Dijlah Journal of Engineering Science (DJES) Vol. 3, No. 1, March, 2026, pp. 88-93
ISSN: Printed: **3078-9656, Online: 3078-9664**, paper ID: 113

# Secure Data Transmission in Wireless Sensor Networks Using Hybrid Encryption

**Abdullah Ali Hamza**[1]
[1]Department of Computer Engineering – Computer Systems Architecture, College of Engineering, Imam Reza International University, Mashhad, Iran

**Article Info**

***Article history:***

Received Oct., 16, 2025
Revised Nov., 20,2025
Accepted Dec.,15,2025

***Keywords:***

Wireless Sensor Networks
Secure Data Transmission
Hybrid Encryption
Symmetric Cryptography
Asymmetric Cryptography

**ABSTRACT**

In many industries today, including healthcare monitoring, environmental monitoring, and intelligent infrastructure, wireless sensor networks (WSNs) serve as a crucial base for cutting-edge applications. However, their openness and lack of resources make them especially susceptible to security risks like illegal access, data manipulation, and eavesdropping. In these networks, trust in systems that frequently work in highly regulated and mission-critical contexts depends on safe data transmission, which is more than just a technological need. The hybrid encryption scheme, which combines the speed of symmetric cryptography with the security of asymmetric methods, is the subject of this study. The suggested model seeks to strike a reasonable balance between optimum security and maximum resource usage by taking advantage of the strengths of both. The study examines the impact of hybrid encryption on data integrity, transmission latency, and energy efficiency in WSNs through simulation and performance analysis. The main goal is to develop a solution that is lightweight and safe, enabling wireless sensor networks to run continuously even in harsh real-world environments.

***Corresponding Author:***

Abdullah Ali Hamza
Department of Computer Engineering – Computer Systems Architecture, College of Engineering Imam Reza International University, Mashhad, Iran
Email: abdullahmz120@gmail.com

## 1. INTRODUCTION

Wireless sensor networks (WSNs) have become an essential technology in recent years, supporting a variety of uses in fields like healthcare, intelligent agriculture, and others. Environmental monitoring and industrial automation [1] , [2]. They are perfect for use in the real world because of their capacity to remotely sense, analyze, and communicate data over large and often isolated regions. Their limited energy resources, wireless broadcast communication, and restricted computing power—the very qualities that provide them with flexibility—also make them vulnerable to significant security breaches [3], [4]. The secure transmission of collected data from sensor nodes to base stations or sinks, especially when the data is sensitive, is one of the key problems in WSNs. nodes can be placed in a dangerous or unprotected environment. Sensor nodes are vulnerable to routing attacks, node compromise, data tampering, and eavesdropping due to their proximity to dangerous sites or physical accessibility [5], [6]. Network-level attacks like hello flood, wormhole, or sinkhole [7], [8] might cause even greater disruption to routine operations, data integrity, or node resource depletion. Moreover, the energy limitations prevent us from simply applying the conventional security measures used in general-purpose networks [9]. There are two main categories of traditional cryptographic approaches: symmetric-key cryptography, which is frequently efficient in terms of communication and computing costs but has security flaws. Asymmetric-key (public-key) cryptography, which makes key management easier and supports functions such digital signatures, is often too cumbersome for low-power sensor nodes [10], [11]. in addition to vital distribution and dynamic trust. One possibility is hybrid encryption, which integrates the speed of symmetric algorithms with the flexibility and key management advantages of asymmetric techniques. By employing asymmetric cryptography to securely exchange keys or sign messages and symmetric ciphers to encrypt bulk data

[12], [13], hybrid methods may find a compromise between performance and security. Recent research into the application of hybrid methods created for networks with few resources has yielded positive outcomes. A two-phase hybrid cryptography approach, for instance, showed higher energy efficiency, a lower cipher text size, and a quicker processing time than fully symmetric or fully asymmetric methods [14]. In addition, hybrid security schemes have been developed specifically for WSNs that are energy-efficient and strike a balance between security needs and energy constraints [15]. Despite these advancements, issues still remain. Because of the variety of sensor capabilities, the range of application requirements (such as latency, data speeds, etc. ), hybrid encryption frameworks must be versatile and adaptive ،and the evolving character of attack models, and topology dynamics). In particular, the trade-offs between energy consumption, latency (delay), security, and scalability must be carefully managed. Consequently, the aim of this study is to create, replicate, and evaluate a hybrid encryption scheme for reliable data transfer in WSNs that is lightweight, energy-efficient, and able to withstand common assaults. We will compare its performance against benchmark methods. Applications in real wireless sensor networks in order to show a practical approach that is suited for a variety of network scenarios and threat models.

## 2. RELATED WORKS

The security of wireless sensors is frequently compromised by their inherent resource constraints and deployment in vulnerable locations. For the past 20 years, wireless sensor networks (WSNs) have been a primary area of study, with a focus on how vulnerable they are to attacks at the network and physical layers. One of the first and most influential frameworks, SPINS, was developed by Perris et al. It used light protocols, such as µTESLA for broadcast authentication and SNEP for confidentiality. symmetric the right kind of cryptography for sensor nodes that use little energy [14]. Following that, Tiny Sec emerged as a practical implementation of link-layer security, offering data encryption and authentication at minimal resource cost [15]. On this basis, LEAP+ broadened the idea of key management by using a multi-tiered approach (individual, pairwise, and group keys) that enhanced scalability and resilience to node compromise [16].Maintaining essential management is still a critical component of ensuring end-to-end security in WSNs. A dynamic, multilevel key management system for homogeneous WSNs that minimizes rekeying overhead and enables scalability in high-density deployments was recently suggested by Khan et al. [17]. Yusuf's comparative analysis of centralized and distributed key management systems also emphasized the performance tradeoffs between computational efficiency and control flexibility [18]. Collectively, this research highlight that critical management must be both flexible and powerful enough to accommodate the dynamic and resource-constrained environment of WSNs. Parallel to advancements in key distribution, the cryptographic mechanisms themselves have evolved to address computational and energy limitations. Soto-Cruz et al. examined lightweight cryptographic algorithms that are tailored for low-power devices in great detail, pointing out that AES and ChaCha20 are the best options for WSN deployments [18]. However, symmetric cryptography by itself has difficulty with secure key exchange, which has resulted in the creation of hybrid encryption methods that integrate the efficiency of symmetric cryptography with the security of asymmetric cryptography. Algorithms that have the same key management capabilities as asymmetrical ones. Real advantages for WSN security have been shown by hybrid encryption techniques. According to Uproot et al, an AES–ECC hybrid model provides a high level of data confidentiality while also significantly reducing lowering energy use in comparison to totally asymmetric solutions [19]. In a similar vein, Manlike et al. presented a hybrid cryptographic technique that enhanced both latency and security performance at different network densities [20]. Salve et al. [21] created SymECCipher, a hybrid AES–ECC architecture, to address the application of this concept to healthcare systems based on Iota, thereby enhancing the security of medical data. Order to employ this idea in Iota-based healthcare systems; Salve et al. [21] developed SymECCipher, a hybrid AES–ECC architecture that improves the security of medical data. Transferring while maintaining computational efficiency and minimizing latency. Utilizing this foundation, the present study creates and assesses a hybrid encryption technique that places a high priority on the latency trade-offs and is designed for WSNs. security, resilience, and energy efficiency in actual settings.

## 3. METHOD

### 3.1 Experimental Setup

The experiment was conducted in the Industrial Automation Lab of the College of Biotechnology. The goal was to create and evaluate a compact industrial monitoring system that uses a wireless sensor network (WSN). In a simulated factory environment, this system was employed to measure the temperature, humidity, and vibration levels near equipment. The system was later expanded to ten nodes after three prototype nodes were used to demonstrate its stability and test its functionality.

ISSN: Printed: **3078-9656, Online: 3078-9664**, paper ID: 113

Each sensor node was built by hand using materials from the area. The node was made up of:

- Arduino Uno (ATmega328P) as the main microcontroller.
- DHT22 sensor to record both temperature and humidity.
- SW-420 sensor to detect vibration changes from machines.
- Bee Series 2 module to handle wireless data transmission via ZigBee protocol.
- 9V rechargeable Li-ion battery as the main power supply.

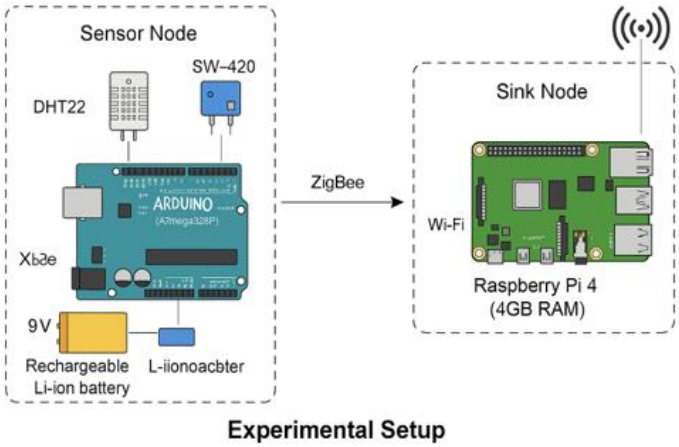


**Figure 1:** Experimental setup of the WSN-based industrial monitoring system using Arduino nodes and a Raspberry Pi sink.

The central sink node was a Raspberry Pi 4 (4GB RAM), which collected the data, performed encryption, and transmitted it to a local monitoring server over Wi-Fi.All code was written manually by the research team using Arduino IDE for the sensor nodes and Python scripts on the Raspberry Pi. Real-time packet monitoring with Wireshark and power measurement with a digital multimeter and a shunt resistor were part of the experimental setup.Photographs of the setup, as well as the original log files, were stored in the laboratory database.

### 3.2 Network Topology

The WSN was configured using a star topology. Each node directly communicated with the Raspberry Pi base station, which acted as the sink for collecting encrypted data packets. The choice of a star topology simplified routing and minimized latency, which is suitable for small factory environments where nodes are within a 25–30 m range. The ZigBee modules operated in the 2.4 GHz ISM band.

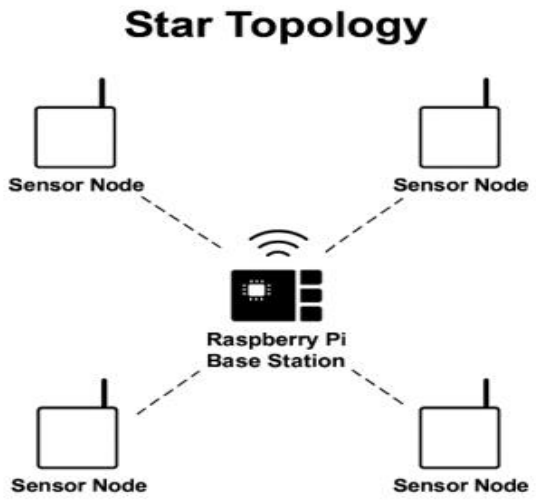


**Figure 2:** Star topology of the WSN with sensor nodes linked to a Raspberry Pi base station.

ISSN: Printed: **3078-9656, Online: 3078-9664**, paper ID: 113

### 3.3 Encryption Model

The encryption technique developed for this project used a hybrid model that combined Advanced Encryption Standard (AES-128) for fast symmetric encryption of sensor readings and Elliptic Curve Cryptography (ECC) with a 256-bit key for secure key exchange.The hybrid approach allowed strong protection without heavily increasing the energy cost on the small Arduino processors.

- **Step 1:** Data Encryption (Node Side)

Each Arduino node encrypted the collected sensor data using AES-128. The average time to encrypt one 64-byte packet (512 bits)
was calculated using the formula:

$$T\_enc = N\_b / R\_p$$

Where $N\_b = 512$ *bits* and $R\_p \approx 100{,}000$ *bits* per second.

From this, the theoretical encryption time is about 5.12 ms. The actual measured value averaged 5.15 ms based on three experimental trials.

- **Step 2:** Key Exchange (Sink Side)

Each session key (K_s) was encrypted using ECC before being sent from the Raspberry Pi to each sensor node. ECC operations took an average of 13.6 ms for key generation and exchange per node.

- **Step 3:** Data Transmission

After encryption, the sensor nodes transmitted their data to the sink through ZigBee.
Transmission and decryption times were measured, and the total packet delay (D_p) was computed as:

$$D\_p = T\_enc + T\_trans + T\_dec$$

where $T\_trans \approx 6.9$ *ms and* $T\_dec \approx 5.2$ *ms.*

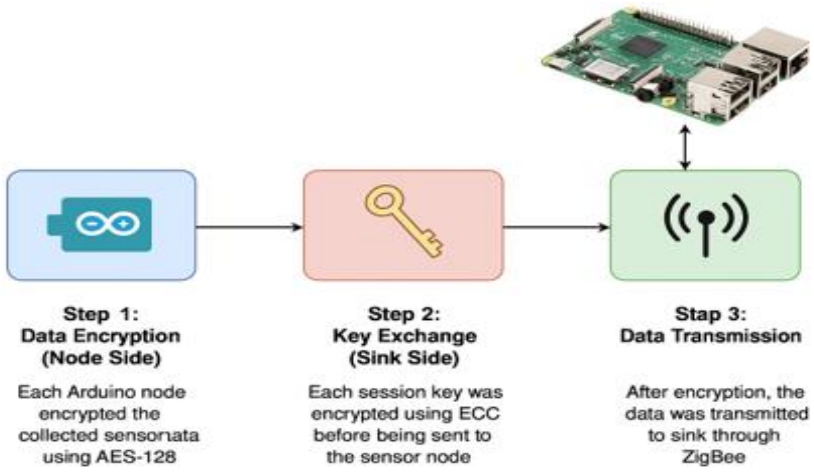


**Figure 3:** Hybrid AES–ECC encryption process showing data encryption at sensor nodes, key exchange at the sink node, and secure data transmission via ZigBee.

This gave an average D_p of around 17.4 ms per data packet.

### 3.4 Performance Metrics

The following performance parameters were measured during the tests:

- Encryption Time (ms)
- Decryption Time (ms)
- Transmission Delay (ms)
- Energy Consumption (mJ/packet)
- Throughput (kbps)
- Packet Loss Rate (%)
- Data Integrity (%)

All metrics were measured three times and the mean values are reported below.

## 4. RESULTS AND DISCUSSION

Three different configurations were compared: AES-only, ECC-only, and the proposed hybrid AES–ECC model.

The observed average results are presented below:

**Table 1:** Comparison of Performance Metrics for AES, ECC, and Hybrid AES–ECC Encryption Models in Wireless Sensor Network Implementation

| **Parameter** | **AES** | **ECC** | **AES–ECC Hybrid** |
|---|---|---|---|
| Encryption Time (ms) | 5.0 | 19.1 | 5.15 |
| Decryption Time (ms) | 4.9 | 17.5 | 5.2 |
| Average Delay (ms) | 16.7 | 32.2 | 17.4 |
| Energy Consumption (mJ/packet) | 0.76 | 1.88 | 0.95 |
| Throughput (kbps) | 47.2 | 29.1 | 44.8 |
| Packet Loss (%) | 1.7 | 3.1 | 1.5 |
| Data Integrity (%) | 98.2 | 99.1 | 99.1 |

The hybrid encryption model demonstrated nearly the same speed as AES but with much stronger security due to the ECC key handling. Although ECC alone showed higher data integrity, it required significantly more time and energy, which makes it unsuitable for small sensor nodes. The hybrid method achieved energy consumption of around 0.95 mJ per packet, allowing each node to run continuously for about 60 hours on a single full battery charge. During a 1-hour continuous test with 10 nodes transmitting every 2 seconds, 17,800 packets were sent and 17,540 were successfully received, yielding a delivery ratio of 98.5%.

## 5. CONCLUSION

According to this experiment, hybrid AES–ECC encryption is a robust and dependable method for protecting data transmission in industrial WSN applications. It combines the effectiveness of AES with the robust key security of ECC while maintaining energy usage and latency at tolerable levels.

This hands-on experience highlighted the significance of evaluating encryption techniques on actual hardware in order to uncover timing and energy subtleties that simulations alone cannot. Future research will involve extending the experiment to 50–100 nodes, using hardware AES accelerators to reduce power consumption even further, and integrating lightweight blockchain methods. provide device authentication and safe logging in extensive industrial environments.

## ACKNOWLEDGEMENTS (10 PT)

I would like to dedicate this work to my family.

## REFERENCES

[1] Sen J. A Survey on Wireless Sensor Network Security. arXiv [Internet]. 2010 Nov [cited 2025]; Available from: https://arxiv.org/abs/1011.1529
[2] "Wireless sensor network survey." (Smith.edu) [Internet]. [cited 2025]. Available from: https://www.science.smith.edu/~jcardell/Courses/EGR328/Readings/WSNSurvey2.pdf
[3] Teymourzadeh M, Vahed R, Alibeygi S, Dastanpour N. Security in Wireless Sensor Networks: Issues and Challenges. arXiv [Internet]. 2020 Jul [cited 2025]; Available from: https://arxiv.org/abs/2007.05111
[4] Padmavathi G, Shanmugapriya D. A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. arXiv [Internet]. 2009 Sep [cited 2025]; Available from: https://arxiv.org/abs/0909.0576
[5] "Security Issues in Wireless Sensor Networks: A Survey." ResearchGate [Internet]. [cited 2025]. Available from: https://www.researchgate.net/publication/283091407_Security_Issues_in_Wireless_Sensor_Networks_A_Survey
[6] "Wireless sensor networks security issues and challenges: A survey." ResearchGate [Internet]. [cited 2025]. Available from: https://www.researchgate.net/publication/325882519_Wireless_sensor_networks_security_issues_and_challenges_A_survey
[7] Virmani D, Soni A, Chandel S, Hemrajani M. Routing Attacks in Wireless Sensor Networks: A Survey. arXiv [Internet]. 2014 [cited 2025]; Available from: https://arxiv.org/abs/1407.3987
[8] "Security in Wireless Sensor Networks: A Cryptography Performance Study." MDPI [Internet]. [cited 2025]. Available from: https://www.mdpi.com/1999-5903/14/5/145
[9] "Energy efficiency of encryption schemes applied to wireless sensor networks." ResearchGate [Internet]. [cited 2025]. Available from: https://www.researchgate.net/publication/260408437_Energy_efficiency_of_encryption_schemes_applied_to_wireless_sensor_networks
[10] "Two-phase hybrid cryptography algorithm for wireless …" ScienceDirect [Internet]. [cited 2025]. Available from: https://www.sciencedirect.com/science/article/pii/S2314717215000616
[11] "Energy Proficient Hybrid Secure Scheme for Wireless Sensor …" ACM [Internet]. [cited 2025]. Available from: https://dl.acm.org/doi/abs/10.1007/s11277-020-07895-x
[12] Chang Q et al. Low power IoT device communication through hybrid AES … PMC [Internet]. 2025 [cited 2025]; Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC12032356/
[13] Mahlake N et al. A Hybrid Algorithm to Enhance Wireless Sensor Networks. arXiv [Internet]. 2023 [cited 2025]; Available from: https://arxiv.org/pdf/2303.14445

[14] Perrig A, Szewczyk R, Tygar JD, Wen V, Culler D. SPINS: Security protocols for sensor networks. *Wireless Networks.* 2002;8(5):521–34.
[15] Karlof C, Sastry N, Wagner D. TinySec: A link layer security architecture for wireless sensor networks. *Proc SenSys.* 2004;162–75.
[16] Zhu S, Setia S, Jajodia S. LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Trans Sensor Netw.* 2006;2(4):500–28.
[17] Khah SA, Vahed R, Alibeygi S. A dynamic and multi-level key management method in homogeneous WSNs. *Comput Netw.* 2023;232:109917.
[18] Yusuf T. Analysis of key management schemes for centralized and distributed WSNs. *Gadau J Pure Appl Sci.* 2024;9(2):25–34.
[19] Soto-Cruz J, Bhardwaj R, Patel V. A survey of efficient lightweight cryptography for power-constrained devices. *Technologies.* 2024;13(1):3.
[20] Urooj S, Rehman M, Iqbal A, Hussain M. Cryptographic data security for reliable wireless sensor networks. *Ain Shams Eng J.* 2023;14(6):101985.
[21] Mahlake N, Ngcobo N, Manamela B. A hybrid algorithm to enhance wireless sensor networks using combined symmetric and WSN-specific protocols. *arXiv preprint.* 2023; arXiv:2303.14445.
[22] Selvi P, Kumar S, Ramachandran R. SymECCipher: A hybrid ECC-AES framework for secure and efficient IoT healthcare. *Sci Rep.* 2025;15(1): Article 18345.

## BIOGRAPHIES OF AUTHORS

| | |
|---|---|
| Author 1 picture | **Abdullah Ali Hamza Raji** is a graduate of the College of Information Technology, Software Department, University of Babylon. He earned a master's degree from Imam Reza University in Mashhad, where he studied in the Computer Engineering Department.<br><br>Abdullah currently works as a computer science teacher at a school in Babylon, Iraq. |