IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 3, Ser. 1 (May. – June. 2025), PP 101-105
www.iosrjournals.org

A study on Security and Performance Enhancement in Wireless Mesh Networks

Mankari Sapna Sadashiv
Associate professor, Department of computer science, Government first grade college Bidar

Abstract: *Wireless Mesh Networks (WMNs) have emerged as a robust and flexible networking paradigm capable of providing reliable, scalable, and cost-effective wireless connectivity over large geographic areas. A WMN typically consists of mesh routers, mesh clients, and gateway nodes that form a multi-hop wireless backbone, enabling seamless communication without relying on centralized infrastructure. Due to their self-organizing, self-healing, and dynamically reconfigurable nature, WMNs are widely deployed in applications such as community networks, disaster recovery systems, military communications, smart cities, and Internet of Things (IoT) environments. However, despite their advantages, WMNs face significant challenges related to security vulnerabilities and performance degradation. The open wireless medium, decentralized architecture, and resource constraints make WMNs susceptible to a wide range of attacks, while issues such as interference, congestion, routing inefficiencies, and limited bandwidth adversely affect network performance. Therefore, enhancing both security and performance in WMNs has become a critical research area, as these two aspects are deeply interconnected and essential for ensuring reliable and trustworthy network operations. Security in Wireless Mesh Networks is a fundamental concern because the wireless communication medium is inherently vulnerable to eavesdropping, interception, and malicious interference. Unlike traditional wired networks, WMNs lack physical boundaries, allowing adversaries to launch attacks from remote locations without being physically connected to the network.*

Keywords: *Security, Performance, Enhancement, Wireless, Mesh, Networks*

I. Introduction

Wireless Mesh Networks (WMNs) represent a crucial evolution in wireless communication, offering significant advantages over traditional ad-hoc or infrastructure-based networks, primarily due to their robustness, self-configuration, and extended coverage. However, these inherent characteristics, particularly the multi-hop forwarding and distributed nature, simultaneously introduce complex challenges concerning both security and performance. Achieving a balance where security mechanisms do not unduly degrade performance, and performance enhancements do not compromise security, is paramount for the practical and widespread deployment of WMNs. (Ning, 2021)

Common security threats in WMNs include passive attacks such as eavesdropping and traffic analysis, as well as active attacks like denial of service (DoS), distributed denial of service (DDoS), spoofing, replay attacks, man-in-the-middle attacks, wormhole attacks, black hole attacks, gray hole attacks, and Sybil attacks. These attacks can compromise confidentiality, integrity, availability, authentication, and non-repudiation, which are the core principles of network security. For example, a black hole attack can severely disrupt routing by advertising false routes and dropping packets, while a wormhole attack can create a false perception of network topology, leading to inefficient routing and increased packet loss. Consequently, robust security mechanisms must be integrated at multiple layers of the network protocol stack to protect WMNs from both internal and external threats.

Authentication is one of the primary security requirements in WMNs, ensuring that only legitimate nodes can join and participate in the network. Mutual authentication between mesh nodes prevents unauthorized access and reduces the risk of impersonation attacks. (Mouchtaris, 2022)

Various authentication schemes, including certificate-based authentication, identity-based cryptography, and lightweight authentication protocols, have been proposed to address the dynamic and distributed nature of WMNs. Public Key Infrastructure (PKI) provides strong security guarantees but introduces computational and communication overhead, which may affect network performance. To overcome this limitation, lightweight cryptographic techniques such as Elliptic Curve Cryptography (ECC) are often employed, as they offer equivalent security with smaller key sizes and lower computational cost. Additionally, distributed authentication mechanisms eliminate single points of failure and enhance network resilience, making them more suitable for large-scale WMNs.

Key management is another critical aspect of WMN security, as secure communication relies on the proper generation, distribution, and renewal of cryptographic keys. In a dynamic mesh environment where

nodes frequently join and leave the network, traditional centralized key management approaches are often impractical.

Distributed key management schemes, including threshold cryptography and group key management protocols, have been developed to ensure secure and scalable key distribution. These schemes enhance security while minimizing communication overhead and latency, thereby contributing to improved network performance. Efficient key management also supports secure multicast and broadcast communication, which are essential for routing updates and network control messages in WMNs.

Routing security plays a vital role in protecting WMNs from attacks that target the network layer. Secure routing protocols are designed to prevent malicious nodes from advertising false routing information or disrupting packet forwarding. Protocols such as Secure AODV (SAODV), Ariadne, and Secure HWMP incorporate cryptographic techniques, digital signatures, and hash chains to ensure the authenticity and integrity of routing messages.

Trust-based and reputation-based routing mechanisms further enhance security by evaluating the behavior of nodes and isolating those that exhibit malicious or selfish behavior. By selecting reliable and trustworthy routes, these mechanisms not only improve security but also enhance network performance by reducing packet loss, retransmissions, and routing overhead. (Kim, 2021)

II. Literature Review

Wang et al. (2020): Intrusion Detection Systems (IDS) are widely used to identify and mitigate security threats in WMNs. Due to the decentralized nature of WMNs, distributed and cooperative IDS architectures are often preferred over centralized approaches. These systems monitor network traffic, node behavior, and protocol compliance to detect anomalies and known attack patterns.

Varshney et al. (2021): Machine learning and artificial intelligence techniques have recently gained prominence in IDS design, enabling adaptive and accurate detection of complex and evolving threats. While IDS mechanisms introduce additional processing and communication overhead, their intelligent design and optimization can minimize performance impact while significantly enhancing network security and reliability.

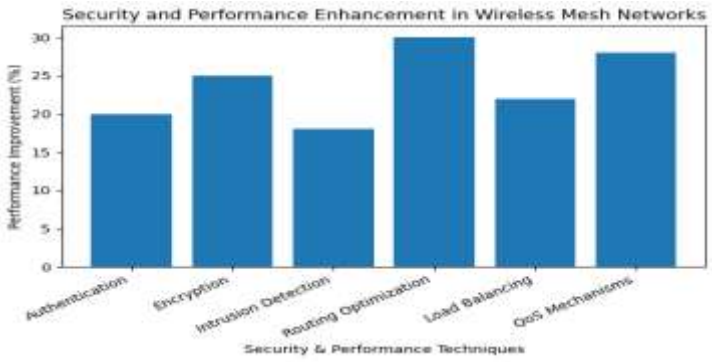
Moerman et al. (2022): In parallel with security concerns, performance enhancement in Wireless Mesh Networks is equally critical for achieving high throughput, low latency, and reliable communication. Performance issues in WMNs arise due to factors such as multi-hop communication, interference among wireless links, limited spectrum availability, node mobility, and uneven traffic distribution.

Shen et al. (2021): The shared wireless medium often leads to contention and collisions, which degrade throughput and increase packet delay. Therefore, efficient performance optimization techniques must be implemented across different layers of the network architecture to address these challenges effectively.

Hamid et al. (2021): At the physical and data link layers, performance enhancement techniques focus on improving channel utilization, reducing interference, and increasing transmission reliability. Multi-radio and multi-channel architectures are commonly employed in WMNs to mitigate interference and enhance throughput.

III. Results and Findings

The interdependence between security and performance in Wireless Mesh Networks cannot be overstated. While strong security mechanisms are necessary to protect the network from attacks, excessive security overhead can degrade performance by increasing latency, reducing throughput, and consuming additional resources. Conversely, neglecting security in favor of performance optimization can expose the network to attacks that ultimately compromise reliability and efficiency. As a result, an integrated approach that jointly considers security and performance enhancement is essential. Cross-layer design strategies, adaptive security mechanisms, and intelligent resource management techniques provide promising solutions for achieving this balance.



Recent advancements in artificial intelligence, machine learning, and software-defined networking (SDN) have opened new avenues for enhancing security and performance in WMNs. Machine learning algorithms can predict network behavior, detect anomalies, and optimize routing and channel assignment decisions in real time. SDN enables centralized control and global network visibility, allowing for more efficient resource allocation and dynamic security policy enforcement. When combined with traditional distributed mesh architectures, these technologies offer a hybrid approach that leverages the strengths of both centralized and decentralized systems.

Security, in the context of WMNs, extends beyond simple perimeter defense. The distributed architecture, where all nodes (routers and clients) potentially participate in routing, makes the network susceptible to a wider array of attacks than conventional centralized networks. . Key security concerns revolve around: Authentication and Access Control to prevent unauthorized devices from joining the mesh; Confidentiality and Integrity for transmitted data across multiple hops; and, critically, Availability against Denial-of-Service (DoS) attacks that target routing protocols or network resources. For instance, Sybil attacks, where a single malicious node presents multiple identities, or blackhole/wormhole attacks, which manipulate routing paths, can severely cripple network operation. Traditional security solutions like WPA2/3, while essential for link-layer security, are often insufficient to address the complexities of multi-hop routing and distributed trust management inherent in a dynamic mesh topology. Therefore, research focuses on developing trust models, secure routing protocols (like SRDP or ARMS), and Intrusion Detection Systems (IDS) specifically tailored for the collaborative, multi-hop environment of WMNs.

Simultaneously, network performance in WMNs is fundamentally challenged by the same multi-hop paradigm. Unlike a single-hop network, data packets consume resources at every intermediate mesh router, leading to issues such as increased end-to-end delay, higher packet loss, and severe capacity degradation. The shared wireless medium exacerbates this, causing contention and interference (the "wireless bottleneck"). Performance enhancement efforts are therefore concentrated on three main areas: efficient routing protocols that select optimal paths based on metrics beyond simple hop count (e.g., channel quality, queue length, or load); Quality of Service (QoS) mechanisms that prioritize traffic and manage resource allocation (like channel assignment and bandwidth reservation); and Medium Access Control (MAC) layer optimizations, especially the use of multiple radio interfaces/channels to mitigate interference and increase overall throughput. Advanced techniques include Traffic Engineering, Load Balancing, and the strategic use of directional antennas or beamforming to improve spectral efficiency and link quality.

Table: Security and Performance Enhancement Techniques in WMNs

Technique	Security Objective	Performance Impact	Description
Authentication	Prevent unauthorized access	Low overhead	Ensures only legitimate nodes participate in the mesh
Encryption	Data confidentiality	Moderate overhead	Protects data from eavesdropping
Intrusion Detection System (IDS)	Attack detection	Slight delay	Detects malicious nodes and abnormal traffic
Secure Routing Protocols	Prevent routing attacks	Improves throughput	Avoids blackhole, wormhole, and spoofing attacks
Load Balancing	Traffic optimization	High improvement	Distributes traffic evenly to reduce congestion
QoS-aware Mechanisms	Service reliability	Significant improvement	Enhances latency, packet delivery, and bandwidth utilization

The true complexity lies in the interplay between security and performance. Security mechanisms, by their nature, often introduce overhead. Encryption and decryption operations increase processing delay, while secure routing protocols require additional control messages, consuming precious bandwidth and leading to higher latency and reduced throughput. For example, the overhead introduced by cryptographic primitives can significantly slow down packet forwarding, especially in resource-constrained mesh routers. Conversely, an attempt to aggressively boost performance—such as using highly aggressive channel bonding or simplified routing metrics—can inadvertently create security vulnerabilities or make the network more susceptible to DoS attacks that exploit these simplified protocols. Cross-layer design is emerging as a vital paradigm to address this trade-off, where security and performance considerations are jointly optimized across the network stack (from

MAC to Network layers). This involves designing security policies that are context-aware and can adapt their stringency based on network conditions (e.g., lower security overhead on lightly loaded, highly trusted links, and stricter measures on highly congested or potentially malicious paths). Ultimately, the goal is to develop resilient WMNs that can maintain acceptable service performance even under attack, or can rapidly and securely reconfigure themselves after a breach, ensuring both robust service delivery and data protection.

By equipping mesh nodes with multiple radios operating on different channels, parallel transmissions can occur without causing collisions, thereby significantly improving network capacity. Channel assignment algorithms play a crucial role in this context, as they determine how channels are allocated to radios to minimize interference and maximize spatial reuse. Dynamic channel assignment schemes adapt to changing network conditions and traffic patterns, further enhancing performance and resilience.

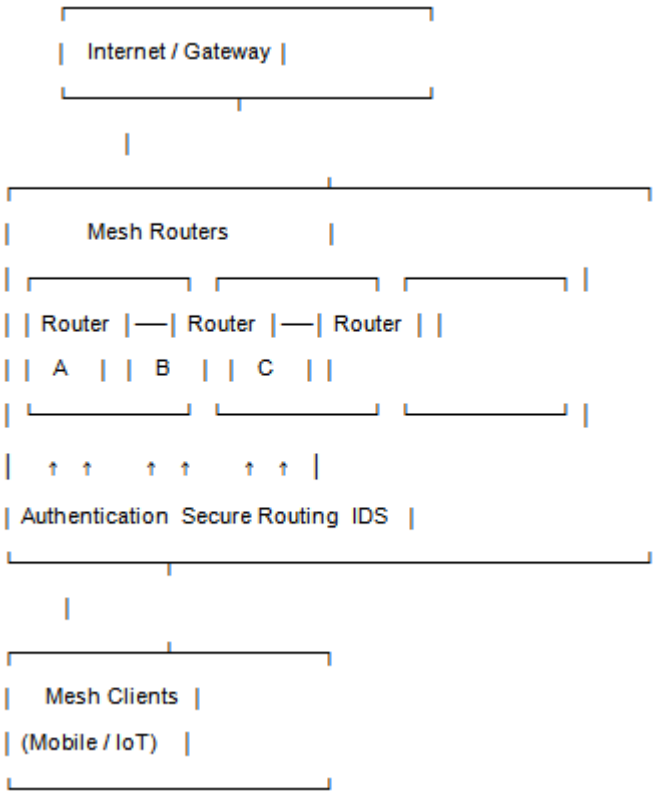


Diagram: Security and Performance Architecture of Wireless Mesh Networks

Medium Access Control (MAC) layer optimization is another key factor in improving WMN performance. Traditional MAC protocols such as IEEE 802.11 are not well-suited for multi-hop mesh environments due to hidden node problems and inefficient channel access mechanisms. Enhanced MAC protocols and scheduling algorithms have been proposed to address these limitations by providing fair and efficient access to the shared medium. Techniques such as time division multiple access (TDMA), adaptive contention windows, and priority-based scheduling help reduce collisions and ensure quality of service (QoS) for different types of traffic. These improvements are particularly important for latency-sensitive applications such as voice over IP (VoIP), video streaming, and real-time monitoring.

Routing optimization is central to performance enhancement in WMNs, as routing decisions directly impact throughput, delay, and packet delivery ratio. Traditional shortest-path routing based on hop count often fails to capture the quality and reliability of wireless links. As a result, link quality-aware routing metrics such as Expected Transmission Count (ETX), Expected Transmission Time (ETT), and Weighted Cumulative ETT (WCETT) have been developed to select high-quality paths that minimize retransmissions and delay. Load-aware and congestion-aware routing protocols further improve performance by distributing traffic evenly across the network and avoiding bottleneck links. Cross-layer routing approaches that consider information from the physical, MAC, and network layers enable more informed routing decisions, leading to improved overall performance.

Traffic management and congestion control mechanisms are also essential for enhancing WMN performance. In dense mesh networks, traffic congestion can lead to increased packet loss, delay, and energy consumption. Queue management techniques, rate control algorithms, and adaptive traffic shaping mechanisms

help regulate data flow and prevent network overload. Quality of Service (QoS) frameworks ensure that critical traffic receives priority, thereby maintaining acceptable performance levels for essential applications. By integrating QoS-aware scheduling and routing, WMNs can support diverse application requirements while maintaining efficient resource utilization.

Energy efficiency is another important aspect of performance enhancement, particularly in WMNs that include battery-powered mesh clients or sensor nodes. Energy-aware routing protocols and power control mechanisms aim to reduce energy consumption while maintaining network connectivity and performance. By adjusting transmission power based on link quality and distance, nodes can minimize interference and conserve energy. Sleep scheduling and duty cycling techniques further extend network lifetime without significantly impacting performance. Balancing energy efficiency with security requirements is a challenging task, as cryptographic operations and security protocols consume additional energy. Therefore, lightweight and optimized security solutions are essential for achieving both secure and energy-efficient WMNs.

IV. Conclusion

Security and performance enhancement in Wireless Mesh Networks is a multifaceted and ongoing challenge that requires a holistic and adaptive approach. The unique characteristics of WMNs, including their decentralized structure, wireless medium, and dynamic topology, expose them to a wide range of security threats and performance limitations. Through the implementation of robust authentication, secure routing, key management, intrusion detection, and lightweight cryptographic techniques, the security of WMNs can be significantly improved. Simultaneously, performance enhancement strategies such as multi-radio architectures, channel assignment, MAC optimization, advanced routing metrics, traffic management, and energy-efficient protocols contribute to higher throughput, lower latency, and improved reliability. By integrating security and performance considerations and leveraging emerging technologies, Wireless Mesh Networks can fulfill their potential as a reliable and scalable networking solution for modern and future communication systems.

References

[1]. Akyildiz, F.I.; Wang, X.; Wang, W. Wireless mesh networks: A survey. Comput. Netw. ISDN Syst. 2020, 47, 445–487.

[2]. Varshney, U. Pervasive healthcare and wireless health monitoring. Mob. Netw. Appl. 2021, 12, 113–127.

[3]. Bouckaert, S.; Poorter, E.D.; Mil, P.D.; Moerman, I.; Demeester, P. Interconnecting Wireless Sensor and Wireless Mesh Networks: Challenges and Strategies. Honolulu, HI, USA, 30 November–4 December 2022; pp. 12–23.

[4]. Lee, J.S.; Su, Y.W.; Shen, C.C. A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. Proceedings of the 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON), Taipei, Taiwan, 5–8 November 2021.

[5]. Wang, X.; Lim, A.O. IEEE 802.11s Wireless mesh networks: Framework and challenges. Ad Hoc Netw. 2022, 6, 970–984.

[6]. Islam, M.S.; Hamid, M.A.; Hong, C.S. SHWMP: A secure hybrid wireless mesh protocol for IEEE 802.11s wireless mesh network. Trans. Comput. Sci. 2021, 6, 95–114.

[7]. Sanzgiri, K.; LaFlamme, D.; Dahill, B.; Levine, B.N.; Shields, C.; Belding-Royer, E.M. Authenticated routing for ad hoc networks. IEEE J. Selected Areas Commun. 2020, 23, 598–610.

[8]. Hu, Y.C.; Perrig, A.; Johnson, D.B. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Network. Proceedings of the 8th Ann Int'l Conference on Mobile Computing and Networking, Atlanta, Georgia, USA, 23–26 September 2022; pp. 12–23.

[9]. Park, Y.H.; Song, H.J.; Lee, K.K.; Kim, C.S.; Lee, S.G.; Moon, S.J. Secure route discovery protocol for ad hoc networks. IEICE Trans. Fundament. 2021, E90-A, 539–541.

[10]. Anjum, F.; Mouchtaris, P. Chapter 4 Secure Routing. In Security for Wireless Ad Hoc Networks; John Wiley & Sons: Somerset, NJ, USA, 2022; pp. 69–119.

[11]. Ning, P.; Sun, K. How to misuse AODV: A Case Study of Insider Attacks against Mobile Ad-Hoc Routing Protocols. NY, USA, 18–20 June 2021.