**Journal of Information Systems Engineering and Management**
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

# Impact and Countermeasures of Malware Attacks on Energy-Efficient Wireless Sensor Networks

*Leena Arya[1], Sudeep Varshney[2], Atkuri Venkata Naga Chandra Sekhar[3], Mandalapu Sivaparvathi[4], Venkata Rajani Katuri[5], Ravi Rastogi[6] and Syed Mohd Faisal[7]

[1]Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh-522302, India

leenaarya18@gmail.com[1]

[2]Professor and Head, Department of Computer Science & Engineering, Sharda School of Computing Science & Engineering, Sharda University, Gautam Buddh Nagar, UP-201301, India

sudeep.varshney@sharda.ac.in[2]

[3]Professor, Department of Information Technology, Sasi Institute of Technology & Engineering, Near Aerodrome, Tadepalligudem, West Godavari District, AP-534101, India

dravncsekharprof@gmail.com[3]

[4]Assistant Professor, Department of Computer Science and Engineering, MAM Women's Engineering College, Kesanupalli Village, Narasaraopet, District Palnadu, Andhra Pradesh-522601, India

sivaparvathi1242@gmail.com[4]

[5]Assistant Professor, Department of Computer Science Engineering, GITAM University, Rudraram, Hyderabad, Telangana-502329, India

kvrajanirajesh@gmail.com[5]

[6]Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh-522302, India

ravikumarrastogi@gmail.com[6]

[7]Assistant Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh-522302, India

smfaisalcse@gmail.com[7]

*Corresponding Author-

Name-Dr. Leena Arya

Email-leenaarya18@gmail.com

**Journal of Information Systems Engineering and Management**
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

**ARTICLE INFO**

Received: 20 Dec 2024

Revised: 18 Feb 2025

Accepted: 28 Feb 2025

**ABSTRACT**

Wireless Sensor Networks (WSNs) play a significant role in various applications such as environmental monitoring, healthcare, industrial automation, and smart cities. However, a WSN suffers from resource constraints, i.e., low energy and low computational capability, which makes it vulnerable to a broad range of malware attacks. These attacks, including sleep deprivation, blackhole, and worm propagation, can significantly compromise network performance, drain energy resources, and disrupt data transmission. This paper explores the impact of malware attacks on energy-efficient WSNs and evaluates existing and proposed countermeasures to enhance security while maintaining energy efficiency. This paper proposed a multi-layered security framework incorporating Adaptive Intrusion Detection Systems (IDS), secure routing protocols, and lightweight cryptographic methods by analysing how malware affects energy consumption and overall network stability. The methodology for threat mitigation yielded lesser overhead since it aims to build robust WSNs with a long-lasting defence mechanism against emerging security issues. The methodology guaranteed security and reliability in communication, prolonging the network operation's lifespan while still dealing with malware threats in energy-limited WSNs.

**Keyword**: Blackhole Attacks, Data Integrity, Intrusion Detection System (IDS), Secure Routing Protocols, Sleep Deprivation Attacks

## 1. Introduction

Wireless Sensor Networks (WSNs) are now significant enablers in various applications, such as environmental monitoring, health and medical care, smart cities, industrial automation, and many others. WSNs consist of spatially distributed sensor nodes designed to aggregate, process, and wirelessly communicate, usually in resource-constrained settings with limited energy, memory, and computational resources. Energy efficiency must be needed in WSNS because a more extended network lifetime is required to sustain reliable data transmission. However, all this dependence on scarce resources makes WSNs vulnerable to different types of security threats, especially malware, that can severely affect the functionality of networks and exhaust energy resources [1].

Malware attacks on WSNs may have various forms. These include sleep deprivation attacks, blackhole attacks, worm propagation, and denial-of-service (DoS) attacks. For example, sleep deprivation attacks refer to the depletion of the node's energy for a node such that it may never get the chance to enter the low-power states; thus, it consumes all the power of the battery [2] (Padmavathi and Shanmugapriya, 2009). Blackhole attack refers to malicious nodes that attract and discard the data packets and compromise data integrity and communication [3]. The propagation of worms and other malware worsens the scenario by spreading over a network, raising communication overhead, causing severe energy consumption, and engendering network instability.

As such, working on the practical development of countermeasures against malware attacks in WSNs is critical. Intrusion Detection Systems (IDS) have been broadly considered for identifying and mitigating malicious activities in WSNs. IDS approaches usually employ signature-based, anomaly-based, or hybrid methods to detect suspicious activity [4]. Secure routing protocols have also been proposed to prevent routing-based attacks by enhancing data integrity and preventing malicious

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

nodes from halting communication [3]. Lightweight cryptographic protocols and energy-efficient security solutions have also been studied to protect communication with minimal energy overhead.

However, in this context, malware attacks do not stop changing, introducing new challenges to the secured WSNs. Adaptive, scalable, and energy-aware solutions best suited to the particular constraints of WSNs are required to deal with these challenges. This paper aims to analyze the impact of malware attacks on energy efficiency, the overall performance of WSNs, and their existing and proposed countermeasures. This work aims to provide an all-rounded review of the mechanisms through which malware impacts WSNs and, by analysing different security countermeasures, gives an insight into more robust and energy-efficient WSN systems given emerging threats [5-6].

This work contributed to building the most resilient yet energy-efficient WSNs in terms of malicious threats through malware mechanisms influencing energy consumption and the effectiveness of security strategies. A good example of malware exploitation in WSNs is the "Sybil Attack," in which one malicious node assumes numerous identities, interrupting the routing process and wasting all the network resources while authenticating the nodes' identities. Similarly, attacks such as the "HELLO flood attack" send control packets to bomb nodes to increase energy expenditure through unnecessary processing at network entry points [7].

## 2. Related Work

Ojha et al. (2021) [1] suggested a better model for predicting the stability of wireless sensor networks (WSNs) against malware attacks, proposing methods to promote network resilience and minimize susceptibility to malware spread. Padmavathi and Shanmugapriya (2009) [2] surveyed various attacks and security mechanisms in WSNs, discussing the challenges and countermeasures necessary to protect these networks from malicious activities. Karlof and Wagner (2003) [3] analyzed secure routing in WSNs, focusing on the vulnerabilities that make these networks susceptible to attacks like routing misbehaviors and providing countermeasures to mitigate such threats. Bhattasali and Chaki (2011) [4] surveyed recent intrusion detection systems (IDS) for WSNs, highlighting different methodologies and frameworks to detect malicious activities and enhance network security. Arya et al. (2024) [5] presented AI-powered threat detection and safety measures for IoT and WSNs, discussing how artificial intelligence can enhance security and efficient threat detection in these resource-constrained environments. Nagaraj et al. (2023) [6] developed a secure encryption technique with energy optimization using a random permutation pseudo algorithm in IoT-based WSNs to ensure energy-efficient secure communication. Douceur (2002) [7] introduced the Sybil attack, which allows malicious nodes to impersonate multiple identities, disrupting the functionality of WSNs, and provided methods to counteract such attacks. Almaiah et al. (2023) [8] proposed an enhanced dynamic Bayesian network approach to improve the security of IoT medical data systems, ensuring the integrity and confidentiality of sensitive data in wireless communication. Hart and Martinez (2006) [9] discussed the revolution in Earth system science by environmental sensor networks, detailing their application in climate and environmental monitoring. Alemdar and Ersoy (2010) [10] surveyed the use of WSNs in healthcare applications, examining the potential and challenges of deploying these networks for medical monitoring and data collection. Sinha et al. (2017) [11] surveyed security vulnerabilities, attacks, and countermeasures in WSNs, mainly focusing on security risks at various OSI model layers and proposing mitigation strategies. Butun et al. (2019) [12] reviewed vulnerabilities, attacks, and countermeasures specific to the Internet of Things (IoT), detailing how these threats apply to IoT-enabled WSNs and presenting solutions for robust security. Tomic et al. (2018) [13] introduced "Antilizer," a self-healing security mechanism for WSNs that provides runtime protection by automatically recovering from security breaches. Wang et al. (2006) [14] provided a comprehensive survey of security issues in WSNs, discussing various attacks and proposing solutions to improve the overall security of these networks. Shahzad et al. (2017) [15] discussed active attacks on WSNs, such as jamming and eavesdropping, and their countermeasures, providing a detailed

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

overview of defense mechanisms against these threats. Awasthi et al. (2023) [16] explored the dissemination of malware in rechargeable WSNs and suggested an epidemiological approach to enhance network lifespan while combating the spread of malware. Martin-del Rey (2024) [17] proposed a novel model for malware propagation in WSNs, helping to understand how malware spreads within these networks and how its effects can be mitigated. Ahmad et al. (2022) [18] provided an overview of machine learning-based security solutions for WSNs, discussing the challenges of using AI in securing sensor networks and their potential applications. Behiry and Aly (2024) [19] proposed a hybrid feature reduction technique combined with AI and machine learning methods for detecting cyberattacks in WSNs, showcasing their application for enhanced security. Butun et al. (2014) [20] surveyed various intrusion detection systems (IDS) for WSNs, categorizing existing methods and evaluating their effectiveness in detecting and mitigating malicious activities. Chelli (2015) [21] discussed the security issues in WSNs, emphasizing attacks and countermeasures necessary to protect the network's integrity and ensure reliable communication. Elsawy et al. (2020) [22] presented spatial firewalls as a method for quarantining malware epidemics in large-scale massive WSNs, offering a unique approach to mitigating malware spread in extensive networks. Bandekar and Javaid (2018) [23] examined the effect of cyberattacks on low-power IoT devices, emphasising energy limitations and suggesting mitigation techniques for such devices under attack situations.

## 3. Overview of Wireless Sensor Networks(WSN)

Wireless Sensor Networks (WSNs) have become significantly important as significant building blocks of present communication technology. With real-time monitoring and control applications across domains, WSNs consist of spatially distributed autonomous nodes that can sense environmental conditions such as temperature, humidity, light, motion, pressure and other climatic conditions. In doing so, such networks can wirelessly collect, process, and transmit data applicable in many sectors like environmental monitoring, healthcare, industrial automation, military operations, and smart cities. They communicate this information wirelessly to a central locale for further analysis and processing [8].

### 3.1. Architecture and Components of WSNs

The basic architecture of WSNs is a layered structure in which the sensor nodes collaborate in extracting and forwarding the data to the centralized node or gateway. The key components are as follows:

- Sensor Nodes: These nodes include all the hardware components, such as sensing, processing, and wireless communication. They have low power, memory, and computation characteristics and, thus, must perform operations that reduce energy and extend their lifetime.
- Base Stations (Sink Nodes): The base stations act as sinks whereby sensor data is aggregated and forwarded to other network elements or the end-users. They may often have more power and processing capacity than regular sensor nodes.
- Communication Modules: Depending on the application requirements, wireless sensor nodes exploit different communication protocols, including Zigbee, Bluetooth, and low-power Wi-Fi.

### 3.2. Energy-Efficient Wireless Sensor Networks (WSNs) Attacks

Energy efficiency is a primary concern in Wireless Sensor Networks (WSNs) due to resource-constrained nodes. Security challenges, such as eavesdropping, node tampering, and data modification, further complicate the implementation of adequate security protocols [11-14]. WSNs are vulnerable to malware attacks that exploit network protocol and node hardware weaknesses [15]. Common malware types include worms, injected viruses, and sleep deprivation attacks, which drain energy and degrade performance. Malware attacks in energy-efficient WSNs exploit the existing weaknesses in network protocols, node hardware, or software layers to compromise network

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

functionality. These attacks can lead to significant energy consumption due to increased communication overhead, network instability, and compromised data integrity [16]. Consequently, WSNs face reduced lifetime and performance, necessitating efficient security solutions that balance threat mitigation with minimal energy consumption [17].

## 4. Counter against Malware Attacks in Energy-Efficient WSNs

To counteract the increasing rate of malware assaults in energy-conscious wireless sensor networks (WSNs) [18], a multifaceted use of prevention, detection, mitigation, and recovery mechanisms is indispensable. Prevention measures like secure boot, access controls, and network segmentation restrict malware infections. Detection methods, including signature-based, anomaly-based, and hybrid detection approaches [19], provide a means to identify malicious activities with minimal resource consumption. Energy-efficient Intrusion Detection Systems (IDS) are also proposed to ensure scalability without adding significant overhead [20]. Once malware is detected, containment strategies like node isolation, blocklisting, and software patch management are applied to stop its spread and minimize damage. Recovery mechanisms, such as system restoration and self-healing, ensure the network returns to normal operation while maintaining security. Energy-constrained security models, including lightweight cryptography, efficient key management, and dynamically adapted security, help protect WSNs while minimizing energy usage [21]. Secure routing protocols, like LEACH, are also implemented to safeguard data transmission against routing-based attacks [22-23]. These combined strategies ensure that WSNs can operate securely and efficiently even with malware threats.

## 5. Proposed Methodology

### 5.1. System Model and Assumptions

**5.1.1. Network Model:** The Wireless Sensor Network (WSN) consists of 100 sensor nodes dispersed uniformly over an area of 500x500m. Each node communicates with a central base station via multi-hop routing to ensure efficient data collection and transmission.

**5.1.2. Energy Model:** The energy consumption for transmitting a $k$-bit packet over a distance $d$ is shown by equation (1):

$$E_{tx}(k,d) = E_{elec} \times k + E_{amp} \times k \times d^2 \quad \text{-(1)}$$

where:

- $E_{elec}$ is the energy consumed per bit (50 nJ/bit)
- $E_{amp}$ is the energy consumed by the amplifier (100 pJ/bit/m$^2$)
- $k$=512 bits is the packet size.

**5.1.3. Attack Model:** The network is subjected to different malware attacks, such as sleep deprivation attacks, blackhole attacks, and worm propagation.

### 5.2. Malware Detection Mechanism

Adaptive Intrusion Detection System (IDS)-The IDS combines signature-based and anomaly-based detection mechanisms to identify malicious nodes using equations (2), (3), and (4).

True Positive Rate (TPR):

$$TPR = \frac{True\ Positives}{True\ Positives + False\ Negatives} \quad \text{-(2)}$$

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

False Positive Rate (FPR):

$$FPR = \frac{False\ Positives}{False\ Positives + True\ Negatives} \quad -(3)$$

Detection Probability $P_d$:

$$P_d = \frac{Number\ of\ correctly\ detected\ malicious\ nodes}{Total\ number\ of\ malicious\ nodes} \quad -(4)$$

### 5.3. Energy-Efficient Security Protocols

Secure Routing Protocols- Secure routing is achieved through node authentication and encryption. Clustering techniques are employed to reduce energy consumption. The total energy consumption for a node during secure communication is shown in equation (5):

$$E_{total} = E_{tx} + E_{rx} + E_{sec} \quad -(5)$$

where:

- $E_{rx}$ is the energy consumed for receiving data.
- $E_{sec}$ is the energy overhead due to security measures.

### 5.4. Mitigation and Recovery Mechanisms

Node Quarantine Mechanism- The mechanism identifies and isolates compromised nodes to prevent malware propagation. The probability of successful quarantine $P_q$ is given by equation (6):

$$P_q = 1 - \left(\frac{Number\ of\ undetected\ malicious\ nodes}{Total\ number\ of\ nodes}\right) \quad -(6)$$

### 5.5. Experimental Evaluation and Metrics

The proposed methodology is evaluated using the following performance metrics and system parameters, as shown in Table 1. The detection accuracy is demonstrated by the equation (7):

$$\text{Detection Accuracy: } \frac{TP+TN}{TP+TN+FP+FN} \quad -(7)$$

- Energy Consumption: Measured in joules per node per hour.
- Packet Delivery Ratio (PDR): The ratio of successfully delivered packets to the total packets sent.
- Latency: Time taken for data traversal across the network.

Table 1: System Parameters for Simulation

| Parameter | Value |
|---|---|
| Number of Nodes ($N$) | 100 |
| Simulation Area ($A$) | 500 x 500 $m^2$ |
| Energy per Bit ($E_{elec}$ ) | 50 nJ/bit |
| Amplifier Energy ($E_{amp}$) | 100 pJ/bit/$m^2$ |
| Packet Size ($k$) | 512 bits |
| Malware Scenarios | Sleep Deprivation, Blackhole, Worm Propagation |

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

## 6. Results and Discussion

Table 2 and Figure 2. represent the TPR vs. FPR in the Detection Performance Metrics represent the detection capability of the IDS. The very high TPR, at 94.5%, reflects the almost perfect discovery of all the malicious nodes. The low FPR, at 4.1%, and perfect accuracy in fewer false alarms mean hardly any genuine nodes get misclassified as malicious. Such an accuracy of detection is critical for keeping the network's stability level and allowing for unnecessary intervention. The effectiveness of the IDS proves that the proposed security framework can detect and isolate threats accurately and reliably. As such, the overall resilience of the network would be enhanced.

Table 2: Detection Performance Metrics

| Metric | Value |
|---|---|
| True Positive Rate (TPR) | 94.5% |
| False Positive Rate (FPR) | 4.1% |
| Precision | 95.2% |
| Recall | 94.5% |

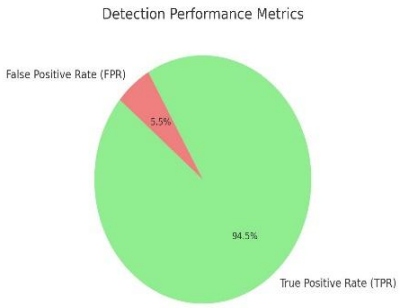


Figure 2. Detection Performance Metrics

Table 3 represents the network performance metrics for those without security and those with security.

Table 3: Network Performance Metrics

| Metric | Without Security | With Security |
|---|---|---|
| Packet Delivery Ratio (PDR) | 62% | 91% |
| Average Latency (ms) | 15 | 19 |
| Energy Consumption (J) | 0.75 | 0.87 |
| Node Lifetime (hours) | 180 | 170 |

Figure 3 represents the Packet Delivery Ratio Comparison of both cases and clearly shows improvements in network packet delivery since it introduces security measures. In this case, without

**Journal of Information Systems Engineering and Management**
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

incorporating security into the network, an outcome of 62% of PDR is noticed, meaning that the network is quite vulnerable to data loss or disruption due to attacks by malware. On the other hand, establishing the proposed security protocols increases by 91%, as shown in the comparison of the PDR graphs. An improvement in this aspect supports the point that the scheme ensures smooth and effective communication in case of malicious attacks against the network.

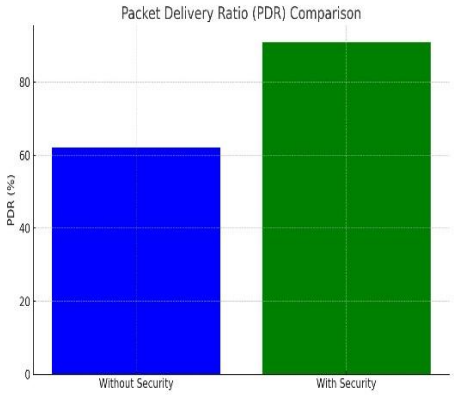


Figure 3 Packet Delivery Ratio (PDR) Comparison

The network latency when security measures are in place is moderate. According to Figure.4, there will be increased latency when security measures are implemented, increasing from 15 ms to 19 ms. These extra processing-related latencies are caused by extra intrusion detection and encryption mechanisms to secure the data flow. Although these operations increase Latency, they only have a marginal impact and are well within the tolerance limits for WSN applications. This, therefore, indicates that added security does not outweigh the cost of added delay to networks, thus guaranteeing data delivery securely without much deterioration in performance.

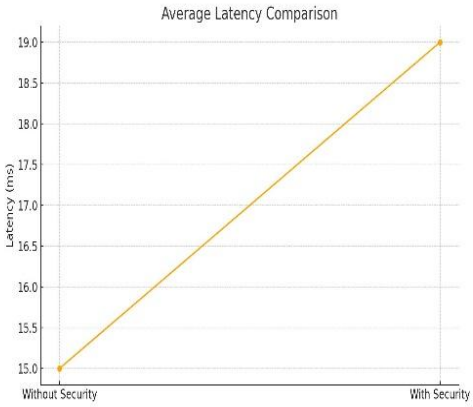


Figure 4 Average Latency Comparison

In Figure 5, energy consumption per node is slightly higher without security measures. This slight increase accounts for added support energy for secure routing, intrusion detection, and data encryption operations. With that increase notwithstanding, the fact still is that there is very little energy overhead, meaning this comes up as lightweight security mechanisms that are very energy

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

efficient. It ensures that the network is operationally viable without compromising its energy efficiency.

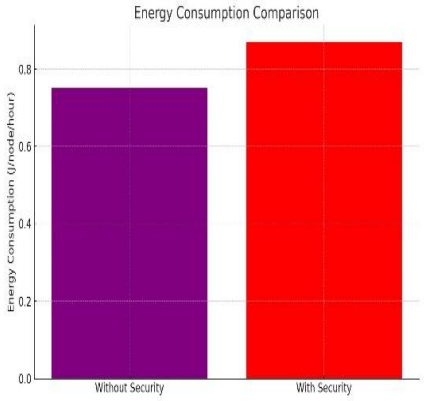


Figure 5 Energy Consumption Comparison

Figure 6 presents the node lifetime in a secure environment versus a non-secure environment, with the latter showing a node lifetime of 180 hours compared to a node lifetime of 170 hours in the former. Again, this is some decrease due to the extra energy overhead from these security mechanisms, including encryption and intrusion detection measures. To summarise, the reductions are acceptable for trade-off against unmatched network security and reliability brought into the network. Being low impact on the lifetime of nodes, these have been designed to be lightweight so that network functionality and resilience are preserved without excessively depleting energy resources.

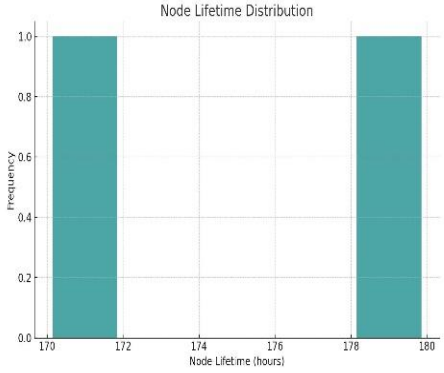


Figure 6 Node Lifetime Distribution

## 7. Conclusion

Wireless Sensor Networks (WSNs) are key areas of potential applications like environmental monitoring, healthcare, and industrial automation. However, they are prone to malware attacks that degrade their performance and energy efficiency. Some malware attacks include sleep deprivation, blackhole, and worm propagation, which significantly degrade the working of WSNs in terms of increased energy consumption, data integrity disruption, and reduced network lifespan. The security work has adopted a multi-layered security framework consisting of a proper adaptive intrusion detection system, energy-efficient secure routing protocols, and mitigation and recovery mechanisms. The IDS could run with both signature-based and anomaly-based detection methods since, in this

Research Article

case, it was followed by a true positive rate of about 94.5% and a false positive rate of 4.1%, showing its capability to mainly recognize malicious nodes while keeping the rate of false alarms to a minimum. This capability is crucial to the stability of the network; it also reduces unnecessary intervention. The analysis further shows that the security measures improve key network metrics such as Packet Delivery Ratio. Thus, without security measurements, the PDR was at 62%, but with security measures, it went up to 91%. It is not untrue that with this improvement, the framework retains reliable and consistent communication even under attack conditions. However, there was a minor increase in average latency from 15 ms to 19 ms and energy consumption from 0.75 J/node/hour to 0.87 J/node/hour because of additional overheads from security mechanisms. A moderate decrease in node lifetime from 180 hours to 170 hours reflects the necessity of the energy trade-off needed to make the network resilient.

## REFERENCES

[1] Ojha, R. P., Srivastava, P. K., Sanyal, G., et al. (2021). Improved model for the stability analysis of wireless sensor network against malware attacks. *Wireless Personal Communications, 116*, 2525–2548. https://doi.org/10.1007/s11277-020-07809-x

[2] Padmavathi, G., & Shanmugapriya, D. (2009). A survey of attacks, security mechanisms, and challenges in wireless sensor networks. *International Journal of Computer Science and Information Security, 4*(1-2), 1-9.

[3] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Networks, 1*, 293–315. https://doi.org/10.1016/S1570-8705(03)00008-8

[4] Bhattasali, T., & Chaki, R. (2011). A survey of recent intrusion detection systems for wireless sensor networks. In *Advances in Network Security and Applications. CNSA 2011* (Vol. 196, pp. 199–209). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-22540-6_27

[5] Arya, L., Sharma, Y. K., Devi, S., Padmanaban, H., & Kumar, R. (2024). Securing the Internet of Things: AI-powered threat detection and safety measures. In *Proceedings of International Conference on Recent Innovations in Computing. ICRIC 2023* (Vol. 1195, pp. 81–91). Springer, Singapore. https://doi.org/10.1007/978-981-97-3442-9_7

[6] Nagaraj, S., et al. (2023). Improved secure encryption with energy optimization using random permutation pseudo algorithm based on the Internet of Things in wireless sensor networks. *Energies, 16*(8). https://doi.org/10.3390/en16010008

[7] Douceur, J. R. (2002). The Sybil attack. In *Springer International Workshop on Peer-to-Peer Systems* (pp. 251–260). https://doi.org/10.1007/3-540-45748-8_24

[8] Almaiah, M. A., Yelisetti, S., Arya, L., Babu Christopher, N. K., Kaliappan, K., Vellaisamy, P., Hajjej, F., & Alkdour, T. (2023). A novel approach for improving the security of IoT–medical data systems using an enhanced dynamic Bayesian network. *Electronics, 12*, 4316. https://doi.org/10.3390/electronics12204316

[9] Hart, J. K., & Martinez, K. (2006). Environmental sensor networks: A revolution in earth system science? *Earth-Science Reviews, 78*, 177–191. https://doi.org/10.1016/j.earscirev.2006.05.001

[10] Alemdar, H., & Ersoy, C. (2010). Wireless sensor networks for healthcare: A survey. *Computer Networks, 54*, 2688–2710. https://doi.org/10.1016/j.comnet.2010.05.003

[11] Sinha, P., Jha, V. K., Rai, A. K., & Bhushan, B. (2017). Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey.

Research Article

In *2017 International Conference on Signal Processing and Communication (ICSPC)* (pp. 288–293). https://doi.org/10.1109/CSPC.2017.8305855

[12] Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks and countermeasures. *IEEE Communications Surveys & Tutorials, 22*(1), 616–644.

[13] Tomic, P., Chen, P. Y., Breza, M. J., & McCann, J. A. (2018). Antilizer: Run time self-healing security for wireless sensor networks. *IEEE Transactions on Dependable and Secure Computing, 17*(1), 1–14.

[14] Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks. *IEEE Communications Surveys & Tutorials, 8*(2), 2–23.

[15] Shahzad, F., Pasha, M., & Ahmad, A. (2017). A survey of active attacks on wireless sensor networks and their countermeasures. *Journal of Network and Computer Applications, 97*, 229–248.

[16] Awasthi, S., Srivastava, P. K., Kumar, N., et al. (2023). A study of the dissemination of malware and the enhancement of the lifespan of rechargeable wireless sensor networks: An epidemiological approach. *SN Computer Science, 4*, 851. https://doi.org/10.1007/s42979-023-02312-z

[17] Martin-del Rey, A. (2024). A novel model for malware propagation on wireless sensor networks. *Mathematical Biosciences and Engineering, 21*(4), 176.

[18] Ahmad, R., Wazirali, R., & Abu-Ain, T. (2022). Machine learning for wireless sensor networks security: An overview of challenges and issues. *Sensors, 22*, 4730. https://doi.org/10.3390/s22134730

[19] Behiry, M. H., & Aly, M. (2024). Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods. *Journal of Big Data, 11*, 16. https://doi.org/10.1186/s40537-023-00870-w

[20] Butun, I., Morgera, S. D., & Sankar, R. (2014). A survey of intrusion detection systems in wireless sensor networks. *IEEE Communications Surveys & Tutorials, 16*(1), 266–282. https://doi.org/10.1109/SURV.2013.050113.00191

[21] Chelli, K. (2015). Security issues in wireless sensor networks: Attacks and countermeasures. *Proceedings of the World Congress on Engineering, 1*, 1–5.

[22] Elsawy, H., Kishk, M. A., & Alouini, M. S. (2020). Spatial firewalls: Quarantining malware epidemics in large-scale massive wireless networks. *IEEE Wireless Communications, 27*(5), 6–13.

[23] Bandekar, A., & Javaid, A. Y. (2018). Cyber-attack mitigation and impact analysis for low-power IoT devices. *arXiv preprint, arXiv:1807.11850*.