IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 4, Issue 6, November 2024

Impact Factor: 7.57

An Analysis of Dynamic DDoS Entry Point Localization in Software-Defined WANs

Vaidehi Shah
Independent Researcher
shahvaidehi4795@gmail.com

Abstract: *Software-Defined Wide Area Networks (SD-WANs) are an expanded version of Software-Defined Networking (SDN) that allow modern services and applications to utilize a programmable, adaptive, and efficient wide-area connection. As the Internet of Things (IoT) grows in importance in everyday life, so does the frequency of Distributed Denial of Service (DDoS) attacks. Due to the dispersed nature of the IoT and the limited resources it possesses, SD-WANs are easy prey. These assaults are extremely difficult to detect and localize due to their distributed nature and dynamic traffic patterns, which allow them to elude static criteria and basic profiling methods. Beginning with a description of SDN architecture and the vulnerabilities that are built into it and frequently used by attackers, this article gives a comprehensive study of dynamic DDoS entry point localization in SD-WANs. In addition, it identifies the most prevalent types of distributed denial of service assaults in an SDN environment and reviews recent research on DDoS detection and mitigation. Research in this area focusses on various defence strategies, including hybrid, ensemble, and deep learning-based models; it also includes statistical, policy-based, and moving target defence methods. Research shows that there has been a lot of headway, but no complete answers to the problem of intelligent and dynamic entry point localization in the current literature. Therefore, to fortify SD-WAN defences against ever-changing DDoS threats, this article highlights important hurdles and unanswered questions in SDN security and calls for the creation of adaptive, real-time detection systems.*

Keywords*:* SD-WAN, Software-Defined Networking (SDN), Distributed Denial of Service (DDoS), IOT Security, Entry Point Localization, Machine Learning, Deep Learning, Dynamic Detection, Network Security

I. INTRODUCTION

Software-Defined Wide Area Networks, or SD-WANs, have changed the way standard WAN architectures work in big ways. When they were first thought of in Google's B4 data centers, SD-WANs were meant to allow high link utilisation, dynamic traffic steering, elastic computing, and centralized control of cloud systems that are spread out geographically [1]. The control plane and the data plane are kept separate in SD-WAN, which is different from legacy networks that use hardware-centric control, rely on one vendor, and have complicated management. This change in design makes it possible for centralized orchestration, high levels of scalability, and wide-area traffic forwarding that is both cost-effective and aware of the application [2]. SD-WAN is very important for the growth of cloud-based services, the Internet of Things (IoT), fog computing, and smart city infrastructure because it ensures that networks are connected well and are managed in a flexible way [3]. While SD-WANs have these benefits, they also bring new security risks because they are built on centralized controllers and have both programmable interfaces and virtualized functions.

DDoS attacks are especially inconvenient. Availability might be compromised, preventing normal access and destabilizing services by DDoS attacks, which bombard a target with too much traffic to process in a multi-source attack. Such attacks are particularly harmful in SD-WAN scenarios where topology and flow changes can quickly overwhelm any malicious activity [4]. Entry point localization determination of the point or the line of attack traffic entry, is a very important process of successful detection of possible DDoS attacks and mitigation in contemporary

DOI: 10.48175/IJARSCT-22565

threat environments. This is however becoming more complicated with SD-WANs because of dynamic routing, virtualization and abstraction of the network functions.

The reputable response against it is dynamic and smart detection methods. Unlike signature-based Intrusion Detection Systems (IDS), ML-based IDS have higher accuracy as it learns the traffic patterns and detects anomalies [5]. Moreover, the study utilizes the statistical solutions to point out the deviations in the traffic dispersion, e.g. by studying the entropy. Future solutions will make use of the capabilities of SDN, specifically programmable control and visibility everywhere, which allows responding in real time. What is more, innovative technologies, such as Network Function Virtualization (NFV), enable the fast implementation of virtual firewalls and mitigation functions, whereas Moving Target Defense (MTD) dynamically changes network parameters to prevent attacker knowledge gathering and constrain their attacks. Some of the tools such as Honeynets collect knowledge of attacker behavior, which is useful in distributed and collaborative threat intelligence.

The development of the 5G and network slicing has presented opportunities and complexities [6]. Network slices virtual partitions tailored for specific service requirements can be dynamically deployed and managed, but also present new surfaces for DDoS exploitation. Therefore, dynamic DDoS entry point localization must adapt to these multi-layered, segmented, and software-driven environments [7]. SD-WAN's agility and programmability make it both a robust platform for modern enterprise networking and a challenging surface for DDoS defense [8]. As DDoS attack vectors evolve, so must the localization techniques be emphasizing dynamic monitoring, adaptive learning models, context-aware analysis, and controller-driven orchestration.

A. Structure of the Paper

The structure of this paper is as follows: Section II outlines the fundamentals of SD-WANs and DDoS in SD-WANs. Section III covers Entry Point Localization in SD-WANs with motivation. Section IV discusses techniques for DDoS Entry Point Localization. Section V presents future perspectives and challenges associated with DDoS attacks in SD-WANs. Section VI reviews recent literature, and Section VII concludes with future research directions.

II. FUNDAMENTALS CONCEPTS: DDOS ATTACKS IN SD-WANS

A novel approach to wide area network design, software-defined wide area networks (SD-WANs) provide efficient and cost-effective centralization of network management across geographically distributed networks. In contrast to traditional WANs and conventional software-defined networking (SDN), the objective of software-defined wide area networks (SD-WAN) is to connect mission-critical locations such as data centers, branch offices, and cloud endpoints [9]. It enables centralized control, dynamic policy enforcement, real-time monitoring, and simplified network management, eliminating the need for manual configurations on individual devices [10]. By supporting application-aware routing and Quality of Experience (QoE)-driven policies, SD-WAN enhances operational efficiency and user experience. Nonetheless, SD-WAN is experiencing one major complication after another due to the growing importance of security. Centralized control plane, virtualized components, and dynamic connectivity cause SD-WANs to be susceptible to multiple threats, particularly DDoS which has the potential of affecting the availability of services through congesting network resources. Recent studies have centered on mitigating these deficiencies, evaluating the failures of the past WAN design, and spearheading the innovations that incorporate the latest technologies, including NFV and machine learning and zero-trust security architectures. These new developments are meant to increase SD-WAN resistance to new forms of attacks and help to shift to a more stable and multi-objective networking architecture.

A. Architecture of Software-Defined Wide Area Network

Traditional wide-area network designs are rigid and ill-equipped to meet the adaptability demands of today's networks. Solving this problem with SD-WAN allows for more flexibility and innovation while also improving management and streamlining operations. SD-WAN allows for more flexibility and central coordination by separating the control and data planes. The logical and physical architectures depicted in Figure 1 illustrate these improvements over conventional WANs.

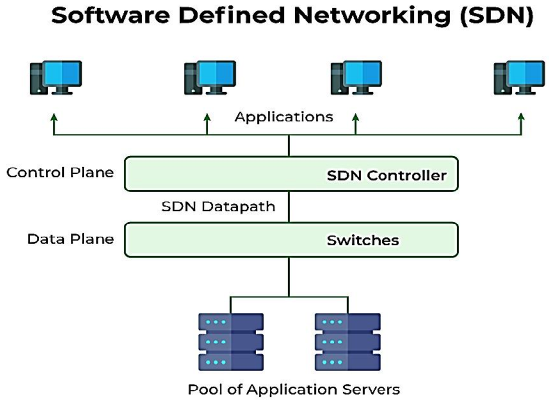

Figure 1: Software-defined wide area network: logical and physical architecture

The layers of the architecture of SDN in regards to their functions and main functionalities that may be modified in accordance to diversified variety of use cases:

1. Data Forwarding Layer:

This layer contains many kinds of routers and switches. They are capable of exchanging data using both wireless and wired means of communication. The sole function of an SDN switch is to forward packets in response to instructions from the controller. Every switch keeps a packet-specific flow table for use in packet-forwarding decision-making. The rule, action, and counter columns form the framework of the flowchart. The rule specifies the proper values for each field in the packet header. Whenever a new packet arrives, the switch checks the flow table to see which rule applies. When two field values are equal, the switch raises the counter value by doing what it should. Similarly, if there is inconsistency in the field values, the switch will inform the controller. Once the optimal course of action has been determined, the packet can be forwarded, dropped, or further rules can be added to the switches by the controller.

2. Control Layer:

There is at least one controller in it. The controller, sometimes referred to as the "brain of SDN," is in charge of executing the complex control mechanisms. The control layer is in charge of the whole network and all of the switches inside it. A common southbound application programming interface (OpenFlow) allows the SDN controller and switches to communicate. It can see the whole network in it. An interface called the east-west bound API is used to connect several controllers when they are employed. Thanks to this interface, they are able to exchange crucial data with one another. A group of switches is managed by each controller in a multi-controller scenario.

3. Application Layer

facilitates the natural-sounding communication of network requirements between application developers and network providers, with the ability to translate requirements stated at a high level into network configurations that comply with rules. With an increasing number of apps having complex and frequently conflicting requirements, it is essential to tailor network laws to each program according to its unique characteristics. In order to keep consumers happy, a live video streaming service needs both a high bandwidth and minimal latency, which are incompatible goals. Application developers and network providers might be more involved in network governance through the application layer.

B. DDoS Attacks in SD-WANs.

A DDoS attack can overload a SD-WAN components and interrupt essential services. In order to make the targeted systems or services, email, banks, and websites inaccessible, these assaults aim to deplete vital resources including bandwidth, memory, and computing power. Attackers use centralized control and programmability of SD-WAN architecture to flood communications channels or create conditions to exploit protocol-level attacks like TCP retransmission or HTTP keep alive requests in order to saturate network infrastructure. However, a more aggressive type, called DDoS, introduces proficient networks of botnets of compromised IoT or other devices infected with malware to flood that slide towards a target IP address or SD-WAN structure element with a great deal of malicious traffic [11]. This results in table-miss events at SDN switches, overwhelming limited TCAM storage, straining controller processing capabilities, and saturating the bandwidth of the switch-controller link. Differentiating between legal and malicious flows is made more difficult by the dynamic and linked nature of SD-WAN. This makes mitigation measures more difficult and increases the risk of network-wide interruption and the many varieties of DDoS and DDoS assaults include protocol attacks, application layer attacks, and volumetric attacks:

Here are the Types of DDOS Attacks are as follows:

1. Zero-Day Attacks

These attacks take advantage of loopholes in the network's software or hardware. It is difficult to combat these vulnerabilities because neither the seller nor the public is aware of them.

2. Reflection Attacks

Reflection attacks magnify attack traffic by exploiting susceptible protocols. The attacker in a reflection attack, on the other hand, increases the volume of attack traffic by sending requests to external servers, which in turn send responses to the target network. Although DDoS assaults of this kind can happen on slow networks as well as fast ones, the massive amounts of traffic that these attacks can produce make them far more destructive on the former.

3. DNS Amplification

The DNS amplification technique, which is used in volumetric DDoS attacks, is an improved reflection attack approach. By increasing the outgoing data flow, these attacks overwhelm the bandwidth. There is a plethora of traffic because the attackers are sending information requests to the server, which generate a lot of data. The next step is to fake the reply-to address so they may send the data back to the server. Therefore, in a DNS amplification attack, the malicious actor uses a botnet to flood a publicly accessible DNS server with a huge number of small messages. Name resolution enquiries (DNS queries) are one example of a lengthy request that each of these packets makes.

4. SYN Flood

In SYN flood assaults, the three-way handshake protocol that normally connects clients and servers to TCP is bypassed. Most commonly, a client will send a synchronize (SYN) request to the server to initiate the connection, and the client will then acknowledge the server's response to complete the handshake. If the server does not respond with a final declaration after receiving many synchronization requests, this is known as a SYN flood. After the client and server exchange synchronization requests (SYNs), the handshake concludes with the server sending an acknowledging response (SYN-ACK). By repeatedly sending these synchronization requests without finally declaring their success, SYN floods cause the server to freeze up.

5. Ping of Death

Attacks known as "ping-of-death" are distinct from the more common ICMP echo ping floods. Intentionally causing server-side system failure is the goal of the packet's malicious engineering. The purpose of the data in a conventional ping flood attack is to overwhelm the bandwidth with volume, so it is essentially meaningless. The goal of a ping-of-death assault is to deliver packets that overwhelm the target device, causing it to crash or malfunction. Protocols like UDP and TCP that aren't ICMP can also benefit from this method.

6. Application Layer Attack

Application layer DDoS attacks include DNS floods. The criminal frequently communicates with a web server or application as part of this strategy. In reality, web browsers orchestrate all interactions to maximize server resources, making it appear as though normal user activity is occurring. The bad guy might employ POST requests to manipulate databases or GET queries to retrieve URLs to images or documents.

C. Entry Point Localisation: Definition and Relevance

The process of determining the initial sites of malicious traffic's entrance into a wide-area network, also known as Entry Point Localization, is useful for network managers in tracing, mitigating, and responding to distributed denial-of-service attacks in SD-WANs. Since SD-WANs exploit internet connectivity via public connections, which are inherently more vulnerable to DDoS attacks, this is particularly relevant to them. Evidence from research such as the "SD-WAN Flood Tracer", which monitors malicious traffic at the point of entrance to SD-WAN, lends credence to the idea that the entry point localization issue is significant. Devices and applications exposed to the internet through a distributed wide area network (SD-WAN) greatly increase the attack surface and make the attack more problematic; as a result, detection and mitigation techniques are necessary due to the fact that DDoS attacks can increase by as much as 200%. Maintaining the availability and performance of appealing business applications offered via SD-WANs relies on appropriately selecting entry points, which enables concentrated DDoS removal and minimizes an attack surface.

1. Dynamic vs Static Localization Approaches.

Dynamic and static localization approaches differ primarily in adaptability and responsiveness to network conditions. Static localization relies on predefined rules, configurations, and historical data, making it simpler and less resource-intensive but less effective in evolving network environments. In contrast, dynamic localization adapts to real-time traffic patterns and network topology changes, often leveraging machine learning, flow telemetry, or graph-based techniques for improved accuracy and faster response. While static methods are suitable for stable networks, dynamic approaches are better suited for complex, high-speed, and software-defined networks, such as SD-WANs.

Table I shows the comparison of static and dynamic localizations are follows:

Table 1: Static Localization vs Dynamic Localization approaches

Aspect	Static Localization Approaches	Dynamic Localization Approaches
Definition	Use predefined rules, configurations, or static network views	Adaptively analyze real-time traffic and conditions for localization
Adaptability	Low – does not adjust to network changes	High – responds to dynamic traffic and topology variations
Data Dependency	Based on historical or static configuration data	Uses live telemetry, flow statistics, or machine learning models
Accuracy in Real-time Scenarios	Often low due to outdated assumptions	High, as it reacts to current attack patterns
Computation Overhead	Low – simple processing and fewer resources needed	Higher – requires real-time data processing and model execution
Scalability	Limited scalability in large, dynamic networks	More scalable when optimized for distributed data collection
Techniques Used	Routing table lookup, ACLs, manual tracing	Machine learning, graph analysis, entropy-based methods, reinforcement learning
Response Time	Slower in dynamic environments	Fast in adapting and reacting to evolving attacks
Suitability	Static or low-change network environments	SD-WANs, cloud networks, and environments with frequent topology changes

III. MOTIVATION FOR ENTRY POINT LOCALIZATION IN SD-WANS

Entry point localization in SD-WANs is driven by the fact that the modern network infrastructure has been expanding and becoming more complicated, rendering it prone to DDoS attacks. Malicious traffic origin or entry point detection is important in the correct mitigation and response of such attacks. Static security measures that are used to provide security in traditional networks are usually ineffective in dynamically distributed networks like SD-WANs since the traffic patterns are decentralized, and routes are also dynamic. By localizing entry point in the network, it becomes possible to identify where the attack traffic is entering the network and then a localized defensive strategy can be deployed, i.e. rerouting, rate-limiting or blocking the malicious flows at the entry point [12]. It does not only make the

DOI: 10.48175/IJARSCT-22565

intrusion mitigation more responsive and efficient but also ensures a minimal occurrence of collateral damage to genuine traffic, thus increasing network resilience and overall service quality.

A. Application Domains and Enabling Technologies of SDN

Efficient implementation of technologies like blockchain, wireless communication, the Internet of Things, etc., is a crucial necessity to realize the benefits of software-defined networking (SDN) in many applications. Underneath the previously described supporting services for SDN-integrated smart applications, this section lays out the fundamental ideas:

1. Data Centers and Edge Computing

Computing at the edge, or close to the source of data, decreases latency and bandwidth consumption. However, its distributed nature introduces security risks. SDN enhances security and orchestration at the edge, and blockchain integration further secures device communications. SDN-based frameworks in healthcare and mobile edge computing improve load balancing and reduce service migration costs.

2. Software-Defined WAN (SD-WAN)

SD-WAN enables application-aware, secure routing over the Internet, improving performance and reducing dependency on leased lines. Simulation tools like IoT Sim-SDWAN optimize routing across data centers. Dynamic traffic management and healthcare implementations show improvements in latency, security, and trust.

3. LTE and 5G Networks

SDN introduces programmability and centralized control in LTE/5G, enhancing flexibility and security. Blockchain further secures communication in SDN-enabled 5G VANETs.

4. Smart Cities IoT

SDN improves routing, management, and visibility in IoT networks, Smart Grids: SDN enhances efficiency and security in energy systems via secure routing and lightweight DDoS defense, CAVs: SDN enables reliable, low-latency communication and QoS-aware routing in vehicular networks [13], Robotics: SDN facilitates secure communication in smart manufacturing using VLC and edge computing [14], Blockchain: Blockchain ensures trust, integrity, and secure device management in SDN-IoT environments.

5. Softwarization and NFV

SDN and NFV complement each other in providing scalable, programmable networks to facilitate device integration, virtualization and reconfiguration of services.

B. Role of Dynamic and Real-Time Detection.

The detection mechanisms, dynamic and in real-time, are the key to precise location of entry points of Distributed Denial-of-Service (DDoS) attacks in Software-Defined Wide Area Networks (SD-WANs) [15]. In contrast to the static techniques based on pre-calculated thresholds and past baselines, dynamic detection has certain ability to adapt to the changing network conditions, so that anomalous traffic patterns that can reveal DDoS entry points can be detected early and thereby promptly reacted. Flow analytics, ML models, and real time telemetry enable monitoring of traffic across the SD-WAN distributed fabric and malicious ingress nodes can be detected before spreading of attacks. SD-WANs decouple control and data planes in order to enable central decision-making on data gathered in real-time at various edge sites. The strategy can lead to rapid counter measures such as rerouting, throttling or isolating the affected paths to increase situational awareness. Thus, dynamic and real-time detection systems are critical attributes in beefing up SD-WAN systems with advanced and fast-changing DDoS attacks.

DOI: 10.48175/IJARSCT-22565

IV. TECHNIQUES FOR DDOS ENTRY POINT LOCALISATION

DDoS entry point localization is the method to detect the source of attacks which flood networks, applications or services with malicious traffic to the point of denial of service. Attackers often use botnets, which are networks of infected devices that they control remotely, to launch these types of attacks and flood their targets' systems. Effective localization is crucial for mitigating the attack at its source and preventing service disruption. Given the extremely high data rates involved often reaching up to 28,100 Gbps traditional socket-based packet analysis is inadequate for real-time detection, especially with the limitations of 100 Gbps network interface cards (NICs). To address this, advanced techniques such as flow monitoring, telemetry data analysis, entropy-based methods, and machine learning models are employed for scalable and high-speed traffic analysis, enabling accurate and timely detection of the DDoS entry points.

A. Identification of DDOS Attacks

A DDoS attack manifests itself when a service or website becomes very delayed or unavailable. It can find out exactly where DDoS attacks are happening with the help of analysis tools. If an IP address range is sending out an unusually large volume of traffic, it can be because someone is trying to target a certain page or endpoint with a profile that includes information about their device, location, and web browser [16]. To further understand how a basic DDoS attack detection pipeline works, consider Figure 2. Websites that appear slow to load or unavailable, networks that suddenly lose internet access, and computers that become unresponsive are all symptoms of a distributed denial of service attack.

Building a two-dimensional linked list during initialization is the first step in detecting the DDoS assault. This library checks the system's parsing rules. For those who build their applications in C, libpq is the PostgreSQL interface. The PostgreSQL server can be queried and its answers retrieved by applications using the techniques provided by the libpq package.

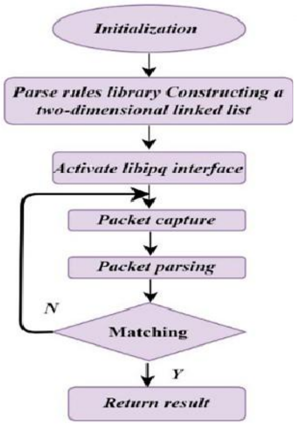
Initialization
Parse rules library Constructing a two-dimensional linked list
Activate libipq interface
Packet capture
Packet parsing
N
Matching
Y
Return result

Figure 2: DDOS Attack Detection Flow

B. Traditional (Static) Localisation Methods.

Traditional or static localization methods for identifying DDoS entry points typically rely on fixed network monitoring strategies, predefined rules, and manual analysis of traffic logs. These approaches often involve the use of static filters, signature-based intrusion detection systems (IDS), flow record analysis, and hop-by-hop traceback mechanisms such as packet marking or logging at routers. IP traceback techniques, including input debugging and controlled flooding, aim to trace attack traffic to its origin by analyzing network paths in a deterministic manner [17]. While these methods were effective in relatively stable and centralized network architectures, they struggle to cope with the dynamic, distributed, and encrypted traffic flows prevalent in modern SD-WAN environments. Moreover, static methods generally lack scalability and adaptability, making them less effective in real-time detection and response scenarios, particularly against rapidly evolving and obfuscated DDoS attack vectors.

DOI: 10.48175/IJARSCT-22565

C. Traditional (Static) Localisation Methods

To address the limitations of static methods, dynamic techniques have emerged, leveraging real-time network data, adaptive algorithms, and intelligent decision-making. These approaches are particularly suited for modern programmable networks.

1. AI and Machine Learning-Based Techniques

ML and DL are two components of AI, which is an umbrella word encompassing methods that enable smart machines to solve problems in the real world by acting like humans. ML is a branch of artificial intelligence that includes a number of algorithms that allow computers to learn using mathematical models in order to identify and categorize SDN DDoS attacks. A few examples of ML techniques that are frequently utilized in intrusion detection systems are K-NN, SVM, DT, ANN, K-means clustering, and quick learning network. Machine learning methods, often known as shallow learning algorithms, perform better than DL, a subset of ML that uses several hidden layers to mimic deep network characteristics. RNNs, CNNs, several others are examples of common DL algorithms.

a. Supervised Learning

The KNN algorithm is designed to cluster data by selecting the closest neighbors using data attributes. It is a supervised learning system. This technique is employed in attack detection domains to categorize network traffic by the measurement of dissimilarity across several feature values [18]. For SDN DDoS attack detection, it proposes an enhanced KNN algorithm. While talking about traffic on an SDN, the amount, regularity, magnitude, and proportion of the traffic are important metrics to keep in mind. With these characteristics, it can detect many different kinds of DDoS attacks. To accomplish this, used the KNN model. The supplied model has been useful in properly detecting DDoS attacks. However, it should be noted that the simulation experiment topology utilized in this work was very simple. It will undoubtedly be a challenging task to achieve real-time detection in a more intricate and real-life environment.

b. Unsupervised Learning

The Techniques of Unsupervised Learning Without tagged data, the objective of unsupervised learning approaches to DDoS entry point localization is to identify and follow the origin of the assaults. They seek to identify potentially malicious nodes in the network by analyzing clustering behaviors, unusual traffic patterns, and statistical trends. By grouping comparable data flows and identifying outliers, can pinpoint the locations of attacks using hierarchical clustering, K-Means, and DBSCAN. Visualization of high-dimensional traffic data can also enhance detection capabilities when employing dimensionality reduction techniques, such as principal component analysis (PCA) and t-SNE.

c. Deep Learning Techniques

DDoS attacks are being carried out by attackers on the rise of the presence of IoT devices connected to the internet and the expansion of network traffic. Attackers are using complex and sophisticated ways to perform these DDoS attacks and this is one reason as to why it is not easy to detect them. These attacks are easy to pull off due to quantities of labelled data needed to perform the attacks, so DDoS attack detection techniques that rely on deep learning could become one of the most effective DDoS attack detectors [19]. DL techniques produce the best detection rate and classification accuracy when a large amount of labelled data is available. The accuracy with which classic ML methods detect DDoS attacks may be lower when compared to DL methods. For DDoS attack detection, DL methods are superior because:

- DL techniques are excellent during training at discovering useful hidden features in the data. A trained DL network can extract features from previously unseen examples and classify such examples well.
- Some DL techniques can learn long-term dependencies of temporal patterns.

ML detection mechanisms excel in efficiently processing multi-dimensional data due to their excellent abstracting and generalizing abilities, even when dealing with detection data with high feature dimensions. ML models have also been successful in tracing attackers, reducing the complexity of traffic data, and recognizing attack types. There is a trade-off between the quality of the input features and the accuracy of the model's detection when using supervised learning approaches, which depend on hand-crafted and annotated features. While unsupervised learning algorithms produce better results in terms of real-time detection, their training consumes more resources and takes longer.

2. Entropy-based Techniques

A system's uncertainty can be effectively measured by applying information theory's proposed information entropy theory and information divergence. One way to evaluate the unpredictability of network traffic is to use the entropy, which is a measure of the probability distribution of a random variable. In order to determine the unpredictability of traffic, entropy-based detection systems usually examine different elements of network packet headers, including source IP, destination IP, and source port. Because hosts communicate independently, traffic attributes like destination IP addresses in typical communication systems often display a high degree of uncertainty. In a distributed denial of service (DDoS) assault, however, traffic patterns change dramatically as several servers send harmful traffic towards a single or small group of targets. Systems are able to identify DDoS attacks more accurately when they combine entropy analysis with intrusion detection and machine learning approaches [20]. Implemented a dynamic thresholding method to circumvent static threshold-based entropy detection's shortcomings, most notably its limited precision [21]. In this method, the entropy values are collected one by one, categorized as normal or attack sets based on their relationship to the current threshold, and the threshold is dynamically changed using the mean and standard deviation of these sets. Thus, investigating more sophisticated methods of dynamic threshold setting seems to be a pressing area for research in entropy-based DDoS detectors going forward.

3. Graph-Based and Topology-Aware Approaches

Topology-wise and Graph-based approaches have gained popularity in detecting DDoS attacks, especially those based on Graph Convolutional Network (GCNs), as they are able to include the high-level and relational nature of the network traffic. GCNs are particularly good at modelling of graph-structured data revealing more complex interactions and patterns which would not have been captured using traditional machine learning techniques. In network security, graphs are implicitly used to describe the network by nodes and edges and GCNs can be used to gain insights into measures of communication actions. As an example, Spatial-Temporal GCNs (ST-GCNs) have been deployed in SDN scenarios, in order to analyze the spatial and temporal invariants of the traffic and thus detect DDoS attacks. Nevertheless, current techniques seem to be skewed towards simple attack cases with well-defined traffic differentiation and possibly rely on centrally located routers which can represent a vulnerability. The more sophisticated implementations compensate these shortcomings by including dynamic DDoS traffic where packet volume varies as well as implementing peer-to-peer network infrastructures thus increasing their resiliation to lossy and unstable encounters. This is what makes GCN-based methods with topology awareness quite relevant to real network systems that are dynamic.

D. Hybrid Approaches

Hybrid methods include a combination of two or more localization methods in order to take advantage of their complementary properties. As an example, the ML-based anomaly detection may be combined with graph-based tracing to transfer context-sensitive localization, or in another case substitute entropy measurements may spur another reinforcement learning agent to launch more extensive interrogation. The coherent objectives of these composite frameworks are to strike a balance between the efficiencies of detection, computing overhead, and reactive latencies thus being very appropriate in highly hierarchical and dynamic environments of SD-WAN environments. Recent studies discuss the subsequent combination of hybrid models and centralized coordination and better visibility of network layers using the SDN controllers.

V. FUTURE PERSPECTIVES: OPPORTUNITIES AND CHALLENGES OF DDOS ATTACKS IN SD-WANS

The latest developments in SD-WAN-based multi-objective networking, such as network function virtualization (NFV), machine learning in networking (MLN), and novel transport protocols, are covered in this section. Software-Defined Wide Area Networks (SD-WANs) are highlighted because it is more vulnerable to DDoS assaults, which can also be dynamic and target specific. It is not an easy process to discover these entrance sites in SD-WAN setups due to the dynamic routing methods, decentralized architecture, and significant levels of traffic variability:

A. Dynamic Nature of Attacks

The DDoS attacks are very dynamic in terms of traffic patterns, attack vectors, and entry points which frequently vary in the course of an ongoing attack. This dynamism makes the static rule-based detection systems fail, and the current dynamic detection systems are adaptive and real-time.

B. Traceability and Source Obfuscation

The source of DDoS traffic, as well as where it has entered the SD-WAN network, is naturally hard to detect. Hackers frequently use IP spoofing or proxy relay or botnets spread over geographically dispersed locations and this makes the traceback process difficult.

C. Scalability and Performance Constraints

SD-WANs normally handle huge amounts of distributed traffic. However, incorporating real-time mechanisms of detecting and localizing DDoS in such environments adds computational overhead and latency issues which may impact performance and expandability of the network.

D. Security and Privacy Trade-offs

Localization schemes can be challenging to implement in a manner that is traffic- and deep-packet-inspection aware, requiring heavy examination on traffic. Such actions can compromise on privacy of users or even breach data protection law, which creates a major policy dilemma to service providers on security matters.

E. False Positives and Detection Reliability

Automated detection systems, especially those which use heuristic or threshold-based schemes are prone to the problem of false positives. Incorrect identification of benign traffic as malicious can lead to unnecessary disruptions and a degradation in user experience and trust.

1. Trends and Future Directions in Automation, Digital Tools with Practical Implications

Network function virtualization (SDN) is quickly becoming an essential component of smart city and other digital infrastructures for intelligent network management and automation. By utilizing the SDN controller, administrators and developers of networks are able to put into action state-of-the-art networking models, applications, and designs. Although it brings about innovative ideas, this adaptability also poses security risks and causes problems in the networking field and academic studies. Here go over some of the unanswered questions and potential avenues for further study on the safe incorporation of SDN design into smart city communication networks. Here are the main points of the research and how it will be carried out:

- Analysis of controller software implementations before smart city communication system integration to find potential design weaknesses and frequent mistakes.
- Investigation of the dispersed SDN control plane's policy collision and integration difficulty.
- Securing application authorization and access in a way that meets the needs of distinguished operations within the restrictions of networking overhead.
- Improvements in scalability to forestall the development of sophisticated assaults that exploit the immersion of controllers into data channels.
- Dealing with the domino effect of inadequacy that results from using multiple SDN controllers.
- The use of intent-based networking (IBN) and blockchain technology can improve software-defined networking (SDN) and the intelligent decision-making capabilities of businesses.

SDN offers centralized control and programmability, enhancing policy enforcement and scalability through digital tools such as software controllers, automated configuration systems, and programmable APIs. However, this digital reliance introduces significant security challenges. The SDN controller, being the central command unit, becomes a critical target for cyberattacks, and its compromise can disrupt the entire network [22]. Vulnerabilities across the control, data, and application planes, such as insecure APIs, flow rule manipulation, and limited adoption of protocols like TLS, expose the infrastructure to threats, including DDoS attacks, teleportation exploits, and malicious applications. In order to ensure such risks are curbed, robust digital security should be implemented such as use of artificial intelligence on intrusion detection technique with powerful authentication strategy, end to end encryption and use of fine grain access

DOI: 10.48175/IJARSCT-22565

controls. Proactive security systems to incorporate digital intelligence and modeling of attacker behavior is vital to have a strong and secure implementation of SDN.

VI. LITERATURE REVIEW

This section presents a review of existing studies on dynamic DDoS entry point localization in Software-Defined WANs, highlighting various approaches, integration challenges, and emerging trends in the field. Table II highlights key approaches, key findings, challenges, and future directions, offering insights into current trends and research gaps.

Haseeb-ur-rehman et al. (2023) intends to analyze and contrast the various methods used to identify DDoS attacks based on ML methods including k-means, K-Nearest Neighbors (KNN) and NB applied in IDSs and flow-based IDSs and issue data paths to filter packets in order to determine performance of HSN. This review presents the major aspects to judge the accuracy of high-speed networks, thorough taxonomy of DDoS attacks, and categorizes the methods of detection. In addition, the available literature is reviewed with the use of qualitative analysis, in accordance with the factors obtained on a taxonomy of irregular traffic pattern detection as provided. Various areas of research are proposed to assist various researchers to identify and design the most appropriate solution as it throws light to the problems and challenges faced in DDoS attacks in high-speed networks [23].

Bhayo et al. (2023) Provide an SDN-WISE IoT controller a machine learning strategy for detecting DDoS assaults. They have set up a testbed environment to simulate the generation of DDoS attack traffic and included a detection module based on machine learning into the controller. A logging mechanism is integrated into the SDN-WISE controller to capture traffic. This mechanism sends information from the network logs to a log file, which is subsequently pre-processed and transformed into a dataset. An integrated ML sub-module for DDoS detection in the SDN-WISE controller, which classifies packets in the SDN-IoT network using the NB, DT, and SVM algorithms. They compare the outcomes generated by the machine learning DDoS detection block and evaluate the operational versions of the suggested framework under different traffic simulation scenarios [24].

Ouamri et al. (2022) SD-WANs encounter the flow migration problem when the controller's processing capability is restricted. One or more CPEs placed at a location that forwards service traffic might be part of the data plane. An innovative method that optimizes the balancing process while limiting latency has been developed to tackle this problem. This method is based on DRL. Based on what knows. Their suggested solution outperforms previous baseline methods and reduces load balancing, according to the simulation results. The promise of SD-WANs to alleviate channel congestion and facilitate interconnection across multiple networks and clouds is enormous [25].

Troia et al. (2022) propose a test SD-WAN that can optimize high-priority applications (such as real-time video streaming) that are sensitive to delays and minimize network disruptions caused by downtimes. The systems for monitoring SD-WAN and traffic engineering are both a component of it. While one system makes use of an SD-WAN controller program, the other makes use of an extended Berkeley Packet Filter (eBPF) technology to keep tabs on TCP flows. In order to facilitate rapid recovery and resilience in the face of unforeseen congestion, it orchestrates network traffic according to monitoring metrics. One is located at the Politecnico di Milano and the other is in a different building; both are used within the municipal network of an Italian city. Overall service availability improved, and they were able to meet the strict quality of service standards for delay-sensitive services using their SD-WAN solution. [26].

Dayal and Srivastava (2021) introduced the SD-WAN Flood Tracer as a method for determining where an attack originated within an SD-WAN. An internal traceback identifies sources near a single controller in the first stage of the two-stage traceback technique. The second step is to pinpoint the origin near another controller using an external traceback. Legitimate traffic is shielded from DDoS attacks by using such a global traceback method. However, this approach might potentially be extended to track additional causes of anomalies in addition to DDoS attacks. The traceback approach converges the trace fast and is lightweight, causing little overhead on the communication channel. To protect the integrity of valid network communications, the suggested scheme can easily pinpoint the origin of anomalies both inside and outside the network [27].

Haque et al. (2021) suggest a mathematical model for deploying SDN SBCs in a way that maintains service during DDoS attacks. Their model includes two separate capabilities that can be adjusted with a number of input factors. It starts by figuring out how many main controllers, under typical conditions, should be placed at various nodes.

Secondly, it suggests the ideal configuration of smart backup controllers to deal with varying degrees of distributed denial of service assaults. The model's objective is to enhance DDoS assault resistance while optimizing the total cost according to the parameters. Model efficacy in minimizing total costs while preparing for SDN dependability in the event of DDoS attacks is demonstrated by simulated results [28].

This Table II compares more recent papers that involve localizing dynamic DDoS entry points in SD-WANs, noting several ML, DRL, and optimization methods, main contributions including better detection and resilience, scaling and real-time limitations, and future interests

Table 2: Literature summary on Dynamic DDoS Entry Point Localization in Software-Defined WANs

References	Study Focus	Methods/ Approaches	Key Findings	Challenges	Future Work
Haseeb-ur-rehman et al. (2023)	Comparison of ML techniques for DDoS detection in high-speed networks	DDoS detection taxonomy: K-means, KNN, and Naive Bayes	Assesses HSN performance metrics; offers a taxonomy for DDoS assaults and detection methods	Identifying optimal detection approaches for irregular traffic in HSNs	Suggests further research on designing lightweight, high-accuracy IDS for high-speed networks
Bhayo, et al. (2023)	SDN-WISE IoT controller that uses ML for DDoS detection	Naive Bayes, Decision Tree, SVM; testbed simulation with SDN-WISE controller	Successfully integrates ML-based detection in SDN controller; evaluates model performance under different traffic scenarios	Limited scalability and real-time adaptability in heterogeneous IoT environments	Improving ML models for interactive IoT-SDN settings to enable adaptive detection in real-time
Ouamri et al. (2022)	Migration of flows in SD-WANs using DRL with controller limitations	Dynamic Recurrent Learning (DRL); latency-aware workflow balancing	DRL significantly reduces load imbalance and latency compared to traditional approaches	Limited processing power of SDN controllers in real-world scenarios	Extending DRL model adaptability to multi-cloud, multi-tenant SD-WAN environments
Troia, et al. (2022)	Real-time traffic optimization and resilience in SD-WAN	eBPF-based Transport-layer Passive Monitoring (TPM), SDN traffic engineering	Proposed solution increases availability and meets QoS requirements for delay-sensitive services like video streaming	Handling unanticipated congestion and scaling for wider deployment	Expanding system capabilities for broader service types and multi-site network orchestration
Dayal, et al. (2021)	Traceback mechanism for detecting DDoS sources in SD-WAN	SD-WAN Flood Tracer: internal and external traceback schemes	Lightweight scheme efficiently traces internal and external sources; minimises communication overhead	Ensuring traceback scalability across multiple SDN controllers	Investigating traceback for other network anomalies and extending scalability to large-scale SD-WANs
Haque et al. (2021)	Optimisation model for SDN controller deployment for	Mathematical optimisation model for primary and smart backup	Effectively plans reliable SDN architecture; balances DDoS resistance with	Managing cost-performance trade-offs for different attack	Incorporating dynamic traffic and adaptive controller selection

	DDoS resilience	controller placement	cost efficiency	levels	based on real-time threat detection

VII. CONCLUSION AND FUTURE WORK

A look at DDoS attacks on SDN networks that has already been done, along with a quick look at ML and DL methods. Security problems with SDN are still a big problem, even though it is used in many real-life situations. A lot of people have problems with DDoS attacks in SDN. This study looks at those problems and shows a few common ways to find and stop DDoS attacks in SDN settings. Based on how well these methods work in real time, how many network resources they use, and the kinds of DDoS attacks that can happen, the pros and cons of these methods are looked at. An in-depth look at the research on new ways to find and stop DDoS attacks and other security problems in SDNs is presented in this publication. The taxonomy shows new trends in DDoS defence mechanisms, including the use of statistical models, machine learning, blockchain, network function virtualization, honeynet, network slicing, and moving target defence in SDN. It also lists the strengths and weaknesses of each method. Despite not being specifically made to provide security, these taxonomies include groups of methods that do just that. The writer wants to use threat intelligence to create models of attackers, come up with dynamic defence strategies that use SDN programming, find DDoS attacks early and pinpoint attackers' locations, reduce the amount of work that controllers have to do, and make it possible to track down attackers. There are some problems with the proposed DLADSC method that need to be fixed before it can be used in future DDoS detection studies.

REFERENCES

[1] N. P. Mwanza and J. Kalita, “Detecting DDoS Attacks in Software Defined Networks Using Deep Learning Techniques: A Survey,” Int. J. Netw. Secur., vol. 25, no. 2, p. 360, 2023, doi: 10.6633/IJNS.202303.

[2] A. Goyal, “Optimising Software Lifecycle Management through Predictive Maintenance : Insights and Best Practices,” Int. J. Sci. Res. Arch., vol. 07, no. 02, pp. 693–702, 2022.

[3] N. Patel, “Sustainable Smart Cities : Leveraging IoT and Data Analytics for Energy Efficiency and Urban Development,” J. Emerg. Technol. Innov. Res., vol. 8, no. 3, 2021.

[4] A. B. Wankhede and P. Chandran, “A Study on DDOS Attacks, Danger, and its Prevention,” Int. J. Adv. Res. Sci. Commun. Technol., vol. 2, no. 1, pp. 51–57, Jul. 2022, doi: 10.48175/IJARSCT-5645.

[5] S. Singamsetty, “Fuzzy-Optimized Lightweight Cyber-Attack Detection For Secure Edge-Based IoT Networks,” J. Crit. Rev., vol. 6, no. 07, pp. 1028–1033, 2019, doi: 10.53555/jcr.v6:i7.13156.

[6] A. Kushwaha, P. Pathak, and S. Gupta, “Review of optimize load balancing algorithms in cloud,” Int. J. Distrib. Cloud Comput., vol. 4, no. 2, pp. 1–9, 2016.

[7] I. A. Valdovinos, J. A. Pérez-Díaz, K.-K. R. Choo, and J. F. Botero, “Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges and future directions,” J. Netw. Comput. Appl., vol. 187, Aug. 2021, doi: 10.1016/j.jnca.2021.103093.

[8] W. Ben Jaballah, M. Conti, and C. Lal, “Security and design requirements for software-defined VANETs,” Comput. Networks, vol. 169, Mar. 2020, doi: 10.1016/j.comnet.2020.107099.

[9] J. H. Cox et al., “Advancing Software-Defined Networks: A Survey,” IEEE Access, vol. 5, pp. 25487–25526, 2017, doi: 10.1109/ACCESS.2017.2762291.

[10] Z. Yang, Y. Cui, B. Li, Y. Liu, and Y. Xu, “Software-defined wide area network (SD-WAN): architecture, advances and opportunities,” in Proceedings - International Conference on Computer Communications and Networks, ICCCN, 2019. doi: 10.1109/ICCCN.2019.8847124.

[11] K. M. R. Seetharaman, “Internet of Things (IoT) Applications in SAP: A Survey of Trends, Challenges, and Opportunities,” Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 2, pp. 499–508, Mar. 2021, doi: 10.48175/IJARSCT-6268B.

[12] J. Bhatia, Y. Modi, S. Tanwar, and M. Bhavsar, “Software defined vehicular networks: A comprehensive review,” Int. J. Commun. Syst., vol. 32, no. 12, 2019, doi: 10.1002/dac.4005.

[13] Geeta, S. Gupta, and S. Prakash, “QoS and Load Balancing in Cloud Computing-an Aaccess for Performance Enhancement Using Agent Based Software,” Int. J. Innov. Technol. Explor. Eng., vol. 8, no. 11s, pp. 641–644, 2019, doi: 10.35940/ijitee.K1107.09811S19.

[14] P. Choudhary and P. Potdar, “Robotics in STEM Education: Enhancing Engagement, Skills, and Future Readiness,” Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 1, p. 11, 2023.

[15] N. Malali, “View of Real-Time Liability Monitoring in Annuities Using Actuarial Dashboards on Streaming Data,” Asian J. Comput. Sci. Eng., vol. 8, no. 1, pp. 1–7, 2023.

[16] R. Vishwakarma and A. K. Jain, “A survey of DDoS attacking techniques and defence mechanisms in the IoT network,” Telecommun. Syst., vol. 73, no. 1, pp. 3–25, Jan. 2020, doi: 10.1007/s11235-019-00599-z.

[17] C. Urrea and D. Benítez, “Software-Defined Networking Solutions, Architecture and Controllers for the Industrial Internet of Things: A Review,” Sensors, vol. 21, no. 19, Oct. 2021, doi: 10.3390/s21196585.

[18] S. Dong and M. Sarem, “DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks,” IEEE Access, vol. 8, pp. 5039–5048, 2020, doi: 10.1109/ACCESS.2019.2963077.

[19] R. Taheri, H. Ahmed, and E. Arslan, “Deep learning for the security of software-defined networks: a review,” Cluster Comput., vol. 26, no. 5, pp. 3089–3112, Oct. 2023, doi: 10.1007/s10586-023-04069-9.

[20] R. N. Carvalho, J. L. Bordim, and E. A. P. Alchieri, “Entropy-based DoS attack identification in SDN,” in Proceedings - 2019 IEEE 33rd International Parallel and Distributed Processing Symposium Workshops, IPDPSW, 2019. doi: 10.1109/IPDPSW.2019.00108.

[21] A. Balasubramanian, “Dynamic dependency management in software projects using clustering algorithms,” Int. J. Core Eng. Manag., vol. 7, no. 4, pp. 244–255, 2022.

[22] S. S. S. Neeli, “Critical Cybersecurity Strategies for Database Protection against Cyber Attacks,” J. Artif. Intell. Mach. Learn. Data Sci., vol. 1, no. 1, 2023.

[23] R. M. A. Haseeb-ur-rehman et al., “High-Speed Network DDoS Attack Detection: A Survey,” Sensors, vol. 23, no. 15, 2023, doi: 10.3390/s23156850.

[24] J. Bhayo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir, and D. Draheim, “Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks,” Eng. Appl. Artif. Intell., vol. 123, Aug. 2023, doi: 10.1016/j.engappai.2023.106432.

[25] M. A. Ouamri, G. Barb, D. Singh, and F. Alexa, “Load Balancing Optimization in Software-Defined Wide Area Networking (SD-WAN) using Deep Reinforcement Learning,” in 2022 International Symposium on Electronics and Telecommunications (ISETC), IEEE, Nov. 2022, pp. 1–6. doi: 10.1109/ISETC56213.2022.10010335.

[26] S. Troia, M. Mazzara, M. Savi, L. M. M. Zorello, and G. Maier, “Resilience of Delay-Sensitive Services With Transport-Layer Monitoring in SD-WAN,” IEEE Trans. Netw. Serv. Manag., vol. 19, no. 3, pp. 2652–2663, Sep. 2022, doi: 10.1109/TNSM.2022.3191943.

[27] N. Dayal and S. Srivastava, “SD-WAN Flood Tracer: Tracking the entry points of DDoS attack flows in WAN,” Comput. Networks, vol. 186, Feb. 2021, doi: 10.1016/j.comnet.2021.107813.

[28] M. R. Haque et al., “Automated Controller Placement for Software-Defined Networks to Resist DDoS Attacks,” Comput. Mater. Contin., vol. 68, no. 3, pp. 3147–3165, 2021, doi: 10.32604/cmc.2021.016591.

DOI: 10.48175/IJARSCT-22565