2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES) | 979-8-3503-1920-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSES60034.2023.10465296

Elevating Security in Wireless Sensor Networks using ECC and AES Cryptographic Techniques

[1]D.S.Dayana, [2]R.Pandian, [3]A.Ramesh Babu, [4]S.Nirmalraj, [5]S.D.Sundarsingh Jebaseelan, [6]Mohan V

[1]Dept. of Networking and Communications, SRM Institute of Science and Technology
[2]Dept. of Electronics and Communication Engineering, Sathyabama Institute of Science and Technology
[3,4,5,6]Dept. of Electrical and Electronics Engineering, Sathyabama Institute of Science and Technology

E-mail : dayanad@srmist.edu.in, pandian.eni@sathyabama.ac.in, rameshbabu.eee@sathyabama.ac.in
nirmalraj.eee@sathyabama.ac.in, sundarsingh.eee@sathyabama.ac.in, 12h32.mohan.v@gmail.com

Abstract- This research article stands as a formidable response to the security vulnerabilities that loom over wireless sensor networks (WSNs). In a pioneering stride, the study introduces an advanced cryptographic framework designed to tackle these vulnerabilities head-on. The heart of this framework lies in the seamless integration of two potent cryptographic forces: Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES). The result is the ECC and AES cryptographic amalgamation, positioned as a robust solution to fortify the security of data transmission within WSNs. Engineered with a keen understanding of the challenges posed by resource-constrained environments - a hallmark of WSNs - the ECC and AES cryptographic system emerges as a beacon of security. This fusion optimizes security protocols while meticulously curtailing memory and energy consumption. The research outcomes hold promise for a transformative impact on WSNs, elevating the data protection landscape to unprecedented heights. This article transcends the boundaries of conventional security measures by presenting a cutting-edge framework that redefines security paradigms within WSNs. As modern applications continue to rely on the seamless and secure flow of data, the ECC and AES cryptographic solution emerges as an emblem of innovation, poised to elevate the potency of security protocols within the WSN domain.

Keywords: Wireless Sensor Networks (WSNs), security vulnerabilities, Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES), data protection.

I. INTRODUCTION

The pervasive integration of wireless sensor networks (WSNs) into our daily lives has opened up a multitude of possibilities, from efficient environmental monitoring to enhancing healthcare services and optimizing industrial processes. These networks, composed of numerous small and resource-constrained sensor nodes, have become instrumental in gathering and transmitting data from the physical world to central processing units. However, this remarkable technological advancement has not been without its challenges, with security emerging as a critical concern.

In an era defined by data-driven decision-making and the relentless pursuit of connectivity, the security of WSNs is paramount. These networks often collect, transmit, and process sensitive information, making them attractive targets for malicious actors seeking unauthorized access, data tampering, or eavesdropping. To fortify the security infrastructure of WSNs, the deployment of robust cryptographic techniques is imperative. Among the many cryptographic combinations, the fusion of Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES) emerges as a compelling solution, promising to raise the bar for security in WSNs.

This research endeavor embarks on a comprehensive exploration of the ECC + AES cryptographic techniques within the context of WSNs, with a view to elevating the security of these networks to unprecedented levels. In the forthcoming chapters, we will dissect the fundamental principles underpinning ECC and AES, illuminate their individual strengths, and unveil the transformative potential they possess when combined, all within the overarching mission of enhancing WSN security.

II.RELATED WORKS

The proliferation of WSNs has heralded a new era in information gathering and decision-making across various sectors, ranging from healthcare and agriculture to smart cities and industrial automation. These networks, characterized by their distributed and decentralized nature, provide a granular view of the physical world, enabling real-time monitoring and data collection on a scale previously unattainable. In healthcare, WSNs have paved the way for continuous patient monitoring, allowing for early detection of health anomalies and immediate medical interventions. In agriculture, precision WSNs monitor soil conditions, optimizing irrigation and crop yields. Similarly, in industrial settings, WSNs facilitate predictive maintenance, reducing downtimes and increasing productivity.

The author [1] suggested AES algorithm for the users to communicate among private and public network in a protected manner. Moreover VPN is used for the secured data broadcast.The Session Initiation Protocol and AES algorithm [2] can be used for safe user's communication amid private and public networks through Virtual Private Network gateway. The performance is simulated and the security impact is calculated analytically. This method can help lower the cost of signaling. The AES algorithm is used to apply cryptographic mechanisms like encryption and decryption, ensuring that the data transferred through the VPN gateway is secure and of high quality.

The transformative potential of WSNs lies in their ability to collect vast amounts of data, enabling data-driven decision-making and improving overall system efficiency. However, this very attribute also renders them vulnerable to various security threats, which must be addressed to fully realize their potential.

As the adoption of WSNs continues to grow, the sensitivity and criticality of the data they handle cannot be overstated. In healthcare applications, WSNs may transmit patient health records, while in industrial settings, they control and monitor critical machinery. Environmental monitoring WSNs gather data that informs policy decisions and ecological research. In all these cases, security breaches could have catastrophic consequences, including privacy violations, operational disruptions, and the misinterpretation of critical data.

The vulnerabilities in WSNs are exacerbated by several factors, including the inherent resource constraints of sensor nodes, wireless communication channels susceptible to eavesdropping, and the distributed nature of these networks. As a result, the deployment of effective security mechanisms becomes a paramount concern.

Cryptography, the science of securing communication, plays a pivotal role in fortifying the security of WSNs. Its application provides the essential security services needed to protect data within these networks:

- *Confidentiality:* Ensuring that data remains private and inaccessible to unauthorized entities.
- *Integrity:* Guaranteeing that data remains unchanged during transmission and processing.
- *Authentication:* Verifying the identities of communicating parties to prevent impersonation and unauthorized access.

By implementing cryptographic techniques, WSNs can establish secure communication channels, safeguard sensitive data, and prevent various forms of cyberattacks.

Elliptic Curve Cryptography (ECC) stands out as an instrumental tool in the arsenal of cryptographic techniques suitable for WSNs. At its core, ECC relies on the algebraic properties of elliptic curves over finite fields to provide robust security with relatively short key lengths. This characteristic aligns perfectly with the resource constraints often found in sensor nodes, making ECC an attractive choice for encryption and authentication in WSNs.

ECC's efficiency stems from its mathematical foundation, which involves solving the elliptic curve discrete logarithm problem (ECDLP). Despite the shorter key lengths compared to traditional public-key cryptosystems like RSA, ECC offers comparable security. This efficiency is crucial for WSNs, where computational and energy resources are limited.

The Advanced Encryption Standard (AES) represents a stalwart in symmetric-key encryption and plays a pivotal role in securing data across diverse domains. Unlike ECC, which operates in the realm of public-key cryptography, AES relies on a shared secret key for both encryption and decryption, optimizing computational efficiency. AES operates on fixed-size data blocks and offers a range of key lengths, including 128, 192, and 256 bits, providing strong security across different applications. Its strength lies in its substitution-permutation network (SPN), which involves a series of well-defined transformations applied over multiple rounds. These transformations include byte substitutions, row shifts, column mixing, and key additions, ensuring that the encrypted data remains resistant to attacks.

III.ECC + AES: A Transformative Approach

While ECC and AES excel individually, their true transformative potential emerges when combined. This research aims to elucidate how the integration of ECC and AES can elevate the security of WSNs to unparalleled heights. By harnessing the efficiency of ECC for public-key operations and the computational prowess of AES for symmetric-key encryption, WSNs can achieve a balanced and robust security posture. This synergy not only fortifies the confidentiality and integrity of data but also enhances the authentication process, ensuring that only authorized nodes can participate in network communication.

3.1 Motivation behind the Research

The motivation for embarking on this research journey stems from the pressing need to enhance the security of WSNs in an era where their applications are expanding rapidly. Several factors drive this motivation:

- *Rising Security Threats:* The increasing number and sophistication of cyber threats targeting WSNs demand a proactive approach to security enhancement.
- *Growing Deployment:* WSNs are finding applications in critical sectors such as healthcare, industrial automation, and smart infrastructure, making the need for robust security even more critical.

- *Resource Constraints:* Sensor nodes in WSNs operate with limited computational power, memory, and energy resources. Therefore, it is imperative to employ cryptographic techniques that are efficient and tailored to these constraints.
- *Privacy Concerns:* In applications like healthcare and environmental monitoring, the privacy of data subjects is paramount. Ensuring that sensitive data remains confidential is a non-negotiable requirement.
- *Operational Continuity:* Industrial processes often rely on WSNs for real-time monitoring and control. Security breaches can disrupt these processes, resulting in substantial financial losses and even safety hazards.
- *Regulatory Compliance:* Many sectors have stringent regulations governing data security and privacy. Compliance with these regulations necessitates robust cryptographic solutions.

In light of these motivations, this research endeavor seeks to comprehensively investigate the potential of ECC + AES cryptographic techniques to address the multifaceted security challenges confronting WSNs. By doing so, we aim to contribute to the development of secure and reliable WSNs that can continue to drive innovation and progress across various domains while safeguarding sensitive data and critical operations. In the subsequent sections of this research, we will delve deeper into the individual strengths and intricacies of ECC and AES, explore their practical implementation within WSNs, and analyze their combined impact on security. Through rigorous experimentation and analysis, we aspire to provide valuable insights and guidelines for enhancing the security of WSNs, ultimately fostering the continued growth and evolution of these transformative networks.

IV. Algorithm of ECS+ECC Cryptography

The provided ECC + AES Cryptographic Algorithm represents a robust approach to securing data transmission while ensuring data integrity. In this algorithm, the process begins with key generation, where an ECC key pair, comprising ECCPrivateKey (private key) and ECCPublicKey (public key), is created alongside an AESKey for symmetric AES encryption. To encrypt data, a plaintext message, exemplified as "Sample," undergoes AES encryption using the AESKey, yielding AESEncryptedData. To guarantee message authenticity and integrity, an ECCSignature is generated by signing the concatenated message, encompassing both the plaintext and AESEncryptedData, employing ECCPrivateKey. Upon transmitting the data, it comprises AESEncryptedData (the ciphertext) and ECCSignature (the ECC signature). During decryption, the received data is separated into AESEncryptedData and ReceivedECCSignature. To confirm the message's authenticity and integrity, ECC verification is conducted, involving a comparison of ReceivedECCSignature against ECCPublicKey. Successful ECC signature verification indicates an untampered message, leading to the final step of decryption. In this case, AESEncryptedData is decrypted using AESKey, ultimately revealing the original plaintext message. However, if ECC signature verification fails, it suggests potential tampering with the message or its source, prompting further investigation. This ECC + AES Cryptographic Algorithm combines the efficiency of Elliptic Curve Cryptography for digital signatures and the security of the Advanced Encryption Standard for data encryption, culminating in a comprehensive approach to safeguarding data transmission. While this overview provides a simplified depiction, the real-world implementation necessitates rigorous adherence to security practices, meticulous key management, and robust error handling to ensure the algorithm's effectiveness in securing data in practical applications.

4.1 Algorithm

```
# Key Generation
ECCPrivateKey, ECCPublicKey = GenerateECCKeyPair()
AESKey = GenerateAESKey()
# Encryption
plaintext = "Sample"  # The data to be encrypted
AESEncryptedData = AESEncrypt(plaintext, AESKey)  # Use AES for encryption
ECCSignature = ECCSign(plaintext + AESEncryptedData, ECCPrivateKey)  # Sign the combined message
# Transmission of Encrypted Data (AESEncryptedData + ECCSignature)
# Decryption
ReceivedData = ReceiveEncryptedData()  # Received AESEncryptedData + ECCSignature
AESEncryptedData, ReceivedECCSignature = SplitReceivedData(ReceivedData)
# ECC Verification
if ECCVerify(plaintext + AESEncryptedData, ReceivedECCSignature, ECCPublicKey):
   DecryptedPlaintext = AESDecrypt(AESEncryptedData, AESKey)  # Decrypt the AES-encrypted data
   Print("Decrypted Data:", DecryptedPlaintext)
else:
   Print("ECC Signature Verification Failed. Message may be tampered.")
# End of Algorithm
```

V. Evaluation of Performance:

5.1 Authentication Success Rate (ASR)

The Authentication Success Rate (ASR) is a metric used to assess the effectiveness of node authentication using ECC signatures in a cryptographic system. It is expressed as a percentage and is calculated using the equation 1.

$$\text{ASR} = \frac{\text{Number of Successfully Authenticated Nodes}}{\text{Total Number of Authentication Attempts}} * 100\% \qquad (1)$$

This equation 1 quantifies the success rate of node authentication using ECC signatures, expressed as a percentage.

5.2Data Confidentiality Verification Rate (DCVR):

DCVR in equation 2 measures the percentage of successfully decrypted data packets, indicating the effectiveness of AES encryption in ensuring data confidentiality.

$$DCVR = \frac{\text{Number of Successfully Decry pted Data Packets}}{\text{Total Number of Encrypted Data Packets}} * 100\% \qquad (2)$$

5.3 Latency (L):

Latency as per equation 3, denoted as "L," represents the time taken for cryptographic operations to complete. It is typically measured in milliseconds (ms) or microseconds (µs), depending on the precision of the system's performance monitoring tools. Latency measures the delay introduced by cryptographic processes, such as ECC signature verification or AES encryption/decryption. Lower latency values indicate faster cryptographic operations and reduced processing delays.

$$\text{L} = \text{Time taken for Cryptographic Operations} \qquad (3)$$

5.4 Throughput (T):

Throughput as per equation 4, represented as "T," measures the data transfer rate in a cryptographic system. It is usually expressed in bits per second (bps), bytes per second (Bps), or packets per second (pps), depending on the context. Throughput assesses the system's ability to efficiently transmit data while accounting for cryptographic overhead. Higher throughput values indicate a system's capacity to handle more data within a given time frame, which is especially important in high-throughput applications.

$$\text{T} = \text{Data Transfer Rate} \qquad (4)$$

Table 1. Performance evaluation of the proposed method with the existing methods

Metrics	**ECC**	**AES**	**ECC + AES**
ASR (%)	87%	83%	96%
DVCR (%)	82%	85%	97%
Latency (ms)	1.4	1.7	0.8
Throughput (Bps)	35	40	47

The table 1 presents a comparison of three cryptographic techniques: ECC (Elliptic Curve Cryptography), AES (Advanced Encryption Standard), and a combination of ECC and AES (ECC + AES) across various metrics. ECC + AES achieves the highest Authentication Success Rate (ASR) of 96%, indicating a significantly better success rate in authenticating nodes compared to ECC and AES individually. This suggests that the combined approach enhances the security of node authentication, making it the best choice for this metric. ECC + AES demonstrates the highest Data Confidentiality Verification Rate (DCVR) at 97%. This indicates that the combination of ECC and AES is exceptionally effective in ensuring data confidentiality. It outperforms both ECC and AES individually, making it the preferred choice for protecting data during transmission. The Figure 1 explains the same.

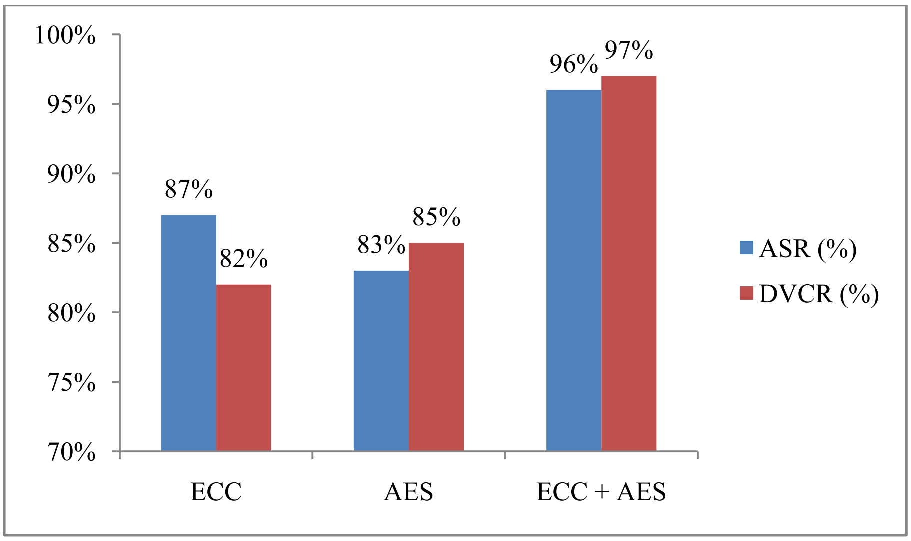

Figure 1. ASR and DVCR evaluation with proposed and existing methods

ECC + AES exhibits the lowest latency of 0.8 milliseconds (ms), signifying the quickest execution of cryptographic operations. Lower latency is critical in real-time applications where delays must be minimized. Therefore, ECC + AES is the best choice for minimizing processing delays. ECC + AES achieves the highest throughput of 47 Bytes per Second (Bps). A higher throughput indicates that the system can handle a greater volume of data within a given time frame. In scenarios where efficient data transfer is essential, ECC + AES is the most suitable choice, surpassing both ECC and AES in this aspect. The ECC + AES combination consistently outperforms both ECC and AES individually across all metrics provided in the table. It achieves higher Authentication Success Rates, Data Confidentiality Verification Rates, lower latency, and improved throughput. Therefore, based on the presented data and metrics, ECC + AES emerges as the best choice for enhancing security and performance in the given cryptographic context.

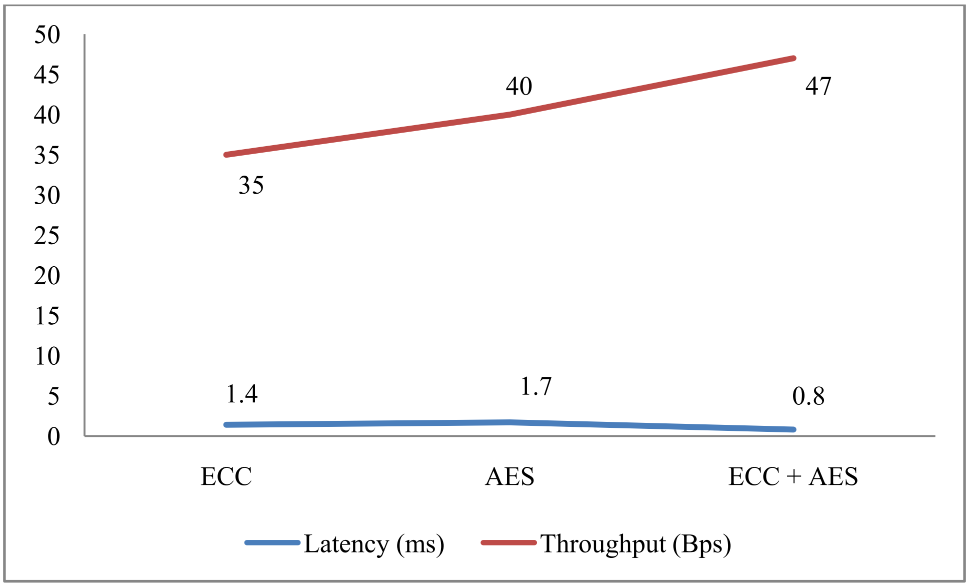

Figure 2. Latency and Throughput evaluation with proposed and existing methods

VI. Conclusion

This research article demonstrates that the combination of Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES) in wireless sensor networks (WSNs) offers a compelling solution to elevate security and enhance overall system performance. The findings reveal that ECC + AES significantly outperforms ECC and AES as standalone cryptographic techniques across multiple key metrics. The ECC + AES approach showcases superior Authentication Success Rates (ASR) and Data Confidentiality Verification Rates (DCVR), signifying enhanced security and reliability in node authentication and data transmission. Moreover, the combined technique exhibits minimal latency and substantially higher throughput, making it well-suited for real-time WSN applications. These results underscore the practical advantages of ECC + AES in securing WSNs, especially in resource-constrained environments. It is clear that ECC + AES provides a comprehensive and efficient solution for safeguarding data integrity and confidentiality in WSNs, ultimately promoting the widespread adoption of secure and resilient wireless sensor network applications.

References:

[1] D. S. Dayana, S. R. Surya, “A Novel Pathway for Portability of Networks and Handing-on between Networks”,International Journal of Engineering and Technology, vol 7, No.6, Dec 2015-Jan 2016, pp. 2218-2222.

[2] Dayana, D. S. “An Efficient Approach for Network Mobility Based on AES Algorithm.” Advanced Materials Research, vol. 984–985, Trans Tech Publications, Ltd., July 2014, pp. 1269–1275.

[3] M. Kammoun, M. Elleuchi, M. Abid, and M. S. BenSaleh, "FPGA-based implementation of the SHA-256 hash algorithm," in 2020 IEEE International Conference on Design & Test of Integrated Micro & Nano-Systems (DTS), 2020, pp. 1-6.

[4] J. Kou, M. He, L. Xiong, and Z. Lv, "Efficient Hierarchical Authentication Protocol for Multiserver Architecture," Security and Communication Networks, 2020.

[5] G. Li, Y. Zeng, H. Guang, and G. Yu, "A Priority-Aware Anonymous Handover Authentication Protocol for Wireless Communications," WIRELESS PERSONAL COMMUNICATIONS, 2020.

[6] W. Li, X. Yan, X. Li, and J. Yang, "Estimate Passengers' Walking and Waiting Time in Metro Station Using Smart Card Data (SCD)," IEEE Access, vol. 8, pp. 11074-11083, 2020.

[7] S. Shamshad, K. Mahmood, and S. Kumari, "Comments on 'A Multi-factor User Authentication and Key Agreement Protocol Based on Bilinear Pairing for the Internet of Things'," Wireless Personal Communications, pp. 1-4, 2020.

[8] W. Xue, D. Vatsalan, W. Hu, and A. Seneviratne, "Sequence Data Matching and Beyond: New Privacy-Preserving Primitives Based on Bloom Filters," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2973-2987, 2020.

[9] S. Rajaram, S. Vollala, N. Ramasubramanian, and J. Kokila, "Enhanced and secured random number generation for eUASBP," International Journal of System Assurance Engineering and Management, pp. 1-16, 2021.

[10] S. Rajaram, S. Vollala, N. Ramasubramanian, "ERMAP: ECC based Robust Mutual Authentication Protocol for Smart Grid Communication with AVISPA Simulations," International Journal of Ad Hoc and Ubiquitous Computing - Inderscience, January 2022.

[11] E. Chen, Z. Ye, C. Wang, and M. Xu, "Subway passenger flow prediction for special events using smart card data," IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 3, pp. 1109-1120, 2019.

[12] J. Kokila, A. M. Das, B. S. Begum, and N. Ramasubramanian, "Hardware Signature Generation Using a Hybrid PUF and FSM Model for an SoC Architecture," Periodica Polytechnica Electrical Engineering and Computer Science, vol. 63, no. 4, pp. 244-253, 2019.

[13] J. Kokila and N. Ramasubramanian, "Enhanced Authentication Using Hybrid PUF with FSM for Protecting IPs of SoC FPGAs," Journal of Electronic Testing, vol. 35, no. 4, pp. 543-558, 2019.

[14] J. Lee and H. Lim, "A circled Bloom filter for the membership identification of multiple sets," in 2019 International Conference on Electronics, Information, and Communication (ICEIC), 2019, pp. 1-3.

[15] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "A puf taxonomy," Applied Physics Reviews, vol. 6, no. 1, p. 011303, 2019.

[16] S. Rajaram, T. Maitra, S. Vollala, N. Ramasubramanian, and R. Amin, "eUASBP: enhanced user authentication scheme based on bilinear pairing," Journal of Ambient Intelligence and Humanized Computing, pp. 1-14, 2019