U.P.B. Sci. Bull., Series C, Vol. 86, Iss. 4, 2024 ISSN 2286-3540

# COMPARING WSN PERFORMANCE: TRADITIONAL VS. SDN APPROACH

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

*The proliferation of Wireless Sensor Networks (WSN) in various applications has necessitated the exploration of network architectures that can ensure efficient, scalable, and reliable communication. This study presents a comparative performance evaluation of traditional networking paradigms and Software-Defined Networking (SDN)-based architectures within WSN. Utilizing the Floodlight SDN controller and Mininet-WiFi emulator, we conducted a series of experiments across three different network topologies, varying the number of hosts and access points. The performance metrics focused on are average latency, packet loss percentage, and throughput. The results demonstrate a considerable improvement in all measured parameters under the SDN-based environment compared to the traditional setup. Specifically, SDN environments consistently showcased lower latency, minimal packet loss, and higher throughput, with the most notable difference observed in smaller network configurations. The findings suggest that SDN, with its centralized control plane, can significantly enhance the performance of WSNs, particularly in scenarios demanding rapid scalability and dynamic traffic management. This study underscores the potential of SDN architectures in optimizing WSN operations and lays the groundwork for future research in this domain.*

**Keywords**: WSN, SDN, Mininet-wifi, Floodlight Controller, Metrics.

## 1. Introduction

Wireless Sensor Networks (WSNs) have emerged as a critical component of modern communication ecosystems, underpinning a multitude of applications ranging from environmental monitoring to healthcare, industrial automation, and smart cities [1]. WSNs typically consist of spatially distributed autonomous sensors that cooperatively monitor physical or environmental conditions, like temperature, sound, vibration, pressure, motion, or pollutants, at different locations. As the demand for such networks skyrockets, driven by the Internet of Things (IoT)

[1] PhD Candidate, Faculty of Automatic Control and Computer Science, University of Science and Technology POLITEHNICA Bucharest. Soran Technical college, Erbil Polytechnic University, Erbil, Iraq, e-mail: diyar.hamad@epu.edu.iq, kherota.yalda@epu.edu.iq.

[2] PhD eng., Computer Engineering, Kahramanmaras Sutcu Imam University, Kahramanmaras, e-mail: iokumus@ksu.edu.tr.

[3] PhD eng., Dept. of Computer Science, University of Science and Technology POLITEHNICA Bucharest, e-mail: nicolae.tapus@upb.ro.

expansion, the efficient, reliable and timely transfer of the collected data becomes paramount [2].

The traditional networking paradigms employed in WSNs, while foundational, have struggled to keep pace with the rapidly evolving requirements of these complex networks [3]. Issues such as network congestion, dynamic topology changes, and the need for efficient resource utilization pose significant challenges [4][5]. Furthermore, the conventional distributed network control mechanisms often fall short in providing the required agility and scalability due to their inherent design, which separates the data plane from the control plane.

Software-Defined Networking (SDN) has been posited as a revolutionary approach to network management that could potentially address these challenges [6]. By decoupling the network control logic from the underlying routers and switches, SDN offers a centralized view of the entire network, which is particularly beneficial for WSNs where the network conditions can change unpredictably [7]. This centralization facilitates more sophisticated network management strategies, enabling rapid reconfiguration and optimization of network resources to meet the demands of various applications [8].

The motivation for this study arises from the critical need to empirically evaluate the performance benefits of SDN-based WSNs over traditional network configurations. While the theoretical advantages of SDN are well-documented, there is a lack of comprehensive practical evaluations that demonstrate these benefits within the context of WSNs. Hence, this study aims to fill this gap by providing empirical data on the performance differentials between traditional and SDN-based WSNs in terms of latency, packet loss, and throughput.

To this end, we have designed an experimental framework using the Floodlight SDN controller [9] and Mininet-WiFi [10], a popular network emulator, to simulate WSNs with varying sizes and complexities. By comparing the performance of these networks under both traditional and SDN-based control mechanisms, this study seeks to offer tangible insights into the scalability, efficiency, and reliability of SDN in WSN applications.

The selection of performance metrics-latency, packet loss, and throughput—provides a comprehensive view of the network's operational characteristics. Latency measures the time taken for a data packet to traverse from one point in the network to another, which is crucial for time-sensitive applications. Packet loss indicates the reliability of the network in delivering data packets, which directly impacts the quality of service. Throughput, or the rate at which data is successfully delivered over the network, reflects the network's capacity to handle traffic. Together, these metrics encapsulate the essential aspects of network performance that can make or break the effectiveness of WSN deployments.

## 2. Background and Related Work

The advent of Wireless Sensor Networks (WSNs) marked a significant milestone in the domain of wireless communication, empowering a diverse range of applications with remote sensing capabilities. Traditional WSNs are typically constructed with nodes that are responsible for data collection and packet forwarding, utilizing classic networking protocols like ZigBee, 6LoWPAN, or proprietary standards tailored for specific use cases [11] [12]. The operational paradigm of these networks has been inherently decentralized, with each node making local decisions regarding data transmission based on the protocol's logic. This approach, while facilitating a degree of robustness against single points of failure, often results in inefficiencies due to the lack of global network knowledge, leading to suboptimal path selections, congestion, and collisions, particularly as the network scales.

Software-Defined Networking (SDN), in stark contrast, introduces a paradigm shift by centralizing the control logic in a manner that abstracts the decision-making process from the individual network devices to a central controller [13]. This architectural change enables a global view of the network, which can be leveraged to optimize traffic flow, manage resources more efficiently, and dynamically adjust to changing network conditions. In the context of WSNs, SDN's central control can mitigate many of the issues inherent to traditional networking by enabling coordinated management of network resources and by providing the flexibility needed to adapt to the dynamics of WSN environments [14].

Prevailing literature provides a myriad of insights into the benefits of SDN in various networking scenarios [15]. However, the application of SDN principles to WSNs is a relatively nascent research area with limited empirical studies. Notable works have explored the theoretical benefits of SDN in WSNs, suggesting improvements in energy consumption, network lifetime, and management overhead. Yet, empirical evaluations, particularly comparative ones that provide measurable outcomes of SDN versus traditional network performance in WSNs, remain scarce [16].

Among the few comparative studies that exist, some have demonstrated the potential for SDN to enhance network performance metrics such as end-to-end delay, jitter, and throughput in simulated environments. Others have focused on specific aspects of WSNs, like energy efficiency or the impact of SDN on node computation and communication overhead. However, these studies often focus on isolated aspects of network performance or on simulations that do not encapsulate the complexities of large-scale, real-world WSN deployments.

Our study seeks to contribute to this body of knowledge by providing a comprehensive empirical evaluation of both SDN-based and traditional network architectures in a controlled yet realistic WSN simulation environment. We extend the existing research by not only considering the fundamental performance metrics but also by examining how these metrics are affected by the scale of the network. By incrementally increasing the number of hosts and access points in our simulations, we aim to offer a granular view of how network performance scales in both SDN-based and traditional WSNs. This approach allows us to provide insights into the scalability and adaptability of SDN within WSNs, which are critical factors for their application in burgeoning IoT infrastructures.

In summary, while the theoretical and simulated benefits of SDN in WSNs have been addressed in the literature, this study aims to fill the gap with practical, empirical evidence demonstrating the advantages of SDN in WSNs across a spectrum of network scales. Our work not only corroborates previous findings but also provides a unique contribution by illustrating the impact of network size on the performance benefits of SDN, thereby offering a more nuanced understanding of SDN's potential in real-world WSN applications.

## 3. Research Methodology and Design

The objective of our experimental study was to conduct a systematic performance evaluation of Wireless Sensor Networks (WSNs) under two different network architectures: the traditional approach and the Software-Defined Networking (SDN) paradigm. To achieve this, we meticulously designed a series of experiments using state-of-the-art network simulation tools capable of accurately modeling both traditional and SDN-based WSNs.

### 3.1 Performance Metrics

Our evaluation focused on three key performance metrics that are crucial indicators of network performance in WSN environments:

A. Latency: Measured as the average time taken for a data packet to travel from a source host to a destination host. This metric is indicative of the network's responsiveness and is critical for time-sensitive applications.

B. Packet Loss: Quantified as the percentage of data packets that failed to reach their destination. Packet loss reflects the network's reliability and its ability to deliver data under varying conditions.

C. Throughput: Evaluated as the average rate at which data packets are successfully delivered across the network. Throughput is a measure of the network's capacity and efficiency in handling data traffic.

### 3.2 Network Topologies

We developed three distinct network topologies to evaluate the performance of both network architectures across varying levels of complexity and scale. The first topology employs a bus configuration, followed by a mesh topology, and finally a tree topology.

In the small-scale scenario described, we present two configurations: one featuring a traditional network setup without Software-Defined Networking (SDN), and the other incorporating SDN advancements. Fig. 1 illustrates the traditional network topology, comprising 5 hosts connected to 2 access points in a straightforward, manually configured Wireless Sensor Network (WSN) deployment. Contrarily, Fig. 2 showcases the same network configuration enhanced with SDN capabilities. Here, an SDN controller centrally manages connections and dynamically optimizes the network, emphasizing the advantages of SDN in enhancing flexibility, efficiency, and control in WSN deployments. Both topologies are configured as a Bus topology.

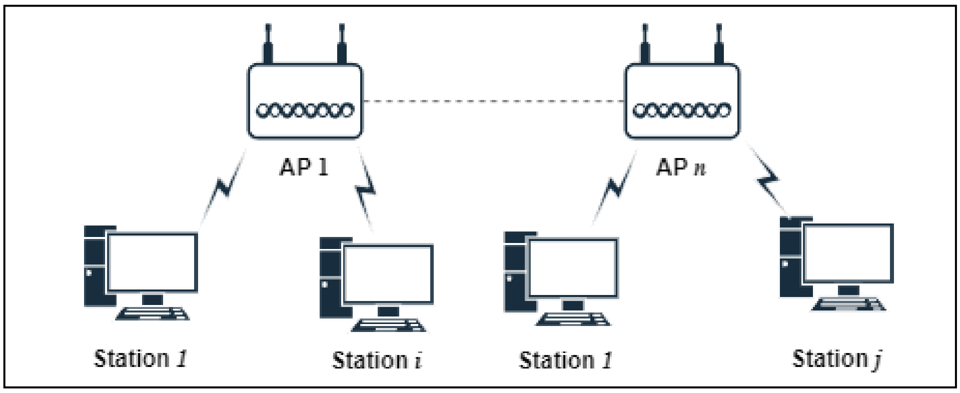

Fig. 1: Traditional network topology

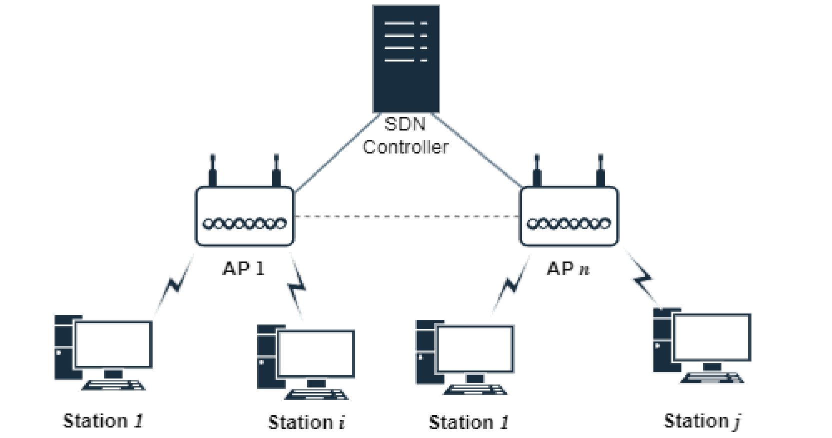

Fig. 2: Network topology based on SDN

In the second topology, we examine both a conventional network model without SDN and an enhanced model that incorporates SDN, each designed to manage the increased complexity of connecting 12 hosts through 4 access points and they configured as a Mesh topology. The traditional network model handles this expanded setup by adapting to the heightened demands for communication and management overhead. Meanwhile, the SDN-integrated model demonstrates how the SDN controller optimizes network paths, manages traffic more efficiently, and provides centralized control to handle the larger number of hosts and access points. This illustrates the scalable benefits of SDN in managing more complex network infrastructures.

The last topology is Tree, it involving 32 hosts connected through 8 access points, the network complexity significantly increases. This configuration simulates an extensive Wireless Sensor Network (WSN) environment, presenting substantial demands on network resources and management. The setup illustrates the challenges of scaling network infrastructure to support high connectivity levels in complex scenarios. Given the intricacy and extensive nature of this network, creating a detailed figure to accurately represent its topology is challenging. Such complexity underscores the need for advanced network management and resource allocation strategies to efficiently handle the increased communication and administrative overhead in such deployments.

In the topologies depicted in Figs. 1 and 2, ‘*n’* represents the number of access points, while ‘n and *j*’ represents the number of stations belongs to access points. Each topology was meticulously designed to emulate realistic Wireless Sensor Network (WSN) deployments. In this context, the hosts correspond to sensor nodes, whereas the access points serve as gateways facilitating communication between the sensor nodes and the network infrastructure.

## 4. Experimental Setup and Configuration

### 4.1 Mininet-WiFi

A fork of the well-known Mininet network emulator, Mininet-WiFi extends Mininet's capabilities to emulate wireless and mobile networks, including WSNs [18]. It offers the flexibility to create custom network topologies and simulate various network conditions and configurations, making it an ideal tool for our experiments [19].

### 4.2 Floodlight Controller

An open-source, Java-based SDN controller that was chosen for its widespread use in the research community and its compatibility with various SDN protocols, including OpenFlow [17]. The Floodlight controller acted as the central decision-making entity in our SDN-based network simulations, providing a real-time, comprehensive view of the network state and facilitating dynamic traffic management and network reconfiguration.

### 4.3 Software Configurations

The Mininet-WiFi emulator was configured to simulate the behavior of wireless sensors and access points with specific attention to wireless communication parameters such as signal range, interference, and mobility patterns. In the SDN scenarios, the Floodlight controller was configured to manage the network using OpenFlow protocols, implementing various flow rules and policies to optimize network performance.

In traditional network scenarios, we employed standard WSN protocols without the intervention of an SDN controller, relying on the autonomous decision-making of each node based on the predefined protocol logic.

## 5. Analysis and Results

Our experimental results manifest a compelling comparative analysis between Software-Defined Networking (SDN) environments and traditional network architectures within Wireless Sensor Networks (WSNs). The performance metrics evaluated were latency, packet loss, and throughput, and the experiments were conducted across three topologies with varying numbers of hosts and access points. The network traffic was generated using the Iperf tool with a consistent bandwidth of 5 Mbits over a duration of five minutes for each test.

Each experiment was run multiple times to ensure statistical significance, and the results were averaged to account for any anomalies or outliers. Care was taken to maintain consistent environmental conditions across all simulations to ensure the comparability of results.

The following sections will present the results derived from these experiments and provide an analysis of the performance of traditional versus SDN-based WSNs across the three network topologies and the measured metrics.

***Latency:***

The latency across network topologies indicates a clear performance disparity between SDN and traditional networks. In the graph representing latency, the SDN environment for the smallest topology which its Bus topology recorded an average latency of merely 1.59 ms, which starkly contrasts with the traditional network's 29.8 ms. As network complexity increases, SDN latency climbs but does so at a rate that remains below that of the traditional approach. At the largest scale of topology which its Tree topology, the latency in the SDN environment was recorded at 18.63 ms, compared to the traditional network's 25.73 ms. This indicates that

SDN's centralized control mechanism maintains a significant advantage in managing communication delays, even as the network scales.

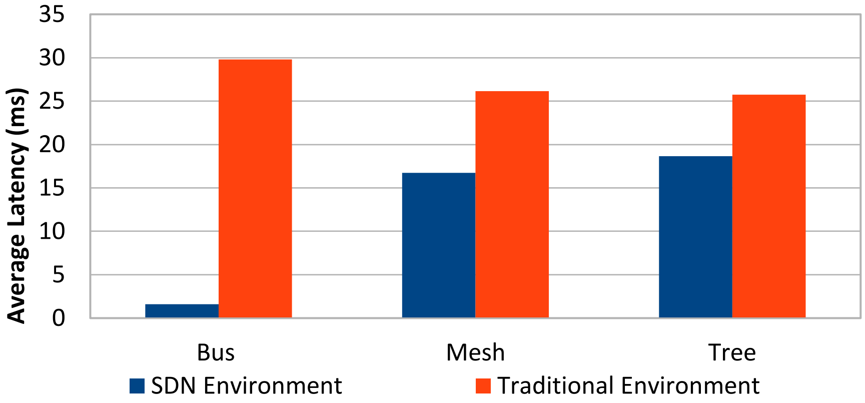

Fig. 3: Average Latency

***Packet Loss:***

Fig. 4 compares packet loss percentages across different topologies. In the bus topology, SDN achieved 0% packet loss, while traditional networks had 5%. In the Mesh topology, SDN maintained 0.83% packet loss compared to traditional networks' 5.83%. This trend suggests increasing packet loss with network complexity, but SDN consistently outperforms traditional networks, underscoring its reliability in WSNs.

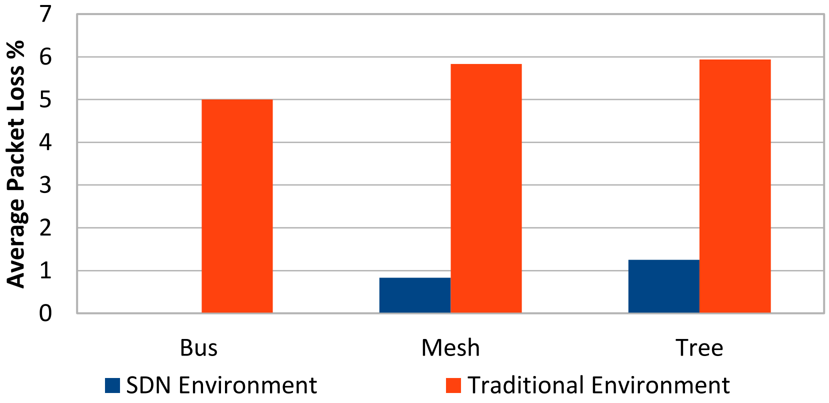

Fig. 4: Average Packet Loss

***Throughput***

Throughput, a critical measure of network efficiency, is depicted in Fig. 5. The SDN environment's superiority is most pronounced in the Bus topology, with an impressive throughput of 82.75 Mbits/s, which significantly outperforms the traditional network's throughput of 10 Mbits/s. This differential narrows as the network expands; however, SDN throughput remains notably higher across all scales. For instance, in the Tree evaluated topology, SDN achieves a throughput of

53.18 Mbits/s, compared to 30.78 Mbits/s in the traditional setup. This reinforces the notion that SDN architectures are better suited to manage and sustain higher data transfer rates within WSNs.

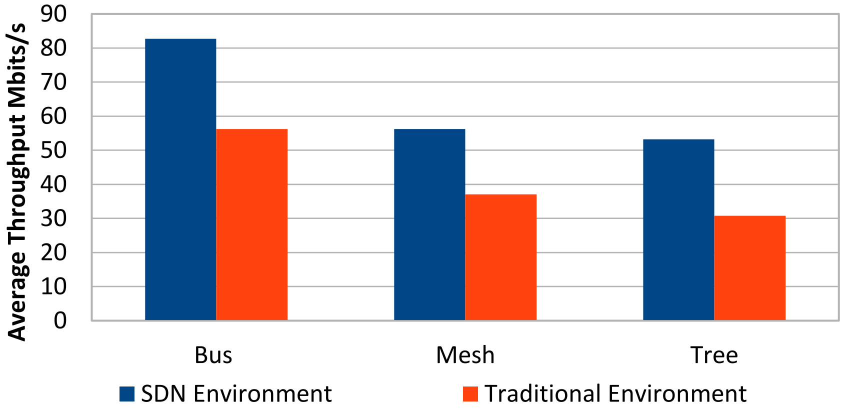

Fig. 5: Average Throughput

The graphical representations of our data succinctly illustrate the performance benefits of SDN over traditional networking in WSNs. The trends highlighted by the graphs indicate that SDN maintains a consistent performance advantage across all evaluated scales and metrics. This is especially pertinent when considering the deployment of WSNs in real-world scenarios, where network reliability, responsiveness, and efficiency are paramount.

Forevermore, the experimental results clearly demonstrate the performance benefits of SDN over traditional networking. SDN's centralized control plane, dynamic path optimization, and efficient traffic management lead to lower latency, reduced packet loss, and higher throughput. These advantages make SDN a compelling choice for modern and scalable network infrastructures, especially as network complexity increases.

This analysis confirms that transitioning to an SDN-based network can significantly enhance performance, making it an attractive option for organizations looking to optimize their network operations.

The prevailing preference for traditional networking over Software-Defined Networking (SDN), despite SDN's demonstrated performance superiority, persists within many organizations. This preference is largely due to factors such as significant investments in legacy infrastructure, complexities in implementing and managing SDN environments, skill gaps among network administrators, interoperability concerns, and compatibility issues with existing network components. Additionally, concerns about vendor lock-in, migration risks, and perceived cost-benefit ratios contribute to the reluctance to adopt SDN, particularly in risk-averse or highly regulated industries. However, as SDN continues to mature and address implementation challenges, it may gain broader acceptance, especially as organizations prioritize modernization efforts and digital transformation initiatives.

## 6. Environmental Aspects

The results from our comparative analysis between Software-Defined Networking (SDN) and traditional network architectures within Wireless Sensor Networks (WSNs) elucidate several key insights into the efficacy of SDN in enhancing network performance. The empirical data exhibit that SDN environments outperform traditional networks across all measured performance metrics—latency, packet loss, and throughput—irrespective of the network's scale. This section will delve into the analysis of these results, exploring the underlying factors contributing to SDN's superior performance and the implications of these findings for real-world applications.

### 6.1 Underlying Factors for SDN's Superior Performance

Centralized Control and Global Network View: One of the fundamental advantages of SDN is its centralized control plane, which maintains a global view of the network state. This comprehensive perspective allows the SDN controller to make informed and optimized decisions for routing and data forwarding. Unlike traditional networks, where decisions are made locally and independently at each node, often with incomplete information, SDN's approach can minimize latency by selecting the most efficient paths and dynamically adapting to network changes.

Dynamic Traffic Management: SDN controllers can implement sophisticated traffic engineering policies, such as load balancing and prioritization of critical data flows. In our experiments, the reduced packet loss and higher throughput in SDN environments can be attributed to such dynamic traffic management capabilities, which efficiently utilize available network resources and swiftly rectify congestion issues.

Automated Network Reconfiguration: In response to network events or changing performance demands, SDN can reconfigure network flows in real-time. This agility was observed in our results, where SDN maintained performance consistency even as the network scaled, suggesting an inherent ability to adapt to increasing loads and complexity.

### 6.2 Emerging Developments and Insights

Scalability: The data revealed a pattern of increasing latency and packet loss with the growth in network size for both SDN and traditional networks. However, the rate of increase was substantially lower in SDN environments, indicating a more scalable network architecture. This trend is particularly relevant for IoT applications, where networks are expected to expand dynamically and operate reliably at scale.

Consistency in Performance: Across different topologies, SDN exhibited less variance in performance metrics compared to traditional networks. This consistency is indicative of the robustness of SDN-controlled networks, which is critical for applications that require a high level of reliability, such as healthcare monitoring systems or industrial control networks.

High Throughput Maintenance: Even as the number of hosts and access points increased, SDN managed to sustain higher throughput levels compared to traditional networks. This suggests that SDN architectures are potentially more effective in handling high-density networks with extensive data transmission requirements, such as video surveillance systems or large-scale environmental sensing applications.

### 6.3 Implications for Real-World Applications

The empirical evidence from our study suggests that SDN's architectural advantages could be highly beneficial in real-world WSN deployments. For instance, in smart city infrastructures, where a multitude of sensors collect vast amounts of data, SDN's ability to manage traffic efficiently and maintain high throughput can translate into more timely and accurate data analysis.

In mission-critical applications, where decisions must be made in real-time, such as in autonomous vehicle coordination or emergency response systems, the lower latency and packet loss rates associated with SDN can provide the reliability and responsiveness needed.

Moreover, the scalability of SDN makes it a suitable choice for IoT ecosystems, which are characterized by their vast, dynamic, and heterogeneous nature. The capacity of SDN to adapt to changing network conditions and manage diverse traffic types is aligned with the needs of IoT applications, which often involve integrating new devices and varying data flows. The out-performance of SDN in our experiments highlights its potential to serve as the backbone for modern WSNs. The positive trends observed in SDN environments underscore its suitability for a wide range of applications, particularly those that are dynamic, data-intensive, and scale-sensitive. As we look towards increasingly interconnected and automated environments, SDN stands out as a promising solution to meet the complex demands of future networking challenges.

## 7. Conclusion

The extensive comparative analysis conducted in this study provides valuable insights into the performance of Software-Defined Networking (SDN) compared to traditional network architectures within Wireless Sensor Networks (WSNs). Through meticulous experimentation using the Floodlight SDN controller and Mininet-WiFi across three network topologies, we have gathered empirical data that clearly demonstrates the superiority of SDN in terms of latency, packet loss, and throughput.

The results have unequivocally shown that SDN environments offer substantial improvements in network performance. Latency, a critical metric for real-time applications, was significantly lower in SDN environments across all network scales. Packet loss was minimal, ensuring reliable data delivery which is indispensable for the integrity of sensor data in WSN applications. Throughput, indicative of the network's capacity to handle traffic, was consistently higher in SDN environments, suggesting that SDN is well-equipped to manage the high data loads characteristic of burgeoning IoT infrastructures.

This study's findings suggest that SDN holds the promise to overcome the limitations of traditional WSNs, particularly in scalability and efficient traffic management. These traits are essential for the deployment of WSNs in diverse applications, ranging from smart cities and industrial automation to environmental monitoring and healthcare systems.

Furthermore, the consistency and adaptability of SDN as observed in the results imply that SDN can serve as a robust foundation for the next generation of WSNs, which will require dynamic network management and high reliability to support complex applications and services.

As we move forward, it is imperative that the research community and industry stakeholders consider the integration of SDN principles into the design and development of WSNs. Our study contributes to the body of knowledge by providing empirical evidence of the benefits of SDN, paving the way for future research to explore the full potential of SDN in WSNs and related fields.

In conclusion, the transition to SDN-based WSNs holds significant potential to enhance the capabilities of sensor networks, making them more efficient, scalable, and reliable. This evolution is not merely an incremental improvement but a necessary stride toward realizing the full potential of WSNs in an increasingly interconnected world.

## REFERENCES

[1] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W.-C. Hong, “Internet of Things: Evolution, Concerns and Security Challenges,” Sensors, vol. 21, no. 5, p. 1809, Mar. 2021, doi: 10.3390/s21051809.

[2] D. Kanellopoulos, V. K. Sharma, T. Panagiotakopoulos, and A. Kameas, “Networking Architectures and Protocols for IoT Applications in Smart Cities: Recent Developments and Perspectives,” Electronics (Basel), vol. 12, no. 11, p. 2490, May 2023, doi: 10.3390/electronics12112490.

[3] A. K. Gautam and R. Kumar, “A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks,” SN Appl Sci, vol. 3, no. 1, p. 50, Jan. 2021, doi: 10.1007/s42452-020-04089-9.

[4] K. Gulati, R. S. Kumar Boddu, D. Kapila, S. L. Bangare, N. Chandnani, and G. Saravanan, “A review paper on wireless sensor network techniques in Internet of Things (IoT),” Mater Today Proc, vol. 51, pp. 161–165, 2022, doi: 10.1016/j.matpr.2021.05.067.

[5] K. M. Awan, P. A. Shah, K. Iqbal, S. Gillani, W. Ahmad, and Y. Nam, “Underwater Wireless Sensor Networks: A Review of Recent Issues and Challenges,” Wirel Commun Mob Comput, vol. 2019, pp. 1–20, Jan. 2019, doi: 10.1155/2019/6470359.

[6] A. Hodaei and S. Babaie, “A Survey on Traffic Management in Software-Defined Networks: Challenges, Effective Approaches, and Potential Measures,” Wirel Pers Commun, vol. 118, no. 2, pp. 1507–1534, May 2021, doi: 10.1007/s11277-021-08100-3.

[7] M. Fogli, C. Giannelli, and C. Stefanelli, “Software-Defined Networking in wireless ad hoc scenarios: Objectives and control architectures,” Journal of Network and Computer Applications, vol. 203, p. 103387, Jul. 2022, doi: 10.1016/j.jnca.2022.103387.

[8] S. Ahmad and A. H. Mir, “Scalability, Consistency, Reliability and Security in SDN Controllers: A Survey of Diverse SDN Controllers,” Journal of Network and Systems Management, vol. 29, no. 1, p. 9, Jan. 2021, doi: 10.1007/s10922-020-09575-4.

[9] “‘Floodlight Open SDN Controller,’ Open Networking Foundation,.” 2018.

[10] R. R. Fontes, S. Afzal, S. H. B. Brito, M. A. S. Santos, and C. E. Rothenberg, “Mininet-WiFi: Emulating software-defined wireless networks,” in 2015 11th International Conference on Network and Service Management (CNSM), IEEE, Nov. 2015, pp. 384–389. doi: 10.1109/CNSM.2015.7367387.

[11] N. Sabor and M. Abo-Zahhad, “A Comprehensive Survey of Intelligent-Based Hierarchical Routing Protocols for Wireless Sensor Networks,” 2020, pp. 197–257. doi: 10.1007/978-981-15-2125-6_10.

[12] R. Zagrouba and A. Kardi, “Comparative Study of Energy Efficient Routing Techniques in Wireless Sensor Networks,” Information, vol. 12, no. 1, p. 42, Jan. 2021, doi: 10.3390/info12010042.

[13] M. Osman, “Control logic distribution trade-offs in software-defined wireless networks,” Universitat Politècnica de Catalunya, 2022. doi: 10.5821/dissertation-2117-375585.

[14] V. Tyagi and S. Singh, “Network resource management mechanisms in SDN enabled WSNs: A comprehensive review,” Comput Sci Rev, vol. 49, p. 100569, Aug. 2023, doi: 10.1016/j.cosrev.2023.100569.

[15] P. Krishnan and K. Achuthan, “CloudSDN: Enabling SDN Framework for Security and Threat Analytics in Cloud Networks,” 2019, pp. 151–172. doi: 10.1007/978-3-030-20615-4_12.

[16] M. Ndiaye, G. Hancke, and A. Abu-Mahfouz, “Software Defined Networking for Improved Wireless Sensor Network Management: A Survey,” Sensors, vol. 17, no. 5, p. 1031, May 2017, doi: 10.3390/s17051031.

[17] N. Gupta, M. S. Maashi, S. Tanwar, S. Badotra, M. Aljebreen, and S. Bharany, “A Comparative Study of Software Defined Networking Controllers Using Mininet,” Electronics (Basel), vol. 11, no. 17, p. 2715, Aug. 2022, doi: 10.3390/electronics11172715.

[18] R. R. Fontes, S. Afzal, S. H. B. Brito, M. A. S. Santos, and C. E. Rothenberg, “Mininet-WiFi: Emulating software-defined wireless networks,” in 2015 11th International Conference on Network and Service Management (CNSM), IEEE, Nov. 2015, pp. 384–389. doi: 10.1109/CNSM.2015.7367387.

[19] Ankit Kumar, Bhargavi Goswami, and Peter Augustine, “Experimenting with Resilience and Scalability of Wifi Mininet on Small to Large SDN Networks,” International Journal of Recent Technology and Engineering, vol. 7, no. 6, pp. 201–207, 2019.