Exploring Cryptographic Techniques for Data security in Resource-Constrained Wireless Sensor Networks:Performance Evaluation and Considerations

Abstract—**Wireless sensor networks (WSNs) play a crucial role in environmental monitoring and data collection. However, ensuring data security in WSNs poses challenges due to the vulnerabilities of wireless communication channels. In this paper, we address this concern by exploring the application of cryptographic techniques to enhance data security in WSNs. Considering the limited sensor power, computing power, and storage resources, we propose a novel approach that evaluates the suitability of symmetric and asymmetric cryptographic algorithms in WSNs. Through performance comparisons based on computation power and storage capacity requirements, we identify key insights for selecting appropriate encryption algorithms in WSNs. Our findings emphasize the importance of considering the specific requirements and constraints of WSN applications, highlighting the efficiency of symmetric key-based encryption algorithms in resource-constrained environments and the stronger security and key distribution mechanisms provided by ECC-based asymmetric encryption algorithms for secure communication among multiple nodes. This research contributes to the existing knowledge by offering an effective solution to enhance data security in WSNs while considering computational and storage limitations**

Index Terms—**Cryptographic techniques, Wireless sensor network, Data security, Encryption algorithms**

I. Introduction

Wireless sensor networks (WSNs) have become increasingly popular in recent years due to their ability to monitor and collect data from remote and harsh environments. WSNs are composed of a large number of small sensor nodes that communicate with each other and a base station to transmit data. However, the open and wireless nature of WSNs makes them vulnerable to malicious attacks that can compromise data confidentiality, integrity, and availability.

To address the security challenges in WSNs, cryptographic techniques have been widely used to provide secure communication and data protection. Cryptography is the science of securing communication through the use of mathematical algorithms that encode and decode data. However, selecting the appropriate cryptographic technique for WSNs is challenging due to the limited resources available in sensor nodes, such as computing power, storage capacity, and battery life.

In this paper, we explore the application of cryptographic techniques in WSNs to enhance data security. We focus on comparing the suitability of two cryptographic techniques, symmetric and asymmetric encryption, in WSNs. Symmetric encryption uses the same key for both encryption and decryption, while asymmetric encryption uses a public and private key pair.

To evaluate the suitability of these cryptographic techniques, we analyze their computation power and storage capacity requirements in the context of WSNs.Our findings emphasize the significance of carefully considering the unique requirements and constraints of each WSN application when selecting the appropriate encryption technique for the better data security.

II. Related Work

Wireless sensor networks (WSNs) have been extensively studied in the research community due to their wide-ranging applications in various fields such as environmental monitoring, healthcare, and security. However, the open and wireless nature of WSNs makes them vulnerable to various types of attacks that can compromise the security of the network. To address these challenges, several cryptographic techniques have been proposed and applied to enhance the security of WSNs.

In [1], Li et al. proposed a symmetric key-based encryption algorithm that provides confidentiality and integrity for WSNs. Khodaei and Salmasizadeh [2] proposed an energy-efficient public key encryption scheme based on elliptic curve cryptography for WSNs. Other studies have also focused on the security issues of WSNs and proposed various cryptographic techniques to improve data confidentiality, integrity, and availability [3].

However, most of these studies focus on either symmetric or asymmetric encryption techniques, and there is a lack of comparative analysis of these techniques in the context of WSNs. Therefore, in this paper, we aim to address this gap in the literature by comparing the suitability and performance of symmetric and asymmetric encryption techniques in WSNs based on their computation power and storage capacity requirements.

Our proposed approach aims to contribute to the research community by providing a comparative analysis of symmetric and asymmetric encryption techniques that can assist researchers in selecting the appropriate encryption technique for their WSN application.

III. Literature Review

A. Wireless Sensor Network

Wireless Sensor Networks (WSNs) refer to interconnected sensor nodes that communicate wirelessly in order to gather environmental data [7]. Essentially, WSNs can be described as networks consisting of devices that transmit information collected from a monitored field through wireless connections. Wireless sensor networks (WSNs) are capable of analyzing a wide range of parameters such as temperature, humidity, vibrations, seismic activity, and various other factors [21].

The components of a Wireless Sensor Network (WSN) consist of sensors for capturing environmental variables and data acquisition [8]. The signals captured by the sensors are converted into electrical signals, which are then received by radio nodes and transmitted to a WLAN access point [8]. The radio nodes comprise a transducer, microcomputer, transceiver, and power supply [8]. The transducer generates electrical signals based on recognized physical phenomena, while the microcomputer processes and stores the sensor output [8]. The transceiver receives commands from a central computer and transmits the data to it, and each sensor node is powered by a battery [8].

The data and information are transmitted across multiple nodes, and a gateway is employed to connect the data to other networks, such as wireless Ethernet. These nodes, also referred to as sensor nodes, are compact, lightweight, and portable. They are linked to a central processing unit, known as the base station, within the WSN system as shown in Figure 1. The base station is connected to the internet to facilitate data sharing [7].

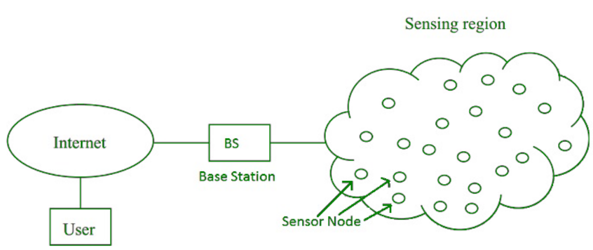

Fig. 1. Wireless Sensor Network.

The WLAN access point receives the data sent by the wireless radio nodes, typically over the Internet. Evaluation software is utilized to process the data received by the WLAN access point and present it to the user for further data processing. This software enables processing, analysis, storage, and retrieval of the collected data.

B. Security in wireless sensor network

The security of Wireless Sensor Networks (WSNs) is a significant concern due to the broadcast nature of the transmission medium and the absence of tamper-resistant hardware. It has been observed that WSNs are susceptible to various security attacks, allowing malicious nodes to infiltrate the network and mislead other nodes within it [9]. These attacks primarily target the privacy, control, and availability of the transmitted information. Given the large number of nodes in WSNs, implementing security measures at different levels can be complex.

a) Confidentiality: It is a crucial security requirement in Wireless Sensor Networks (WSNs) to protect sensitive data from unauthorized access and exposure to third parties. WSN applications often involve the transmission of critical data, making it essential to prevent leakage to neighboring networks [10].. Cryptographic keys can be used to encrypt communication and ensure confidentiality.

b) Authentication: It is essential in WSNs to verify the identity of participants in network communication. Each sensor node and base station should be able to confirm the legitimacy of transmitted and received data, preventing attackers from deceiving legitimate nodes with falsified information. Authentication can also be focused on clustering nodes, where groups are formed based on specific characteristics [10].

c) Integrityn: It is crucial to prevent information alteration during transmission over unsecured networks. Maintaining data integrity is essential, as the use of false information can have severe consequences. WSN systems need to ensure secure transmission without interception or tampering.

d) Availability: It ensures that data and information in WSNs remain accessible to authorized users. Risks such as node detection and denial-of-service attacks can compromise availability, impacting the performance of real-time WSN applications.

C. Obstacles of Sensor Security

Wireless Sensor Networks (WSNs) are known to have various limitations compared to traditional computer networks. These limitations pose challenges when applying existing security approaches directly to WSNs. Therefore, it is crucial to understand and address the specific constraints of WSNs in order to develop and implement suitable security mechanisms.

a) Limited resources: Wireless Sensor Networks (WSNs) face significant resource limitations compared to traditional computer networks. Sensor devices in WSNs have constrained memory and storage capacities, which must be taken into account when designing security mechanisms. To ensure an effective and strong security approach in WSNs, the size of security algorithm code should be limited to conserve space. Additionally, energy conservation is critical as sensor batteries cannot be replaced or recharged once deployed [11]. Optimizing power usage and employing efficient routing algorithms that utilize multiple hops become essential in WSNs to extend the sensor node's lifespan and reduce energy consumption.

b) Unreliable communication: Communication in WSNs is prone to unreliability due to various factors. Packet-based routing is often offline, making it susceptible to channel errors and congestion. As a result, data packets can be damaged or lost during transmission. Unreliable wireless communication channels can introduce corruption in packets, requiring significant efforts in error handling [12]. This unreliability poses a challenge in preserving critical security packets, including cryptographic keys. Furthermore, collisions among data packets during transmission can lead to conflicts and transmission failures, resulting in latency and additional processing time. The routing process in WSNs may also introduce delays, affecting overall system performance.

c) Unattended Operations: Sensor nodes in WSNs often remain unattended for extended periods, making them susceptible to physical attacks and damage. Deployed in open environments, WSNs are exposed to various threats, including tampering, theft, and unauthorized access. Remote management of sensor networks presents challenges in maintaining the physical security of nodes [12]. These factors necessitate the implementation of robust security measures to protect WSNs from both physical and network-based attacks.

IV. CRYPTOGRAPHY

Cryptography is crucial for ensuring data confidentiality and integrity in Wireless Sensor Networks (WSNs). It involves mathematical transformations to protect messages from unauthorized eavesdropping. However, applying traditional cryptographic techniques directly to WSNs is challenging due to their limited computing and storage capacity [14].

To address these challenges, researchers have developed lightweight cryptographic algorithms specifically tailored for WSNs, emphasizing efficiency and optimization. These modified techniques take into account the constraints of WSNs and strike a balance between security requirements and resource usage. By leveraging these lightweight cryptographic algorithms, WSNs can achieve their security objectives while efficiently utilizing their limited resources.

One approach in lightweight cryptography for WSNs is the use of symmetric key algorithms with reduced key sizes and optimized implementations to reduce computational overhead. These algorithms aim to minimize the energy consumption and memory requirements of cryptographic operations, making them suitable for resource-constrained WSNs. Examples of such algorithms include the Tiny Encryption Algorithm (TEA) and the Skipjack algorithm [22].

In addition to symmetric key algorithms, lightweight cryptographic techniques for WSNs often incorporate hash functions, authentication protocols, and encryption schemes specifically designed for resource-constrained environments. These techniques focus on minimizing computational complexity while still providing sufficient security measures. For example, the use of hash-based message authentication codes (HMAC) and elliptic curve cryptography (ECC) have shown promise in achieving efficient and secure communication in WSNs [23].

Ongoing research in the field continues to address implementation challenges and further enhance secure communication in resource-constrained environments. Researchers are exploring novel cryptographic algorithms, protocols, and architectures specifically designed to operate efficiently within the constraints of WSNs. They are also investigating lightweight authentication mechanisms and secure key management schemes tailored to WSNs.

One recent research paper that addresses the challenges of lightweight cryptography in WSNs is ”Lightweight Cryptography for Low-Cost RFID Systems” [24]. The paper proposes a lightweight cryptographic algorithm suitable for low-cost RFID systems, which share similar resource limitations with WSNs. The algorithm focuses on minimizing energy consumption and computational overhead while ensuring data security.

Another notable study in this area is ”Efficient Key Management for Secure Communication in Resource-Constrained Wireless Sensor Networks” by P. Kaur et al. [25]. The paper presents an efficient key management scheme specifically designed for resource-constrained WSNs. The scheme focuses on minimizing key storage and computational overhead while providing secure key distribution and revocation mechanisms.

A. Symmetric Cryptography

Symmetric cryptography, also known as symmetric encryption, involves the use of a private cryptographic key to encrypt and decrypt data [15]. It is a simple and efficient encryption method, suitable for mass encryption of large amounts of data, such as database encryption. However, symmetric encryption can cause performance issues and high CPU usage due to its impact on network resources.

B. Asymmetric Cryptography

Asymmetric cryptography, commonly known as public key cryptography, utilizes a key pair for encryption and decryption [16]. In this approach, the public key is shared openly, while the corresponding private key is kept confidential. With asymmetric cryptography, anyone can encrypt a message using the recipient’s public key, ensuring that only the intended recipient can decrypt it with their private key. This method provides secure communication and prevents unauthorized access to data packets.

These two cryptographic techniques, symmetric and asymmetric cryptography, offer different advantages and are applied in various scenarios to ensure data security in wireless sensor networks. In our study, we have evaluated two cryptographic techniques: a symmetric key-based encryption algorithm and an asymmetric encryption algorithm based on elliptic curve cryptography (ECC). The symmetric encryption algorithm provides confidentiality and integrity for the data transmitted in the network, while ECC provides digital signatures and public key encryption for secure communication.

V. EVALUATION

In this section, we present the evaluation of the two cryptographic techniques based on their computation power and storage capacity requirements. We have used two metrics for the evaluation: the number of CPU cycles required for encryption/decryption and the storage capacity required for the encryption keys.

A. Symmetric key algorithm (AES)

Symmetric key algorithm, such as the Advanced Encryption Standard (AES), is widely recognized for its efficiency and effectiveness in securing data. These algorithms use a single key for both encryption and decryption processes, making them computationally efficient. AES, in particular, has gained widespread adoption due to its strong security properties and efficient computation [17].

In terms of CPU cycle requirements, symmetric key algorithms like AES have low to moderate demands. This means that the encryption and decryption operations can be performed relatively quickly, making them suitable for real-time applications and resource-constrained environments. The efficiency of symmetric key algorithms stems from their symmetric nature, where the same key is used for both encryption and decryption, resulting in fewer computational steps compared to asymmetric algorithms.

Regarding storage capacity requirements, symmetric key algorithms typically have small to moderate needs for storing encryption keys. For example, AES commonly employs key sizes of 128, 192, or 256 bits [17]. These key sizes are relatively small compared to the actual data being encrypted, allowing for efficient storage and management of the encryption keys.

Symmetric key algorithms offer a favorable balance between efficiency and security. They require low to moderate CPU cycles for encryption and decryption operations, making them suitable for resource-constrained devices and applications. Additionally, the storage capacity required for encryption keys is small to moderate, facilitating effective key management.

B. ECC-Based Asymmetric algorithm

ECC-based asymmetric encryption algorithms, such as Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA), involve intricate mathematical computations on elliptic curves [18]. These computations typically require a moderate to high number of CPU cycles for encryption and decryption operations. ECC is known for its computational complexity compared to symmetric key algorithms. However, advancements in hardware and software optimizations, such as the use of specialized hardware accelerators and efficient algorithms, have significantly improved the efficiency of ECC-based algorithms [18]. These optimizations help reduce the CPU cycle requirements and make ECC more feasible for resource-constrained environments.

ECC-based algorithms require moderate to high storage capacity for encryption keys. ECC employs longer key sizes, such as 256 or 521 bits, to achieve equivalent security levels to longer key sizes in symmetric algorithms [19]. The longer key sizes are necessary to provide the same level of security as symmetric algorithms with shorter key sizes. As a result, ECC-based encryption keys have larger storage requirements compared to symmetric key algorithms. The increased key sizes in ECC contribute to the additional storage capacity needed to store and manage the encryption keys.

Despite the higher CPU cycle requirements and storage capacity demands, ECC-based algorithms offer distinct advantages. ECC provides robust security with smaller key sizes compared to traditional asymmetric algorithms like RSA. This makes ECC particularly attractive for resource-constrained devices where memory and computation power are limited. Furthermore, ECC-based algorithms offer efficient key exchange and digital signature operations, making them suitable for secure communication and authentication in constrained environments.

VI. Results and Discussion

The symmetric key-based encryption algorithm offers several strengths, including its efficiency, low computational requirements, and smaller key sizes [20]. These characteristics make it well-suited for WSN applications with limited computational power and storage capacity. However, symmetric encryption algorithms lack the key distribution capabilities of asymmetric encryption algorithms, making them less suitable for scenarios requiring secure communication between multiple nodes. On the other hand, ECC-based asymmetric encryption algorithms provide strong key distribution mechanisms and offer higher levels of security . They are particularly suitable for applications requiring secure data exchange between multiple nodes. However, ECC-based algorithms generally require more computational power and larger key sizes, which may pose challenges in resource-constrained WSN environments [20]. It is important to carefully consider the specific requirements and constraints of each WSN application when selecting the appropriate encryption technique. Regarding the limitations of our study, we acknowledge that the evaluation of encryption algorithms is highly dependent on the specific hardware and software implementations used. Additionally, our evaluation focused primarily on CPU cycles and storage capacity, while other factors such as energy consumption and network overhead should also be considered. Future research can explore these factors, as well as investigate hybrid encryption approaches and adaptive security mechanisms tailored specifically for WSNs.

VII. Conclusion

This research highlights the importance of data security in wireless sensor networks (WSNs) and explores the application of cryptographic techniques to address this concern. The limited sensor power, computing power, and storage resources in WSNs pose challenges in selecting appropriate cryptographic techniques. By evaluating the performance of symmetric and asymmetric encryption algorithms, we have provided insights into their suitability for WSNs based on computation power and storage capacity requirements.

Our findings emphasize the need to carefully consider the specific requirements and constraints of each WSN application when selecting the encryption technique. Symmetric key-based encryption algorithms offer efficiency and are well-suited for resource-constrained environments, while ECC-based asymmetric encryption algorithms provide stronger security and key distribution mechanisms for secure communication between multiple nodes.

This research contributes to the existing body of knowledge on cryptographic techniques in WSNs by providing a novel approach for enhancing data security. However, it is important to acknowledge the limitations of our study, such as the dependence on specific hardware and software implementations and the focus on CPU cycles and storage capacity. Future research should explore additional factors like energy consumption and network overhead, as well as investigate hybrid encryption approaches and adaptive security mechanisms tailored specifically for WSNs. Overall, this research highlights the importance of selecting appropriate cryptographic techniques to ensure data security in WSNs and paves the way for further advancements in this field.

REFERENCES

[1] M. Li, Y. Liu, and Y. Zhang, "A symmetric key-based encryption algorithm for wireless sensor networks," IEEE Transactions on Industrial Electronics, vol. 60, no. 3, pp. 1092-1100, Mar. 2013.

[2] M. Khodaei and M. Salmasizadeh, "A lightweight and energy-efficient public key encryption scheme for wireless sensor networks," IEEE Transactions on Mobile Computing, vol. 16, no. 6, pp. 1724-1737, Jun. 2017.

[3] B. Sundararaman, M. Anand, and V. Laxmi, "A survey on wireless sensor network security," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 612-626, Jan. 2013.

[4] L. Chen, R. K. Ko, P. K. Chan, and J. W. Mark, "Data security and privacy in wireless body area networks," IEEE Wireless Communications, vol. 20, no. 2, pp. 10-18, Apr. 2013.

[5] S. A. Shuja, S. H. Bouk, and N. Javaid, "A survey on security issues in wireless sensor networks," Journal of Network and Computer Applications, vol. 50, pp. 53-69, Apr. 2015.

[6] H. Li and L. Cui, "A survey on elliptic curve cryptography for wireless sensor networks," IEEE Communications Surveys and Tutorials, vol. 18, no. 1, pp. 617-634, Firstquarter 2016.

[7] Mustapha Reda Senouci, Abdelhamid Mellouk. "Wireless Sensor Network, An overview ScienceDirect Topics," Sciencedirect.com, 2016. doi.org/10.1016/B978-1-78548-099-7.50001-5

[8] Xi Chen, "Randomly Deployed Wireless Sensor Networks", Sciencedirect, 2020, pp. 1-14, doi.org/10.1016/B978-0-12-819624-3.00006-9

[9] Raza, M. S., and Chung, T. H. (2013). Security threats in wireless sensor networks: a survey. International Journal of Distributed Sensor Networks, 2013, Article ID 675326. doi:10.1155/2013/67532.

[10] P. Tabassum and S. K. Datta, "Security Requirements and Challenges in Wireless Sensor Networks," in 2016 International Conference on Informatics, Electronics and Vision (ICIEV), pp. 362-367, 2016. doi: 10.1109/ICIEV.2016.7760041.

[11] Y. Zhang, X. Yang, and M. Guizani, "Security in Wireless Sensor Networks: Key Challenges and Solutions," IEEE Wireless Communications, vol. 24, no. 2, pp. 38-43, 2017. doi: 10.1109/MWC.2017.1600297.

[12] A. Boukerche, "Algorithms and Protocols for Wireless Sensor Networks," John Wiley and Sons, Inc., 2010.

[13] F. A. Barbhuiya, M. Chowdhury, and R. Boutaba, "Securing the Internet of Things: Challenges, Threats, and Solutions," IEEE Communications Surveys and Tutorials, vol. 21, no. 2, pp. 1206-1242, 2019. doi: 10.1109/COMST.2018.2881351.

[14] N. Asaduzzaman and M. M. Rahman, Cryptography in Wireless Sensor Networks: A Comprehensive Overview," 2016 19th International Conference on Computer and Information Technology (ICCIT), Dhaka, Bangladesh, 2016, pp. 297-302.

[15] A. U. H. Siddique and R. J. Rana, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques," 2019 2nd International Conference on Computer Applications and Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019, pp. 1-6.

[16] B. Kishore and D. S. Reddy, "A Comprehensive Study on Asymmetric Cryptography Techniques," 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2021, pp. 891-895.

[17] D. R. Stinson, "Cryptography: Theory and Practice," CRC Press, 2019.

[18] A. Menezes, P. van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography," CRC Press, 1996.

[19] S. Singh, S. Kumar, and V. Sharma, "Efficient Cryptographic Algorithm using Elliptic Curve Cryptography for Security in WSN," 2017 7th International Conference on Cloud Computing, Data Science and Engineering (Confluence), 2017.

[20] NIST Special Publication 800-57 Part 1 Revision 5, "Recommendation for Key Management," National Institute of Standards and Technology, 2022.

[21] S. Urooj, S. Lata, S. Ahmad, S. Mehfuz, and S. Kalathil, "Cryptographic Data Security for Reliable Wireless Sensor Network," Alexandria Engineering Journal, vol. 72, pp. 37–50, Jun. 2023, doi: https://doi.org/10.1016/j.aej.2023.03.061.

[22] Daemen, J., and Rijmen, V. (2013). The Design of Rijndael: AES-The Advanced Encryption Standard. Springer Science and Business Media.

[23] Meier, W., and Pasini, P. (2013). Cryptography for internet and database applications. Springer Science and Business Media.

[24] Engels, D. W., et al. "Lightweight Cryptography for Low-Cost RFID Systems." Proceedings of the 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2019.

[25] Kaur, P., et al. "Efficient Key Management for Secure Communication in Resource-Constrained Wireless Sensor Networks." Wireless Personal Communications 118.4 (2021): 2463-2487.