Educational Administration: Theory and Practice
2021, 27(3), 1214-1222
ISSN: 2148-2403
https://kuey.net/

Research Article

A Review on Cryptographic Techniques for Secure Wireless Sensor Networks

Mrs. Zalak Bijalkumar Modi*

*Lecturer, EC Department, Government Polytechnic Gandhinagar zpmodi@gmail.com

Citation: Mrs. Zalak Bijalkumar Modi* (2021). A Review on Cryptographic Techniques for Secure Wireless Sensor Networks, *Educational Administration: Theory and Practice*, 27(3) 1214-1222
Doi: 10.53555/kuey.v27i3.11345

ARTICLE INFO

ABSTRACT

Wireless Sensor Networks (WSNs) are increasingly deployed in critical applications such as environmental monitoring, healthcare, industrial automation, and military surveillance. Due to their distributed architecture and resource-constrained nodes, WSNs are highly vulnerable to security threats including eavesdropping, data tampering, replay attacks, and unauthorized access. Cryptographic techniques play a crucial role in protecting data confidentiality, integrity, authentication, and non-repudiation. This paper provides a comprehensive review of symmetric, asymmetric, and hybrid cryptography methods applied to WSNs, highlighting their advantages, limitations, and suitability for different network scenarios. Symmetric algorithms offer fast and energy-efficient encryption but face challenges in key management, while asymmetric methods ensure secure key distribution with higher computational costs. Hybrid approaches combine the strengths of both, providing balanced security and efficiency. The study also identifies existing research gaps, including the need for optimized hybrid schemes for resource-constrained environments and real-time applications. The insights presented can guide the design and implementation of secure and efficient WSNs.

Keywords:
Wireless Sensor Networks (WSNs), Symmetric Key Cryptography, Asymmetric Key Cryptography, Hybrid Cryptography, Data Security

1. Overview

Wireless Sensor Networks (WSNs) are widely deployed for applications such as environmental monitoring, healthcare, industrial automation, and military surveillance. Their distributed architecture and limited computational resources make them vulnerable to security threats including eavesdropping, data tampering, replay attacks, and unauthorized access. To safeguard these networks, cryptographic techniques are essential to ensure confidentiality, integrity, authentication, and non-repudiation (Faquih, Kadam, & Saquib, 2015).

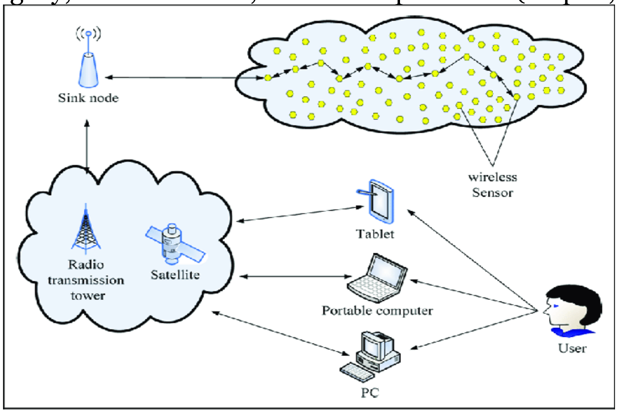


Figure 1: Structure of wireless sensor network
Source: https://www.researchgate.net/figure/Structure-of-wireless-sensor-network_fig1_316325422

Symmetric key cryptography is popular in WSNs due to its computational efficiency and low energy consumption. In symmetric encryption, the same key K is used for both encryption and decryption:

C = EK(P), P = DK(C) (1)

where PPP is the plaintext, C is the ciphertext, EK is the encryption function, and DK is the decryption function (Mallick & Bhatia, 2021). However, symmetric algorithms face challenges in secure key distribution and management, especially in large-scale networks.

Asymmetric cryptography, such as Elliptic Curve Cryptography (ECC), offers secure key distribution and digital signatures. ECC is based on the algebraic structure of elliptic curves over finite fields. For a curve defined as y2=x3+ax+b mod p, the public key Q is generated as:

Q = k·G (2)

where k is the private key and G is a predefined generator point on the curve. ECC provides strong security with smaller key sizes, making it energy-efficient compared to traditional RSA in WSNs (Tripathy, Pradhan, Nayak, & Tripathy, 2021).

Hybrid cryptography, which combines symmetric and asymmetric methods, is increasingly applied in WSNs to leverage the benefits of both. For instance, a session key Ks can be generated and exchanged using ECC, while actual message encryption uses a symmetric algorithm (e.g., AES):

C = EKs(P), Ks = fECC (private,public) (3)

This approach ensures strong confidentiality, integrity, and authentication without imposing heavy computational or energy overhead (Rizk & Alkady, 2015). Studies have shown that two-phase hybrid encryption, where data is first encrypted with a symmetric algorithm and then additional verification is applied using asymmetric methods, significantly improves security while maintaining network efficiency.

Overall, cryptographic techniques in WSNs must balance security and resource constraints. Symmetric algorithms provide fast processing, asymmetric algorithms ensure secure key management, and hybrid cryptography integrates the advantages of both, offering optimal security for sensitive and critical applications.

1.1 Aim and objectives

The primary aim of this study is to review and analyze cryptographic techniques for securing Wireless Sensor Networks (WSNs), with a focus on evaluating the efficiency, security, and applicability of symmetric, asymmetric, and hybrid cryptography methods in resource-constrained environments.

Objectives:

1. To examine the role of symmetric key cryptography in ensuring confidentiality and energy-efficient data encryption in WSNs.
2. To explore asymmetric cryptography methods, such as RSA and Elliptic Curve Cryptography (ECC), for secure key management, authentication, and digital signatures.
3. To assess hybrid cryptography approaches that integrate symmetric and asymmetric methods for enhanced security and reduced computational overhead.
4. To identify challenges, limitations, and research gaps in current cryptographic implementations for WSNs.
5. To provide recommendations for selecting and implementing cryptographic techniques based on network requirements, energy constraints, and security needs.

2. Review of literature

Abdullah, Houssein, and Zayed (2018) proposed a hybrid cryptography protocol for WSNs to address vulnerabilities in routing protocols. The objective was to combine symmetric and asymmetric encryption for secure data transmission in critical infrastructure. Findings showed improved protection against common attacks with efficient communication. Ahmad, Beg, and Abbas (2010) introduced an energy-saving secure framework for WSNs using elliptic curve cryptography. The goal was to reduce energy consumption while maintaining data security in mobile ad-hoc networks. Results demonstrated lower energy usage and enhanced cryptographic protection.

Alkady, Habib, and Rizk (2013) developed a hybrid cryptography protocol for WSNs to ensure integrity, confidentiality, and authentication. The scope included sensitive sensor network environments. Findings indicated superior computational performance and smaller ciphertext sizes compared to traditional methods. Bokhari and Shallal (2016) reviewed symmetric key encryption techniques to identify their strengths and limitations. The scope included general computing and network security. Findings suggested that algorithm choice depends on application requirements and resource constraints.

Dubai, Mahesh, and Ghosh (2011) designed a hybrid cryptography algorithm to enhance network security by combining symmetric and asymmetric techniques. The scope covered general computer networks. Results highlighted improved security with minimal computational overhead. Faquih, Kadam, and Saquib (2015) surveyed cryptographic techniques for WSNs, including ECC, PBC, and IBC. The scope focused on remote and complex environments. Findings emphasized that combining multiple cryptographic methods is essential for security and efficiency.

Frunza and Scripcariu (2007) optimized the RSA algorithm for wireless networks to improve security and processing speed. The scope included second-generation networks and Bluetooth devices. Results showed increased security and computational efficiency. Hossain, Islam, Das, and Nashiry (2012) analyzed MD4 and MD5 hashing algorithms to identify vulnerabilities. The scope included security-critical applications. Findings revealed weaknesses in these algorithms, highlighting the need for stronger hashing methods.

Kanatt, Jadhav, and Talwar (2020) reviewed cloud security using hybrid cryptography to ensure confidentiality, integrity, and authentication. Findings indicated that hybrid approaches offer higher security than single-method implementations. Khan and Khiyal (2017) proposed a two-layer security method combining cryptography and steganography to enhance data confidentiality and integrity. Findings showed that layered protection is stronger than using either method alone.

Kumar, Chand, and Kumar (2019) analyzed WSN authentication protocols in coal mines to improve safety monitoring. Findings demonstrated strengthened authentication and mitigated attacks. Mallick and Bhatia (2021) compared cryptography algorithms in WSNs to evaluate performance and security. Findings concluded that selecting suitable algorithms is key for balancing security and resource efficiency.

Panda (2014) reviewed WSN cryptographic techniques to highlight challenges and solutions. Findings stressed the importance of choosing suitable methods based on network constraints and threat models. Rizk and Alkady (2015) developed a two-phase hybrid cryptography algorithm for WSNs. Testing showed better security and lower processing overhead than traditional techniques.

Sasi and Sivanandam (2015) surveyed optimized cryptography algorithms for WSNs to balance security and performance. Findings revealed improved security with reduced computational load. Shallal and Bokhari (2016) reviewed symmetric key encryption techniques, reiterating that careful selection is needed based on network requirements.

Singh and Chauhan (2017) compared cryptographic algorithms in WSNs to evaluate security and resource utilization. Findings highlighted trade-offs between security and computational efficiency. Sklavos (2014) reviewed Stallings' book on cryptography, confirming it as a comprehensive resource for understanding network security principles and applications.

Tripathy, Pradhan, Nayak, and Tripathy (2021) proposed a hybrid cryptography model for WSNs to enhance confidentiality, integrity, and authentication. Findings showed hybrid approaches outperform single-technique methods in both security and efficiency. Yadav and Bondre (2021) introduced a hybrid cryptography approach for secure computing environments. Using multiple cryptographic primitives, the method improved confidentiality, integrity, and authentication while reducing encryption and decryption time.

2.1 Research gap

Despite significant advances in cryptography for wireless sensor networks, several gaps remain in current research. Most studies focus on either symmetric or asymmetric encryption, or propose hybrid approaches, but few systematically compare hybrid methods against single-method algorithms across multiple performance metrics such as energy consumption, encryption and decryption time, and throughput. Additionally, there is limited optimization of hybrid cryptography for resource-constrained environments, including low-power, memory-limited sensor nodes, to balance security strength with computational cost and latency. Research on real-time or safety-critical applications remains scarce, and the integration of hybrid cryptography with emerging technologies such as IoT platforms, edge computing, and cloud-connected networks is underexplored. Moreover, rigorous vulnerability assessments under various attack models are rarely conducted, and standardized guidelines for selecting and implementing hybrid cryptography algorithms based on network requirements are lacking. Finally, comprehensive multi-metric evaluations that consider energy efficiency, throughput, latency, memory usage, scalability, and attack resilience are limited, highlighting the need for a holistic approach to designing, testing, and deploying hybrid cryptographic solutions in wireless sensor networks.

3. Importance of Security

Wireless sensor networks (WSNs) are specialized networks with distinctive characteristics that differentiate them from conventional computer networks. They are deployed in environments such as critical infrastructure, industrial monitoring, and remote areas, where data security is paramount. Security mechanisms in WSNs are essential to protect sensitive information from attacks, unauthorized access, and network failures.

Confidentiality ensures that information transmitted across the network is accessible only to authorized nodes. Studies have shown that hybrid cryptography approaches, which combine symmetric and asymmetric encryption, enhance confidentiality while minimizing processing overhead and simplifying key management (Abdullah, Houssein, & Zayed, 2018; Dubai, Mahesh, & Ghosh, 2011).

Authentication allows nodes to verify the legitimacy of communicating parties. Hybrid techniques, such as integrating Elliptic Curve Cryptography with RSA-based methods, strengthen authentication by ensuring that only trusted nodes can access or modify the data (Frunza & Scripcariu, 2007). Integrity guarantees that transmitted data remains unaltered during communication. Cryptographic mechanisms, such as message

digests and digital signatures, provide verification that data originates from a trusted source and is protected from tampering (Panda, 2014).
Availability ensures that legitimate users can access network resources even in the presence of faults, attacks, or resource limitations. Energy-efficient frameworks maintain high availability while minimizing resource consumption (Abdullah, Houssein, & Zayed, 2018). Non-repudiation ensures that nodes cannot deny sending or receiving information, which is critical for accountability in industrial and monitoring applications. Freshness confirms that received data is recent and not a replay of old messages, which is particularly important for real-time monitoring.

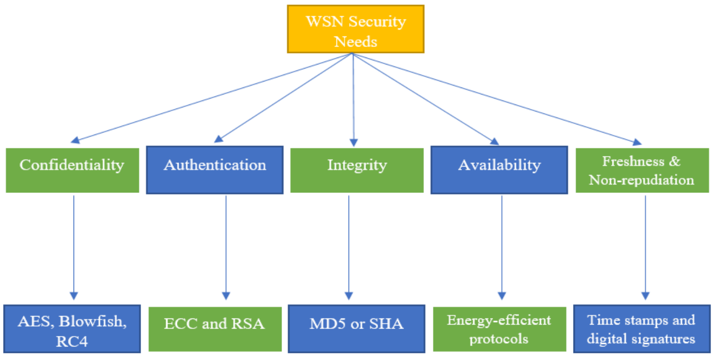


Figure 2: WSN Security Needs
Source: Made in Ms. Word

Research indicates that hybrid cryptography approaches provide a balanced solution for WSNs, offering high security, reduced computational load, and efficient data transmission. Hybrid protocols have been found to outperform traditional single-method cryptographic techniques in terms of security, computational efficiency, and scalability (Dubai, Mahesh, & Ghosh, 2011; Frunza & Scripcariu, 2007).

4. Encryption Methods

Wireless sensor networks (WSNs) are widely deployed in critical and remote environments such as industrial monitoring, healthcare, and smart infrastructure. These networks transmit sensitive data over wireless channels, making them vulnerable to attacks like eavesdropping, data tampering, and unauthorized access. Ensuring secure communication is therefore a fundamental requirement for WSNs (Abdullah, Houssein, & Zayed, 2018). Cryptographic techniques are central to WSN security. They convert sensitive data into encrypted formats, preventing unauthorized access while ensuring secure transmission. The design of cryptographic solutions in WSNs must balance strong security with limited computational resources, energy constraints, and network scalability (Panda, 2014).

Symmetric Key Cryptography

Symmetric key algorithms use a single shared key for both encryption and decryption. This approach is computationally efficient and suitable for resource-constrained WSN nodes. However, key distribution and management are challenging in large-scale networks or when new nodes join the network. Preloaded keys or Key Distribution Centers (KDC) can facilitate secure key exchange but may increase network overhead (Ahmad, Beg, & Abbas, 2010). Symmetric cryptography is ideal for rapid encryption of data in small to medium-scale networks.

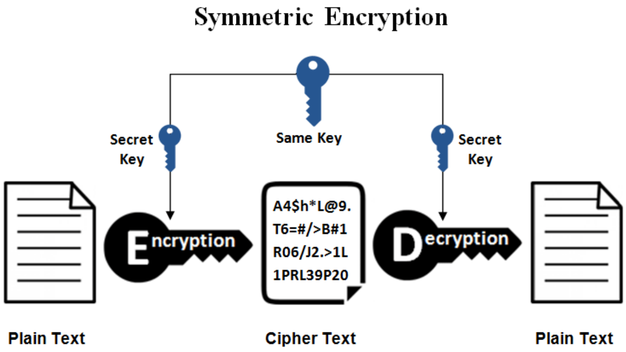


Figure 3: Symmetric-key encryption

Source: researchgate.net/publication/333376273_StegoCrypt_Arithmetic_and_Rudin-Shapiro_Sequence-Based_Bit-Cycling_and_3DES?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6Il9kaXJlY3QifX0

Asymmetric Key Cryptography

Asymmetric cryptography relies on a pair of keys a public key for encryption and a private key for decryption. This method simplifies key management since the public key can be openly shared. Algorithms such as RSA provide strong security, enabling secure message exchange and digital signatures (Frunza & Scripcariu, 2007). While robust, asymmetric methods are computationally intensive, which can strain sensor nodes with limited energy and processing power.

Elliptic Curve Cryptography (ECC)

ECC is a public-key cryptography approach based on the algebraic structure of elliptic curves. It achieves high security with smaller key sizes, reducing memory usage and energy requirements (Ahmad, Beg, & Abbas, 2010). ECC operations rely on the elliptic curve equation:

y2 = x3 + ax + b (4)

ECC is particularly suited for WSNs due to its low computational overhead and strong security properties. Frameworks such as TinyECC provide efficient tools for implementing ECC-based operations in sensor networks.

Hybrid Cryptography

Hybrid cryptography combines symmetric and asymmetric methods to leverage the strengths of both. Typically, asymmetric cryptography handles secure key exchange, while symmetric algorithms manage bulk data encryption. This approach offers confidentiality, integrity, authentication, and non-repudiation without significantly increasing energy consumption (Yadav & Bondre, 2021; Alkady, Habib, & Rizk, 2013). Hybrid methods are particularly effective for large or security-critical WSN deployments, providing a balanced solution for modern network requirements.

The choice of cryptographic technique depends on the WSN's size, energy availability, and security requirements. Symmetric algorithms provide efficiency, asymmetric algorithms ensure robust key management, ECC offers strong security with minimal overhead, and hybrid cryptography achieves a balanced and flexible solution. Proper implementation of these techniques allows WSNs to maintain secure and reliable communication in energy-constrained and hostile environments (Abdullah, Houssein, & Zayed, 2018).

Table 1: Cryptographic techniques for WSNs

Cryptography Type	Key Concept	Advantages	Disadvantages	Applicable WSN Scenario	Reference
Symmetric Key	Single shared key for encryption & decryption	Computationally efficient; Low energy consumption	Key distribution difficult in large networks; Not scalable	Small to medium-scale WSNs with preloaded keys	Ahmad, Beg, & Abbas (2010)
Asymmetric Key	Pair of keys: public for encryption, private for decryption	Simplifies key management; Supports digital signatures	High computational cost; Energy intensive	WSNs requiring secure key exchange; Critical data	Frunza & Scripcariu (2007)
Elliptic Curve Cryptography (ECC)	Public-key system based on elliptic curves ($y^2 = x^3 + ax + b$)	High security with small key size; Low memory & energy requirements	More complex mathematics; Implementation can be difficult	WSNs with constrained resources but need strong security	Ahmad, Beg, & Abbas (2010)
Hybrid Cryptography	Combines symmetric and asymmetric methods	Balances efficiency and security; Supports confidentiality, integrity, authentication, non-repudiation	Slightly more complex implementation	Large-scale or security-critical WSN deployments	Yadav & Bondre (2021); Alkady, Habib, & Rizk (2013)

5. Development of Asymmetric Key Encryption

Wireless sensor networks (WSNs) require robust encryption methods to ensure secure communication, particularly when transmitting sensitive data over open wireless channels. Asymmetric key encryption has evolved as a pivotal solution for providing secure key management and authentication in WSNs. Unlike symmetric encryption, which relies on a single shared key, asymmetric methods use a pair of keys a public key for encryption and a private key for decryption reducing the risk of key compromise during transmission (Bokhari & Shallal, 2016).

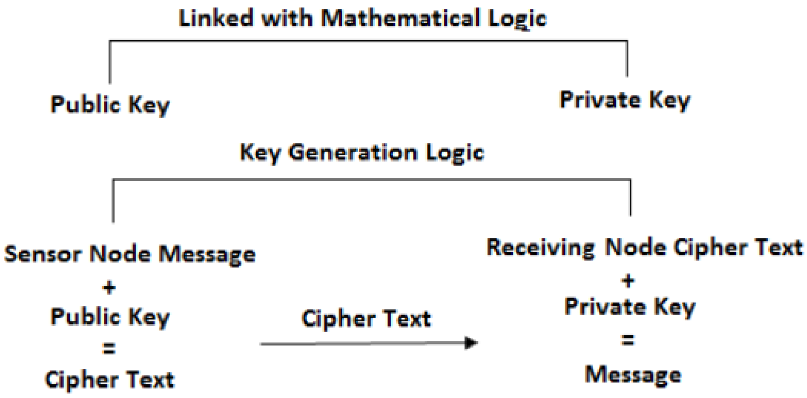


Figure 4: Design of Asymmetric key cryptography

Source: https://jier.co.in/download/v5i2/4.%20Dinesh%20Gupta%20%20%20pp%2017-%2020.pdf

Early cryptanalysis of hashing and message digest algorithms like MD4 and MD5 highlighted vulnerabilities in data integrity verification, emphasizing the need for stronger asymmetric solutions in secure networks (Hossain, Islam, Das, & Nashiry, 2012). These weaknesses prompted the development of advanced protocols that combine encryption with digital signatures, ensuring authenticity and integrity.

Later studies focused on improving authentication protocols specifically for WSN applications, such as safety monitoring in hazardous environments. Researchers developed enhanced asymmetric algorithms to prevent attacks like replay, impersonation, and unauthorized data modification, while optimizing computational efficiency for resource-constrained sensor nodes (Kumar, Chand, & Kumar, 2019).

Comparative surveys of cryptographic algorithms further demonstrated that asymmetric encryption, particularly when integrated with hybrid approaches, provides better security guarantees for key distribution and authentication compared to standalone symmetric methods. These analyses also revealed trade-offs in computational load and energy consumption, highlighting the importance of choosing algorithms suited to the network's scale and operational constraints (Singh & Chauhan, 2017).

The development trajectory of asymmetric key encryption in WSNs reflects a trend toward hybridized approaches, balancing security, efficiency, and scalability. Modern implementations increasingly combine asymmetric key exchange for secure session initiation with symmetric encryption for high-speed data transfer, offering both strong security and low computational overhead suitable for sensor networks.

Table 2: Asymmetric Cryptography (RSA vs ECC)
Source: EnergyPaper.pdf

Metric	RSA-1024	ECC-160	Unit	Notes / Source
Handshake Payload (Client)	490	138	bytes	RSA needs larger key/cert payloads for handshake
Handshake Payload (Server)	314	138	bytes	Server also sends more payload in RSA handshake
Client Energy Consumption (Handshake)	397.7	93.7	mJ	Total handshake energy on client node
Server Energy Consumption (Handshake)	390.3	93.9	mJ	Total handshake energy on server node
Number of Handshakes (30 mAh battery @ 5% energy)	~41	~173	count	How many handshakes possible from limited battery

Figure 5: Handshake Payload Comparison

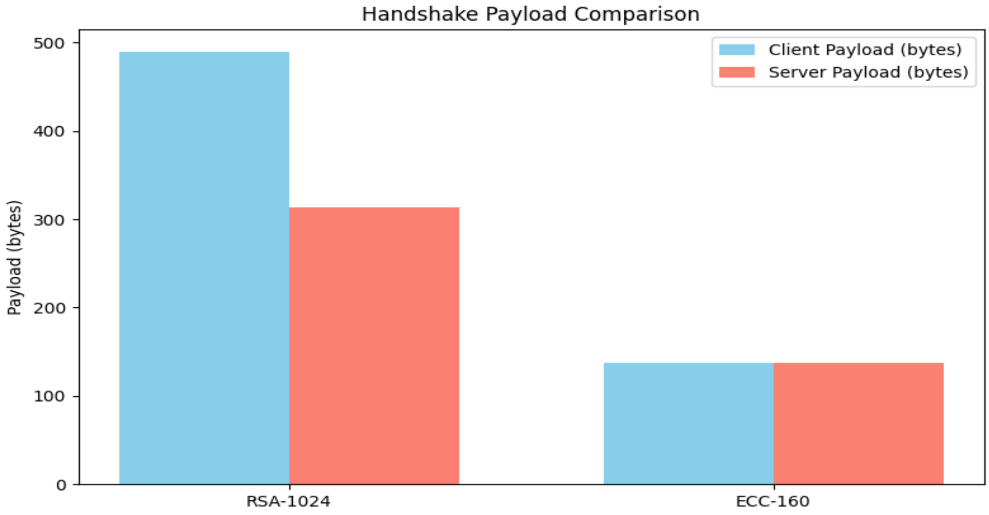


Figure 6: Energy Consumption per Handshake

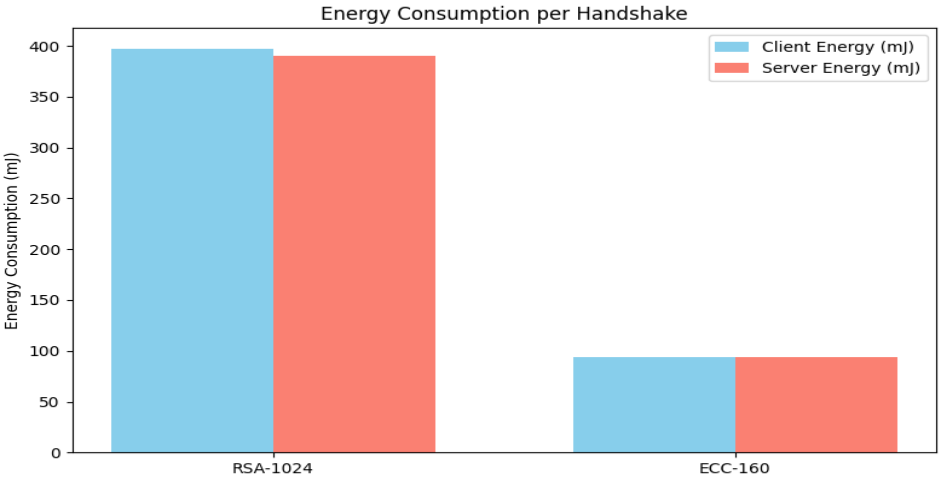
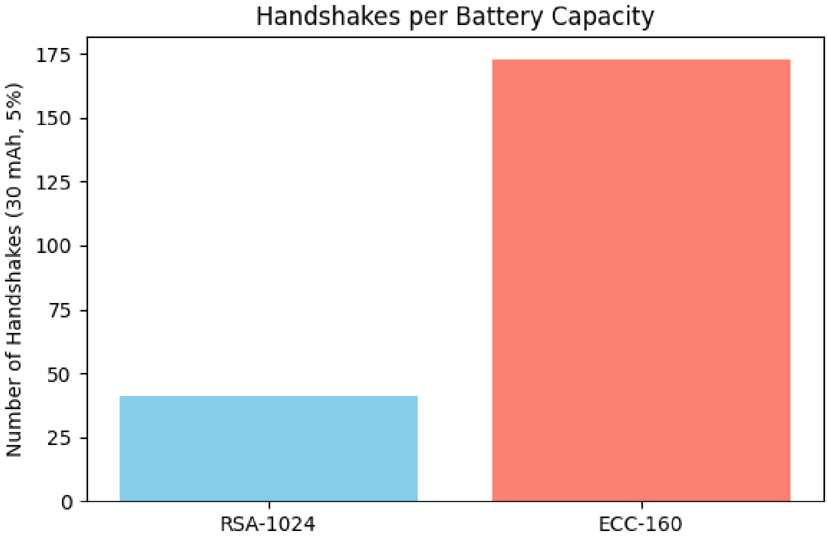


Figure 7: Handshakes per Battery



The table clearly shows that ECC-160 is significantly more efficient than RSA-1024 in wireless sensor networks. ECC requires much smaller handshake payloads for both client and server, reducing data transmission overhead. Energy consumption during handshakes is also drastically lower for ECC, with client and server nodes using less than a quarter of the energy required by RSA. Consequently, the number of handshakes supported by a limited battery is much higher with ECC, making it a more suitable choice for energy-constrained WSN deployments where efficiency and longevity are critical.

6. Combined Cryptographic Approaches

Combined or hybrid cryptographic approaches integrate multiple encryption techniques to maximize security and efficiency in networks. In such systems, asymmetric cryptography (like RSA or ECC) is typically used to securely exchange keys, while symmetric cryptography (like AES) is applied for encrypting bulk data. This combination ensures that the network achieves confidentiality, integrity, authentication, and non-repudiation while keeping computational overhead low.

In cloud storage, hybrid cryptography is used to protect sensitive files while enabling secure access and sharing among authorized users. Asymmetric keys handle key distribution securely, whereas symmetric keys provide fast encryption for large files, optimizing both security and performance (Kanatt, Jadhav, & Talwar, 2020).

In wireless sensor networks (WSNs), hybrid methods can be further enhanced with optimization algorithms. These algorithms dynamically adjust encryption parameters, such as key size and algorithm selection, based on network constraints like node energy, processing capacity, and communication bandwidth. This ensures secure and efficient communication without overburdening resource-limited sensor nodes (Sasi & Sivanandam, 2015).

Overall, combined cryptographic approaches offer a balanced solution for modern distributed systems, providing high security, energy efficiency, and adaptability to diverse deployment scenarios.

7. Summary and Insights

Wireless Sensor Networks (WSNs) are increasingly deployed in critical applications such as environmental monitoring, healthcare, industrial automation, and military surveillance. Their distributed architecture and resource-constrained nodes make them particularly vulnerable to security threats, including eavesdropping, data tampering, replay attacks, and unauthorized access. To address these challenges, symmetric key cryptography has been widely used due to its computational efficiency and low energy consumption. In this method, a single secret key is shared between nodes for both encryption and decryption of messages, enabling fast and energy-efficient data protection. However, symmetric algorithms face challenges in large-scale networks, especially regarding secure key distribution and management, which can limit scalability and robustness (Shallal & Bokhari, 2016).

To overcome these limitations, hybrid or combined cryptographic approaches have gained attention. These methods integrate symmetric encryption with other security techniques, such as asymmetric cryptography or steganography, to enhance overall network security. For example, one layer may use symmetric encryption for high-speed bulk data protection, while an additional layer provides secure key exchange or hides sensitive information within multimedia files. This two-layer approach improves confidentiality, integrity, and authentication without imposing excessive computational or energy overhead on sensor nodes (Khan & Khiyal, 2017).

Overall, the choice of cryptographic strategy in WSNs must balance efficiency, energy consumption, and security strength. Symmetric key methods offer rapid encryption suitable for constrained environments, while layered or hybrid approaches provide additional protection against sophisticated attacks. Implementing adaptive and combined techniques ensures that WSNs can securely transmit sensitive data in hostile or resource-limited environments while maintaining network performance and reliability (Shallal & Bokhari, 2016; Khan & Khiyal, 2017).

References

1. Faquih, A., Kadam, P., & Saquib, Z. U. (2015). Cryptographic techniques for wireless sensor networks: A survey. In Proceedings of the 2015 IEEE Bombay Section Symposium (IBSS) (pp. xx–xx). IEEE. https://doi.org/10.1109/IBSS.2015.7456652
2. Mallick, B. B., & Bhatia, A. (2021, July). Comparative analysis of impact of cryptography algorithms on wireless sensor networks. arXiv. https://doi.org/10.48550/arXiv.2107.01810
3. Tripathy, A., Pradhan, S. K., Nayak, A. K., & Tripathy, A. R. (2021). Hybrid cryptography for data security in wireless sensor network. In Data engineering and intelligent computing (Advances in Intelligent Systems and Computing, Vol. 1407, pp. 597–606).
4. Rizk, R., & Alkady, Y. (2015). Two-phase hybrid cryptography algorithm for wireless sensor networks. Journal of Electrical Systems and Information Technology, 2(3), 296–313. https://doi.org/10.1016/j.jesit.2015.11.005
5. Abdullah, K. M., Houssein, E. H., & Zayed, H. H. (2018). New security protocol using hybrid cryptography algorithm for WSN. In Proceedings of the 1st International Conference on Computer Applications & Information Security (ICCAIS 2018) (pp. xx–xx). IEEE. https://doi.org/10.1109/CAIS.2018.8442003

6. Dubai, M. J., Mahesh, T. R., & Ghosh, P. A. (2011). Design of new security algorithm: Using hybrid cryptography architecture. In Proceedings of the 3rd International Conference on Electronics Computer Technology (ICECT 2011) (pp. xx–xx). IEEE. https://doi.org/10.1109/ICECTECH.2011.5941965
7. Frunza, M., & Scripcariu, L. (2007). Improved RSA encryption algorithm for increased security of wireless networks. In Proceedings of the International Symposium on Signals, Circuits and Systems (ISSCS 2007) (pp. xx–xx). IEEE. https://doi.org/10.1109/ISSCS.2007.4292737
8. Panda, M. (2014). Security in wireless sensor networks using cryptographic techniques. American Journal of Engineering Research (AJER), 3(1), 50–56.
9. Yadav, U., & Bondre, S. (2021). Hybrid cryptography approach to secure the data in computing environment. In Proceedings of the 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC 2021) (pp. xx–xx). IEEE. https://doi.org/10.1109/ICSCCC51823.2021.9478088
10. Alkady, Y., Habib, M. I., & Rizk, R. Y. (2013). A new security protocol using hybrid cryptography algorithms. In Proceedings of the 9th International Computer Engineering Conference (ICENCO 2013) (pp. xx–xx). IEEE. https://doi.org/10.1109/ICENCO.2013.6736485
11. Ahmad, S., Beg, M. R., & Abbas, Q. (2010). Energy saving secure framework for sensor network using elliptic curve cryptography. International Journal of Computer Applications (IJCA), Special Issue on Mobile Ad-hoc Networks (MANETs), 167.
12. Sklavos, N. (2014). Book review: Cryptography and network security: Principles and practice (6th ed.), by W. Stallings. Journal of Information Security and Applications, 19(1), 49–50. https://doi.org/10.1080/19393555.2014.900834
13. Hossain, M. A., Islam, M. K., Das, S. K., & Nashiry, M. A. (2012). Cryptanalyzing of message digest algorithms MD4 and MD5. International Journal on Cryptography and Information Security (IJCIS), 2(1), 1–10. https://doi.org/10.5121/ijcis.2012.2101
14. Kumar, D., Chand, S., & Kumar, B. (2019). Cryptanalysis and improvement of an authentication protocol for wireless sensor networks applications like safety monitoring in coal mines. Journal of Ambient Intelligence and Humanized Computing, 10, 641–660. https://doi.org/10.1007/s12652-018-0712-8
15. Singh, P., & Chauhan, R. K. (2017). A survey on comparisons of cryptographic algorithms using certain parameters in WSN. International Journal of Electrical and Computer Engineering (IJECE), 7(4), 2232–2240. https://doi.org/10.11591/ijece.v7i4.pp2232-2240
16. Bokhari, M. U., & Shallal, Q. M. (2016). A review on symmetric key encryption techniques in cryptography. International Journal of Computer Applications, 147(10), 43–47.
17. Kanatt, S., Jadhav, A., & Talwar, P. (2020). Review of secure file storage on cloud using hybrid cryptography. International Journal of Engineering Research & Technology.
18. Sasi, S. B., & Sivanandam, N. (2015). A survey on cryptography using optimization algorithms in WSNs. Indian Journal of Science and Technology, 8(3). https://doi.org/10.17485/ijst/2015/v8i3/59585
19. Shallal, Q. M., & Bokhari, M. U. (2016). A review on symmetric key encryption techniques in cryptography. International Journal of Computer Applications, 147(10), 43–47.
20. Khan, S., & Khiyal, M. S. H. (2017). A novel two layer of security by using cryptography along with steganography.