Wireless Mesh Networks (WMN) in IoT Networks

Salih Saad Qarash [1]

Received: 11.11.2024
Revised: 13.11.2024
Accepted: 4.12.2024

[1] General Electricity Company, Libya, Email: salih.garash@academy.edu.ly

Wireless Mesh Networks (WMN) in IoT Networks

Salih Saad Qarash
General Electricity Company, Libya,
salih.garash@academy.edu.ly

Abstract—The Internet of Things (IoT) is one of the most common applications in both industrial operations and home automation, as well as in the world of network engineering. On the other hand, wireless mesh networks (WMNs) are a networking technology that has been discussed for decades but has not been widely used. They can make a significant difference when it comes to networking in today's IoT world. This paper is a brief introduction to WMNs in IoT networks, mentioning the advantages and disadvantages of using WMNs in IoT networks, and highlighting the main challenges these networks face as Energy Efficiency,Scalability,Bandwidth Constraints, Security.

Keywords — : Internet of Things (IoT), Wireless Mesh Networks (WMNs), sensors.

I. INTRODUCTION

With the substantial growth of the semiconductor industry, creating small devices with strong processing and networking capabilities is no longer a dream for engineers. Currently, the Internet of Things (IoT) has become one of the hottest topics in both industry and academia in the field of wireless communications. Today, most research related to IoT devices focuses primarily on data collection and processing units, i.e., creating new sensors. However, the network that integrates IoT devices with the internet is usually left unchanged using current computer networking solutions such as WLAN or Bluetooth. These computer networks were not designed for low-power devices like remote sensors, even if these devices are considered small computers. [1] The single point of failure nature of these networks makes the entire system highly vulnerable to disasters or even harsh environmental conditions where sensors may need to be deployed in hard-to-reach locations.

Additionally, the capacity of the central hub/router of the network can limit the coverage provided by IoT devices, and the range is also constrained by the same factors. Since most of these remote devices are small and battery-operated, power-hungry networking options such as using cellular networks or satellites are not ideal for most remote IoT scenarios. [2]

A wireless mesh network (WMN) is a communication network composed of radio nodes organized in a mesh topology instead of the star topology used in most networks, according to Akyildiz X. Wang in the book on wireless mesh networks. It's not a new concept at all, originating from multi-hop networks in the 1970s from the Packet Radio Network (PRNET) created by the Defense Advanced Research Projects Agency (DARPA) of the U.S. Department of Defense. Later in the 1990s, many other civilian solutions were proposed and established for various purposes such as extending broadband services. [3] The distributed nature of WMNs with their simple configuration is ideal for application in IoT networks to leverage their extended range as well as keep device design simple using smaller mesh modules. Such networks are also more resilient in harsh environments where the network is distributed without a single central point of failure. Wireless Mesh Networks (WMNs) are increasingly used in Internet of Things (IoT) applications due to their scalability and ability to maintain connectivity across devices. However, they face significant vulnerabilities that can jeopardize their performance and security. Wireless Mesh Networks (WMNs) have become an integral part of Internet of Things (IoT) applications, valued for their scalability and ability to maintain robust connectivity across numerous devices. However, these networks face critical challenges that threaten their performance and security. One significant vulnerability is device security, as many IoT devices connected through WMNs rely on weak or default credentials. This leaves them exposed to cyberattacks, enabling unauthorized access. For example, improperly secured smart home devices, such as surveillance cameras or digital locks, have been exploited in security breaches.

Another challenge is scalability. As the number of nodes in a network increases, interference grows, diminishing the overall efficiency. This issue necessitates optimizing routing protocols to balance network loads effectively while minimizing interference.Additionally, energy constraints pose a significant hurdle. Multi-hop communication, a cornerstone of WMNs, requires nodes to relay data packets, leading to rapid energy depletion, especially in energy-constrained setups like sensor-based networks.Addressing these interconnected issues is crucial for the successful deployment of WMNs in IoT environments. Solutions include enforcing stronger security protocols, implementing advanced routing algorithms to manage scalability, and adopting energy-efficient communication strategies to sustain network performance over time. In this paper, I will discuss all these features of WMNs in detail and why these features make WMNs ideal for IoT networks compared to traditional star networks, as well as discuss how to integrate WMNs into current IoT networks or design an IoT network with this new feature from scratch

https://doi.org/10.20428/jst.v30i1.2572

II. WIRELESS MESH NETWORKS

A. Introduction to Wireless Mesh Networks

The main difference between wireless mesh networks (WMNs) and traditional star networks is that WMNs are wireless networks with the ability to dynamically self-organize and self-configure, creating network connections automatically between nodes in the network, while traditional star networks have a star topology meaning all end nodes are connected to a single central point that connects to the upper layer of the network. Figure 1 illustrates the structure of both networks.

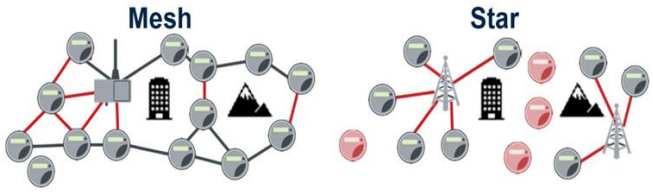

Figure 1: Mesh Networks and Star Networks

Currently, WMNs are adopted in several places mainly in three different forms as follows:

1. Infrastructure/Backbone WMNs

As shown in Figure 2, this type of mesh network involves mesh routers forming infrastructure for clients to connect to. Devices within the coverage area of the mesh router still form a star network, while mesh routers form a network with self-configuring and self-healing links between them. With the gateway function, mesh routers can be connected to the internet. Infrastructure/backbone WMNs are the most used as they are simple and easy to integrate with existing devices by simply installing routers in the mesh networks

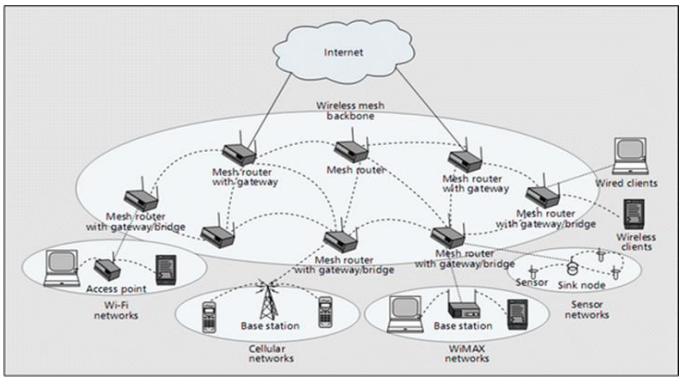

Figure 2: Infrastructure/Backbone WMNs

2. Client WMNs

Client meshing provides peer-to-peer networks between client devices like a large ad hoc network. In this type of architecture, client nodes form the actual network to perform routing and configuration functions as well as provide end-user applications to the clients. Thus, a mesh router is not required for this type of network. Usually, this type of network is not available for internet access. [4]

3. Hybrid WMNs

As shown in Figure 3, hybrid mesh network architecture is a combination of Infrastructure/Backbone WMNs and Client WMNs.

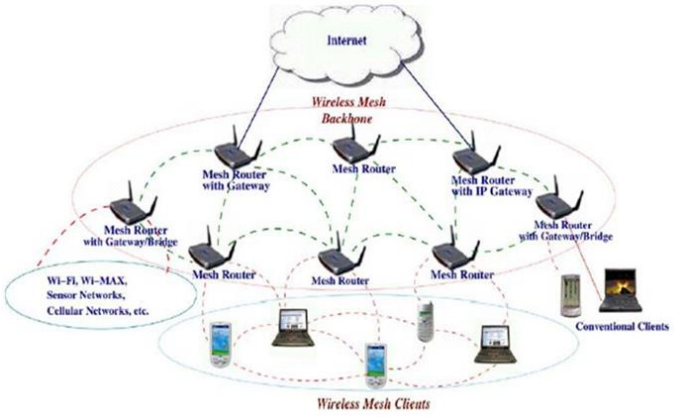

Figure 3: Hybrid WMNs

In hybrid mesh network architecture, mesh clients can access the network through mesh routers as well as directly mesh with other mesh clients. While the infrastructure provides connectivity to other networks such as the internet, routing capabilities for clients enhance connectivity and coverage within the mesh network.

4. Benefits of WMNs in IoT Networks

WMNs can offer numerous advantages to IoT networks, the most notable being network multiplicity. When using the infrastructure mesh network architecture, adding a new router simply requires placing the new device in the field within the range of the existing network. The network range and capacity expand without the need for additional cables and connections. For the hybrid network, this process is even simpler. Placing new IoT devices in the field where the old mesh network covers makes the new sensor work immediately. This is thanks to the self-configuration feature of the network that automatically expands the network. Hence, the network architecture is simpler, and the cost of covering a wider area, especially in rural areas without reliable network coverage everywhere, is significantly lower. [5] Power consumption can also be greatly reduced when connecting remote IoT sensors or other devices

to the network. Devices can connect only to the nearest mesh device rather than a far-off network center, and in the case of the hybrid network, it can be the adjacent node. This can form a chain of IoT devices, reducing the power cost for the network center to cover the farthest device.

*5. **Drawbacks of WMNs in IoT Networks***

Of course, WMNs have some drawbacks. The non-traditional mesh architecture requires support for a new network protocol that must be compatible with the existing network as IoT devices will eventually connect to the internet. Additionally, network repairs when there is a widespread disruption can be more difficult, as it can be challenging to detect disconnections when a large network is fragmented. [6] However, this can be resolved by introducing an error check report into the network packets, but at the cost of a slower network. Finally, delay and network scalability are also affected by the nature of WMNs. As proven by Belding-Royer EM et al. in the famous paper, delay and data rate in the network must also be determined. This may not be an issue in IoT devices, but it should be considered when choosing the right tool for the required task. [7]

III. Applications of WMNs in IoT

A. Home and Personal Networks

Home and personal networks are a great example of how WMNs can make a network more efficient and effective. In a home network scenario, a WMN can be used to ensure that every corner of a large home is covered without needing expensive signal boosters. Every IoT device in the home can easily connect to the network via mesh routers placed around the home. [8]

B. Healthcare and Hospitals

Healthcare and hospital environments are another ideal place for WMNs. Mesh networks can be used to connect medical devices and wireless equipment, ensuring continuous connectivity even if one device fails. These networks can support IoT devices used for patient monitoring, collecting vital data, and transmitting it to doctors in real-time.

C. Smart Cities and Buildings

In smart city and building applications, WMNs can provide reliable and extended connectivity solutions. These networks can be used to connect smart lighting systems, environmental sensors, and security systems, enhancing city management and building infrastructure efficiency.

D. Industry and Smart Factories

Industry and smart factories are environments that can significantly benefit from WMNs. These networks can be used to connect smart machines, sensors, and industrial equipment, enabling real-time data exchange and improving production processes. Mesh networks can enhance operational continuity and reduce unplanned downtimes.

IV. Challenges and Considerations

WMNs face numerous challenges that require innovative and effective solutions to ensure reliable and secure network operation. With advancements in technology and protocols, these challenges can be overcome, and the full benefits of WMNs can be harnessed in IoT environments. Some of these challenges include:

A. Security

- Security risks: WMNs are exposed to a variety of security threats such as man-in-the-middle attacks, Denial of Service (DoS) attacks, and data tampering.
- Data encryption: Securing communications requires strong encryption, which can increase network complexity and resource consumption.

B. Power Management:

- Power consumption: Since many IoT devices are battery-powered, efficient power management is essential to ensure long battery life.
- Efficient protocols: Energy-efficient network protocols are needed to ensure devices remain connected for as long as possible.

C. Bandwidth Constraints:

- Bandwidth distribution: Increasing the number of connected devices requires efficient bandwidth management to ensure performance does not degrade.
- Network congestion: Congestion in the network can lead to data delays and packet loss, affecting the quality of service.

D. Delay and Latency:

- Data transfer delay: The multi-hop nature of the network can increase the delay in data transfer between devices.
- Performance optimization: Routing protocols need to be optimized to ensure minimal delay and latency.

https://doi.org/10.20428/jst.v30i1.2572

E. Scalability:

- Adding new devices: The network must be able to accommodate a large number of new devices without performance degradation.
- Management complexity: As the network grows, managing and monitoring connected devices becomes more complex.

Here is a table summarizing a case study addressing key issues in Wireless Mesh Networks (WMNs). The study explores problems related to security, energy management, bandwidth, latency, and scalability.

Table 1: Challenges and Proposed Solutions

Issue	Details	Results and Proposed Solutions
Security	Vulnerabilities include Denial of Service (DoS), eavesdropping, and man-in-the-middle attacks. Weak encryption and unsecured routing protocols exacerbate risks.[88]	Implement lightweight encryption algorithms and intrusion detection systems to address limited computational capacity in nodes.
Energy Management	Multi-hop communication rapidly depletes node batteries. Nodes serving as intermediaries for packet relay face higher energy consumption.[14]	AI-based adaptive algorithms optimize routing to minimize energy consumption and prolong network lifespan.
Bandwidth	Increased interference in dense networks reduces bandwidth per node. Bandwidth limitations hinder high-speed communication in multimedia or critical IoT applications.	Advanced scheduling and dynamic frequency allocation mitigate interference and improve throughput efficiency.
Latency	Time-sensitive applications face delays due to multi-hop transmission and routing inefficiencies.[15]	AI-driven routing protocols reduce delays by dynamically selecting optimal paths in real time.
Scalability	Larger networks struggle with maintaining stability and throughput as node density increases interference. Hierarchical designs are often suggested.[16]	Introduce hierarchical routing and adjust transmission ranges to minimize node participation in unnecessary transmissions

V. Conclusion

Wireless Mesh Networks (WMNs) offer significant benefits for IoT networks, including scalability, power efficiency, and robust connectivity. However, these networks also face several challenges, including security risks, power management, bandwidth constraints, delay, and scalability issues. Despite these challenges, WMNs have great potential to enhance IoT applications in various fields, such as home networks, healthcare, smart cities, and industry. Future research and development in this field will focus on addressing these challenges and optimizing network performance to fully leverage the capabilities of WMNs in IoT environments.

VI. References

[1] J. Okin, *The Internet Revolution: The Not-for-Dummies Guide to the History, Technology, and Use of the Internet*, 1st ed. Winter Harbor, ME: Ironbound Press, 2005.

[2] P. M. M.-S. and L. E. M. Royer, “An analysis of the optimum node density for ad hoc mobile networks,” 2001.

[3] V. Truong, A. Nayyar, and S. A. Lone, “System performance of wireless sensor network using LoRa–Zigbee hybrid communication,” *Computers, Materials & Continua*, vol. 68, no. 2, pp. 1615–1635, 2021, doi: 10.32604/cmc.2021.016922.

[4] A. M. Khedr, W. Osamy, A. Salim, and A.-A. Salem, "Privacy preserving data mining approach for IoT-based WSN in smart city," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 8, pp. 556–563, 2019, doi: 10.14569/IJACSA.2019.0100873.

[5] V. K. Verma, S. Singh, and N. P. Pathak, "Analytical event-based investigations over Delphi random generator distributions for data dissemination routing protocols in highly dense wireless sensor networks," *Wireless Personal Communications*, vol. 87, no. 4, pp. 1209–1222, Apr. 2016, doi: 10.1007/s11277-015-3049-z.

[6] V. K. Verma, S. Singh, and N. P. Pathak, "Comprehensive event-based estimation of sensor node distribution strategies using classical flooding routing protocol in wireless sensor networks," *Wireless Networks*, vol. 20, no. 8, pp. 2349–2357, Nov. 2014, doi: 10.1007/s11276-014-0739-5.

[7] K. Haseeb, I. U. Din, A. Almogren, and N. Islam, "An energy efficient and secure IoT-based WSN framework: An application to smart agriculture," *Sensors*, vol. 20, no. 7, p. 2081, Apr. 2020, doi: 10.3390/s20072081.

[8] V. K. Verma, K. Ntalianis, S. Singh, and N. P. Pathak, "Data proliferation-based estimations over distribution factor in heterogeneous wireless sensor networks," *Computer Communications*, vol. 124, pp. 111–118, Jun. 2018, doi: 10.1016/j.comcom.2017.09.017.

[9] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," *Phil. Trans. Roy. Soc. London*, vol. A247, pp. 529–551, Apr. 1955.

[10] J. Clerk Maxwell, *A Treatise on Electricity and Magnetism*, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp. 68–73.

[11] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," in *Proc. 9th Annual Conf. Magnetics, Japan*, 1982.

[12] M. Rizwan, "Bluetooth low energy mesh networks: Survey of communication and security protocols," *Sensors*, Jun. 25, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/12/3590.

[13] L. Lei, "Analysis on the scalability issues of wireless mesh networks: Key factors and potential solutions," in *2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9973709.

[14] P. G. Senthilvel, "Enhancing wireless mesh network performance through AI-based routing algorithms," in *2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI)*, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10421320.

[15] X. Wang, "Reducing delay of a wireless mesh network with scalable per-node throughput," in *2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2023.

[16] T. D. R. Thirupurasundari, "Enhancing wireless mesh network performance through AI-based routing algorithms," in *2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI)*, 2023.

https://doi.org/10.20428/jst.v30i1.2572