International Journal on
"Technical and Physical Problems of Engineering"
(IJTPE)
Published by International Organization of IOTPE

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

June 2024 | Issue 59 | Volume 16 | Number 2 | Pages 269-278

EMERGING THREATS IN WSN: A COMPREHENSIVE ANALYSIS OF ROUTING PROTOCOL VULNERABILITIES AND PERFORMANCES RESOURCES IMPACT

A. Toubi A. Hajami

LAVETE Laboratory, Faculty of Science and Technology, Hassan I University, Settat, Morocco
a.toubi@uhp.ac.ma, abdelmajid.hajami@uhp.ac.ma

Abstract- Wireless Sensor Networks (WSNs) have become integral in various applications, ranging from environmental monitoring to defense systems. However, as these networks play increasingly critical roles, their vulnerability to routing protocol attacks has emerged as a significant concern. This paper presents an exhaustive analysis of the vulnerabilities inherent in WSN routing protocols, examining both the security threats and their impact on network performance resources. Through a combination of theoretical analysis and empirical studies, we identify key attack vectors that compromise WSN integrity, including node capture, denial of service, and man-in-the-middle attacks. Furthermore, we evaluate the performance impacts of these security threats, particularly focusing on network lifespan, data transmission efficiency, and energy consumption. Our findings reveal a substantial trade-off between enhancing security measures and maintaining optimal network performance. We propose a series of optimized strategies that aim to fortify WSN against routing protocol attacks while minimizing the adverse effects on network performance. This study not only highlights the urgent need for robust security protocols in WSNs but also provides a framework for developing more resilient and efficient network systems in the face of evolving cybersecurity challenges

Keywords: Wireless Sensor Networks (WSN), Routing Protocol Vulnerabilities, Network Security, Cybersecurity Threats, Performance Impact Analysis, Resource Management, Attack Vectors in WSN, Data Transmission Efficiency, Network Lifespan, Energy Consumption in WSN.

1. INTRODUCTION

Wireless Sensor Networks are characterized by their reliance on distributed sensor nodes, which collaboratively process and transmit data to a central receiver. However, the very nature that makes WSNs efficient and versatile their wireless connectivity and the use of numerous, often unguarded, sensor nodes also render them susceptible to a host of security threats, particularly in their routing protocols. The vulnerabilities in these protocols not only compromise the integrity and confidentiality of data but also have profound implications on the performance and resource efficiency of the network [2].

Recent advancements in cyber-attack methodologies have further accentuated these vulnerabilities, highlighting an urgent need for a comprehensive analysis of routing protocol threats in WSNs. This paper aims to delve into the emerging threats that target the routing protocols in WSNs, critically examining their nature, the underlying causes, and the potential impact on network performance and resource allocation. Through this analysis, we seek to bridge the gap in current research by not only identifying the vulnerabilities but also by assessing the resultant degradation in network efficiency and the strain on limited resources, which are quintessential for the sustainability of WSNs.

To achieve a holistic understanding, this paper first outlines the fundamental architecture of WSNs, emphasizing the role and structure of routing protocols. Subsequently, it categorizes the known and emerging threats, detailing their mechanisms and the specific aspects of routing protocols they exploit. In doing so, the paper sheds light on the multifaceted impact of these vulnerabilities, extending beyond mere data security to encompass performance metrics such as network lifespan, energy consumption [1], and data transmission efficiency. Lastly, the paper endeavors to not only map the landscape of threats but also to evaluate the current countermeasures, thereby identifying gaps in existing security protocols and suggesting avenues for future research and development. Through this comprehensive analysis, this study aims to contribute significantly to the field of WSN security, providing a foundation for the development of more robust, efficient, and resilient routing protocols in face of evolving cyber threats.

2. WSN ARCHITECTURE AND DATA TRANSMISSION

The primary purpose of WSNs is to collect data from the environment and transmit it for analysis, enabling decision-making in various applications [3, 4].

- Applications of Wireless Sensor Networks: Environmental Monitoring: WSNs play a crucial role in environmental data collection, including monitoring

Registered: 230903 | Article Info: 1806 | Accepted: 240522
Reserved: 240112 | Available: 240630

weather conditions, pollution levels, and wildlife activities. They provide real-time data, which is essential for environmental protection and research.

- Healthcare: In healthcare, WSNs are used for patient monitoring and management. Sensors can track patients' vital signs, movements, and even assist in early detection of health issues. They contribute significantly to elderly care and remote health monitoring.
- Military: The military uses WSNs for surveillance, tracking, and security purposes. Sensors can detect enemy movements, monitor secure areas, and assist in reconnaissance missions, providing a technological edge in military operations.
- Smart Cities: In urban areas, WSNs facilitate the creation of smart cities. They manage traffic flow, monitor urban environments, and support energy conservation measures, contributing to more efficient and sustainable urban living.
- Agriculture: WSNs aid in precision agriculture by monitoring soil moisture, crop growth, and environmental conditions. This data helps in efficient water usage, pest control, and yield improvement.
- Industrial Applications: In industries, WSNs are used for monitoring machinery, supply chains, and factory conditions. They assist in predictive maintenance, ensuring safety, and enhancing efficiency [5].

2.1. Components of WSN

In this paragraph we detail the key components of Wireless Sensor Networks (WSNs) and discuss their roles and functionalities. This will provide a comprehensive understanding of how these networks operate.

2.1.1. Sensor Nodes

– Data Collection: These nodes sense physical parameters like temperature, humidity, pressure, motion, or pollutants, depending on their design and purpose.

– Data Processing: Besides sensing, they have the capability to process data and make basic decisions.

– Energy Efficiency: Given their often-limited power supply (usually batteries), they are designed for low energy consumption.

2.1.2. Base Station (or Sink)

➢ Network Coordinator: The base station [5, 6] more powerful in terms of energy, processing, and communication capabilities compared to sensor nodes.

➢ Data Collection Hub: Sensor nodes transmit the data they collect to the base station and performs more substantial data processing or analysis.

➢ Gateway Function: It serves as a gateway between the sensor nodes and the end-users. It can be connected to an external network like the internet, allowing for remote access and control.

➢ Management Role: The base station can manage the network, controlling tasks such as node activation, data querying, and setting parameters for data collection.

➢ Connectivity: This component encompasses the methods and protocols used for data transmission within the WSN.

➢ Wireless Communication: Communication usually occurs wirelessly, using technologies such as Bluetooth, ZigBee, or Wi-Fi, depending on the range and power requirements.

➢ Protocols: Effective communication protocols are crucial for ensuring data integrity, managing power consumption, and optimizing the use of the wireless medium.

➢ Network Topology: The communication network can be structured in various topologies like star, mesh, or tree, each with its own advantages and suitability for different applications [5, 6].

2.2. Methods and Protocols for Data Transmission

Communication in Wireless Sensor Networks (WSNs) is a crucial aspect, as it determines how effectively the network can collect, transmit, and process data. Let's explore the methods and protocols used for data transmission in WSNs [7]. Radio Frequency (RF) Most common method, using frequencies like 2.4 GHz for data transmission. Technologies such as ZigBee, Bluetooth, and Wi-Fi often operate on this principle. Optical Communication Involves using light (like infrared) for communication. Less common and usually limited by line-of-sight requirements. ZigBee is popular for its low power consumption and reliability. Ideal for transmitting small amounts of data over a moderate range. Bluetooth Low Energy (BLE) Used for short-range communication. It is energy efficient, making it suitable for small sensor nodes. 6LoWPAN Enables efficient communication over IP networks, making it easier to connect WSNs with the internet.

2.1.2. Communication within WSNs

❖ Ad-Hoc Networking: Nodes often form an ad-hoc network, communicating with each other directly or through intermediate nodes.

Protocols like LEACH (Low-Energy Adaptive Clustering Hierarchy) or Directed Diffusion are used for efficient data transmission between nodes.

❖ Mesh Networking: In some WSNs, a mesh network is formed where each node can communicate with multiple other nodes, enhancing network reliability and range.

❖ Sensor Node-to-Base Station Communication:

- Direct Communication: In smaller networks, sensor nodes can directly transmit their data to the base station.
- Multi-Hop Communication: In larger networks, data may pass through several sensor nodes and route to the base station, helping to conserve energy and broaden the network's coverage. Data Aggregation: Intermediate nodes have the capability to compile data from various sensors and then send it to the base station, which minimizes the data transmission volume and conserves energy.

❖ Energy-Efficient Communication:

Duty Cycling Nodes switch between active and sleep modes to conserve energy. Data Compression Reducing the size of the data packet for transmission to save energy [11].

3. ROUTING PROTOCOL VULNERABILITIES IN WSN

3.1. Importance of Routing Protocols in WSNs

Understanding their importance involves recognizing what they are and how they significantly impact the functionality and effectiveness of WSNs. Routing protocols in WSNs are rules or algorithms that dictate how data is forwarded from sensor nodes to the base station. Unlike traditional networks, routing in WSNs faces unique challenges due to factors like limited energy resources, node mobility, and variable network topology. They ensure data is transmitted in the most efficient way possible, conserving energy and maximizing network lifespan. Routing protocols help in organizing how nodes communicate, often determining network topology (like tree, star, or mesh). They enhance network reliability by finding new paths when the usual route is unavailable (due to node failure, for example). routing protocols can adapt to changes in network size, maintaining performance as the network grows or shrinks.

The most critical criterion. Since sensor nodes have limited power, protocols must minimize energy consumption, extending the network's operational lifetime. Techniques like data aggregation and avoiding redundant data transmissions are key strategies. Protocols must accommodate varying network sizes - from a few nodes to thousands. They should maintain efficiency and performance regardless of network scale. Ensure consistent and accurate data transmission, even in the presence of node or link failures. Mechanisms to detect and recover from failures are essential. Important in time-sensitive applications. Protocols should facilitate timely data delivery. Balance between latency and energy consumption is often required. Even distribution of workload among nodes to prevent early exhaustion of any single node. They help in prolonging the overall network lifespan. Ability to adapt to changes in network conditions, such as node mobility or varying environmental factors.

3.2. Types of Routing Protocols

Routing protocols in WSN can be categorized based on their network structure and operational principles. Let's explore three primary types: Flat, Hierarchical, and Location-Based Protocols, discussing their strengths and weaknesses.

3.2.1. Flat Routing Protocols

- Examples: Directed Diffusion, SPIN for Sensor Protocols for Information via Negotiation.

3.2.1.1. Strengths

- Simplicity: They are generally simpler to implement and manage.
- Uniform Energy Usage: Each node typically has the same role, leading to uniform energy consumption across the network. Suitable for Small Networks, flat protocols are often well-suited for smaller networks with less complexity.

3.2.1.2. Weaknesses

- Scalability Issues: They don't scale well to larger networks due to increased data transmission overhead and management complexity.
- Energy Inefficiency in Large Networks: In larger deployments, nodes may deplete their energy quickly due to constant participation in data routing.

3.2.2. Hierarchical Routing Protocols

- Examples: LEACH for Low Energy Adaptive Clustering Hierarchy and PEGASIS for Power-Efficient Gathering in Sensor Information Systems.

3.2.2.1. Strengths

- Energy Efficiency: By organizing nodes into clusters, they reduce the number of transmissions required.
- Scalability: Better suited for larger networks due to the cluster-based approach.
- Extended Network Lifetime: Hierarchical structures tend to balance the energy consumption across the network, extending the overall network lifetime.

3.2.2.2. Weaknesses

- Cluster Formation Overhead: Forming and maintaining clusters can introduce additional overhead.
- Cluster Head Energy Depletion: Cluster heads can deplete their energy faster due to the extra burden of data aggregation and communication with the base station.

3.2.3. Location-Based Routing Protocols

- Examples: GEAR for Geographical and Energy Aware Routing. GPSR for Greedy Perimeter Stateless Routing.

3.2.3.1. Strengths

- Reduced Overhead: By using location information, they can reduce the routing overhead, as decisions are made based on the destination's location.
- Energy Efficiency: They often lead to more energy-efficient routes since data is forwarded in the direction of the destination.
- Effectiveness in Mobility Scenarios: Particularly useful in networks where sensor node mobility is a factor.

3.2.3.2. Weaknesses

- Dependency on Location Information: Their effectiveness is heavily reliant on accurate location information, which requires additional hardware (like GPS). Increased Hardware Cost:
- The need for GPS or other localization mechanisms can increase the cost and energy consumption of nodes.

3.3. WSNs Common Vulnerabilities in Routing Protocols

Wireless Sensor Networks are vulnerable to a range of security risks, especially in terms of their routing protocols, Wireless Sensor Networks are prone to security threats. Recognizing these weaknesses is essential for maintaining the networks' security and dependability. Let's delve into some typical vulnerabilities and the ways attackers might exploit them.

3.3.1. Sybil Attacks

• Explanation: During a Sybil attack, a harmful node falsely assumes multiple identities or pretends to have fake identities. This can disrupt various network functions, including routing, resource allocation, and reputation systems.

• Exploitation: Attackers can use these multiple identities to create an illusion of high traffic density in certain parts of the network, influencing routing decisions. It can also undermine trust mechanisms in the network by skewing voting or reputation systems.

3.3.2. Wormhole Attacks

• Explanation: This attack involves an attacker receiving packets at one point in the network and tunneling them to another point. This tunnel between two colluding attackers is the "wormhole."

• Exploitation: Attackers can use wormholes to reroute network traffic through the wormhole, eavesdropping on the data or selectively dropping packets to disrupt the network. It can also be used to create a false scenario of shortest path routes, misleading the network's routing protocols.

3.3.3. Sinkhole Attacks

• Explanation: In a sinkhole attack, a compromised node attracts all or a disproportionate amount of network traffic to itself. This is often achieved by the attacking node presenting itself as the most attractive or efficient route.

• Exploitation: Once the traffic is attracted to the sinkhole, the attacker can perform selective forwarding or data dropping, leading to a loss of important information. The attacker might also use the sinkhole to launch further attacks, like modifying the data or performing a Sybil attack.

3.3.4. Blackhole Attacks

• Explanation: Similar to sinkhole attacks, in blackhole attacks, the malicious node falsely advertises good routes to the base station. Once the traffic is routed through this node, it simply drops all the packets.

• Exploitation: This attack can lead to significant data loss as packets are never delivered to their intended destination. It disrupts the network's data flow and can be particularly damaging if critical, real-time data is lost.

3.4. Impact of Vulnerabilities on WSN Performance

In the next section we will Analyze how these vulnerabilities affect network performance, including data integrity, network lifespan, and energy consumption. Providing a scenario that illustrating the impact of attacks already cited. To create a scenario of an attack on a Wireless Sensor Network (WSN) routing protocol with Sybil, Wormhole, Sinkhole, and Blackhole attacks, we need to simulate the behavior of 150 nodes over a duration of one hour. The simulation will track and record metrics like latency, throughput, energy consumption, and Quality of Service (QoS) of transmission nodes. Here's a conceptual framework for how this simulation could be structured.

3.4.1 Simulation Environment

Network Topology: 150 nodes distributed in a simulated area (Figure 1), possibly with varying densities to mimic real-world conditions. In this paper, we'll simulate the DDOS attack with different routing protocols and study the variation in metrics for each protocol. The connections between nodes depend on their proximity to each other, simulating a realistic network topology.

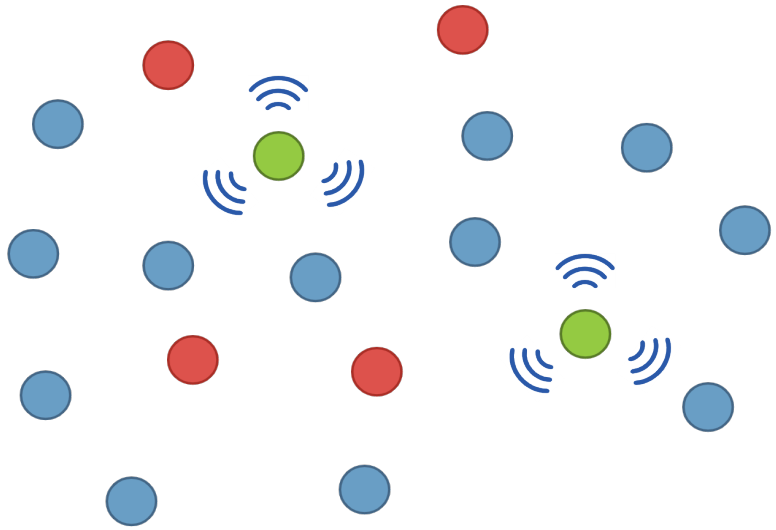

Figure 1. Representing an example of wireless sensor (WS) nodes in a DDoS attack context

• Blue Nodes are a normal node (70% of total).
• Red Nodes are a suspicious node (20% of total).
• Green Nodes: BTS nodes (the remaining 10%).

❖ Metrics to Measure:

- Latency: Time taken for a packet to travel from source to destination.
- Throughput: Total successful messages delivered over a channel in a given period.

- Energy Consumption: Energy used by nodes during communication, idle, and attack scenarios.
- Quality of Service (QoS): This could include packet delivery ratio, network stability, etc.

For simulation we use several tools like Python, NetworkX, NumPy, Matplotlib to simulating and analyzing network behaviors, particularly in scenarios like a DDoS attack on a wireless sensor network. The Python environment offers a flexible and powerful platform for such computational tasks, making it a popular choice in both academic and professional settings for network analysis, data visualization, and simulation studies.

4. SIMULATION RESULTS

We'll start by analyzing the impact of DDOS attacks on network performance, using the SPIN protocol [Figure 2].

- Blue Nodes are a normal node.
- Red Nodes are a suspicious Malicious nodes initiating the DDoS attack.
- Green Nodes: BTS nodes.
- Yellow Nodes: Nodes under attack, receiving an excessive number of requests or data.

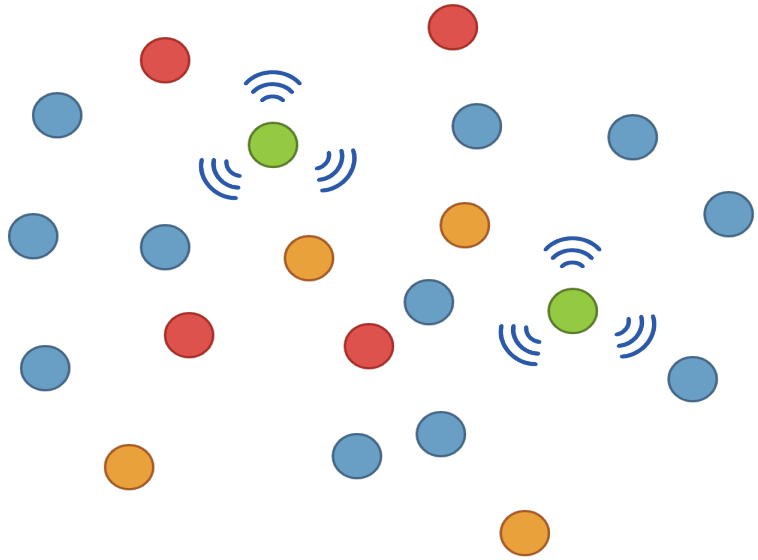

Figure 2. An example of DDOS Attacks with SPN Protocol

To analyze the impact of a DDoS attack on throughput and energy consumption in a wireless sensor network using the SPIN protocol, we'll need to consider several factors and make some assumptions for the simulation. Here's how we can approach it:

- Throughput: Normally, throughput is measured as the rate of successful message delivery over a communication channel. In a DDoS scenario, the throughput is expected to decrease as the network becomes congested with fake or excessive requests.
- Energy Consumption: Sensor nodes consume energy for three main tasks: sensing, communication, and data processing. In a DDoS attack scenario, the increased communication (especially receiving and transmitting) significantly increases energy consumption as Figure 3.

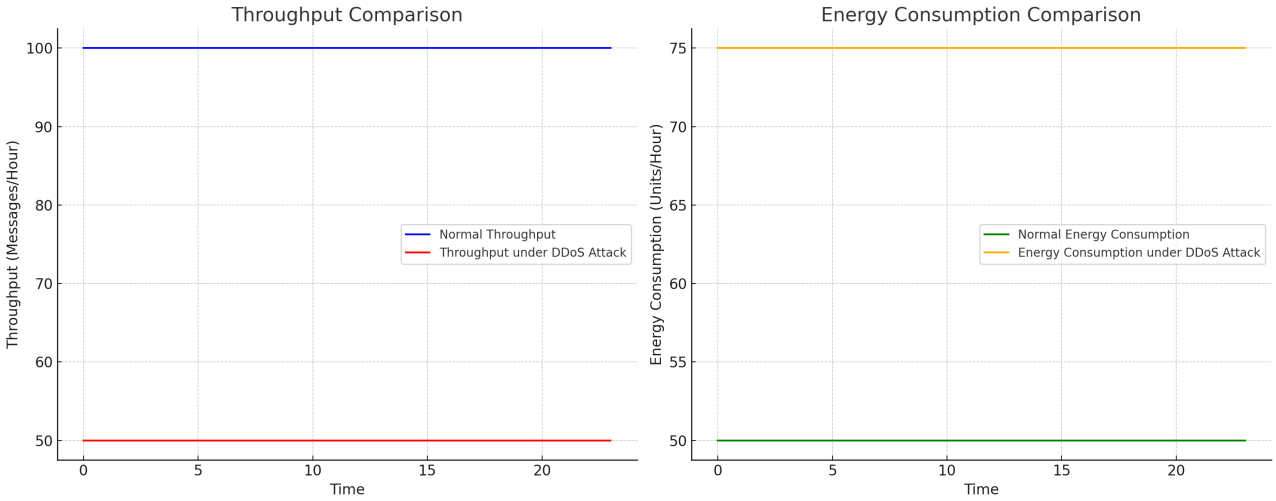

Figure 3. The impact of a SPN Protocol DDoS attack on throughput and energy consumption

Throughput Comparison:
Blue Line (Normal Throughput): Represents a steady state of message delivery, assumed as 100 messages per hour.
Red Line (Throughput under DDoS Attack): Shows a significant decrease to 50 messages per hour, representing a 50% drop. This is due to network congestion caused by the DDoS attack, which leads to a reduced rate of successful message delivery.

➢ Energy Consumption Comparison:
- Green Line (Normal Energy Consumption): Indicates a constant rate of energy consumption, assumed as 50 units per hour.
- Orange Line (Energy Consumption under DDoS Attack): Displays a 50% increase to 75 units per hour.

The rise in energy consumption is attributed to the additional processing and communication load on the nodes due to the excessive and often fake traffic generated by the DDoS attack.

The DDoS attack severely affects the network's capacity to transmit legitimate data. The halving of throughput indicates a significant degradation in network performance. The increased energy demand during the attack can drain the limited energy resources of sensor nodes, potentially leading to earlier-than-expected network failures or reduced operational lifespan.

Simulating a DDoS attack on a network of 150 wireless sensor (WS) nodes using the LEACH protocol (Figure 4) involves a more complex setup compared to the SPIN protocol, due to the hierarchical nature of LEACH. In LEACH, nodes form local clusters, each with a designated node serving as the cluster head (CH) for its respective cluster.

- Blue Nodes: Normal nodes.
- Red Nodes: Malicious nodes initiating the DDoS attack.
- Green Nodes: Cluster Heads (CHs).

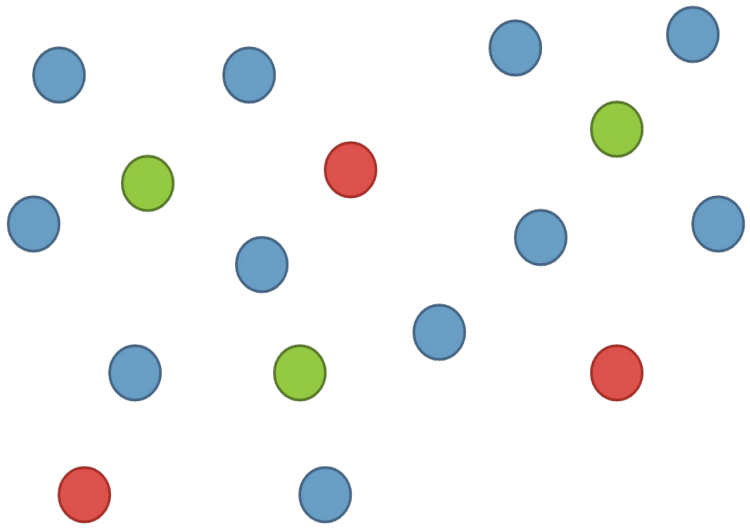

Figure 4. DDOS Attacks with LEACH Protocol

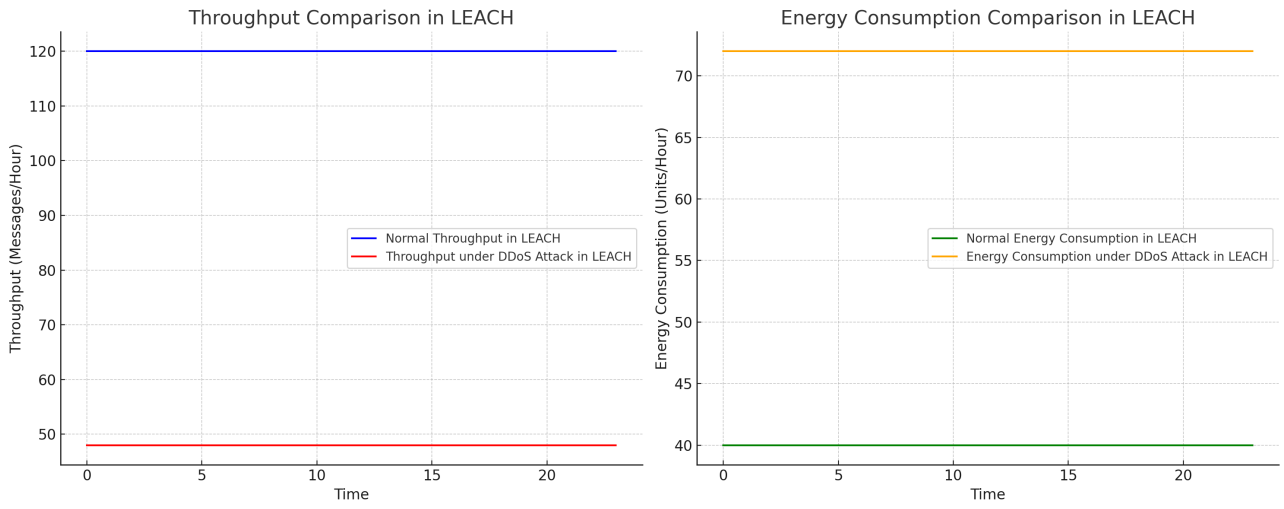

Figure 5. The impact of a LEACH DDoS attack on throughput and energy consumption

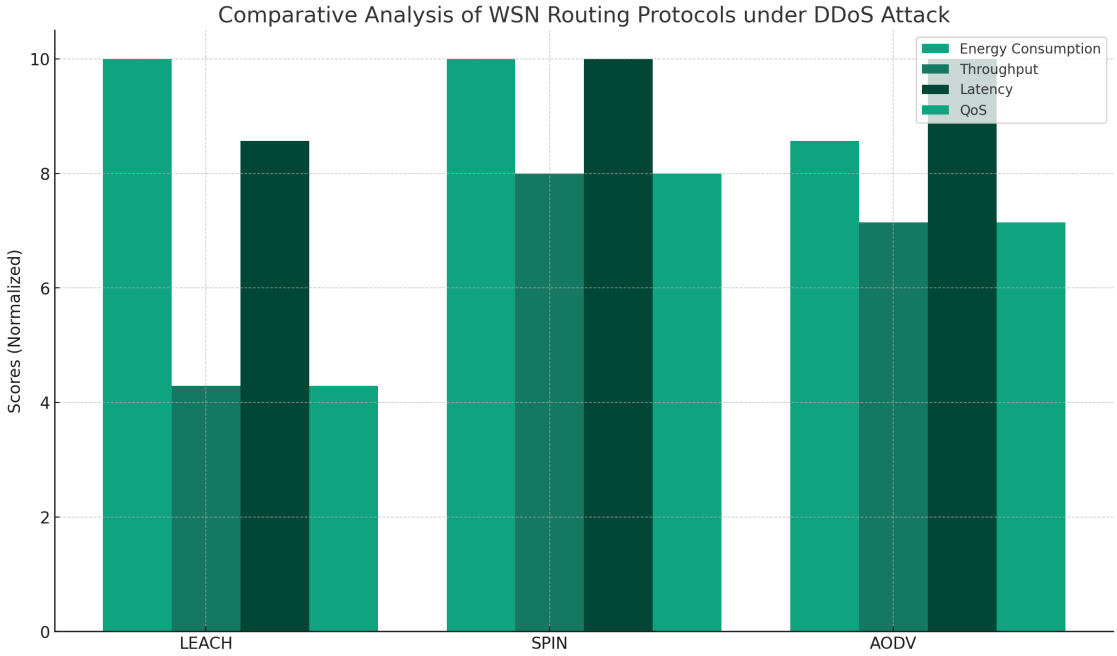

Figure 6. WSN routing protocol comparative analysis

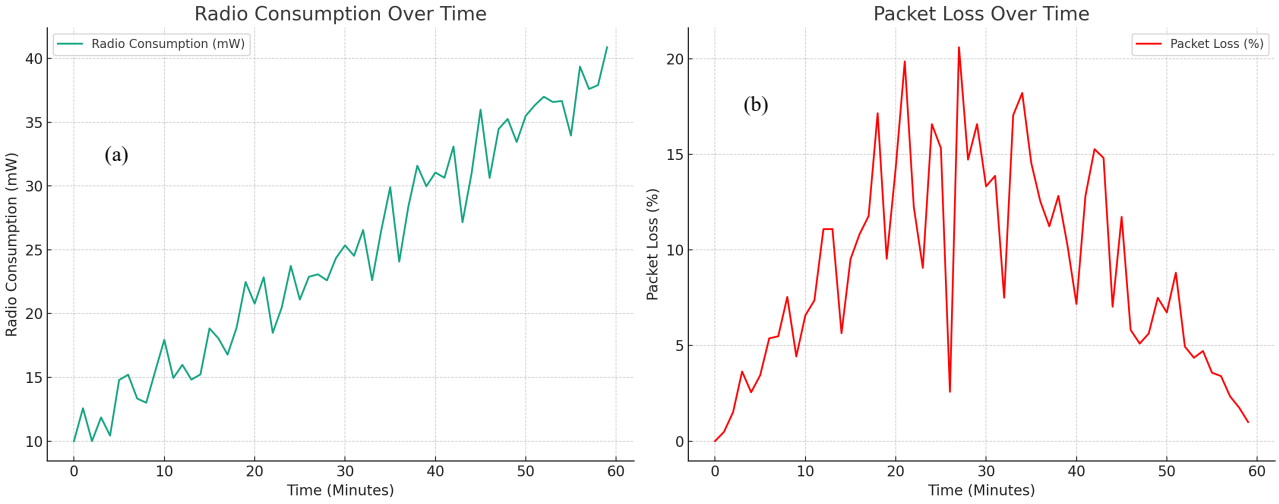

Figure 7. Radio consumption and packet loss during DDOS attack simulation

The simulated graphs [Figure 5] show the impact of a DDoS attack on throughput and energy consumption using the LEACH protocol:

➢ Throughput Comparison in LEACH:

Blue Line (Normal Throughput in LEACH): Represents a steady state of higher throughput, assumed to be 120 messages per hour, benefitting from data aggregation at Cluster Heads (CHs).

Red Line (Throughput under DDoS Attack in LEACH): Shows a significant decrease to about 48 messages per hour (60% decrease). This decrease is due to the disruption of data aggregation at CHs and possible presence of fake CHs in the DDoS scenario.

➢ Energy Consumption Comparison in LEACH:

- Green Line (Normal Energy Consumption in LEACH): Indicates a constant and lower rate of energy consumption, assumed as 40 units per hour, due to the efficient rotation of CHs.

- Orange Line (Energy Consumption under DDoS Attack in LEACH): Displays a substantial increase to about 72 units per hour (80% increase). The rise in energy consumption is due to the additional load on CHs and the network overall, as they deal with excessive and often malicious data traffic.

- Throughput Impact: The DDoS attack severely hampers the network's throughput, more drastically in LEACH due to the disruption of the CH mechanism, which is critical for efficient data transmission.

- Energy Consumption Impact: The increased energy demand during the attack is particularly concerning in LEACH, as the protocol aims to conserve energy through CH rotation. The attack leads to quicker depletion of energy resources in sensor nodes, potentially causing premature network failure.

This simulation highlights the vulnerability of hierarchical WSNs like those using LEACH to DDoS attacks. The attack's impact is significant, affecting both the network's ability to transmit data efficiently and its overall energy sustainability. The graph (Figure 6) provides a comparative analysis of different Wireless Sensor Network (WSN) routing protocols under the impact of a DDoS attack, focusing on four key metrics: energy consumption, throughput, latency, and Quality of Service (QoS), represented by the Packet Delivery Ratio (PDR).

- LEACH: While LEACH is efficient in normal conditions, its performance under DDoS attack is significantly impacted, especially in terms of energy consumption and QoS.
- SPIN: Shows moderate resilience to DDoS attacks across all metrics, balancing energy consumption with throughput and latency.
- AODV: Exhibits relative strength in maintaining throughput and QoS under attack, but at the cost of increased energy consumption and latency.

This comparative analysis highlights how different WSN routing protocols can be variably impacted by DDoS attacks.

4.1. Radio Consumption Over Time

Graph (Figure 7a) shows the radio consumption in milliwatts (mW) over the course of 60 minutes. You can observe an increasing trend, which could represent the heightened activity during a DDoS attack, followed by a stabilization as the network adjusts or the attack subsides.

➢ Observations

- Initial Stable Consumption: The graph starts with a relatively stable radio consumption. This likely represents the normal operating conditions of the network.
- Gradual Increase: There is a noticeable increase in consumption over time. This could be due to the escalation of the DDoS attack, where nodes are increasingly engaged in transmitting, receiving, or processing data packets.
- Plateau Phase: Towards the end, the consumption plateaus. This might indicate that the network has reached a saturated state of energy consumption, possibly because nodes are constantly active due to the attack.

➢ Implications

- Energy Efficiency Concerns: The increasing trend in energy consumption suggests that the network is under stress. This is critical in scenarios where nodes are energy-constrained, like in wireless sensor networks.
- Network Sustainability: The plateau might indicate a limit to how much additional load the network can handle. If the attack were to intensify further, it could lead to node failures due to energy depletion.

4.2. Packet Loss Over Time

Graph (Figure 7b) illustrates the packet loss percentage over the same period. It starts low, peaks (possibly during the peak of the attack), and then decreases, possibly due to adaptive mechanisms in the network or the end of the attack.

➢ Observations

- Initial Low Packet Loss: The low packet loss at the beginning suggests that the network is initially handling communications efficiently.
- Peak in Packet Loss: The peak represents the worst period of the DDoS attack. High packet loss implies that a significant portion of the data is not reaching its intended destination.
- Subsequent Decrease: The decrease after the peak might suggest that the network is adapting to the attack, possibly through some inherent resilience mechanisms, or that the intensity of the attack is decreasing.

➢ Implications

- Network Performance Degradation: High packet loss is indicative of poor network performance. During the peak period, the network is likely struggling to maintain effective communication.
- Potential Adaptive Responses: The decrease in packet loss could suggest that the network has mechanisms to adapt to such attacks, or it could also mean that the attack has become less intense.

6. CONCLUSIONS

Wireless Sensor Networks (WSNs) are increasingly pivotal in various sectors, including environmental monitoring, healthcare, military, and industrial processes. However, the rising dependence on these networks also escalates their vulnerability to various emerging threats, particularly cyber-attacks like Distributed Denial of Service (DDoS). This analysis aimed to underscore the vulnerabilities of different WSN routing protocols – LEACH, SPIN, and AODV – and their performance impact under DDoS attack conditions, focusing on critical metrics such as energy consumption, throughput, latency, and Quality of Service (QoS).

Each protocol exhibits unique weaknesses under DDoS conditions. LEACH, with its clustering mechanism, showed significant energy consumption and a decrease in QoS, indicating its vulnerability to attacks targeting cluster heads. SPIN, being data-centric, maintained moderate performance across metrics but was not immune to the deleterious effects of increased traffic. AODV, while maintaining better throughput and QoS, suffered in terms of energy efficiency and latency.

A critical factor for WSNs, given their often-limited power resources. The analysis revealed that DDoS attacks could exacerbate energy depletion, with LEACH being the most affected. This highlights the need for energy-efficient routing protocols coupled with robust security measures.
Throughput drastically reduced in all protocols under attack, with LEACH being the most impacted. Latency, an essential factor for real-time applications, was adversely affected, especially in AODV, suggesting that attack-resilient routing mechanisms are crucial for maintaining operational efficiency.

Measured via Packet Delivery Ratio (PDR), was notably compromised in DDoS scenarios. LEACH's performance was significantly hindered, while AODV showed relative resilience, indicating the importance of QoS considerations in protocol design, especially for

critical applications. The analysis underlines the imperative for integrating advanced security features into WSN routing protocols. Strategies such as intrusion detection systems, secure clustering algorithms, and authentication mechanisms should be explored and integrated.

- Energy Efficiency: Given the severe impact of DDoS attacks on energy resources, future protocol designs must balance energy efficiency with security. Techniques such as energy-aware routing, efficient cluster head rotation, and sleep/wake scheduling could be crucial.
- Adaptability and Scalability: Protocols should be adaptable to varying network conditions and scalable to handle the expanding size and complexity of modern WSNs.
- Cross-Layer Designs: There's potential in exploring cross-layer designs that integrate routing, MAC, and physical layer strategies to enhance overall network resilience and efficiency.

This comprehensive analysis delineates that while WSNs are potent tools, their efficacy and sustainability are heavily contingent on the resilience and efficiency of their routing protocols. As emerging threats, particularly cyber-attacks, evolve in sophistication, so must the strategies to mitigate them. The future of WSNs lies in a holistic approach that synergizes energy efficiency, robust security, and adaptive performance, ensuring that these networks can withstand and thrive in the face of evolving cyber threats.

NOMENCLATURES

1. Acronyms

QoS	Quality of Service
PDR	Packet Delivery Ratio
CH	Cluster Head
IoT	Internet of Things

ACKNOWLEDGEMENTS

The authors wish to thank the LAVET Committee Laboratory, Faculty of Science and Technology, Hassan I University, Settat, Morocco for support.

REFERENCES

[1] Z. Mottaghinia, A. Ghaffari, "Fuzzy Logic-Based Distance and Energy-Aware Routing Protocol in Delay-Tolerant Mobile Sensor Networks", Wirel. Pers., Vol. 100, pp. 957-976, January 2018.

[2] J. Lorincz, N. Ukic, D. Begusic, "Throughput Comparison of AODV-UU and DSR-UU Protocol Implementations in Multi-Hop Static Environments", The 9th International Conference on Telecommunications, IEEE, pp. 195-202, June 2007.

[3] L. Qing, Q. Zhu, M. Wang, "Design of a Distributed Energy-Efficient Clustering Algorithm for Heterogeneous Wireless Sensor Networks", Vol. 29, pp. 2230-2237, August 2006.

[4] S.J. Jazebi, A. Ghaffari, "Risa: Routing Scheme for Internet of Things Using Shuffled Frog Leaping Optimization Algorithm", Vol. 11, pp. 4273-4283, January 2020.

[5] W. Ke, O. Yangrui, J. Hong, Z. Heli, L. Xi, "Energy Aware Hierarchical Cluster-Based Routing Protocol for WSNS", J. China Univ. Post Telecommun., Vol. 23, pp. 46-52, April 2016.

[6] G.S. Kumar, P.M. Vinu, K.P. Jacob, "Mobility Metric-Based Leach-Mobile Protocol", 16th International Conference on Advanced Computing and Communications, IEEE, pp. 248-253, January 2008.

[7] Z. Liao, J. Wang, S. Zhang, J. Cao, G. Min, "Minimizing Movement for Target Coverage and Network Connectivity in Mobile Sensor Networks", IEEE Trans. Parallel Distrib. Syst., Vol. 26, pp. 1971-1983, July 2015.

[8] P.G.V. Naranjo, M. Shojafar, H. Mostafaei, Z. Pooranian, E. Baccarelli, "P-Sep: A Prolong Stable Election Routing Algorithm for Energy-Limited Heterogeneous Fog-Supported Wireless Sensor Networks", J. Supercomput, Vol. 73, pp. 733-755, June 2017.

[9] T. Hintsch, S. Irnich, "Large Multiple Neighborhood Search for the Clustered Vehicle Routing Problem", Eur. J. Oper. Res., Vol. 270, pp. 118-131, October 2018.

[10] M.R. Mundada, V. CyrilRaj, T. Bhuvaneswari, "Energy Aware Multi-Hop Multi-Path Hierarchical (EAMMH) Routing Protocol for Wireless Sensor Networks", Eur. J. Sci. Res. Vol. 88, pp. 520-530, October 2012.

[11] N.K. Nehra, M. Kumar, R. Patel, "Neural Network Based Energy Efficient Clustering and Routing in Wireless Sensor Networks", First International Conference on Networks and Communications, IEEE, pp. 34-39, December 2009.

[12] H. Junping, J. Yuhui, D. Liang, "A Time-Based Cluster-Head Selection Algorithm for Leach", The 2008 IEEE Symposium on Computers and Communications, IEEE, pp. 1172-1176, July 2008.

[13] D.S. Kim, Y.J. Chung, "Self-Organization Routing Protocol Supporting Mobile Nodes for Wireless Sensor Network", The First International Multi-Symposiums on Computer and Computational Sciences (IMSCCS'06), IEEE, pp. 622-626, June 2006.

[14] E. Mohsenifard, A. Ghaffari, "Data Aggregation Tree Structure in Wireless Sensor Networks Using Cuckoo Optimization Algorithm", Inf. Syst. Telecommun. Vol. 4 pp. 182-190, October 2016.

[15] Y. Haddi, A. Kharchaf, A. Moumen, "Study of a Mobile Robot's Obstacle Avoidance Behavior in a Radioactive Environment with a High Level of Autonomy", International Journal on Technical and Physical Problems on Engineering (IJTPE), Issue 50, Vol. 14, No. 1, pp. 34-41, March 2022.

[16] V. Jain, Y. Jain, H. Dhingra, D. Saini, M.C. Taplamacioglu, M. Saka, "A Systematic Literature Review on QR Code Detection and Pre-Processing", International Journal on Technical and Physical Problems on Engineering (IJTPE), Issue 46, Vol. 13, No. 1, pp. 111-119, March 2021.

BIOGRAPHIES

Na me: **Ayoub**
Surname: **Toubi**
Birthday: 19.05.1994
Birthplace: Rabat, Morocco
Bachelor: Telecommunication Networks and Technologies, Faculty of Science and Technology, Hassan I University, Settat, Morocco, 2015
Master: Information Systems Security, National School of Applied Sciences, Ibn Tofail University, Kenitra, Morocco, 2018
Doctorate: Student, Routing Protocols for Multimedia in IOT, LAVETE Laboratory, Faculty of Science and Technology, Hassan I University, Settat, Morocco, Since 2021
Research Interests: WSN Routing Protocol, Cyber Security, and Smart Sensor Memory Issues
Scientific Publications: 2 Papers, 1 Poster

Na me: **Abdelmajid**
Surname: **Hajami**
Birthday: 01.01.1975
Birthplace: Marrakech, Morocco
Bachelor: Advanced Studies Diploma in Networks, Computing, Telecommunications and Multimedia, Mohammed V University, Rabat, Morocco, 2004
Master: Advanced Studies Diploma in Networks, Computing, Telecommunications, and Multimedia, Mohammed V University, Rabat, Morocco, 2006
Doctorate: Networking, Telecommunications and Multimedia, Mohammed V University, Rabat, Morocco, 2010
The Last Scientific Position: Prof., Faculty of Sciences and Technologies, Hassan I University, Settat, Morocco, Since 2011
Research Interests: Health Systems, Policy, Environmental Studies
Scientific Publications: 31 Papers, 1 Book, 1 Thesis
Scientific Memberships: IEEE