharma, A. Mishra, A recent survey on DDoS attacks and defense mechanisms, in: International Conference on Parallel Distributed Computing Technologies and Applications, Springer, 2011, pp. 570–580.
[39] Catalin Cimpanu, DDoS botnets have abused three zero-days in LILIN video recorders for months ZDNet, 2020, https://www.zdnet.com/article/DDoS-botnets-have-abused-three-zero-days-in-lilin-video-recorders-for-months/. (Accessed on 10 June 2021).
[40] S. Fichera, L. Galluccio, S.C. Grancagnolo, G. Morabito, S. Palazzo, OPERETTA: an openflow based remedy to mitigate TCP synflood attacks against web servers, Comput. Networks 89100 (2015).
[41] R. Vishwakarma, A.K. Jain, A survey of DDoS attacking techniques and defence mechanisms in the IoT network, Telecommun. Syst. 73 (1) (2020) 3–25.
[42] K.M. Sudar, M. Beulah, P. Deepalakshmi, P. Nagaraj, P. Chinnasamy, Detection of distributed denial of service attacks in SDN using machine learning techniques, in: 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2021, pp. 1–5, https://doi.org/10.1109/ICCCI50826.2021.9402517.
[43] F. Hu, Q. Hao, K. Bao, A survey on software-defined network and OpenFlow: from concept to implementation, IEEE Commun. Surveys Tut. 16 (4) (2014) 2181–2206. May.
[44] M.F. Thompson, Effects of a honeypot on the cyber grand challenge final event, IEEE Secur. Privacy 16 (2) (2018) 37–41. Mar.
[45] Z. Zhan, M. Xu, S. Xu, Characterizing honeypot-captured cyber attacks: statistical framework and case study, IEEE Trans. Inf. Forensics Secur. 8 (11) (2013) 1775–1789. Nov.
[46] X. Jiang, D. Xua, Y.M. Wang, Collapsar: aVM-based honeyfarm and reverse honeyfarm architecture for network attack capture and detention, J. Parallel Distrib. Comput. 4 (10) (2006) 1165–1180.
[47] M. Walfish, M. Vutukuru, H. Balakrishnan, D. Karger, S. Shenker, DDoS defense by offense, ACM Trans. Comput. Syst. 28 (1) (2010) 61–80.
[48] P. Wang, L. Wu, R. Cunningham, C. Zou, Honeypot detection in advanced botnet attacks, Int. J. Inf. Comput. Secur. 4 (1) (2010) 30–51.
[49] O. Hayatle, A. Youssef, H. Otrok, Dempster-Shafer evidence combining for anti-honeypot technologies, Inf. Sec. J.: A Glob. Perspect. 21 (6) (2012) 306–316.
[50] X. Luo, Q. Yan, M. Wang, W. Huang, Using MTD and SDN-based honeypots to defend DDoS attacks in IoT, in: 2019 Computing, Communications and IoT Applications (ComComAp), Shenzhen, China, 2019, pp. 392–395, https://doi.org/10.1109/ComComAp46287.2019.9018775.
[51] L. Cui, F.R. Yu, Q. Yan, When big data meets software-defined networking: SDN for big data and big data for SDN, IEEE Netw. 30 (2016) 58–65. January.
[52] J. Steinberger, B. Kuhnert, C. Dietz, L. Ball, A. Sperotto, H. Baier, A. Pras, G. Dreo, DDoS defense using MTD and SDN, in: NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, 2018, pp. 1–9. April.
[53] A. Irum, M.A. Khan, A. Noor, B. Shabir, DDoS detection and prevention in Internet of Things, EasyChair (2486) (2020) 1–7.
[54] V. Ravi, R. Chaganti, M. Alazab, Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system, Comput. Electr. Eng. 102 (2022) 108156.
[55] R. Lohiya, T. Ankit, Application domains, evaluation data sets, and research challenges of IoT: a systematic review, IEEE Internet Things J. 8 (2020) 8774–8798.
[56] G.A.N. Segura, S. Skaperas, A. Chorti, L. Mamatas, C.B. Margi, Denial of service attacks detection in software-defined wireless sensor networks, in: 2020 IEEE International Conference on Communications Workshops (ICC Workshops), IEEE, 2020, pp. 1–7.
[57] K. Bhushan, B.B. Gupta, Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment, J. Ambient Intell. Human Comput. 10 (2019) 1985–1997, https://doi.org/10.1007/s12652-018-0800-9.
[58] R. Vishwakarma, A.K. Jain, A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks, in: 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), IEEE, 2019, pp. 1019–1024.
[59] N.N. Dao, T.V. Phan, U. Sa'ad, J. Kim, T. Bauschert, D.T. Do, S. Cho, Securing heterogeneous IoT with intelligent DDoS attack behavior learning, IEEE Syst. J. (2021), 1–10 June.
[60] U. Javaid, A.K. Siang, M.N. Aman, B. Sikdar, Mitigating loT device based DDoS attacks using blockchain, in: Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, 2018, pp. 71–76.
[61] S.S. Bhunia, M. Gurusamy, Dynamic attack detection and mitigation in IoT using SDN, in: Proceedings of the 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, Australia, 2017, pp. 1–6.
[62] M. Bailey, J. Oberheide, J. Andersen, Z.M. Mao, F. Jahanian, J. Nazario, Automated classification and analysis of internet malware, in: Proceedings of the International Workshop on Recent Advances in Intrusion Detection, 4637, Berlin, Heidelberg, 2007, pp. 178–197.
[63] M. Shurman, R. Khrais, A. Yateem, DoS and DDoS attack detection using deep learning and IDS, Int. Arab J. Inf. Technol. 17 (4A) (2020) 655–661. June.
[64] N.N. Tuan, P.H. Hung, N.D. Nghia, N.V. Tho, T.V. Phan, N.H. Thanh, A DDoS attack mitigation scheme in ISP networks using machine learning based on sdn, Electronics (Basel) 9 (2020) 413.
[65] K.S. Sahoo, B.K. Tripathy, K. Naik, S. Ramasubbareddy, B. Balusamy, M. Khari, D. Burgos, An evolutionary SVM model for DDoS attack detection in software defined networks, IEEE Access 8 (2020) 132502–132513.
[66] J.N. Bakker, B. Ng, W.K. Seah, Can machine learning techniques be effectively used in real networks against DDoS attacks?, in: Proceedings of the IEEE Conference on Computer Communication and Networks, Hangzhou, China, 2018, 30 July–2 August.
[67] H. Polat, O. Polat, A. Cetin, Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models, Sustainability 12 (2020) 1035.
[68] S. Dong, M. Sarem, Ddos attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks, IEEE Access 8 (2019) 5039–5048.
[69] S.S. Mohammed, R. Hussain, O. Senko, B. Bimaganbetov, J. Lee, F. Hussain, M.Z. A. Bhuiyan, A new machine learning-based collaborative DDoS mitigation

mechanism in software-defined network, in: Proceedings of the IEEE Conference on Wireless and Mobile Computing, Networking and Communications, Limassol, Cyprus, 2018, 15–17 October.
[70] O.E. Tayfour, M.N. Marsono, Collaborative detection and mitigation of distributed denial-of-service attacks on software-defined network, Mob. Netw. Appl. 25 (2020) 1338–1347.
[71] J. Liu, Y. Lai, S. Zhang, Fl-guard: a detection and defense system for DDoS attack in SDN, in: Proceedings of the 2017 International Conference on Cryptography, Security and Privacy, ACM, 2017, pp. 107–111.
[72] T. Xu, D. Gao, P. Dong, H. Zhang, C.H. Foh, H.C. Chao, Defending against new-flow attack in SDN-based internet of things, IEEE Access 5 (2017) 3431–3443.
[73] H. Wang, B. Wu, SDN-based hybrid honeypot for attack capture, in: 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), IEEE, 2019, pp. 1602–1606.
[74] Zarca, A.M., Bernabe, J., Skarmeta, A., Calero, J., 2020. Virtual IoT honeynets to mitigate cyberattacks in sdn/nfv-enabled IoT networks.
[75] Revathi, M., Ramalingam, V., Amutha, B., 2021. A machine learning based detection and mitigation of the DDoS attack by using SDN controller framework.
[76] A. Zaalouk, R. Khondoker, R. Marx, K. Bayarou, Orchsec: an orchestra-tor-based architecture for enhancing network-security using network monitoring and SDN control functions, in: Network Operations and Management Symposium (NOMS), IEEE, 2014, pp. 1–9.
[77] K. Kim, Y. You, M. Park, K. Lee, DDoS mitigation: decentralized CDN using private blockchain, in: International Conference on Ubiquitous and Future Networks, ICUFN, IEEE Computer Society, 2018, pp. 693–696. Vol. 2018-July.

Chandrapal Singh completed M.tech. from National Institute of Technology, Kurukshetra, India. He has received his B.tech degree in Information Technology from REC Banda, India. His research interests include, Cyber Security, Machine Learning and Deep Learning, Compueter Network and Information Security. Currently he is working in Bharat Electronics Limited (BEL-CRL) as a member of research staff.

Dr. Ankit kumar Jain is presently working as Assistant Professor in National Institute of Technology, Kurukshetra, since September 2013. He received Master of technology from Indian Institute of Information Technology Allahabad (IIIT) India. Dr. Jain received PhD degree from National Institute of Technology, Kurukshetra in the area of Information and Cyber Security. He has more than 70 research papers in International journals and conferences of high repute including Elsevier, Springer, Taylor & Francis, Inderscience, IEEE, etc. His general research interest is in the area of Information and Cyber security, Phishing Website Detection, Web security, Mobile Security, IoT Security, Online Social Networks and Machine Learning. Email: ankitjain@nitkkr.ac.in