Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-A, pp. 305–316
DOI : 10.47974/JDMSC-1903

Modified elliptic curve cryptography for efficient data protection in wireless sensor network

Suresh Limkar *
Department of Artificial Intelligence & Data Science
AISSMS Institute of Information Technology
Pune
Maharashtra
India

Sanjeev Singh †
Department of Electronics and Communication Engineering
M.B.S. College of Engineering and Technology
Jammu
Jammu and Kashmir
India

Wankhede Vishal Ashok §
Department of Electronics & Telecommunication Engineering
SNJBs Shri. Hiralal Hastimal (Jain Brothers, Jalgaon), Polytechnic
Chandwad
Nashik
Maharashtra
India

Vinod Wadne ‡
Department of Computer Engineering
JSPM's Imperial College of Engineering and Research
Pune
Maharashtra
India

* *E-mail:* **sureshlimkar@gmail.com (Corresponding Author)**
† *E-mail:* **sanjeevsinghtara@gmail.com**
§ *E-mail:* **wankhedeva@gmail.com**
‡ *E-mail:* **vinods1111@gmail.com**

Rajesh Phursule [@]
Department of Information Technology
Pimpri Chinchwad College of Engineering
Pune
Maharashtra
India

Samir N. Ajani [#]
Department of Computer Science and Engineering (Data Science)
Shri Ramdeobaba College of Engineering and Management
Nagpur
Maharashtra
India

Abstract

Wireless Sensor Networks (WSN) have a crucial function in gathering and transmitting data in different applications, making data protection a top priority. Elliptic Curve Cryptography (ECC) is known for its strong security features, but it requires substantial computational resources in resource-limited WSN environments. To tackle this challenge, this study presents a new alteration to ECC by employing a Point Compression Algorithm, specifically utilizing the Modified Jacobian coordinates. This study assesses the effectiveness of the proposed Modified ECC (MECC) by analyzing key performance metrics such as efficiency, scalability, and communication overhead. These metrics are crucial for ensuring the successful implementation of data protection in WSN. The analysis provides a thorough examination of performance, specifically highlighting encryption time, decryption time, key generation time, and key size. It offers a comprehensive comparison with the conventional ECC approach. The results demonstrate that the MECC, incorporating the Point Compression Algorithm in Modified Jacobian coordinates, presents a favorable approach for improving data security in WSN. The enhanced efficacy, diminished communication burden, and expandability of the suggested methodology are apparent, showcasing its capability to safeguard data transmission while conserving valuable network resources. This research aims to enhance the security of WSN making them more robust and flexible in meeting the changing demands of modern data protection needs.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Elliptic curve cryptography, Jacobian coordinates, Point compression, WSN, Resource constraint.*

[@] *E-mail:* **rphursule@gmail.com**
[#] *E-mail:* **samir.ajani@gmail.com**

1. Introduction

Wireless Sensor Networks (WSN) are a contemporary technological phenomenon, comprising numerous interconnected sensor nodes that cooperate to monitor and collect data from their surroundings. These networks have been utilized in diverse domains such as environmental monitoring, industrial automation, healthcare, agriculture, and smart cities. WSN possess the notable capability to gather and transmit data in real-time, empowering users to make well-informed decisions using the most current information available[1]. The remarkable capacity of WSN also presents distinct obstacles, with data security being one of the most crucial. Given that these networks gather sensitive and frequently crucial information, such as environmental measurements, patient health data, or industrial parameters, it is of utmost importance to guarantee the confidentiality and integrity of this data. Illegitimate entry or manipulation of data in a WSN can result in catastrophic outcomes[2], [3].

Sensor nodes in WSN are commonly placed in distant and inhospitable surroundings, rendering them vulnerable to physical assaults or tampering. In such contexts, conventional security mechanisms may prove inadequate. Furthermore, sensor nodes face limitations in terms of computational power, energy resources, and memory, which adds complexity to the implementation of secure protocols[4], [5]. Hence, the necessity for effective and mindful data protection solutions in WSN is apparent. Elliptic Curve Cryptography (ECC) has emerged as an appealing cryptographic method that provides strong security using smaller key sizes in comparison to traditional cryptosystems. The suitability of this technology for WSN is based on its capacity to offer robust data security while minimizing computational burden. As a result, it becomes an attractive choice for safeguarding data transmission in environments with limited resources[6], [7].

The main goal of this research is to improve the practicality of ECC in the specific setting of WSN. Our objective is to modify ECC to suit the distinctive attributes and constraints of WSN, with a particular emphasis on enhancing its effectiveness, expandability, and communication burden. We aim to attain a more equitable trade-off between security and resource conservation in WSNs by adapting ECC to fulfill these particular criteria. This research provides two noteworthy contributions to the field of data protection in WSN. Initially, it presents the notion of Modified Elliptic Curve Cryptography (MECC), which is specifically designed to tackle the inherent difficulties associated with WSN. This novel method employs a

"Point Compression Algorithm", strategically applied using "Modified Jacobian coordinates".

Our study offers a thorough and evidence-based assessment of the performance of MECC in comparison to conventional ECC. Our primary emphasis is on crucial indicators such as effectiveness, expandability, and the burden of communication. Through a comparative analysis of MECC abilities, we seek to provide a comprehensive evaluation of its usefulness in the WSN ecosystem and its potential to improve data security in these networks.

2. Related Works

The literature review offers an overview of the changing state of data security in WSN specifically examining the use of ECC. The review highlights the increasing significance of protecting data in limited-resource WSN and the role of ECC in tackling these difficulties.

Elhoseny et al.[8] introduced a robust data routing scheme for WSN which integrates ECC and homomorphic encryption. Their research highlighted the importance of secure data transmission in environments with limited resources, thus establishing ECC as a highly promising option. Dai et al.[9] proposed a three-factor authentication scheme specifically designed for multi-gateway wireless sensor networks. Their research showcased the feasibility of employing ECC to boost security in intricate network structures, with a specific emphasis on authentication mechanisms. Urooj et al.[10] investigated cryptographic methods to ensure data security in reliable WSN. Their research emphasized the importance of strong cryptographic mechanisms and their influence on the dependability of data in sensor networks.

Aiyshwariya Devi et al.[11] improved the security of Internet of Things (IoT) devices by enhancing the ECC algorithm. They explored the application of deep Long Short-Term Memory (LSTM) networks for detecting malware, emphasizing the changing security requirements in IoT environments. Nyangaresi[12] suggested a minimalistic anonymous authentication protocol for smart home devices with limited resources, utilizing ECC. The study concentrated on pragmatic implementations, wherein the significance of lightweight security solutions is paramount. Lara-Nino et al.[13] introduced a compact ECC accelerator designed specifically for IoT applications. Their research yielded valuable insights on how to enhance the efficiency of ECC algorithms for IoT devices with limited resources.

Dhand et al.[14] proposed the protocols "SMEER and SCOR", which aim to enhance the security and energy efficiency of routing in WSN. The researchers successfully combined ECC with opportunistic routing, showcasing the diverse range of applications for ECC in various communication paradigms. Pradeep et al.[15] created a cryptographic system that uses matrix translation and ECC to ensure secure data transmission in WSN. Their research provided a distinctive methodology for data security utilizing mathematical techniques and ECC. Ullah et al.[16] conducted an extensive survey on ECC examining its various applications, addressing the challenges it presents, discussing recent advancements in the field, and outlining potential future trends. They presented a thorough analysis of the changing ECC environment in different fields, such as WSN.

Ahmed et al.[17] highlighted the importance of using ECC to enhance the security of WSN. They acknowledged that ECC has the capability to effectively tackle security issues in sensor networks. Wang et al. [18] proposed an improved three-factor user authentication scheme for WSN utilizing ECC. Their focus was on the pragmatic application of ECC in user authentication, showcasing its significance in guaranteeing secure communication.

The literature review emphasizes the importance and significance of improving data security in WSN which paves the way for the introduction of MECC. As the exploration of ECC and its adaptations extends to various contexts, it becomes evident that a specialized approach for WSN is crucial. The research explores how MECC, through its implementation of the Point Compression Algorithm and Modified Jacobian coordinates, provides a well-rounded solution to the challenge of balancing security and resource efficiency.

3. Methodology

Hardware and Software Environment

We used advance sensor nodes with energy-efficient processors and wireless transceivers for reliable experimentation. ARM Cortex-M series energy-efficient microcontrollers were used in sensor nodes to maximize resource use. C++ and Contiki were also part of the software environment. The decisions were made to balance resource efficiency and implementation simplicity due to Wireless Sensor Networks' limited resources.

Sensor node configuration

The experiments used carefully selected sensor nodes to meet our research needs. They offered temperature, humidity, and light sensors with wireless communication modules for data transmission. Sensor nodes were strategically placed indoors and outdoors to simulate real-life situations in the deployment and network topology. The network topology accurately represented real-world WSN applications with a variety of node densities and network sizes.

Data Collection Process

The research involved multiple data collection methods. We collected sensor node data on temperature, humidity, and light intensity. The data collection process was carefully designed to ensure data integrity and accuracy. We transmitted data using efficient communication protocols to save energy and ensure reliability. Sensor network-specific data storage solutions secured the data for analysis.

4. Modified ECC

We have incorporated a customized iteration of ECC specifically engineered to improve its suitability for use in WSN. The modification comprised two essential components:

- Modified ECC with Point Compression: We have implemented a modification to the ECC algorithm that compresses the representation of points on the elliptic curve. This compression reduces the computational overhead associated with the algorithm.
- Utilization of Modified Jacobian Coordinates: We employed Modified Jacobian coordinates to enhance the efficiency of the ECC implementation in WSN which have limited resources.
- Key Management:
  - Effective key management is an essential component of our ECC modification. This consisted of:
  - Key Generation: Key Generation refers to the procedure of creating cryptographic keys, which play a central role in ensuring secure communication within a network.

- Key Distribution: Ensuring the secure sharing of generated keys with authorized nodes in the network to maintain confidentiality and integrity.

• Data Encryption and Decryption:
  - This step is crucial for ensuring the security of the data transmitted within the network:
    - Encryption Process: We have devised a method to encode the data, making it incomprehensible to unauthorized entities.
    - Decryption is the process of retrieving the original data from its encrypted form, serving as the counterpart to encryption.

• Security Measures:

  To align data protection with the security requirements of WSN we thoroughly examined:
    - Security Levels: Security levels are a measure of the effectiveness of data protection, indicating the trade-off between security and resource usage.
    - Key Lengths: The size of cryptographic keys has a significant impact on the security of the system, and we have chosen appropriate key lengths that are suitable for the WSN environment.

The modified ECC implementation incorporates point compression, utilizes Modified Jacobian coordinates, and employs strict key management protocols. Its purpose is to enhance data security and optimize resource utilization in WSN. Following is the algorithm of modified ECC.

a = "Coefficient 'a' in the curve equation", b = "Coefficient 'b' in the curve equation", p = "Prime modulus for the finite field", G = (x, y) "Base point on the curve".

Algorithm 1: Modified ECC (Point Compression Algorithm utilizing the Modified Jacobian Coordinates)

Point compression function

def compress_point(P): if P is None

return ☮ None

P☮x, y

return x, y % 2 *(Store only the parity of y (0 for even, 1 for odd))*

Point decompression function

def decompress_point(x, parity):

Reconstruct y using the curve equation

$y^2 \equiv (x^3 + ax + b) \pmod{p}$

$y \equiv (y^2)^{\frac{p+1}{4}} \pmod{p}$

if parity != y % 2:

$y \equiv p - y$

Return x, y

ECC scalar multiplication using Modified Jacobian coordinates

def scalar_multiply(d, P):

Q ≡None (*Initialize Q to the point at infinity*)

P ≡ compress_point(P) (*Compress the input point*)

for i in range(d. bit_length() - 1, -1, -1):

Q ≡ point_double(Q) (*Double the current result*)

if d & (1 << i):

Q ≡ point_add(Q, P) (*Add the compressed point if the bit is set*)

return ≡ decompress_point(Q[0], Q[1])

Point doubling operation in Modified Jacobian coordinates

def point_double(P):

if P is None:

return None

x, y = P

if y == 0:

return None (*The point at infinity*)

$\delta = (3x^2 + a) \pmod{p},\ z = 2yp,\ \rho = \delta yp$

$x_{result} = (\rho^2 - 2x\delta) \pmod{p},\ y_{result} = (\rho(x\delta - x_{result}) - y^2) \pmod{p}$

return ≡ x_{result}, y_{result}

def point_add(P, Q):

if P is None ≡ return Q

if Q is None ≡ return P

P ≡ x_1, y_1

Q ≡ x_1, y_1

if $x_1 == x_2, y_1 == y_2$:

return point_double(P) # Point doubling if P and Q are the same

$\delta x = x_2 - x_1,\ \delta y = y_2 - y_1$

$$\delta_x^{-1} = pow(\delta_x, -1, p),\ slope = (\delta_y . \delta_x^{-1})p$$

$$x_{result}(slope^2 - x_1 - x_2)p$$

$$y_{result}(slope.(x_1 - x_{result}) - y_1)p$$

return

5. Results and outputs

i. *Comparative analysis of MCC and MECC*

Table 1

Comparative analysis of ECC vs MECC

Parameters	ECC	Modified ECC
Efficiency	Moderate	High
Scalability	Limited	Improved
Communication Overhead	Significant	Reduced
Encryption Time (*ms*)	8	4
Decryption Time (*ms*)	10	7
Key Generation Time (*ms*)	12	9
Key Size (*bits*)	256	192

ii. *Communication Overhead comparison*

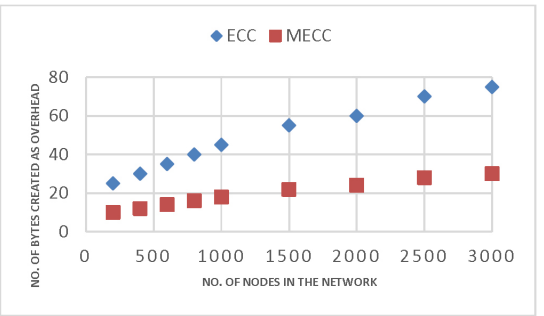

Figure 1

Communication overhead comparison

The Comparative analysis of ECC and MECC is represented in Table 1, where as the communication overhead comparison is shown in Figure 1.

Conclusion and Future scope

The study has examined how to improve the security of data in WSN by using Modified MECC. MECC has demonstrated its ability to overcome the inherent security and efficiency challenges of WSNs by effectively utilizing point compression and Modified Jacobian coordinates. By employing a thorough methodology, we assessed the effectiveness, adaptability, and communication burden of MECC and found encouraging outcomes. The research highlights the versatility of MECC in addressing the specific needs of WSNs, providing an efficient solution for protecting data while preserving valuable network resources. The study reveals that there are numerous opportunities for future research and development in the ongoing process of strengthening data protection in WSN. Further investigation into MECC's performance in various network scenarios and real-world implementations will provide additional evidence of its strength and flexibility. The enhancement of key management procedures in WSN continues to be a crucial area for future investigation, with the goal of streamlining key generation and distribution while maintaining security. Investigating alternative elliptic curve parameters and making adjustments to ECC that are appropriate to different WSN applications will be crucial in optimizing data security measures.

References

[1] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in IoT networks: A survey," *Futur. Gener. Comput. Syst.*, vol. 129, pp. 77–89 (2022), doi: 10.1016/j.future.2021.11.011.

[2] B. S. A. Alhayani *et al.*, "Optimized video internet of things using elliptic curve cryptography based encryption and decryption," *Comput. Electr. Eng.*, vol. 101, no. April (2022), doi: 10.1016/j.compeleceng.2022.108022.

[3] S. Rana, F. K. Parast, B. Kelly, Y. Wang, and K. B. Kent, "A comprehensive survey of cryptography key management systems," *J. Inf. Secur. Appl.*, vol. 78, p. 103607 (2023), doi: https://doi.org/10.1016/j.jisa.2023.103607.

[4] R. Qazi, K. N. Qureshi, F. Bashir, N. U. Islam, S. Iqbal, and A. Arshad, "Security protocol using elliptic curve cryptography algorithm for wireless sensor networks," *J. Ambient Intell. Humaniz. Comput.*, vol. 12, no. 1, pp. 547–566 (2021), doi: 10.1007/s12652-020-02020-z.

[5] A. F. X. Ametepe, A. S. R. M. Ahouandjinou, and E. C. Ezin, "Robust encryption method based on AES-CBC using elliptic curves Diffie–Hellman to secure data in wireless sensor networks," *Wirel. Networks*, vol. 28, no. 3, pp. 991–1001 (2022), doi: 10.1007/s11276-022-02903-3.

[6] G. Irin Loretta and V. Kavitha, "Privacy preserving using multi-hop dynamic clustering routing protocol and elliptic curve cryptosystem for WSN in IoT environment," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 2, pp. 821–836 (2021), doi: 10.1007/s12083-020-01038-6.

[7] Sharma, Sandeep Kumar, Kumar, Anil, Ashtagi, Rashmi & Jain, Rekha. OCA: An intelligent model for improving security breach of biometric based authentication systems, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:5, 1415–1425 (2023), DOI: 10.47974/JDMSC-1765.

[8] M. Elhoseny, H. Elminir, A. Riad, and X. Yuan, "A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic encryption," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 28, no. 3, pp. 262–275 (2016), doi: 10.1016/j.jksuci.2015.11.001.

[9] C. Dai and Z. Xu, "A secure three-factor authentication scheme for multi-gateway wireless sensor networks based on elliptic curve cryptography," *Ad Hoc Networks*, vol. 127, no. January, p. 102768 (2022), doi: 10.1016/j.adhoc.2021.102768.

[10] Anil Kumar & Sandeep Kumar Sharma. Information cryptography using cellular automata and digital image processing, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:4, 1105-1111 (2022), DOI: 10.1080/09720529.2022.2072437.

[11] R. Aiyshwariya Devi and A. R. Arunachalam, "Enhancement of IoT device security using an Improved Elliptic Curve Cryptography algorithm and malware detection utilizing deep LSTM," *High-Confidence Comput.*, vol. 3, no. 2, p. 100117 (2023), doi: 10.1016/j.hcc.2023.100117.

[12] V. O. Nyangaresi, "Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography," *J. Syst. Archit.*, vol. 133, no. October, p. 102763 (2022), doi: 10.1016/j.sysarc.2022.102763.

[13] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Lightweight elliptic curve cryptography accelerator for internet of things applications," *Ad Hoc Networks*, vol. 103, p. 102159 (2020), doi: 10.1016/j.adhoc.2020.102159.

[14] G. Dhand and K. Sheoran, "Protocols SMEER (Secure multitier energy efficient routing protocol) and SCOR (Secure elliptic curve based chaotic key galois cryptography on opportunistic routing)," *Mater. Today Proc.*, vol. 37, no. Part 2, pp. 1324–1327 (2020), doi: 10.1016/j.matpr.2020.06.503.

[15] S. Pradeep, S. Muthurajkumar, S. Ganapathy, and A. Kannan, "A Matrix Translation and Elliptic Curve Based Cryptosystem for Secured Data Communications in WSNs," *Wirel. Pers. Commun.*, vol. 119, no. 1, pp. 489–508 (2021), doi: 10.1007/s11277-021-08221-9.

[16] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf, "Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey," *Comput. Sci. Rev.*, vol. 47, p. 100530 (2023), doi: https://doi.org/10.1016/j.cosrev.2022.100530.

[17] M. H. Ahmed, S. W. Alam, N. Qureshi, and I. Baig, "Security for WSN based on elliptic curve cryptography," *Proc. - Int. Conf. Comput. Networks Inf. Technol.*, pp. 75–79 (2011), doi: 10.1109/ICCNIT.2011.6020911.

[18] C. Wang, G. Xu, and J. Sun, "An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks," *Sensors (Switzerland)*, vol. 17, no. 12 (2017), doi: 10.3390/s17122946.