International Journal of Safety and Security Engineering
Vol. 15, No. 12, December, 2025, pp. 2573-2587
Journal homepage: http://iieta.org/journals/ijsse

Software-Defined Wide Area Network Enhanced IoT Network: Performance Optimization and Security Analysis under Distributed Denial of Service Attack Scenarios

Moussa Malqui[1], Mariyam Ouaissa[1*], Mariya Ouaissa[2], Mohamed Hanine[1]

[1] Laboratory of Information Technologies, Chouaib Doukkali University, El Jadida 24000, Morocco
[2] Laboratory of Computer Science and Smart Systems, Cadi Ayyad University, Marrakech 40000, Morocco

Corresponding Author Email: ouaissa.mariyam@ucd.ac.ma

https://doi.org/10.18280/ijsse.151214

Received: 16 October 2025
Revised: 15 December 2025
Accepted: 24 December 2025
Available online: 31 December 2025

Keywords:
software-defined wide area network, Internet of Things, network performance optimization, Distributed Denial of Service attack resilience, Message Queue Telemetry Transport protocol, Constrained Application Protocol protocol, traffic prioritization

ABSTRACT

The exponential growth of Internet of Things (IoT) deployments imposes stringent demands on network performance and security, particularly in distributed environments where traditional wide area networks (WANs) often fail to meet reliability and flexibility requirements. Software-defined wide area network (SD-WAN) emerges as a promising solution to address these challenges through centralized orchestration and intelligent traffic management. This paper investigates the integration of SD-WAN technology within IoT environments, focusing on its impact on network performance metrics and security resilience. We develop a comprehensive simulation framework using PnetLab with FlexiWAN, incorporating Message Queue Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) traffic models. Our experimental analysis demonstrates that SD-WAN implementation significantly enhances network performance during primary link degradation, reducing latency by up to 85%, jitter by 97%, and packet loss by 99% for CoAP traffic compared to traditional WAN configurations. Furthermore, we propose and evaluate a traffic prioritization policy that effectively allocates network resources to IoT applications over conventional traffic. To assess security implications, we model Distributed Denial of Service (DDoS) attacks within the SD-WAN infrastructure, revealing that CoAP traffic latency increases from 35 ms to 121 ms under 800 Mbps attack traffic, primarily due to increased CPU utilization in SD-WAN devices. The findings underscore both the substantial benefits and inherent vulnerabilities of SD-WAN deployment in IoT contexts, providing practical insights for network architects and highlighting directions for future enhancements through edge computing and AI-driven security mechanisms.

1. INTRODUCTION

The world is continually evolving towards greater intelligence, enhancing human quality of life by simplifying daily activities through interconnected smart systems and devices. To achieve this crucial goal, the main concept of Internet of Things (IoT) first appeared around 1982 with a modified Coke vending machine at Carnegie Mellon University to be able to report the status of its inventory and whether newly loaded drinks were cold or not. This vending machine is considered the first object connected, but the term "Internet of Objects" was coined by Kevin Ashton from Procter and Gamble Cooperation (P&G) in 1999 [1]. Today, the IoT has marked an exponential growth, with billions of connected devices continuously generating massive volumes of data, with requirements for response time, transmission reliability, and security. Most of these devices are frequently deployed in dispersed geographical sites or distributed environments, as is the case for smart cities, industrial networks, healthcare systems, and critical infrastructures.

The evolution of IoT, driven by demands for higher connectivity performance, security, and flexibility, challenges the viability of traditional networks. These legacy systems lack the necessary flexibility, intelligence, and security, while also incurring high costs (e.g., for MPLS deployment). Consequently, they are increasingly unable to meet the demands of modern, revolutionary applications. To address these limitations, the need for an innovative solution arises. This is why the software-defined wide area network (SD-WAN) technology appeared around 2014, combining three technologies: wide area network (WAN), software-defined networks (SDN), and network function virtualization (NFV) [2]. The main goal of this approach is to separate the control plane from the data plane by creating an overlay network that operates on top of the existing underlay network [3], unlike traditional WANs, where the control and data still depend on the current evolution of e hardware. This separation enhances the flexibility of centralized control and management of data networks, allowing for routing over the best path available regardless of the access technologies used, which may include telephone networks, optical fiber, radio access, or the electrical network. Moreover, the overlay also allows for a secure connection between separated sites based on encryption protocols such as IPsec or DTLS [4], depending on the

manufacturer's solution.

Based on these characteristics, the SD-WAN, as a new revolutionary solution, helps to solve the challenges related to critical environments like IoT in terms of network performance, connectivity, and security, thanks to its ability to intelligently manage traffic and multiple types of connections with centralized orchestration based on specified metrics depending on the sensitivity and the criticality of each application. The integration of SD-WAN into decentralized IoT structures enhances continuous network availability, improves service quality, ensures communication protection, and promotes the scalability of installations. Currently, this integration constitutes a strategic direction for companies aiming to establish infrastructures that are intelligent, flexible, and secure. Despite all these advantages and benefits of this technology, there are several challenges that should be analyzed and addressed to ensure the reliability, optimized performance, and security of the SD-WAN network infrastructure.

Many SD-WAN studies focus on IT and OT environments but neglect the IoT environment, which often receives less attention and lacks sufficient research. There are some studies that focus on network performance, while others focus on security in SD-WAN, such as risk assessment analysis in OT environments or Distributed Denial of Service (DDoS) attacks in IT environments. However, there is no work that combines all network performances and security of SD-WAN correlated with resource utilization in an IoT environment by simulating multiple protocols. This work addresses SD-WAN technology in IoT environments by developing a simulation model using PnetLab and the open-source SD-WAN solution FlexiWAN, incorporating Message Queue Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) traffic to evaluate the effect of SD-WAN on IoT environments, then modeling a DDoS attack into this simulation model to evaluate the SD-WAN solution's response to such a cyberattack, and analyzing the relationship between resource consumption and key network performance metrics regarding latency, packet loss, jitter, and bandwidth, highlighting the importance of improving the SD-WAN solution by integrating cutting-edge technologies such as Edge AI, Fog/Edge computing technologies, and zero trust network access (ZTNA) mechanisms. The main contributions of this research paper are:

- Multiple scenario designs that permit the evaluation of the network performance and security of SD-WAN in IoT environments.
- Establishing a detailed and reproducible simulation model based on PnetLab, FlexiWAN, MQTT, and CoAP traffic, which can serve as a reference for future studies on SD-WAN-enabled IoT traffic.
- Evaluating multiple metrics such as latency, jitter, and packet loss correlated with CPU and memory utilization.
- Deploying a new policy to prioritize the IoT traffic (MQTT and CoAP traffic) over the other types of traffic to demonstrate the benefit of SD-WAN in the traffic classification.
- Modeling a DDoS attack to simulate the SD-WAN behavior in a stress case by varying the quantity of traffic transmitted through links.

The rest of this paper is organized as follows: The second section presents the related work and highlights the gap in the literature on SD-WAN in IoT environments. The third section concerns the background, presenting the system model including the functionalities of SD-WAN and IoT and their integration, as well as discussing the security issues related to SD-WAN. The fourth section presents the proposed scheme, which includes a simulation of SD-WAN in an IoT environment using MQTT and CoAP protocols, then a simulation of a DDoS attack within the SD-WAN network. The fifth section illustrates the simulation results with a discussion. Finally, the sixth section concludes this paper.

2. RELATED WORK

In the existing works, to address the various issues and challenges related to network performance and security in IoT environments, numerous solutions were proposed based on SD-WAN and SDN. Nazemi Absardi and Javidan [5] propose a new predictive SD-WAN traffic management method based on a deep recurrent neural network (RNN) for IoT networks in multi-datacenters that aims to enhance the quality of service (QoS) of IoT networks through optimizing the crucial metrics such as end-to-end delay and bandwidth utilization. It ensures its effectiveness by predicting the network state, such as latency and available bandwidth, before the traffic flows arrive, which allows the SD-WAN controller to determine the optimal paths in advance. Unlike the traditional routing methods, this new method has demonstrated its efficacy regarding performance by reducing the latency and ensuring equitable distribution of bandwidth. Similarly, in the literature by Ali and Roh [6], a new method for selecting SDN controllers for the IoT was proposed. The authors emphasize that existing controller selection approaches often overlook the specific characteristics of IoT and the complex interdependencies between them. To refocus on this point, they used an analytical network decision-making process (ANDP)-based technique that evaluates both performance in real-world conditions and features, such as stream query management, scalability, and energy management. The results obtained show an improvement in performance with reduced latency, increased throughput, optimized CPU usage, and enhanced network resilience in case of failure compared to previous methods.

Moreover, the security of SD-WAN plays a crucial role in securing the IoT environments. Saeed [7] explores the role of SD-WAN technology in enhancing security and network approach within intelligent environments, a concept essential in the era of Industry 4.0 and the IoT. This study presents a novel model of network connections with various smart devices and examines the efficiency of SD-WAN compared to traditional network architectures, with an emphasis on flexibility, programmability, and the management of WANs. The obtained results confirm the contribution of this approach to more efficient, secure, and scalable network connections for the future of intelligent environments. Bhayo et al. [8] propose Counter-based DDoS Attack Detection (C-DAD) as a new Software-Defined Internet of Things (SD-IoT)-based framework to provide security services to the IoT network through detecting DDoS attacks based on counter values of different network parameters. The results demonstrate that the framework efficiently detects attacks, thereby minimizing the time of attack detection with minimal consumption of CPU and memory resources. Table 1 summarizes the related works based on topologies and testbeds evaluated.

Table 1. Comparison of topologies and testbeds evaluated

Prior Work	Topology/Testbed	Protocols	Metrics	Security Aspect	Limitations
[5]	Introducing a new predictive SD-WAN traffic management method based on deep RNN for IoT networks in multi-datacenters, in which two edge data centers and one cloud data center are connected to an SD-WAN-based infrastructure network with two IoT applications. This topology was implemented in the IoTSim-Osmosis simulator.	CoAP	Latency, Bandwidth utilization	--	Absence of security aspects Limited to the CoAP protocol in the IoT environment Limited to latency and bandwidth utilization metrics.
[6]	Creating an SDN physical architecture on three controllers using the Mininet emulator with a Python-based API, the topologies of sensor nodes were generated by increasing the number of nodes in a linear physical architecture up to 500, then collecting performance data for each controller.	TCP	Latency, Throughput, CPU usage, Network resilience	--	Absence of the security aspect Despite the study focusing on the IoT environment, the simulation was performed by the TCP protocol without specifying an IoT protocol.
[7]	The experimental setup was composed of two home networks with respective applications. Three interconnected Alcatel-Lucent 7750 IP service edge routers link each network to an Internet Service Provider (ISP) network. To ensure the forwarding function, each home network has a residential gateway built on an open vSwitch. The deployment of the OpenFlow-configurable switch was connected with various virtualized functions.	TCP, UDP, OpenFlow	Network efficiency, Security, scalability	Secure SD-LANs	Metric network performance and security are not evaluated quantitatively. Lack of a clear security approach. Lack of detailed study protocols for intelligent devices.
[8]	Three experiments were performed using varying parameters, such as IoT nodes, attack nodes, packet payload, packet burst, and others, to launch the DDoS attack in the SD-IoT network. These experiments are simulated by using the Cooja simulator with the help of the Contiki OS to create a realistic virtual SD-IoT network, which includes the SDNWISE controller, IoT nodes, and Sensor OpenFlow Switch (SOFS).	CoAP, 6LowPAN, IEEE 802.11.4 protocol	Attack detection time, Throughput, CPU, Memory utilization	Providing security services to the IoT network through the C-DAD framework	C-DAD is limited to operating on the IEEE 802.11.4 protocol. Network performance, is not evaluated as latency or packet loss to be impacted by the C-DAD framework.

Note: SD-WAN = Software-Defined Wide Area Network; IoT = Internet of Things; RNN = Recurrent Neural Network; CoAP = Constrained Application Protocol; SDN = Software-Defined Networking; API = Application Programming Interface; TCP = Transmission Control Protocol; ISP = Internet Service Provider; vSwitch = Virtual Switch; UDP = User Datagram Protocol; OpenFlow = a communications protocol for SDN; DDoS = Distributed Denial of Service; SD-IoT = Software-Defined Internet of Things; 6LowPAN = IPv6 over Low-Power Wireless Personal Area Networks; IEEE 802.11.4 = a standard for low-rate wireless personal area networks; Contiki OS = an open-source operating system for IoT devices; SOFS = Sensor OpenFlow Switch; C-DAD = Counter-Based DDoS Attack Detection.

In the study by Nazemi Absardi and Javidan [5], the simulation was performed on IoTSim-Osmosis to evaluate latency and bandwidth utilization for the CoAP protocol; however, the approach is still limited to the CoAP protocol and specific metrics, and it does not discuss security aspects. In the study by Bhayo et al. [8], the framework was simulated under the Cooja simulator with the SDNWISE controller to evaluate detection time, throughput, and CPU and memory utilization metrics; however, the evaluation is still limited to the CoAP protocol and the specified metrics. Moreover, network performance is not evaluated in terms of latency or packet loss to analyze the impact of the C-DAD framework on network performance. In contrast, our study evaluates two different protocols, MQTT and CoAP, to extend the scope of the IoT environment studied. Furthermore, our analysis evaluates various network and security metrics, including latency, jitter, packet loss, CPU, and memory, with bandwidth varying in the DDoS attack scenario to demonstrate the SD-WAN behavior facing such an attack and its impact on performance in an IoT environment. Moreover, the simulation was performed using a real SD-WAN open-source solution installed in the PnetLab emulator, which gives precise results that are near reality.

3. BACKGROUND

This section provides an overview of the SDN-WAN architecture and its integration with the IoT. It also highlights the key security challenges that arise within this combined ecosystem.

3.1 System model

3.1.1 Software-defined wide area network architecture

SD-WAN is one of the innovative technologies that enhances network connectivity in the world by addressing the limitations of traditional WANs regarding network and security performance. Unlike the traditional WAN that depends on specific hardware, this innovative technology focuses on separating the control plane from the data plane by decoupling the network management and control from physical hardware through SDN and NFV. These two

technologies enable the creation of an overlay network built on top of an existing underlying physical network, by which the dispersed geographical sites can be connected in a secure manner through an encrypted tunnel using an encryption protocol such as IPsec or DTLS protocols, allowing for centralized control and flexible network management of all dispersed sites of an organization.

Unlike traditional WAN architecture, the SD-WAN architecture is a centralized, flexible, and scalable network management solution that can adjust to different application types and modern business requirements, offering a QoS and quality of experience that can be affected in the traditional WAN by long distances, facilitating congestion, packet loss, transmission delays, and stability. To address these constraints related to the traditional WAN, the SD-WAN architecture is based on creating a virtual network over the physical network that allows centralized traffic control and network management by routing the traffic in a secure and intelligent manner. SD-WAN architecture consists of three planes, as presented in Figure 1: the data plane, the control plane, and the orchestration plane [9].

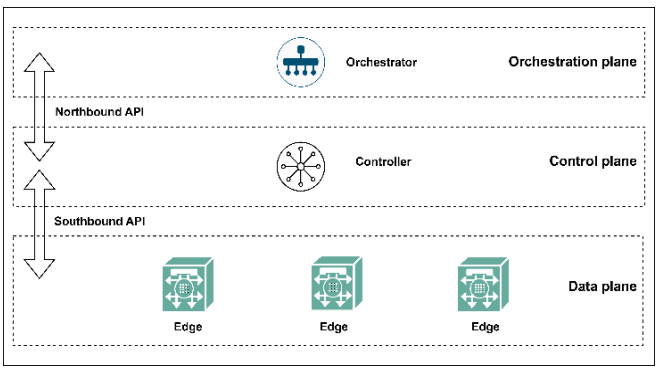

Figure 1. Software-defined wide area network (SD-WAN) architecture

Data plane: It constitutes the infrastructure layer responsible for packet transmission, facilitating communications between multiple disparate sites, including headquarters, branch sites, and cloud infrastructures and services based on the control plane's decisions [10]. The communication is guaranteed by the tunnels established between the SD-WAN edge devices deployed at each site. The connection between the controller and the edge devices is established via the Southbound Application Programming Interface (API) (OpenFlow, etc.) [11].

Control plane: It represents the main layer in the SD-WAN architecture and includes the controller (or several controllers) as the central brain, which decides the traffic forwarding based on multiple metrics to identify the best paths to route the traffic [12]. Such as in the case of path deficiencies or congestion, the controller will intelligently and dynamically route the traffic through the available and best path, which is also accountable for regulating and managing the configuration of protocols on devices connected in the data plane through southbound APIs, as well as connected to the orchestrator in the orchestration plane through northbound APIs.

Orchestration plane: It provides an interface for easy and centralized management of policy and strategy deployments at the controller, and it is responsible for automating the management of large deployments, such as the zero touch provisioning (ZTP) concept, which allows configuration to be set up on many SD-WAN edge devices at once without needing to configure each device separately. It also enables monitoring, troubleshooting, analytics, notifications, and reporting services that help administrators optimize the deployed policies and strategies [13]. The main entity in this layer that allows all these functionalities is called the orchestrator, although each manufacturer has its own software solution for it that goes by different names. It might be a stand-alone implementation or a part of the controller that includes multiple sub-entities. This is why some studies include the orchestrator in the control plane, eliminating the orchestration plane.

3.1.2 Path selection

In SD-WAN, the path selection is based on multiple metrics, namely latency, jitter, packet loss, and bandwidth. The controller's decision is based on these metrics calculated by the SD-WAN edge through active or passive monitoring [14]; the active monitoring mechanism is based on small and overhead test packets, such as ICMP or UDP probes, sent continuously by the SD-WAN edge device through all available WAN links to other relevant edge devices or a central reference hub. While the passive monitoring mechanism is based on real traffic analysis to measure these metrics, the SD-WAN edge observes the performance of actual data traffic going through it. The metrics measured:

Latency: Measured in ms, calculated using the round-trip time (RTT). Real latency refers to the total time taken for a packet to travel one way from the source to the destination, while RTT measures the total time for a packet to travel from the source to the destination and back, specifically the duration between sending a SYN and receiving an ACK-SYN in the TCP model. So, the RTT presents the one-way latency. However, the RTT is frequently used as a practical alternative to the real latency regarding the potential asymmetries in the network, which presents a challenge to calculating it. In the SD-WAN, managing latency means ensuring low latency for a real-time application like VoIP or live video streaming. Therefore, the RTT of the packet and the mean RTT of the flow could be calculated as follows:

$$\mathrm{RTT}_i = t_{arrival,i} - t_{departure,i} \tag{1}$$

$$\mathrm{RTT}_m = \frac{1}{n}\sum_{i=1}^{n}\mathrm{RTT}_i \tag{2}$$

where,

$\mathrm{RTT_i}$ is the *RTT* of packet i;

$\mathrm{RTT_m}$ is the mean *RTT* of the flow composed of n packet;

$\mathrm{t_{arrival,i}}$ is the moment at which packet i arrived in return;

$\mathrm{t_{departure,i}}$ is the moment at which packet i is transmitted;

n is the number of packet in the flow.

Packet loss: It presents the percentage of probe packets that fail to reach the destination. In the SD-WAN, managing the packet loss referred to finding the best link to send sensitive data and using some method to manage the traffic, like forward error correction (FEC) and packet duplication.

$$PacketLoss = \frac{Number\ of\ \ packet\ \ failures}{The\ total\ number\ of\ \ packets\ sent} \times 100\% \tag{3}$$

Jitter: It is measured in ms and presents the variation of latency between successive packets. In SD-WAN, managing

jitter is referred to as finding the more stable link to send sensitive data. Therefore, the jitter of flow, composed of n packets, could be calculated by the following formula:

$$J = \frac{1}{n-1}\sum_{i=1}^{n-1}\left|t_{i+1} - t_i\right| \quad (4)$$

where,

t_i is the arrival time of the ith packet;

n is the number of packets in the flow.

Bandwidth: SD-WAN can estimate the available bandwidth through two methods: proactive monitoring through user datagram protocol (UDP) probes and passive monitoring based on current utilization. In the proactive mode, the bandwidth is calculated directly, while in the passive monitoring mode, it can be calculated by the following formula:

$$\begin{aligned} &Available\ Bandwidth \\ &= Total\ bandwidth \\ &- Current\ bandwidth\ utilization \end{aligned} \quad (5)$$

The SD-WAN can mitigate high packet loss and latency using two techniques [15]:

FEC involves sending redundant data to control and correct errors without the need for retransmission. This technique helps anticipate packet drops during transit and eliminates the need for retransmission, which directly reduces the latency.

Packet duplication enables the reduction of data loss by sending duplicate packets through multiple links simultaneously. The first packet received will be used, and other packets will be discarded. It can also help reduce the latency by ensuring faster packet transmission.

Based on these calculated metrics and the path computation method, the controller decides over which path the traffic will be routed. There are many path computation methods [16]:

Priority-based path selection: This method permits routing the traffic through a link with the lower priority or cost.

Load balancing: This method enables load balancing of the traffic through the available or selected links, allowing for the use of all available links or just some to transmit traffic using an appropriate algorithm that improves performance and fault tolerance; if a connection fails, it will be automatically abandoned while ensuring service on the remaining connections. This method can also increase resilience to DDoS attacks.

Dynamic path selection: This method permits routing the traffic through the link with the best quality; it can also be customized by defining the threshold of each metric or selecting the path based on a specified metric.

Traffic shaping and prioritization: This enables defining the QoS for each application based on the differentiated services code point (DSCP) value included in the type of service (TOS) header, which is within the IP header and is used to classify and prioritize network traffic. The utilization of DSCP values allows the SD-WAN edge to implement distinct packet handling strategies based on the type of traffic. By applying this method to critical applications, SD-WAN helps minimize the impact of high latency, ensuring that it receives the necessary bandwidth and minimal delay.

3.1.3 Software-defined wide area network technology based IoT applications

The IoT is one of the smart technologies used to simplify daily life; it refers to a network of connected heterogeneous smart devices that can sense and interact with the external world, operating independently without humans. This independence gives intelligence to these connected devices to make decisions based on their analysis. These devices can include sensors, smartwatches, garage doors, cameras, lamps, etc. Due to the resource constraints of these devices with low computing power, they use lightweight protocols like ZigBee, CoAP, AMQP, or MQTT that are known for their simplicity to avoid the consumption of a significant number of resources. Connecting these smart devices to the internet creates an IoT network, enabling them to communicate with each other over the internet [17].

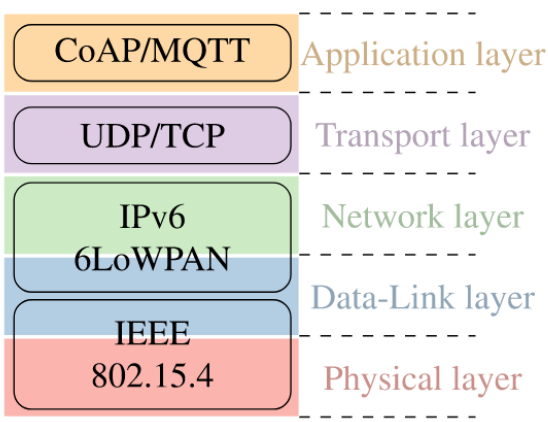

Figure 2. The IoT protocol stack

Figure 2 presents the IoT protocol stack [18], which consists of five layers. The physical layer and data-link layer are defined by the IEEE 802.15.4 standard, on top of which protocols like Zigbee, Thread, or IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) are built, designed for low-data-rate, low-power, and short-range communication. The 6LoWPAN layer is an adaptive layer between the data-link layer and the network that allows IPv6 packets to be transmitted over IEEE 802.15.4 networks; this makes it possible to use IPv6 on IoT constrained devices like sensors and actuators. The transport layer is defined by TCP or UDP; the choice between these two protocols depends on the protocol deployed on the upper layer, which is the application layer, such as MQTT built on TCP or CoAP built on UDP.

CoAP protocol was created by the Internet Engineering Task Force (IETF) specifically for constrained devices and networks in IoT; it is a request/response protocol based on RESTful architecture like HTTP, with the complexity reduced by using UDP, which is characterized by being lightweight and connectionless. The CoAP protocol provides functionalities such as an asynchronous transaction model, a dedicated URI scheme (coap://), and support for unicast and multicast communications. Retransmission is handled through Confirmable (CON) messages, which are retransmitted if no acknowledgment is received. In contrast, Non-confirmable (NON) messages are not retransmitted, meaning packet delivery is not guaranteed and may result in packet loss [19]. To ensure secure communication, DTLS can be used to enable encryption, authentication, and message integrity [20]. This protocol is characterized by sensitivity to packet loss but with low latency.

The MQTT protocol was created by IBM in 1999. This

protocol is based on a publish-subscribe model designed for very lightweight messaging with minimal overhead, as well as the emerging M2M communications or IoT world of connected devices. For security, this protocol is built on TCP rather than CoAP, so TLS/SSL can be deployed to assure the security related to authentication, encryption, and message integrity. This protocol offers various functionalities; it is designed for constrained networks and low bandwidth by ensuring a small amount of transport overhead and limiting protocol exchanges to reduce network traffic in an environment with low bandwidth. Regarding the use of TCP with MQTT, it ensures reliable delivery and packet retransmission, which provides a solution to avoid connection interruption in constrained and unstable networks. Moreover, MQTT supports three levels of QoS, which adds another layer of reliability; QoS 0 depends on the network's performance, and the arrival of the packet is not guaranteed, while QoS 1 assures the message will be delivered at least once with retries if acknowledgment is not received, and for QoS 2 the message will be delivered exactly once, which ensures no duplication [21]. Therefore, this protocol performs better in handling packet loss compared to the CoAP protocol, although it introduces more latency due to retransmission.

SD-WAN technology improves network performance and security via dynamic and intelligent routing, as well as FEC and packet duplication techniques to mitigate packet loss for critical applications, while also securing interconnections between remote sites through tunnel encryption utilizing the IPsec protocol. However, IoT applications often exhibit sensitivity to latency and packet loss, and certain applications, such as those for connected healthcare systems monitoring patients, necessitate real-time performance. Alerts must be communicated promptly to avert a life-threatening emergency. Consequently, similar to the case of autonomous vehicles, the sensors (Light Detection and Ranging (LIDAR), cameras, and radars) must transmit data to the control system in near real-time, as any delay can prevent obstacle detection and cause an accident. The implementation of SD-WAN in an IoT environment will significantly enhance the management of network instability limits and provide improved security via encrypted communications. Taking Connected Healthcare Systems as an example, configuring SD-WAN to prioritize patient monitoring and alert traffic with higher QoS, as well as the activation of FEC and packet duplication, will undoubtedly augment the network's reliability and security in comparison to traditional WAN.

3.2 Security issues in software-defined wide area network

SD-WAN technologies provide significant improvement of network performance by reducing latency, packet loss, jitter, and optimizing bandwidth utilization, security by encrypting traffic between remote sites, scalability, and cost efficiencies for enterprises by migrating from costly MPLS to public internet connections with encryption. This migration from private network to public internet connections, combined with multicloud integration and centralized control, extends the potential attack surface within the SD-WAN environment. The following major security challenges are identified:

3.2.1 The centralized architecture and segmentation issues

Although there are benefits to the centralized architecture of the SD-WAN solution, which provides centralized control and a comprehensive view of network state, it may cause a major security risk related to the controller compromise. If the controller is compromised, the hacker can gain complete unauthorized control over the network, causing major incidents and compromising the confidentiality, integrity, and availability of the infrastructure through traffic flow manipulation, sensitive data theft, or even bringing down the entire network. This case illustrates the major risk of making the SD-WAN infrastructure unavailable due to the compromise of the central brain [22]. Furthermore, if an endpoint is compromised, the SD-WAN architecture's overlays, which mostly span numerous distant locations, branches, data centers, and cloud environments, may cause lateral movement throughout the network if they are not properly segmented or micro-segmented, which allows the compromise of all remote sites connected.

3.2.2 Security between edge devices

On SD-WAN infrastructure, the data going between the devices' edges is often transmitted via the public internet, which is open, shared, and untrusted. Although this data is encrypted using IPsec or DTLS protocols with the advanced encryption algorithms and authentication mechanisms deployed through tunnels, the misconfigurations, outdated cryptographic suites, or zero-day vulnerabilities combined with the use of the public internet can present security risks such as tunnel hijacking, data interception, and denial of service attacks [23]. As an example, the volumetric DoS or DDoS attacks over one of the links connected to SD-WAN can impact the general stability and availability of the SD-WAN network; although the use of multiple link connections, the exploitation of one of them can saturate the bandwidth and increase the resource utilization. On the other hand, the use of encrypted tunnels in many SD-WAN solutions might not provide comprehensive insight into the exchange of east-west data between edge devices. This reduces the effectiveness of classical threat detection tools based on content, which may cause the spread of malware or ransomware among branch locations, a delayed response and remediation to identify the compromised devices or internal threats, and complex implementation of micro-segmentation policies.

3.2.3 Application Programming Interface integration issues

Today, APIs are ubiquitous; they have become a pillar of modern computing and serve as intermediaries to allow different applications, systems, or services to communicate with each other in a standardized and secure manner. Most SD-WAN solutions expose APIs for integration with third-party monitoring, security solutions like SIEM, audit tools, and cloud services through exposing RESTful APIs. While these APIs offer extensibility and interoperability with various platforms, they also present potential security risks with insufficient input validation in API calls, poor token or credential management, the absence of rate limiting, verbose error messages that can expose sensitive information, and insecure third-party scripts interacting with SD-WAN systems. The exploitation of one of these improperly secured APIs can allow data breaches, API DoS attacks, control plane manipulation, and unauthorized configuration changes.

3.2.4 Multi-tenancy and shared infrastructure risks

As is known today, the trends are the migration to cloud infrastructure instead of on-premises infrastructure; this implies the use of managed infrastructure services, which create a multiple-tenant environment where tenants may share

the same infrastructure or some resources. In SD-WAN architecture, the same orchestrator or infrastructure may be shared by several tenants in large-scale installations or managed SD-WAN services. In multi-tenant SD-WAN, multiple security concerns are identified, such as shared resource exploits, inappropriate virtual overlay separation or VLAN tagging, systems for shared logging or monitoring without data segregation, and cross-tenant insight as a result of errors in the orchestration logic. The misconfigs or exploits of one of them may result in policy disagreements, data leaks, or security incidents caused by a misbehaving or exploited neighbor environment.

3.2.5 Artificial Intelligence-powered cyberattacks

Artificial Intelligence (AI) can be exploited to carry out very sophisticated automated attacks on a large scale, such as intercepting encrypted flows with certificate forgery or exploiting vulnerable TLS protocols between SD-WAN edges, automatic discovery of vulnerabilities and adaptation of attack vectors in real time, and rapid exploitation of zero-day vulnerabilities. As well as bypassing automated defenses, AI can learn the behavior of detection systems like firewalls or IDS/IPS and adapt the attack to go unnoticed or appear as legitimate traffic, causing greater damage. Therefore, it is important to take into account this risk in order to understand the concept and evaluate the sophistication level of these attacks to protect the SD-WAN networks [24].

3.2.6 Risk associated with IoT device integration

Despite the benefits of SD-WAN on IoT networks, the integration of IoT devices may expand the attack surface regarding their characteristics, such as wireless access, device mobility, geographic distribution, location awareness, and heterogeneity [25]. These characteristics can cause security issues related to authentication, authorization, and end-user privacy that can be exploited by cybercriminals to launch attacks on the SD-WAN networks, affecting confidentiality, integrity, and availability.

3.2.7 Risk associated with data sovereignty

As described above, the SD-WAN is based on multiple performance metrics to route the traffic intelligently in the best and most secure manner; however, it does not take into account the challenges related to data sovereignty, particularly concerning cloud services. As it is known, each country has its own laws and regulations that manage data sovereignty, such as the European General Data Protection Regulation (EU GDPR), the French SecNumCloud framework created by the French National Agency for the Security of Information Systems (ANSSI), and Moroccan Laws 09-08 and 05-20 with decree no. 2-24-921 [26-28]. This issue is not technical, but it represents a risk associated with security and compliance that should be addressed to align performance with regulatory rules while intelligently routing traffic and respecting laws and regulatory rules.

4. PROPOSED SCHEME

4.1 General description

The proposed scheme is based on two remote sites, the headquarters and the branch office. The headquarters site is composed of an administration server and a central server that includes an MQTT broker and a CoAP controller. The branch office consists of the sensors that send temperature data to the MQTT broker on the central server and of the CoAP actuator that receives commands from the CoAP controller at headquarters. The central server analyzes the temperature sent by sensors; when this temperature exceeds the threshold, the CoAP controller sends the command "ON" to the actuator to turn on the ventilator. When the temperature becomes normal, the CoAP controller sends the command "OFF" to stop the ventilator. At some point, an attacker was introduced to the branch office site to launch a DDoS attack on the administration server at the headquarters site. The remote sites are connected through two internet links, as shown in Figure 3.

The evaluation of this two-site topology is still valid for a multi-branch topology because the SD-WAN controller manages traffic for all branches by applying the same traffic rules depending on the QoS configured. This topology was chosen to simplify the implementation and reduce the simulation's complexity and resource consumption to avoid overloads that affect result precision.

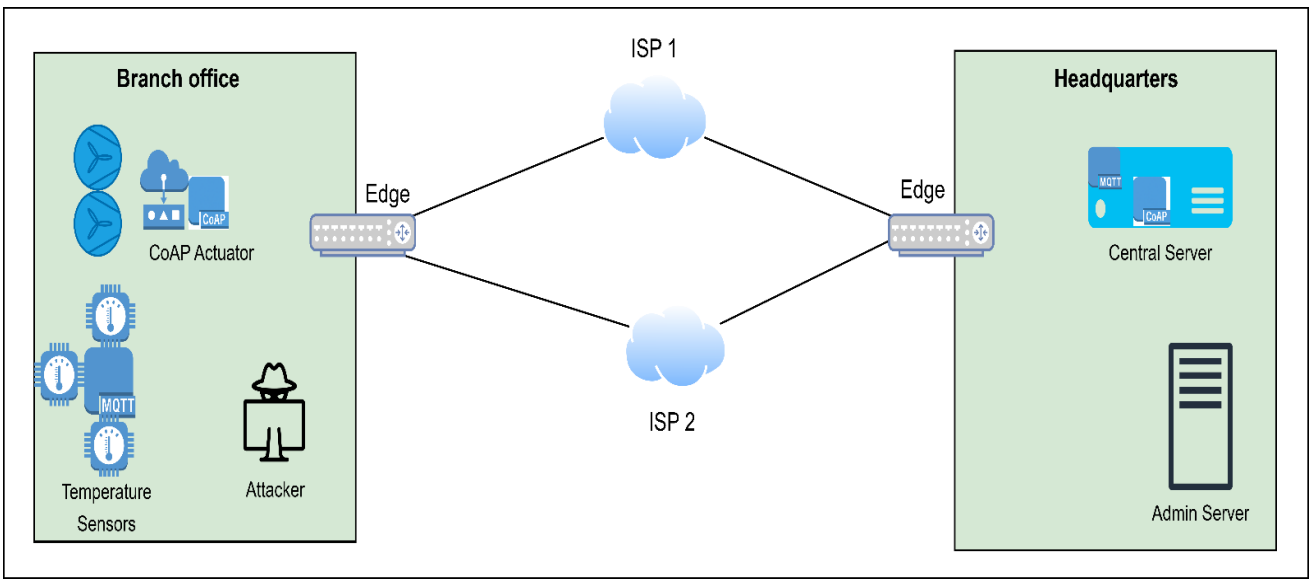

Figure 3. Proposed scheme

4.2 Simulation scheme

An experimental technique was employed to demonstrate the advantages of SD-WAN in IoT environments concerning network performance metrics such as latency, jitter, packet loss, and traffic classification, and then illustrates the behavior of SD-WAN facing DDoS attacks. The Pnetlab emulator was selected due to its cost-effectiveness, resilience, and reliability, and it can simulate SD-WAN networks using virtual machines, making it easier to design, integrate link quality, configure, and test large networks. For the topology, all components were implemented and configured in a single Pnetlab project, along with a VMware Workstation Player, which is free software used to operate virtual machines.

To simulate IoT traffic, the Python scripts were used to deploy an MQTT application based on the MQTT protocol and a CoAP application based on the CoAP protocol with settings described in Table 2. Both of these applications were deployed in two separate virtual machines using Ubuntu 22.04 connected to a central server in the remote site, which includes the MQTT broker and the CoAP controller. The central server is also deployed on Ubuntu 22.04, and all performance measures are displayed via Python scripts.

Table 2. Message Queue Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) settings

MQTT Settings	CoAP Settings
Quality of service (QoS) level: 0	Confirmable (CON) messages
Clean session = True	Message rate: 1 message/sec
Keep-alive: 60 s	Payload size: 5 octets

The connection between sites is based on two links; each link has a specified QoS. In this case, ISP1 is the best one as the primary link, and ISP2 is the secondary link; both links are connected via an edge router to each site. The Netem tool was used to simulate the Internet links with a specified QoS. The Edge router used is the open-source Flexiwan SD-WAN router. The choice of this solution for its cost-effectiveness and capacity to simulate a real SD-WAN network with multiple functionalities, facilitating the design, configuration, and testing of vast topologies. The FlexiRouter was installed at the edge of each site, connected to FlexiManage as a hosted service in the cloud [29], as presented in Figure 4, and the hub-spoke topology was deployed to simplify the configuration of IPsec tunnels between sites.

In the initial system, the Edge router was used without enabling the SD-WAN functionality; the routing was based on the priority link. At some point, the QoS for ISP1 was degraded as described in Table 3, which presents the QoS of each link. After this degradation, the SD-WAN functionality was enabled to evaluate the benefits of the SD-WAN solution in the IoT environment.

Table 3. Links quality parameters

Parameters	ISP1	ISP1 Degraded	ISP2
Bandwidth (Mbps)	100	100	80
Latency (ms)	10	60	10
Jitter (ms)	0.001	16	0.001
Packet loss (%)	0.01	20	0.01

Note: ISP = Internet Service Provider.

For DDoS attack simulation between Headquarters and the branch office, three virtual machines were installed in the branch office using Ubuntu 22.04, including the iperf3 and hping3 tools to launch the DDoS attack on the administration server in Headquarters. On the three virtual machines, hping3 and iperf3 using the UDP protocol were launched with a specified quantity of traffic to analyze the behavior of SD-WAN and the performance of IoT applications during DDoS attacks with varying traffic levels. Table 4 resumes the parameters and simulation tools used.

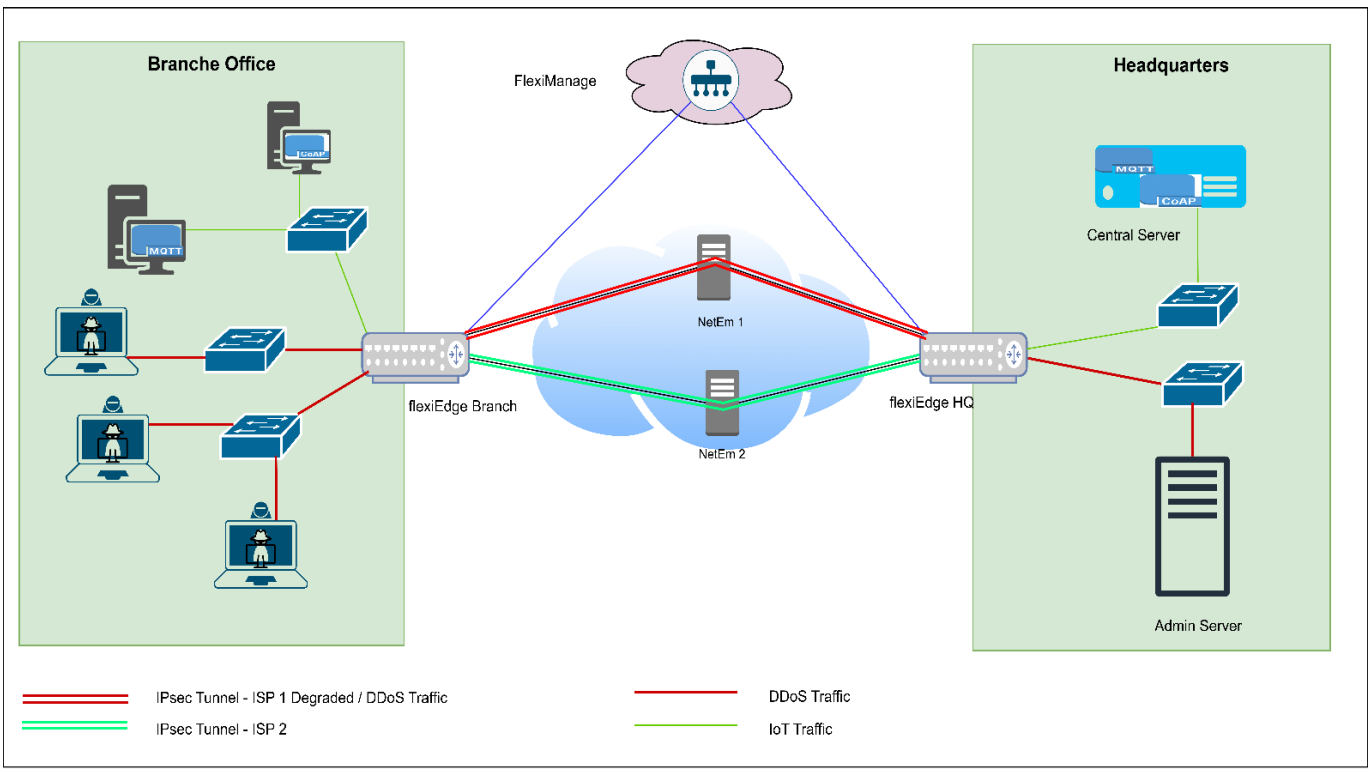

Figure 4. Simulation scheme

Table 4. Simulation parameters and tools

Parameters	Pnetlab	Flexiwan	Central Server	MQTT Sensors's VM	CoAP Actuator's VM	Attacker's VM/Admin Server
CPU	12	4	2			
Memory (Go)	16	8	4			
Version	5.3.13 on Ubuntu 18.04.5 LTS	6.4.32 on Ubuntu 20.04.6 LTS	Ubuntu 22.04.1 LTS			
Tools	--	--	Message Queue Telemetry Transport (MQTT) broker and CoAP controller simulated by Python-based scripts	Temperature sensors simulated by Python-based scripts	Constrained Application Protocol (CoAP) actuator simulated by Python-based scripts	Hping3 only on the attacker's VM, Iperf3

Algorithm 1: Algorithm for IoT Traffic Prioritization

Require:
P: a network packet with destination port and transport protocol
ISP1: ISP1 connection with quality and priority metrics
ISP2: ISP2 connection with quality and priority metrics
Ensure:
s_path: selected path for packet P

```
port <- P.destination_port
protocol <- P.transport_protocol ▷ "UDP" or "TCP"
/* Condition for MQTT or CoAP traffic */
if ((port = 1883 and protocol = "TCP") or ((port = 5683 or port = 5684) and protocol = "UDP")) then
   available_paths ← ∅ ▷ initialize empty set
   for each connection ∈ {ISP1, ISP2} do
      if connection is available, then
         available_paths.add(connection)
      end if
   end for
   /* Select the route with the superior quality from the available connections */
   s_path ← connection ∈ available_paths with max quality score
else
  /* Condition for other traffic */
   available_paths ← ∅ ▷ initialize empty set
   for each connection ∈ {ISP1, ISP2} do
      if connection is available, then
         available_paths.add(connection)
      end if
   end for
/*Select the route with the superior priority from the available connections */
   s_path ← connection ∈ available_paths with max priority score
end if
Return s_path
```

4.3 Scenarios of simulation

In this simulation, three scenarios were introduced; the first compared the performances between the MQTT and CoAP applications, both without and with SD-WAN, while the quality of ISP1 was degraded to demonstrate the benefits of SD-WAN on two types of IoT traffic as described in the proposed scheme. The second scenario concerned the traffic classification based on a new rule deployed to prioritize the IoT traffic (MQTT and CoAP traffic) over the other types of traffic; for the simulation, the ICMP traffic was chosen when the ISP1 connection was degraded. This new rule detects the traffic type based on the destination port. If MQTT or CoAP ports are detected, the traffic will be routed through the connection with the highest quality; otherwise, if other traffic is detected, it will be routed based on the prioritized connection. This process is outlined in Algorithm 1. The last scenario was regarding the DDoS attack simulation. The attackers launched a DDoS attack from the branch office to the administration server in the headquarters. The DDoS traffic was routed only on the primary link, and other traffic was managed by SD-WAN based on the best quality link. In this scenario, the CoAP application was only evaluated to display the impact of the DDoS attack on performance because this type of traffic is more sensitive to packet loss than MQTT traffic. The hping3 and iperf3 tools were used as described in the proposed scheme. The goal of this scenario is to demonstrate the behavior of SD-WAN under a DDoS attack.

5. RESULTS AND DISCUSSION

The three simulation scenarios were performed on a high-end computer equipped with a 12-core processor and 32 GB of RAM. The scenario without SD-WAN served as a reference to measure performance when the quality of the ISP1 link was degraded. The outcomes were assessed on a quantitative level.

5.1 The benefits of a software-defined wide area network for Message Queue Telemetry Transport and Constrained Application Protocol traffic

In this scenario, the simulation was executed 10 times, each comprising 500 requests, to validate the results and mitigate the influence of sporadic spikes on the assessed parameters: jitter, delay, and packet loss. The bandwidth was not assessed as the simulated IoT applications lack a bandwidth limitation; the packet sizes transmitted by the sensors do not necessitate substantial bandwidth.

5.1.1 Latency

The results obtained in Figure 5 show a significant improvement in latency for both applications with the implementation of SD-WAN following the primary link's degradation, with a reduction for the CoAP application from

232 ± 12 ms to 35 ± 0.7 ms and for the MQTT application from 337 ± 19 ms to 32 ± 0.8 ms. Additionally, the data indicate that the MQTT application has a higher latency than the CoAP application. The primary reason for this discrepancy is that TCP-based MQTT requires response times for retransmission, whereas UDP-based CoAP does not. This results in a quicker response time, but it is unreliable.

5.1.2 Jitter

With the implementation of SD-WAN following the primary link's degradation, as shown in Figure 6, jitter was also reduced for the CoAP application from an average of 177 ± 23 ms to 4.85 ± 0.8 ms and for the MQTT application from an average of 246 ± 16 ms to 5 ± 0.7 ms. It was also noticed that the values for the MQTT application are higher than those for the CoAP application. This disparity is mainly due to the retransmission of packets in MQTT, which is based on TCP, whereas the CoAP protocol is based on UDP, which does not handle retransmissions, thereby reducing the response time and the interval between successive packets.

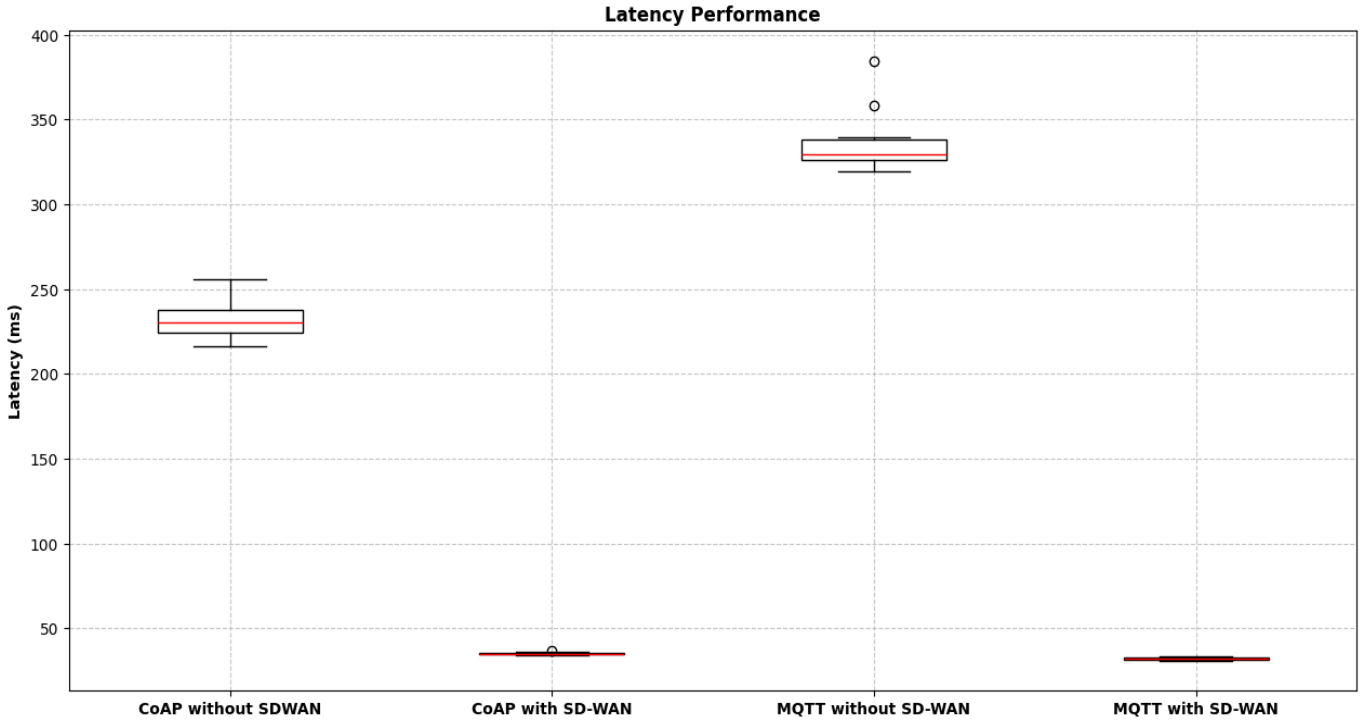

Figure 5. Latency performance

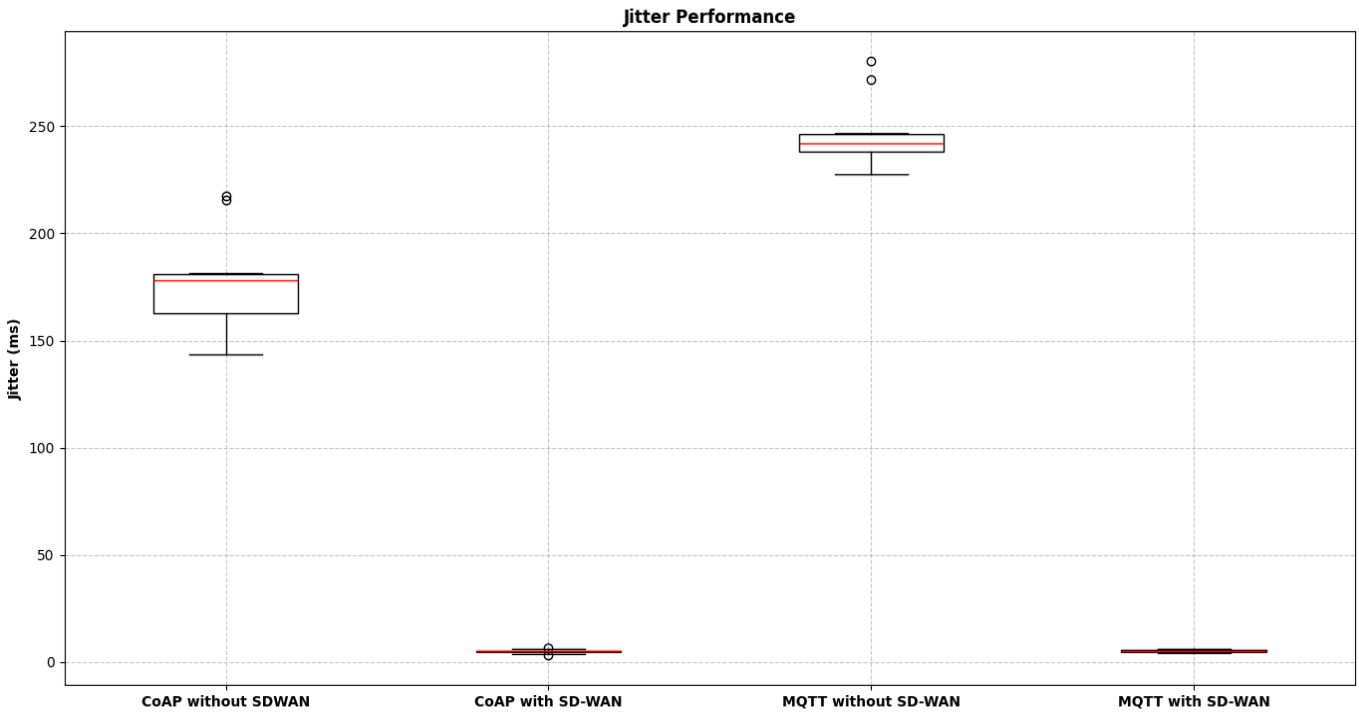

Figure 6. Jitter performance

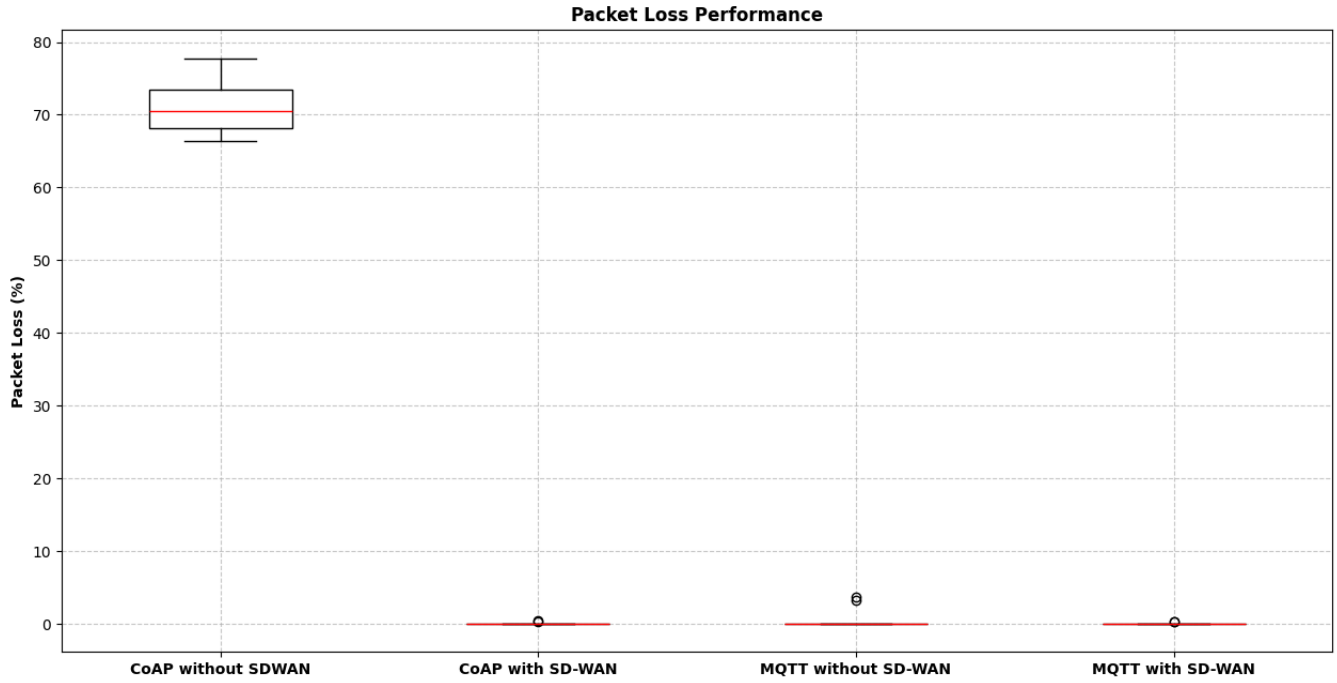

Figure 7. Packet loss performance

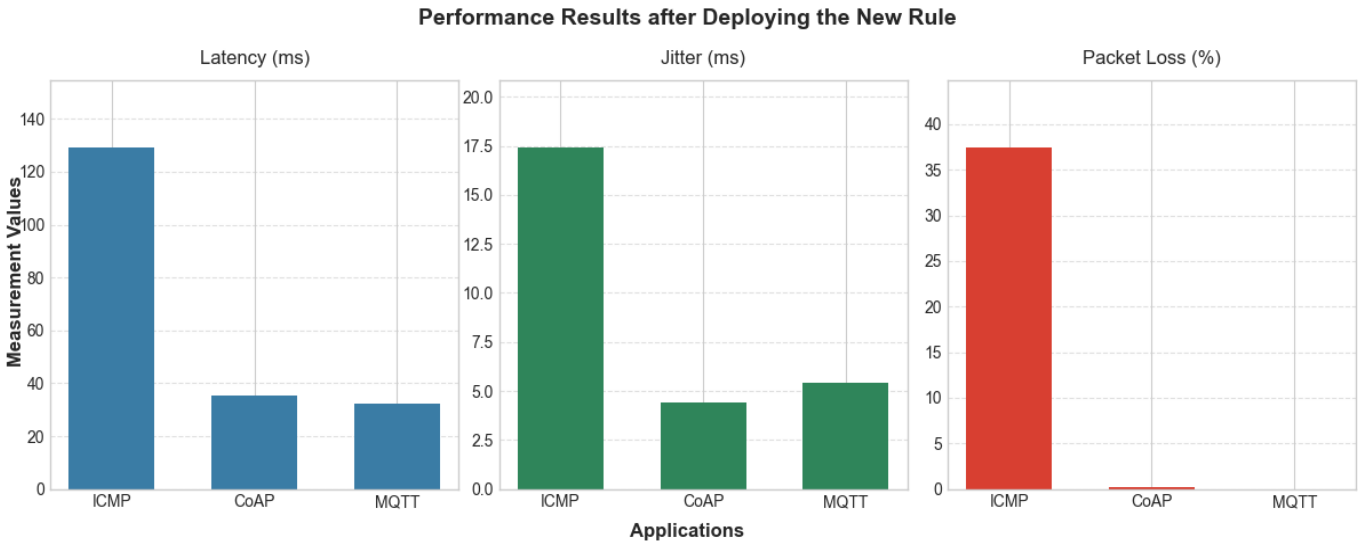

Figure 8. Performance results after deploying the new rule

5.1.3 Packet loss rate

Packet loss differs from delay and jitter scenarios. As shown in Figure 7, an enhancement was observed with the implementation of SD-WAN, particularly for the CoAP application, which experienced a decline in loss from 71 ± 4% to 0.06 ± 0.02%. This is attributed to the CoAP protocol, which operates on UDP and is susceptible to loss without advanced retransmission capabilities, in contrast to MQTT, which utilizes TCP and exhibited a minimal loss rate reduction from 0.6 ± 1.4% to 0.04 ± 0.01%.

The results obtained for this scenario show the usefulness of SD-WAN in improving the performance of IoT applications in terms of latency, jitter, and packet loss according to the constraints and requirements of each application in order to provide a unified framework for application performance regardless of their properties.

5.2 IoT traffic policy performance analysis

The deployment of the new policy that prioritizes IoT traffic of the CoAP and MQTT applications over ICMP traffic has positively impacted the performance of IoT applications compared to ICMP traffic. As illustrated in Figure 8, the latency of ICMP traffic is 129 ms, while it is 32 ms for MQTT and 35 ms for CoAP. For jitter, ICMP traffic has a value of 17 ms compared to 4.5 ms for CoAP and 5.5 ms for MQTT. The same observation is made for packet loss; it is 37.5% for ICMP traffic, whereas it is only 0.2% for CoAP and 0% for MQTT. The results obtained in this scenario show the interest of SD-WAN in classifying and prioritizing one type of traffic over another. This innovative technology allows for the prioritization of traffic based on the requirements of each application, as shown in this scenario with the prioritization of IoT traffic, which is time-sensitive, over ICMP traffic (for

illustrative purposes). This classification is particularly beneficial when the connection quality has deteriorated and the available bandwidth is limited; thus, efficient bandwidth management is essential, tailored to the application type and traffic characteristics, to fulfill each application's requirements and ensure optimal QoS delivery. SD-WAN offers flexible and intelligent traffic classification by the deployment of QoS, which permits an efficient treatment of the available bandwidth usage for each type of traffic based on its criticality by combining priority scheduling and queue scheduling.

5.3 Distributed Denial of Service attack simulation

The results obtained in Figures 9 and 10 show a significant impact of the DDoS attack on the performance of the CoAP application. This impact is notable by the increase in latency from 35 ms before the attack to 56 ms during the attack at 100 Mbps, going up to 121 ms at 800 Mbps. Similarly, the jitter increased from 4.8 ms before the attack to 18 ms during the attack at 100 Mbps, continuing to increase with traffic volume, reaching up to 70 ms at 800 Mbps. For packet loss, an increase was also noted from 0.06% before the attack to 0.1% during the attack at 100 Mbps, continuing to rise with volume, reaching up to 37% at 800 Mbps. The SD-WAN VM's resources were also impacted by this DDoS attack; specifically, CPU usage increased from 67% prior to the attack to 80% during the attack at 100 Mbps, continuing to increase with traffic volume, reaching up to 97% at 800 Mbps, as demonstrated in Figure 11 when the CPU shut down after the DDoS attack stopped. However, the attack did not affect the memory of the SD-WAN solution. The correlation between application performance and SD-WAN resources indicates that CPU usage escalates with the rise in traffic generated by attackers, which justifies the degradation of application performance related to CPU resource consumption, resulting in prolonged processing times for packets traversing the SD-WAN. On the other hand, the DDoS attack targets the primary link, while the CoAP application traffic is routed by the SD-WAN based on the best quality link. Consequently, during the DDoS attack, the IoT traffic is routed over the secondary link, which presents the best quality. Furthermore, DDoS traffic and IoT traffic were separated within the LAN, with each type of traffic having its own dedicated path, as illustrated in Fig. 4. This methodology was used to eliminate the impact of volumetric DDoS traffic on IoT traffic within the LAN, allowing for an evaluation of the DDoS attack's effect on the SD-WAN solution without affecting LAN performance. All this confirms that the DDoS attack on the primary link affected the traffic on the secondary link, which is justified by the consumption of CPU resources for the SD-WAN solution.

This attack was launched by an attacker who somehow gained access to the company's internal network to affect service availability. It might also have been an internal collaborator who was dissatisfied and wanted to retaliate by affecting service availability. Hence the need to properly secure the SD-WAN architecture against such a scenario, especially in the field of IoT, which suffers from a lack of advanced security mechanisms due to the limited resources of IoT devices. This security can be achieved by integrating the cutting-edge technologies, such as edge and fog computing or edge AI, into the SD-WAN architecture with ZTNA mechanisms, which will allow data to be processed closer to its sources with least privilege access, continuous trust checks, and no network exposure. However, the introduction of AI has led to increasingly complex attacks, necessitating the integration of AI-based mechanisms in SD-WAN architecture to anticipate and prevent sophisticated AI-based attacks. Furthermore, it is essential to ensure that security standards are followed when SD-WAN architectures are deployed, such as ISO 27001/27002, NIST, PCI DSS, HDS/HIPAA, and GDPR, as well as other security standards, depending on the company's activity, the business requirements of the applications, and compliance with national and international law.

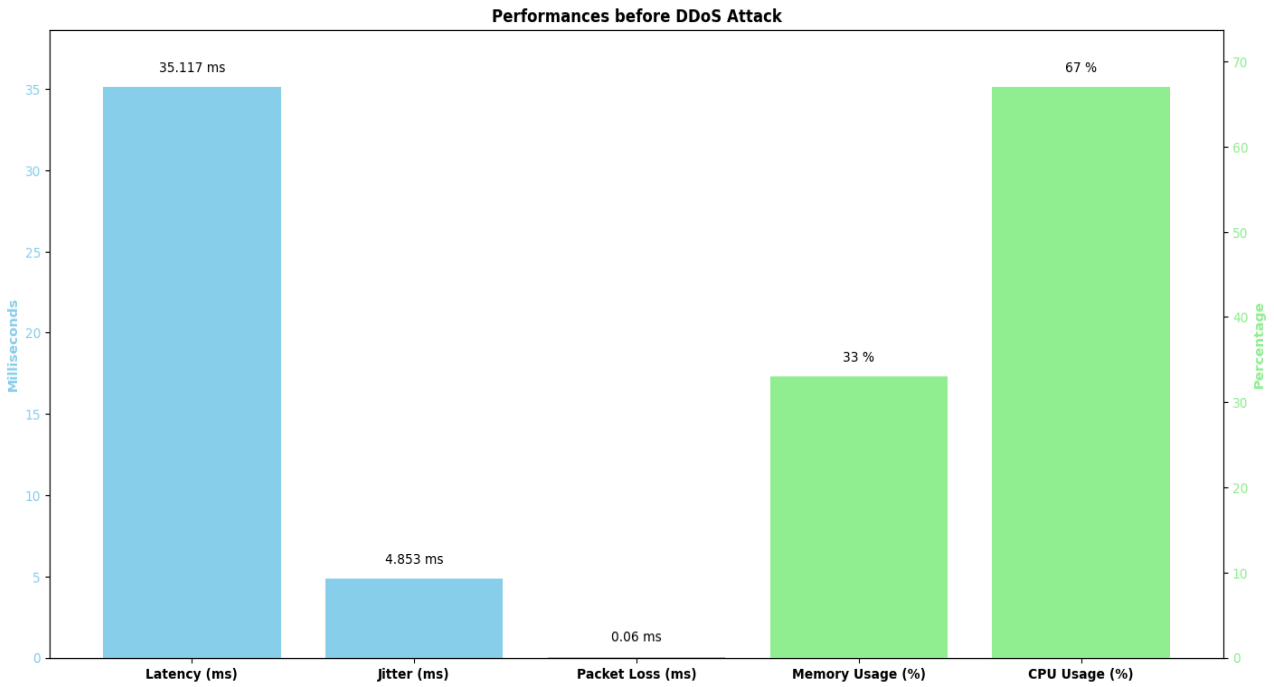

Figure 9. Performances before the Distributed Denial of Service (DDoS) attack

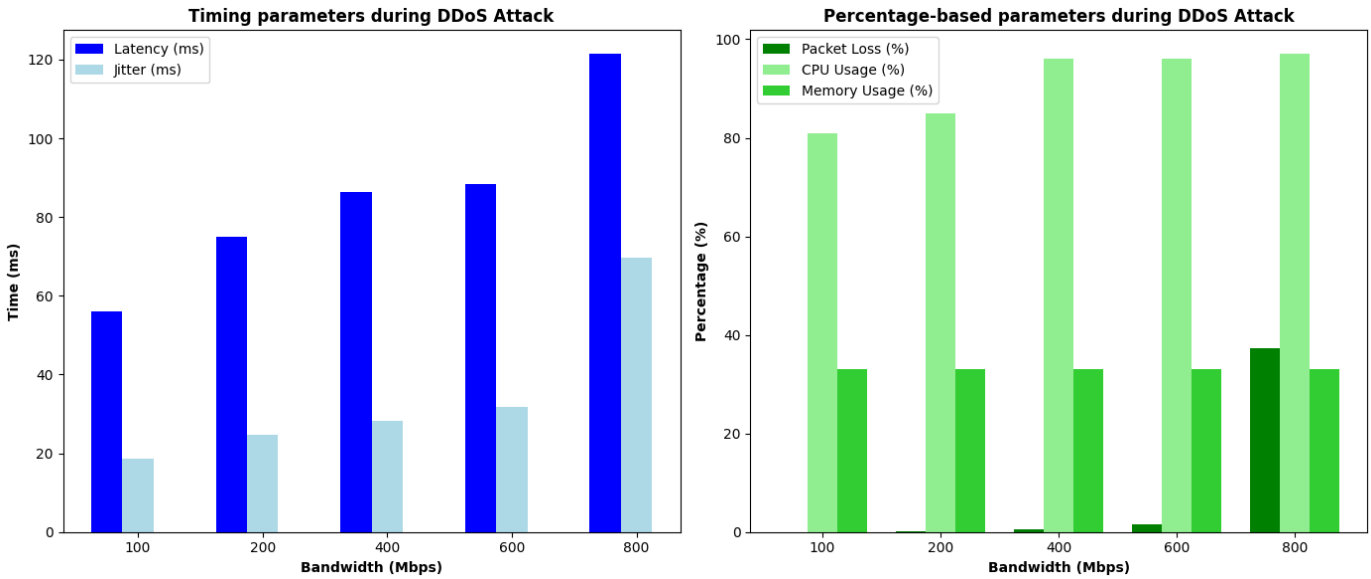

Figure 10. Performances during the Distributed Denial of Service (DDoS) attack

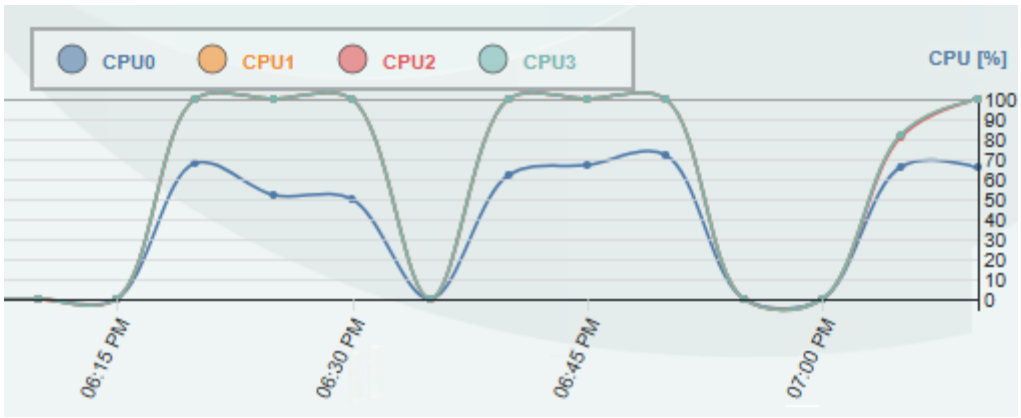

Figure 11. FlexiRouter CPU usage during the Distributed Denial of Service (DDoS) attack

6. CONCLUSIONS

Unlike the traditional WAN, which presents various limitations related to flexibility, performance, security, and high cost, the integration of SD-WAN in the IoT environment plays a crucial role in enhancing the performance and security of IoT applications, providing more flexibility and intelligence, and facilitating network management. This work highlighted the benefits of SD-WAN in IoT environments by simulating the SD-WAN management and control of MQTT and CoAP traffic; the obtained results demonstrate a significant improvement of network performance regarding latency, jitter, and packet loss. This improvement is evidenced by a reduction in latency of up to 84%, jitter by 97%, and packet loss by 99% compared to the performance of the traditional WAN without SD-WAN for CoAP traffic. Additionally, this work emphasized the advantages of SD-WAN in prioritizing traffic by implementing a new policy that allocates priority to MQTT and CoAP traffic over ICMP traffic. To highlight one of the security challenges related to the SD-WAN, the simulation of a DDoS attack within the SD-WAN infrastructure shows a significant performance degradation of CoAP traffic that was caused by affecting SD-WAN resources, particularly CPU utilization. This result illustrates that despite the advantages of SD-WAN in IoT environments, there are several challenges that should encourage thinking to enhance this technology by integrating cutting-edge technologies such as edge/fog computing with Edge AI to optimize network performance and security. As a limitation of this work, we are able to demonstrate the impact of DDoS attacks in SD-WAN architecture for IoT environments without implementing a solution to reduce this impact. For future work, the current platform can be extended to implement fog and edge computing along with edge AI to enhance the metrics evaluated and reduce the effects of DDoS attacks by processing the data closer to the source.

REFERENCES

[1] Abdullah, M. (2025). Optimal feature extraction model for detecting cyberattacks on IoT devices. International Journal of Safety & Security Engineering, 15(3): 405-413. https://doi.org/10.18280/ijsse.150301

[2] Fu, C., Wang, B., Wang, W. (2024). Software-defined wide area networks (SD-WANS): A survey. Electronics, 13(15): 3011. https://doi.org/10.3390/electronics13153011

[3] Naveen, Sharma, A., Ahlawat, N. (2023). SD-WAN: The future of networking. International Journal for Research in Applied Science & Engineering Technology, 11: 328-331. https://doi.org/10.22214/ijraset.2023.51475

[4] Gentile, A.F., Macrì, D., Greco, E., Fazio, P. (2024). IoT IP overlay network security performance analysis with open source infrastructure deployment. Journal of Cybersecurity and Privacy, 4(3): 629-649. https://doi.org/10.3390/jcp4030030

[5] Nazemi Absardi, Z., Javidan, R. (2024). A predictive SD-WAN traffic management method for IoT networks in multi-datacenters using deep RNN. IET Communications, 18(18): 1151-1165. https://doi.org/10.1049/cmu2.12810

[6] Ali, J., Roh, B.H. (2022). A novel scheme for controller selection in software-defined internet-of-things (SD-IoT). Sensors, 22(9): 3591. https://doi.org/10.3390/s22093591

[7] Saeed, M.M. (2023). Security and network approach in smart environments–Role of SD-WAN technology. https://doi.org/10.21203/rs.3.rs-2722344/v1

[8] Bhayo, J., Hameed, S., Shah, S.A. (2020). An efficient counter-based DDoS attack detection framework leveraging software defined IoT (SD-IoT). IEEE Access, 8: 221612-221631. https://doi.org/10.1109/ACCESS.2020.3043082

[9] Malqui, M., Ouaissa, M., Hanine, M., Rao, D.D., Kumawat, R., Kaushik, K. (2025). Enhancing SD-WAN with edge and fog computing: Architectures and challenges. In 2025 2nd International Conference on Multidisciplinary Research and Innovations in Engineering (MRIE), Gurugram, India, pp. 1-5. https://doi.org/10.1109/MRIE66930.2025.11156434

[10] Wang, J., Bewong, M., Zheng, L. (2024). SD-WAN: Hybrid edge cloud network between multi-site SDDC. Computer Networks, 250: 110509. https://doi.org/10.1016/j.comnet.2024.110509

[11] Ouamri, M.A., Alharbi, T., Singh, D., Sylia, Z. (2025). A comprehensive survey on software-defined wide area network (SD-WAN): Principles, opportunities and future challenges. The Journal of Supercomputing, 81(1): 291. https://doi.org/10.1007/s11227-024-06718-1

[12] Segeč, P., Moravčik, M., Uratmová, J., Papán, J., Yeremenko, O. (2020). SD-WAN-architecture, functions and benefits. In 2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA), Košice, Slovenia, pp. 593-599. https://doi.org/10.1109/ICETA51985.2020.9379257

[13] Malqui, M., Ouaissa, M., Ouaissa, M., Hanine, M. (2025). Securing SD-WAN with edge and fog computing: AI-driven optimization and challenges. In AI-Driven Cybersecurity, pp. 262-284. https://doi.org/10.1201/9781003631507-14

[14] Troia, S., Mazzara, M., Savi, M., Zorello, L.M.M., Maier, G. (2022). Resilience of delay-sensitive services with transport-layer monitoring in SD-WAN. IEEE Transactions on Network and Service Management, 19(3): 2652-2663. https://doi.org/10.1109/TNSM.2022.3191943

[15] Ibrahim Hussein, S.A., Zaki, F.W., Ashour, M.M. (2022). Performance evaluation of software-defined wide area network based on queueing theory. IET Networks, 11(3-4): 128-145. https://doi.org/10.1049/ntw2.12039

[16] Saxena, M.C., Sabharwal, M., Bajaj, P. (2023). Exploring path computation techniques in software-defined networking: A review and performance evaluation of centralized, distributed, and hybrid approaches. International Journal on Recent and Innovation Trends in Computing and Communication, 11(9s): 553-567. https://doi.org/10.17762/ijritcc.v11i9s.7468

[17] Tournier, J., Lesueur, F., Le Mouël, F., Guyon, L., Ben-Hassine, H. (2021). A survey of IoT protocols and their security issues through the lens of a generic IoT stack. Internet of Things, 16: 100264. https://doi.org/10.1016/j.iot.2020.100264

[18] Tariq, M.A., Khan, M., Raza Khan, M.T., Kim, D. (2020). Enhancements and challenges in coap—A survey. Sensors, 20(21): 6391. https://doi.org/10.3390/s20216391

[19] Lee, J., Lee, H. (2021). Secure and scalable IoT: An IoT network platform based on network overlay and MAC security. In IFIP International Conference on ICT Systems Security and Privacy Protection, pp. 287-301. https://doi.org/10.1007/978-3-030-78120-0_19

[20] Maawi, K.N.A., Qa'id, M.A.A. (2025). A review on intrusion detection systems for MQTT in IoT environments. International Journal of Safety & Security Engineering, 15(8): 1733-1744. https://doi.org/10.18280/ijsse.150818

[21] Chouikik, M., Ouaissa, M., Ouaissa, M., Boulouard, Z., Kissi, M. (2025). The role of software-defined vehicular networks in society 5.0. Emerging Disruptive Technologies for Society 5.0 in Developing Countries: Challenges and Applications, pp. 237-242. https://doi.org/10.1007/978-3-031-63701-8_20

[22] Chouikik, M., Ouaissa, M., Ouaissa, M., Boulouard, Z., Kissi, M. (2024). Detection and mitigation of DDoS attacks in SDN based intrusion detection system. Bulletin of Electrical Engineering and Informatics, 13(4): 2750-2757. https://doi.org/10.11591/eei.v13i4.7570

[23] Guembe, B., Azeta, A., Misra, S., Osamor, V.C., Fernandez-Sanz, L., Pospelova, V. (2022). The emerging threat of ai-driven cyber attacks: A review. Applied Artificial Intelligence, 36(1): 2037254. https://doi.org/10.1080/08839514.2022.2037254.

[24] Burhan, M., Alam, H., Arsalan, A., Rehman, R.A., Anwar, M., Faheem, M., Ashraf, M.W. (2023). A comprehensive survey on the cooperation of fog computing paradigm-based IoT applications: Layered architecture, real-time security issues, and solutions. IEEE Access, 11: 73303-73329. https://doi.org/10.1109/ACCESS.2023.3294479

[25] European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, OJ L 119, 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[26] Martinez, C., Etxaniz, I., Molinuevo, A., Alonso, J. (2024). Medina catalogue of cloud security controls and metrics: Towards continuous cloud security compliance. Open Research Europe, 4: 90. https://doi.org/10.12688/openreseurope.16669.1

[27] Maleh, Y., Maleh, Y. (2022). National cyber resilience strategy in a Post-COVID-19 world. In Cybersecurity in Morocco, pp. 67-75. https://doi.org/10.1007/978-3-031-18475-8_6

[28] Anass, R., Saliha, A., Khadija, O.T., Ounsa, R. (2018). A comparison of American and Moroccan governmental security approaches. In International Conference Europe Middle East & North Africa Information Systems and Technologies to Support Learning, pp. 352-360. https://doi.org/10.1007/978-3-030-03577-8_39

[29] Bustamante, J.R., Avila-Pesantez, D. (2021). Comparative analysis of Cybersecurity mechanisms in SD-WAN architectures: A preliminary results. In 2021 IEEE Engineering International Research Conference (EIRCON), pp. 1-4. https://doi.org/10.1109/EIRCON52903.2021.9613418