Enhancing IoT scalability and security through SDN

Diyar HAMAD[1,2*], Khirota YALDA[1,2], Nicolae TAPUS[1], Ibrahim Taner OKUMUS[3]

[1] Facultatea de Automatică și Calculatoare, Universitatea Națională de Știință și Tehnologie Politehnica București, Bucharest, Romania
[2] Department of Information Technology, Soran Technical college, Erbil Polytechnic University, Erbil, Kurdistan Region, Iraq
[3] Computer Engineering, Kahramanmaras Sutcu Imam University, Kahramanmaras, Turkey

diyar.hamad@epu.edu.iq, kherota.yalda@epu.edu.iq, nicolae.tapus@upb.ro, iokumus@ksu.edu.tr.

*__Corresponding author:__ Diyar HAMAD
diyar.hamad@epu.edu.iq

Abstract: The proliferation of Internet of Things (IoT) devices introduces significant challenges in network security and scalability. Software-Defined Networking (SDN) emerges as a promising framework to offer more flexible and intelligent network management capabilities. This paper delves into the integration of SDN principles within an IoT environment to bolster security and scalability. Through a proof-of-concept deployment utilizing the Floodlight controller and Mininet-WiFi, the approach involves the collection and analysis of data on average latency, packet loss, throughput, and jitter to evaluate network performance. Additionally, Python scripts and Wireshark are employed for an in-depth network analysis. The findings illustrate that SDN integration can adeptly manage the augmented network load, evidenced by minimal increases in latency and packet loss, while maintaining acceptable throughput and jitter levels. Furthermore, the Floodlight controller's capability to identify and counter Distributed Denial of Service (DDoS) attacks underscores its potential to enhance IoT network security. The results affirm that SDN can significantly elevate the scalability and security of IoT networks, presenting a viable solution to manage the escalating demands of IoT deployments. Future endeavors will aim to extend the network scale and investigate alternative SDN controllers to substantiate the scalability of the conclusions.

Keywords: SDN, IoT, Floodlight, Metrics, Security, Scalability.

1. Introduction

The Internet of Things (IoT) represents a paradigm shift in the digital transformation of various sectors, including smart cities, healthcare, industrial automation, and beyond. The evolution of the Internet with its emerging technologies has propelled the world into the IoT era, improving the quality of life and boosting the global economy (Jayaraman et al., 2023). This burgeoning network of interconnected devices offers unprecedented opportunities for efficiency and innovation (Khan et al., 2022). The architecture of an IoT system comprises various hardware and software components (Saber et al., 2022). IoT devices typically use wireless transmission, employing a wide range of communication standards. These include short-range networks like IEEE 802.15.4 or IEEE 802.11, as well as long-range networks such as GSM, LTE, and 5G (Milošević et al., 2021). However, the rapid proliferation of IoT devices also surfaces critical challenges, particularly in terms of security and scalability. IoT devices, often designed with limited computational resources and prioritizing ease of use over security, become prime targets for cyber threats. The vast scale and distributed nature of IoT deployments further exacerbate these issues, introducing complex challenges for network management (Aldhaheri et al., 2024). Traditional network architectures, with their static configurations and decentralized management models, struggle to adapt to the dynamic and expansive landscape of IoT networks. This gap underscores the urgent need for novel approaches that can ensure robust security and seamless scalability in IoT ecosystems.

As IoT networks continue to expand, they bring to light the limitations of conventional network management and security protocols. The integration of countless IoT devices, each potentially acting as a vector for cyberattacks, intensifies the risk landscape. Distributed Denial of Service (DDoS) attacks, in particular, exploit these vulnerabilities, disrupting services and causing significant operational and financial damage (Salim et al., 2020). Moreover, the scalability challenge is not merely about handling the growing number of devices but also involves managing the diverse and evolving requirements of IoT applications. The static and inflexible nature of traditional network infrastructures is ill-suited for the dynamic, heterogeneous, and voluminous characteristics of IoT

https://doi.org/10.33436/v34i2y202409

deployments. Addressing these dual challenges of security and scalability requires a rethinking of network management strategies to foster a secure, adaptable, and resilient IoT environment (Farahani et al., 2021). The IoT infrastructure can attract cybercriminals, directly affecting consumers. Unlike other consumer technologies, IoT devices often lack security features because they prioritize cost reduction and scalability, leading to limited hardware resources for security measures (Aljahdali et al., 2021).

Software Defined Networking (SDN) is a revolutionary approach that seeks to make network management more flexible, efficient, and programmable. It is particularly relevant in the context of the IoT, where a vast array of heterogeneous devices and technologies must be integrated and managed effectively. SDN serves as a key enabler for emerging technologies such as (Bekri et al., 2020; Stancu et al., 2018).

This research is driven by several key objectives, designed to address the outlined challenges and to advance the integration of IoT with SDN:

- to investigate SDN's role in IoT: exploring how SDN principles can be applied to IoT networks to enhance their security and scalability. The focus is on leveraging the centralized control and programmability of SDN to adapt network behavior dynamically in response to evolving IoT requirements and security threats;
- to implement and evaluate a Proof-of-Concept deployment: utilizing the Floodlight SDN controller and Mininet-WiFi (Fontes et al., 2015) to create a scalable network topology with varying numbers of IoT devices and access points. This deployment aims to simulate real-world IoT network conditions and assess the practical benefits of SDN;
- to analyze network performance and security enhancements: through rigorous data collection and analysis, evaluating how SDN impacts key network performance metrics (latency, packet loss, throughput, jitter) across different scales of IoT deployments. Additionally, assessing the efficacy of SDN-enabled strategies in detecting and mitigating DDoS attacks;
- to provide guidelines for future IoT network implementations: based on the findings, offering insights and recommendations for leveraging SDN in IoT networks, aiming to inform future developments and encourage the adoption of SDN principles for improved IoT network management and security.

This study makes several significant contributions to the fields of IoT and SDN. Firstly, it empirically demonstrates the viability and benefits of integrating SDN with IoT networks, highlighting how SDN's centralized control and programmability can address the critical challenges of security and scalability. The proof-of-concept deployment provides a tangible example of how SDN can enhance network management in IoT contexts, offering a replicable model for future research and practical applications. By systematically analyzing the impact of SDN on network performance and security, this research elucidates the potential of SDN to transform IoT network architectures, ensuring they are more secure, scalable, and adaptable. Furthermore, the detailed examination of SDN's role in mitigating DDoS attacks within IoT networks underscores the practical implications of the findings, showcasing SDN's capacity to safeguard IoT ecosystems against prevalent cyber threats. Ultimately, this work contributes to a deeper understanding of the synergies between SDN and IoT, paving the way for more resilient, efficient, and future-proof network infrastructures.

2. Literature review

2.1. SDN IoT architecture

The integration of SDN with IoT has emerged as a focal point of research, aiming to address the inherent challenges within IoT ecosystems, such as security vulnerabilities and scalability issues. SDN, with its centralized control mechanism, offers a paradigm shift from traditional network architectures, allowing for dynamic network management and enhanced security protocols (Bekri et

al., 2020). Several studies have explored the potential of SDN in optimizing IoT network operations, highlighting its ability to provide flexible control and efficient resource allocation across vast and heterogeneous IoT devices (Li et al., 2020; Siddiqui et al., 2022).

The architecture illustrated in Figure 1 depicts a typical SDN framework adapted for IoT environments, serving as a guide to understanding how SDN can be applied to IoT. At the top of the architecture lies the Application Layer, which contains the IoT applications themselves. These are the end-user applications that leverage the network to deliver services, ranging from simple data collection tasks to complex analytics and decision-making processes (Karmakar et al., 2021). They interact with the network through APIs (Application Programming Interfaces) provided by the Control Layer.

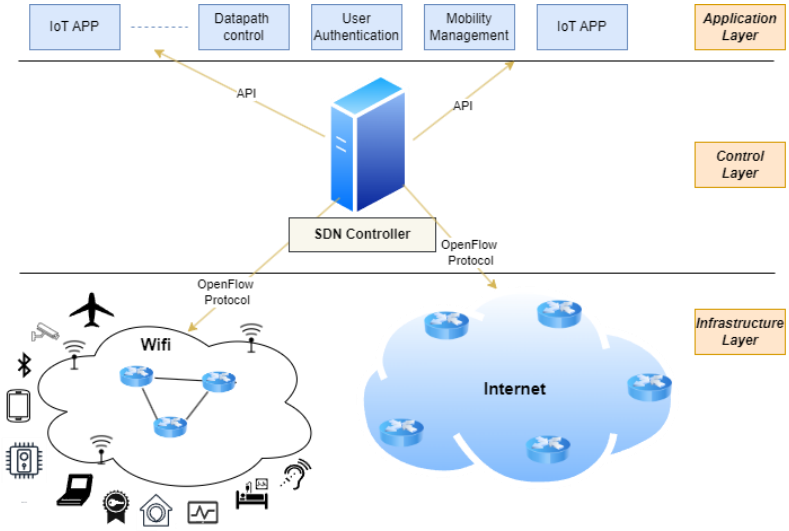

Figure 1. SDN IoT Structure

The Control Layer contains the SDN Controller, which is the core of the SDN architecture. The SDN Controller is responsible for providing the "brains" of the network. It maintains a comprehensive view of the network, making decisions about where to route packets and how to handle network traffic (Hasan et al., 2020). The controller interfaces with the applications above it through APIs for various functions, including:

A. Datapath Control: This is where the controller manages the flow of data through the network, making decisions about routing and handling network congestion.

B. User Authentication: The controller can also manage access to the network, ensuring that only authenticated users and devices are able to communicate.

C. Mobility Management: In IoT, devices may be mobile. The controller must manage their movement across the network, ensuring that connections are maintained seamlessly (Bi et al., 2019).

The bottom layer is the Infrastructure Layer, which is composed of the physical hardware – the switches, routers, and other devices that actually forward the data (Saadeh et al., 2019). In an SDN architecture, these devices are simplified, as they no longer need to maintain complex control protocols. Instead, they are programmed by the controller with simple "flow rules" that tell them how to handle packets.

2.2. Key findings in IoT security and calability

Research on IoT security emphasizes the vulnerability of IoT devices to cyber threats, including DDoS attacks, data breaches, and malware infections (Kumar et al., 2016). The scalability challenge, on the other hand, revolves around managing an exponentially growing number of devices and ensuring reliable communication within the IoT network (Silva et al., 2018). Studies have demonstrated that SDN can significantly enhance IoT security by centralizing security policies and

enabling real-time detection and mitigation of cyber threats (Hassija et al., 2019). Similarly, SDN's role in improving network scalability has been affirmed, with findings indicating its effectiveness in managing network complexity and adapting to changing traffic patterns (Dai et al., 2020). The use cases for IoT devices are diverse, but current trends indicate that all device manufacturers will eventually prioritize security in their selections. A common approach in IoT security is the use of public key infrastructure (PKI), where digital certificates verify the authenticity of a site or an IoT device. These digital certificates establish trust in an IoT device, and when used with infrastructure authentication applications, they can help identify and block access to uncertified or poorly secured devices (Dumitrache & Sandu, 2020).

IoT security has garnered significant attention due to the increasing prevalence of cyber threats targeting connected devices. Previous studies have underscored the vulnerabilities inherent in IoT ecosystems, ranging from device-level vulnerabilities to challenges in securing communication channels. Works by authors such as (Oracevic et al., 2017; Sethi & Sarangi, 2017) have explored various threat models, attack vectors, and proposed security mechanisms. These studies emphasize the need for robust security measures to protect sensitive data and ensure the integrity of IoT deployments. Several works have proposed frameworks and models for integrating SDN within IoT networks to streamline operations and improve efficiency. These include architectures for SDN-based IoT systems that facilitate better device management, data flow control, and network programmability (Alsaeedi et al., 2019). Furthermore, the application of SDN in IoT has been shown to improve Quality of Service (QoS) parameters, such as latency and throughput, by optimizing routing decisions and network configurations based on real-time data (EL-Garoui et al., 2020). The scalability of IoT networks is a crucial consideration as the number of interconnected devices continues to grow exponentially. Existing literature, exemplified by works like (Dorri et al., 2017; Johnson & Patel, 2019), has investigated scalability challenges stemming from the diverse nature of IoT devices, heterogeneous communication protocols, and the strain on traditional network architectures. These studies shed light on the limitations of current scalability solutions and lay the groundwork for exploring innovative approaches to accommodate the burgeoning scale of IoT deployments.

2.3. Role of SDN in IoT security and scalability

Enter SDN, a paradigm-shifting approach to network management that centralizes control and decouples the control plane from the data plane. In the context of IoT security, SDN offers several key advantages. Firstly, by centralizing network intelligence and control, SDN enables real-time threat detection and rapid incident response. Security policies can be dynamically enforced across the network, allowing for swift mitigation of potential security breaches. Moreover, SDN facilitates fine-grained access control and segmentation, isolating IoT devices into distinct security zones and minimizing the lateral movement of threats within the network.

Furthermore, SDN's programmable nature empowers IoT stakeholders to implement proactive security measures, such as anomaly detection and behavior analysis. By leveraging machine learning algorithms and predictive analytics, SDN can identify suspicious patterns and preemptively block malicious activities, enhancing the overall resilience of IoT infrastructures. Additionally, SDN's ability to integrate with existing security frameworks and protocols streamlines the deployment of security solutions, ensuring seamless compatibility across diverse IoT environments. Beyond security, SDN plays a pivotal role in addressing the scalability challenges inherent in IoT deployments. Researchers such as (Ye & Qian, 2017) has proposed novel architectures leveraging SDN principles to address the dynamic and diverse nature of IoT networks. As the number of connected devices continues to proliferate, traditional networking architectures struggle to accommodate the increasing volume of data traffic and resource demands. SDN offers a scalable alternative, enabling dynamic traffic engineering and load balancing to optimize network performance. By intelligently allocating resources and prioritizing critical data flows, SDN ensures efficient utilization of network resources, mitigating congestion and enhancing overall network scalability.

Moreover, SDN's centralized management simplifies the orchestration of IoT deployments, facilitating seamless integration of new devices and protocols. Through programmable interfaces and open standards, SDN enables interoperability across heterogeneous IoT environments, allowing disparate devices to communicate and collaborate effectively. This interoperability fosters ecosystem growth and innovation, empowering organizations to harness the full potential of IoT technologies without being constrained by proprietary protocols or vendor lock-in.

3. Study setup and execution

Before delving into the specifics of SDN and IoT integration, it's essential to outline the experimental procedure undertaken to investigate the efficacy of this integration. The experimental setup aimed to assess the scalability and security enhancements brought about by SDN principles within IoT environments

3.1. SDN and IoT integration

This study employs SDN principles to address the challenges of scalability and security in IoT) networks. By leveraging SDN's centralized control capabilities, the enhancement of network management and security for IoT devices is pursued. The integration process involves the use of the Floodlight SDN controller, a widely recognized open-source SDN controller, which offers a flexible and programmable network management platform. Additionally, Mininet-WiFi, a network emulator capable of creating virtual network topologies that include both wired and wireless nodes, is utilized to simulate an IoT environment (Han et al., 2022; Selvaraju et al., 2021). This setup allows for the dynamic configuration of network behaviors in response to varying demands and threats, showcasing the potential of SDN to improve IoT network operations.

3.2. Deployment scenario

The proof-of-concept deployment is designed to simulate a realistic IoT network environment with escalating complexity and scale. The initial network topology consists of 8 IoT devices connected to 2 Access Points (APs), representing a basic IoT deployment scenario. This setup serves as the baseline for the experiments. The network is progressively expanded in three subsequent stages:

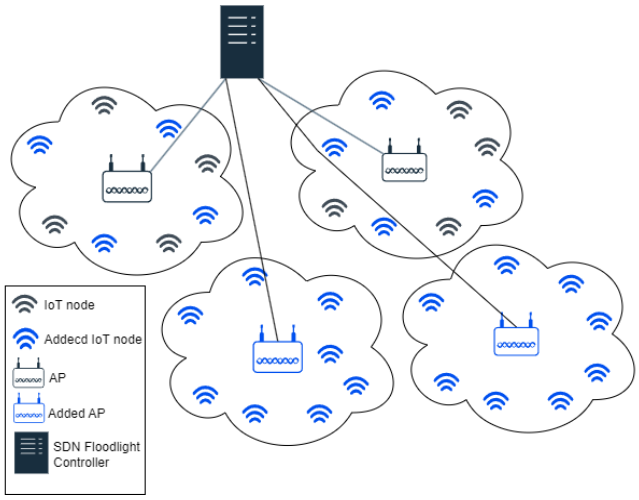

Figure 2. Network topology

Stage 1: Addition of 8 more IoT devices, totaling 16 IoT devices, while maintaining the original 2 APs. This stage tests the network's scalability with an increased number of devices. Figure 2 showing general topology that used in the experiment.

Stage 2: Further expansion to include 32 IoT devices distributed across 4 APs, doubling the number of devices and adding 2 more APs to assess both scalability and the impact on network performance.

Stage 3 of network expansion culminated in an extensive topology consisting of 64 IoT devices and 8 Access Points (APs), marking a substantial increase in network complexity and scale. This phase was specifically designed to rigorously test the capabilities of SDN in managing and securing a large-scale IoT network under demanding conditions. Each stage is designed to evaluate how well SDN principles, applied through the Floodlight controller, can enhance network scalability and security in an increasingly complex IoT environment.

The Floodlight Open SDN Controller was selected for its robust feature set and active community support. It operates as the central intelligence of the network, providing a comprehensive platform for monitoring, decision-making, and control (Zhu et al., 2021). Key capabilities leveraged in this deployment included:

A. Dynamic Flow Management: Automatically adjusting network flows in response to changing network conditions and device requirements.

B. Real-Time Network Monitoring: Observing network performance in real-time to identify and respond to anomalies promptly.

C. Programmability: Enabling the creation of custom network management applications tailored to the specific needs of the IoT deployment.

Mininet-WiFi, a fork of the well-known Mininet network emulator, was utilized to virtualize the IoT devices and APs, enabling a scalable and flexible testing environment (Muthanna et al., 2022). This tool allowed the simulation of a wide variety of network conditions and configurations, making it ideal for this study. It also provided the means to simulate the wireless connectivity that is often used by IoT devices, offering a more realistic network behavior.

3.3. Data collection

Data collection is a critical component of our methodology, enabling the assessment of network performance and the effectiveness of SDN in managing and securing IoT deployments. Two primary tools are employed for this purpose:

Python Scripts: Custom Python scripts are developed to automate the collection of network performance metrics, including average latency, packet loss, throughput, and jitter. These scripts interact with both the Floodlight controller and Mininet-WiFi to extract data from the simulated network. The scripts are designed to run various network scenarios, simulate traffic, and record the performance under different conditions. This automated approach ensures consistency and accuracy in data collection across all stages of the deployment.

Wireshark: Wireshark, a network protocol analyzer, is used to capture and analyze packets flowing through the network. It provides detailed insights into the traffic patterns, including the identification of potential security threats such as DDoS attacks. Wireshark is instrumental in evaluating the Floodlight controller's ability to detect and mitigate malicious activities within the network. By analyzing packet captures before, during, and after DDoS attack simulations, the effectiveness of the SDN-controlled network in maintaining security and performance can be assessed.

The combination of automated data collection through Python scripts and in-depth traffic analysis with Wireshark forms the basis of our empirical evaluation, allowing for a comprehensive understanding of SDN's impact on IoT network scalability and security.

4. Results

This research elucidates the influence of incorporating SDN within IoT frameworks, focusing on distinct levels of network scalability and resilience against security threats, notably Distributed Denial of Service (DDoS) attacks. The presentation of the results was structured using a suite of tables and graphical figures, which detail the network's performance metrics, including average latency, packet loss, throughput, and jitter. These elements collectively portray not only the network's operational metrics at various stages of device integration but also demonstrate the robustness of the SDN-mediated DDoS mitigation techniques. In each stage of our study, a consistent network traffic

was generated for five minuteswith a data rate of 5Mb to ensure a uniform basis for evaluating the network's performance and the effectiveness of the security measures.

4.1. Network performance metrics

Network performance metrics are quantitative measures used to evaluate the efficiency, reliability, and effectiveness of a computer network. These metrics provide insights into how well a network is functioning and whether it meets the required performance criteria. In this study, the key metrics considered are latency, packet loss, throughput, and jitter.

Table 1. Network Performance Metrics Across Different Stages

Metrics	Initial network (8 IoT & 2 Aps)	Stage 1 (16 IoT & 4 APs)	Stage 2 (32 IoT & 6 APs)	Stage 3 (64 IoT & 8 APs)
Latency (ms)	0.90	0.94	0.92	0.99
PacketLoss (%)	0.00	0.00	0.50	0.78
Throughput (Mbits/s)	27.43	30.58	30.80	33.01
Jitter (ms)	0.23	0.38	0.22	0.41

The ratio of IoT devices to Access Points (APs) is a critical factor that influences the performance of a network. As the number of IoT devices per AP increases, the network can experience varying degrees of congestion and competition for resources, impacting the performance metrics.

Average Latency (ms): Latency, a critical performance metric, is depicted in Figure 3. It refers to the delay packets experience as they travel through the network. Starting at 0.90 ms with 8 IoT devices, it experiences a marginal increase as more devices are added, rising to 0.99 ms with 64 devices. Figure 3 shows a slight upward trend, but the latency remains under 1 ms across all stages. This suggests that the network effectively handles the increased traffic without significant delays, demonstrating the scalability and efficiency of the SDN-enabled IoT network.

Overall, the slight increase in latency as the number of devices grows indicates that while the network is becoming more loaded, it still maintains an acceptable performance level. This consistent latency under 1 ms showcases the network's robustness and ability to manage added complexity through optimization efforts, resource allocation strategies, or load balancing mechanisms. Further analysis and monitoring of network performance may be necessary to understand the specific factors contributing to the observed latency patterns.

Average Packet Loss (%): This metric, represented in Figure 4, indicates the percentage of packets that fail to reach their destination. Initially, the network experiences no packet loss with 8 IoT devices. However, as the network grows, packet loss increases slightly, reaching 0.78% with 64 devices. This gradual increase is visualized as a rising line on the graph, indicating that while packet delivery remains largely successful, there is a slight uptick in lost packets. This increase is likely due to factors such as network congestion or transmission errors as more devices are added to the network.

Figure 3. Trends in Latency

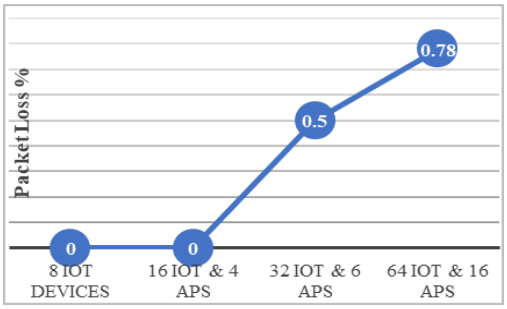

Figure 4. Trends in Packet Loss

The data suggests that the network can handle an increasing number of devices with minimal packet loss, highlighting the effectiveness of the SDN-enabled IoT network in managing traffic. Nonetheless, the slight rise in packet loss indicates areas where further optimization could help

maintain high delivery rates even as network demands grow. Understanding and addressing the causes of packet loss, such as improving congestion control mechanisms and error handling, could further enhance network performance.

Average Throughput (Mbits/s): Throughput, showcased in Figure 5, measures the amount of data successfully delivered over the network within a given time frame. Initially, the network achieves a throughput of 27.43 Mbits/s. As more IoT devices are added, throughput exhibits an upward trend, peaking at 33.01 Mbits/s with 64 devices. This increase, illustrated in the graph, suggests that the network's capacity to handle data transmission improves with scale. This improvement is likely due to the optimized data flow and efficient routing facilitated by the SDN architecture.

The rising trend in throughput underscores the SDN-enabled IoT network's ability to adapt and scale effectively, ensuring that increased device counts do not hinder overall data transmission efficiency. The network's capability to enhance throughput as it expands highlights the benefits of SDN in managing large-scale IoT deployments, ensuring robust and efficient data handling even under growing network demands.

Average Jitter (ms): Jitter, also illustrated in Figure 6, assesses the variability in packet delay. The network begins with a jitter of 0.23 ms, which fluctuates minimally as more devices are added, remaining below 0.5 ms. The graph shows this as minor oscillations, suggesting that the network maintains consistent packet delivery timing despite the increase in traffic and network complexity.

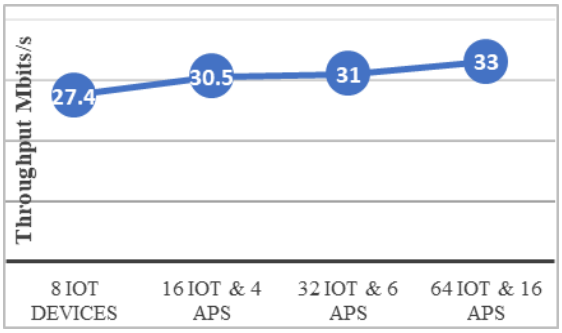

Figure 5. Trends in Throughput

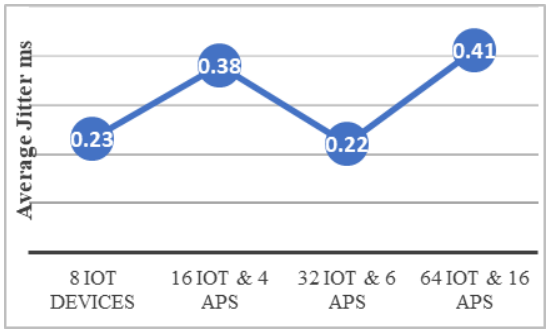

Figure 6. Trends in Jitter

In the context of the figures, these results demonstrate a network that scales effectively in the face of increasing device counts. While there are incremental changes in latency, packet loss, and jitter, the overall network performance remains robust. The throughput increase indicates efficient use of network resources, facilitated by the SDN's ability to dynamically manage the network. The figures visually represent these trends, displaying the network's ability to maintain performance integrity while scaling.

By examining the IoTs per AP ratio, it becomes evident that while increasing the number of APs can help manage the load more efficiently, there are inherent limits to this scalability. Beyond a certain point, the addition of more devices per AP leads to diminishing returns and potential performance degradation, particularly in terms of latency and packet loss.

In conclusion, understanding the relationship between IoT device density and network performance metrics is crucial for optimizing network design and ensuring reliable operation in large-scale IoT deployments. Future work could explore adaptive strategies to dynamically balance the load across APs, further mitigating the impact of high device densities.

Overall, the results suggest that the network exhibits reliable performance with low latency, minimal packet loss, and consistent throughput across different configurations. However, slight variations in packet loss and jitter may occur with increased network scalability, highlighting the importance of monitoring and optimizing network resources to maintain optimal performance. This underlines the effectiveness of SDN in managing IoT networks, ensuring they remain resilient and efficient even as they grow.

4.2. DDoS attack mitigation

The Floodlight SDN controller played a crucial role in detecting and mitigating DDoS attacks. Through real-time monitoring and analysis of network traffic, Floodlight identified unusual spikes and patterns indicative of a DDoS attack. The controller's strategies for mitigating the attack included:

A. Traffic Analysis and Anomaly Detection: Utilizing built-in and custom-developed algorithms to analyze traffic flows and detect anomalies that suggest DDoS activities.

B. Dynamic Reconfiguration of Network Rules: Automatically adjusting network rules to reroute or drop malicious traffic, effectively isolating the attack source without impacting legitimate network communications.

C. Prioritization of Critical Traffic: Implementing QoS policies to ensure that essential services maintain their functionality by prioritizing their traffic over less critical data flows.

D. Isolation of Compromised Devices: Temporarily isolating devices suspected of being part of the DDoS attack to prevent further spread of malicious activities.

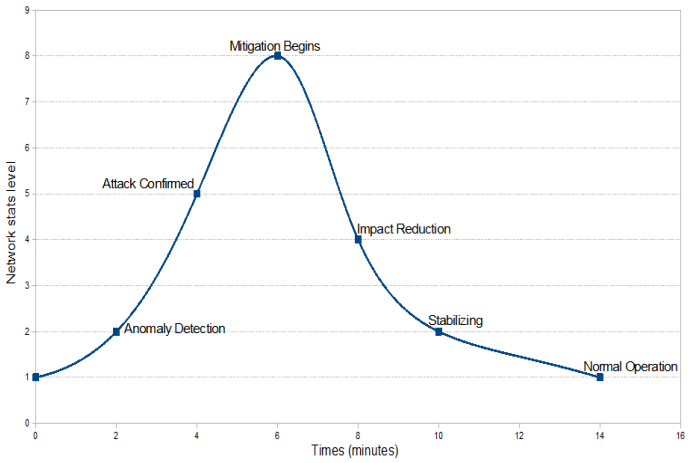

Figure 7. DDoS Attack Detection and Mitigation Timeline

The line chart above shown in Figure 7, illustrates the timeline of DDoS attack detection and mitigation, highlighting the effectiveness of the Floodlight controller's response mechanisms in an IoT network environment. Key moments in the timeline include:

Anomaly Detected (2 minutes): The initial detection of unusual traffic spikes indicative of a potential DDoS attack.

Attack Confirmed (3 minutes): Confirmation of the DDoS attack based on further analysis of traffic patterns.

Mitigation Begins (4 minutes): Implementation of mitigation strategies, such as traffic rerouting and source IP blocking, to minimize the attack's impact.

Impact Reduction (6 minutes): Noticeable reduction in malicious traffic as a result of the implemented mitigation strategies.

Stabilizing (10 minutes): The network begins to stabilize, with the majority of DDoS traffic mitigated.

Normal Operation (15 minutes): The network returns to normal operation, with all DDoS traffic effectively managed.

This timeline was generated based on a network configuration consisting of 32 IoT devices and 6 Access Points (APs). The chosen configuration strikes a balance between complexity and manageability, providing a representative scenario for assessing the SDN controller's capabilities in a mid-sized IoT network.

The influence of network topology on performance levels in detecting and mitigating DDoS attacks is significant. The density of IoT devices per AP and the overall network structure can impact the speed and effectiveness of detection and mitigation. For instance, a higher number of devices per AP can lead to increased traffic congestion, which might delay anomaly detection and response times. Conversely, a well-distributed network with adequate APs can facilitate quicker detection and more efficient mitigation due to reduced congestion and better load management.

In the context of this study, the network's ability to return to normal operation within 15 minutes following the detection of a DDoS attack is considered effective, particularly in a complex and dynamic environment like an IoT network managed by an SDN controller such as Floodlight. However, it is important to clarify whether the factors contributing to this effectiveness, such as severity of the attack, preparedness and automation, network resilience and redundancy, quality of service (QoS) policies, and post-attack analysis, were identified during the experiments or are sourced from existing literature. Without explicit citation or experimental validation within this document, the origin of these factors remains ambiguous. Providing this clarity would enhance the credibility of our findings and ensure proper attribution of insights into the effectiveness of Floodlight SDN controller in mitigating DDoS attacks.

In the context of SDN and IoT, where network configurations can be dynamically adjusted to meet changing conditions, a 15-minute recovery time demonstrates a well-implemented SDN architecture and effective network management policy. However, continuous improvement and adaptation of security measures based on evolving threat landscapes are essential to maintaining network resilience against more sophisticated future attacks.

5. Discussion

The empirical evidence gathered from the proof-of-concept deployment provides a comprehensive evaluation of how SDN principles can be integrated into IoT environments to address the challenges of scalability and security. The primary objectives of enhancing network scalability and security through the application of SDN were successfully met, as demonstrated by the measured network performance metrics and the effective mitigation of DDoS attacks.

5.1. Scalability enhancements

The integration of SDN within the IoT environment notably improved network scalability. As evidenced by the network performance metrics across various deployment stages, the network was capable of accommodating an increasing number of IoT devices and Access Points (APs) with minimal impact on latency and packet loss. This scalability is attributed to the centralized control and dynamic resource allocation capabilities of the SDN architecture, facilitated by the Floodlight controller. The ability to efficiently manage network configurations and adapt to changing traffic patterns ensures that the network can scale to meet the demands of growing IoT deployments without significant degradation in performance.

5.2. Security enhancement

Security is a paramount concern in IoT deployments due to the vast attack surface created by the multitude of interconnected devices. Traditional security approaches often struggle to cope with the dynamic and heterogeneous nature of IoT networks. However, SDN offers several mechanisms to enhance security in IoT environments:

Centralized Policy Enforcement: SDN enables centralized control over network policies, allowing administrators to define and enforce security policies consistently across the entire IoT infrastructure. This centralized approach enhances visibility and control, facilitating rapid responses to security threats.

Dynamic Network Segmentation: SDN allows for dynamic network segmentation based on contextual information, such as device type, user identity, and traffic behavior. By segmenting the

network into distinct security zones, SDN can contain and isolate security breaches, limiting their impact on critical IoT services and resources.

Fine-grained Access Control: With SDN, administrators can implement fine-grained access control policies tailored to the specific requirements of IoT applications. Access control lists (ACLs) can be dynamically updated based on real-time events and context, ensuring that only authorized devices and users can access sensitive resources.

Threat Detection and Mitigation: SDN platforms can integrate with advanced security tools and analytics engines to detect and mitigate security threats in real time. By analyzing network traffic patterns and behavior anomalies, SDN controllers can identify and respond to potential security breaches proactively, minimizing the risk of data loss or service disruption.

Dynamic Security Policy Adaptation: SDN enables dynamic adaptation of security policies in response to evolving threats and changing network conditions. Security policies can be automatically adjusted based on threat intelligence feeds, network performance metrics, and compliance requirements, ensuring continuous protection against emerging security threats.

Network Visualization and Forensics: SDN provides comprehensive network visibility and monitoring capabilities, allowing administrators to visualize network topology, traffic flows, and security events in real time. This visibility facilitates rapid incident response and forensic analysis, enabling security teams to identify the root cause of security incidents and implement remediation measures effectively.

Integration with Security Technologies: SDN platforms can integrate seamlessly with existing security technologies, such as intrusion detection/prevention systems (IDPS), firewalls, and security information and event management (SIEM) solutions. This integration enhances the effectiveness of security controls and enables coordinated responses to security incidents across the entire IoT infrastructure.

Secure Overlay Networks: SDN enables the creation of secure overlay networks that provide encrypted communication channels between IoT devices and applications. By leveraging virtual network overlays and encryption protocols, SDN can protect data in transit from eavesdropping, tampering, and unauthorized access, ensuring end-to-end confidentiality and integrity of IoT communications.

Through these security mechanisms, SDN enhances the overall security posture of IoT deployments, enabling organizations to mitigate security risks effectively and safeguard critical assets and data in an increasingly connected and dynamic IoT landscape.

6. Conclusions

The study explores the integration of SDN principles into the complex landscape of IoT to tackle scalability and security challenges. Using the Floodlight SDN controller and Mininet-WiFi, significant improvements in managing and securing IoT networks are demonstrated. SDN enhances scalability by effectively managing a growing number of IoT devices and Access Points without compromising critical performance metrics like latency and packet loss. It has proven adept at swiftly detecting and mitigating Distributed Denial of Service (DDoS) attacks, often within 15 minutes, showcasing its advantage in maintaining IoT operations' integrity and reliability.

The Floodlight controller's effectiveness in detecting and mitigating DDoS attacks within the IoT environment is notable. The timeline of the DDoS attack mitigation process, from detection to the restoration of normal operations within 15 minutes, demonstrates the controller's efficiency in handling security incidents. Built-in and custom-developed algorithms for traffic analysis and anomaly detection, combined with dynamic network configuration adjustments, played a crucial role in the swift mitigation of the attack. This underscores the Floodlight controller's capabilities in ensuring the network's resilience against such cyber threats, highlighting the benefits of integrating SDN principles for enhanced IoT security.

The integration of SDN into IoT networks, facilitated by controllers like Floodlight, presents a promising approach to overcoming scalability and security challenges. Observed improvements in network performance and security validate SDN's potential to transform IoT network management. However, continuous adaptation and improvement of SDN strategies will be essential to address evolving cyber threats and the increasing complexity of IoT ecosystems. Future research should focus on exploring advanced SDN features, developing sophisticated security mechanisms, and evaluating SDN's impact in larger and more diverse IoT deployments.

In conclusion, this study underscores SDN's effectiveness in enhancing the scalability and security of IoT environments, emphasizing the pivotal role of controllers like Floodlight in achieving these objectives.

REFERENCES

Aldhaheri, A., Alwahedi, F., Ferrag, M. A. & Battah, A. (2024) Deep learning for cyber threat detection in IoT networks: A review. *Internet of Things and Cyber-Physical Systems*. 4, 110–128. doi:10.1016/j.iotcps.2023.09.003.

Aljahdali, A., Aldissi, H., Banafee, S., Sobahi, S. & Nagro, W. (2021) IoT Forensic models analysis. *Romanian Journal of Information Technology and Automatic Control [Revista Română de Informatică și Automatică]*. 31(2), 21–34. doi:10.33436/v31i2y202102.

Alsaeedi, M., Mohamad, M. M. & Al-Roubaiey, A. A. (2019) Toward Adaptive and Scalable OpenFlow-SDN Flow Control: A Survey. *IEEE Access*. 7, 107346–107379. doi:10.1109/ACCESS.2019.2932422.

Bekri, W., Jmal, R. & Chaari Fourati, L. (2020) Internet of Things Management Based on Software Defined Networking: A Survey. *International Journal of Wireless Information Networks.* 27, 385–410. doi:10.1007/s10776-020-00488-2.

Bi, Y., Han, G., Lin, C., Guizani, M. & Wang, X. (2019) Mobility Management for Intro/Inter Domain Handover in Software-Defined Networks. *IEEE Journal on Selected Areas in Communications.* 37(8), 1739–1754. doi:10.1109/JSAC.2019.2927097.

Dai, H.-N., Wong, R. C.-W., Wang, H., Zheng, Z. & Vasilakos, A. V. (2020) Big Data Analytics for Large-scale Wireless Networks. *ACM Computing Surveys.* 52(5), 1–36. doi:10.1145/3337065.

Dorri, A., Kanhere, S. S. & Jurdak, R. (2017) Towards an Optimized BlockChain for IoT. *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*. 173–178. doi:10.1145/3054977.3055003.

Dumitrache, M. & Sandu, I.-E. (2020) Securitatea rețelelor și sisteme de comunicații în medii Smart. *Romanian Journal of Information Technology and Automatic Control [Revista Română de Informatică și Automatică]*. 30(1), 61–70. doi:10.33436/v30i1y202005.

EL-Garoui, L., Pierre, S. & Chamberland, S. (2020) A New SDN-Based Routing Protocol for Improving Delay in Smart City Environments. *Smart Cities.* 3(3), 1004–1021. doi:10.3390/smartcities3030050.

Farahani, B., Firouzi, F. & Luecking, M. (2021) The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. *Journal of Network and Computer Applications*. 177, 102936. doi:10.1016/j.jnca.2020.102936.

Floodlight SDN Controller (n.d.) *Floodlight-Project*. http://www.Projectfloodlight.Org [Accessed 1st February 2024].

Fontes, R. R., Afzal, S., Brito, S. H. B., Santos, M. A. S. & Rothenberg, C. E. (2015) Mininet-WiFi: Emulating software-defined wireless networks. In: *2015 11th International Conference on Network and Service Management (CNSM), Barcelona, Spain.* pp.3 84–389. doi:10.1109/CNSM.2015.7367387.

Han, M. P., Htet, S. Y. & Wuttisttikulkij, L. (2022) Hybrid GNS3 and Mininet-WFi Emulator for SDN Backbone Network Supporting Wireless IoT Traffic. In: *2022 37th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), Phuket, Thailand*. pp.768–771. doi:10.1109/ITC-CSCC55581.2022.9895019.

Hasan, T., Akhunzada, A., Giannetsos, T. & Malik, J. (2020) Orchestrating SDN Control Plane towards Enhanced IoT Security. In: *2020 6th IEEE Conference on Network Softwarization (NetSoft), Ghent, Belgium*. pp.457–464. doi:10.1109/NetSoft48620.2020.9165424.

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P. & Sikdar, B. (2019) A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access.* 7, 82721–82743. doi:10.1109/ACCESS.2019.2924045.

Jayaraman, B., Thanga Nadar Thanga Thai, M., Anand, A. & Anandan, K. R. (2023) Detecting malicious IoT traffic using Machine Learning techniques. *Romanian Journal of Information Technology and Automatic Control [Revista Română de Informatică și Automatică]*. 33(4), 47–58. doi:10.33436/v33i4y202304.

Johnson, R. & Patel, S. (2019) Scalability Challenges in Heterogeneous IoT Environments. *IEEE Transactions on Networking*. 22(4), 789–802.

Karmakar, K. K., Varadharajan, V., Nepal, S. & Tupakula, U. (2021) SDN-Enabled Secure IoT Architecture. *IEEE Internet of Things Journal*. 8(8), 6549–6564. doi:10.1109/JIOT.2020.3043740.

Khan, Y., Su'ud, M. B. M., Alam, M. M., Ahmad, S. F., Ahmad (Ayassrah), A. Y. A. B. & Khan, N. (2022) Application of Internet of Things (IoT) in Sustainable Supply Chain Management. *Sustainability*. 15(1), 694. doi:10.3390/su15010694.

Kumar, S. A., Vealey, T. & Srivastava, H. (2016) Security in Internet of Things: Challenges, Solutions and Future Directions. In: *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 5772–5781. doi:10.1109/HICSS.2016.714.

Li, Y., Su, X., Ding, A. Y., Lindgren, A., Liu, X., Prehofer, C., Riekki, J., Rahmani, R., Tarkoma, S. & Hui, P. (2020) Enhancing the Internet of Things with Knowledge-Driven Software-Defined Networking Technology: Future Perspectives. *Sensors*. 20(12), 3459. doi:10.3390/s20123459.

Milošević, M., Mladenović, V. & Pešović, U. (2021) Evaluation of HTTP/3 Protocol for Internet of Things and Fog Computing Scenarios. *Studies in Informatics and Control*. 30(3), 75–84. doi:10.24846/v30i3y202107.

Muthanna, M. S. A., Alkanhel, R., Muthanna, A., Rafiq, A. & Abdullah, W. A. M. (2022) Towards SDN-Enabled, Intelligent Intrusion Detection System for Internet of Things (IoT). *IEEE Access*. 10, 22756–22768. doi:10.1109/ACCESS.2022.3153716.

Oracevic, A., Dilek, S. & Ozdemir, S. (2017) Security in internet of things: A survey. In: *2017 International Symposium on Networks, Computers and Communications (ISNCC)*, Marrakech, Morocco. pp.1–6. doi:10.1109/ISNCC.2017.8072001.

Saadeh, H., Almobaideen, W., Sabri, K. E. & Saadeh, M. (2019) Hybrid SDN-ICN Architecture Design for the Internet of Things. In: *2019 Sixth International Conference on Software Defined Systems (SDS)*, Rome, Italy. pp. 96–101. doi:10.1109/SDS.2019.8768582.

Saber, A. M., Behiry, M. H. & Amin, M. (2022) Real-Time Optimization for an AVR System Using Enhanced Harris Hawk and IIoT. *Studies in Informatics and Control*. 31(2), 81–94. doi:10.24846/v31i2y202208.

Salim, M. M., Rathore, S. & Park, J. H. (2020) Distributed denial of service attacks and its defenses in IoT: a survey. *The Journal of Supercomputing*. 76(7), 5320–5363. doi:10.1007/s11227-019-02945-z.

Selvaraju, S. P., Balador, A., Fotouhi, H., Vahabi, M. & Bjorkman, M. (2021) Network Management in Heterogeneous IoT Networks. In: *2021 International Wireless Communications and Mobile Computing (IWCMC)*.1581–1586. doi:10.1109/IWCMC51323.2021.9498801.

Sethi, P. & Sarangi, S. R. (2017) Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*. 2017, 1–25. doi:10.1155/2017/9324035.

Siddiqui, S., Hameed, S., Shah, S. A., Ahmad, I., Aneiba, A., Draheim, D. & Dustdar, S. (2022) Toward Software-Defined Networking-Based IoT Frameworks: A Systematic Literature Review, Taxonomy, Open Challenges and Prospects. *IEEE Access*. 10, 70850–70901. doi:10.1109/ACCESS.2022.3188311.

Silva, B. N., Khan, M. & Han, K. (2018) Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sustainable Cities and Society*. 38, 697–713. doi:10.1016/j.scs.2018.01.053.

Stancu, A., Vulpe, A. & Halunga, S. (2018) Evaluation of a Wireless Transport Network Emulator Used for SDN Applications Development. *IEEE Access*. 6, 15870–15883. doi:10.1109/ACCESS.2018.2815844.

Ye, F. & Qian, Y. (2017) A Security Architecture for Networked Internet of Things Devices. In: *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*. 1–6. doi:0.1109/GLOCOM.2017.8254021.

Zhu, L., Karim, M. M., Sharif, K., Xu, C., Li, F., Du, X. & Guizani, M. (2021) SDN Controllers. *ACM Computing Surveys*. 53(6), 1–40. doi:10.1145/3421764.

Diyar Jamal HAMAD received his Bachelor's degree in Computer Science from Soran University in Erbil, Iraq and M.SC degree in Computer Engineering from Kahramanmaras Sutcu Imam University, Kahramanmaras, Turkey. He is currently a Ph.D. candidate in the Computer Science and Engineering Department at the National University of Science and Technology Politehnica Bucharest, Romania. His current research interests include SDN, network management, and cloud and cluster computing.

Khirota Gorgees YALDA received her Bachelor's degree in Computer Science from Salahaddin University in Erbil, Iraq and Master's degree in Computer Engineering from Kahramanmaras Sutcu Imam University, Kahramanmaras, Turkey. She is currently a Ph.D. candidate in the Computer Science department at the National University of Science and Technology Politehnica Bucharest, Romania. Her current research interests include SDN, LSTM, Machine Learning and predictions.

Nicolae TAPUS is a Professor of Computer Science and Engineering, National University of Science and Technology Politehnica Bucharest, Romania. His current research interests include computer architecture, networking, distributed systems, network of sensors, embedded systems.

İbrahim Taner OKUMUS is a Professor of Computer Science and Engineering, Kahramanmaras Sutcu Imam University, Kahramanmaras, Turkey. He received his Bachelor's degree in Electronics and Telecommunications Engineering from Istanbul Technical University, Istanbul, Turkey, and his M.Sc. and Ph.D. in the Electrical and Computer Engineering from Syracuse University, Syracuse, NY, USA. His current research interests include SDN, computer communication, computer networking, and routing algorithms.

This is an open access article distributed under the terms and conditions of the Creative Commons Attribution-NonCommercial 4.0 International License.