Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 2-A, pp. 563–570
DOI : 10.47974/JDMSC-2497

Analyzing the performance of wireless sensor networks using polynomial cryptography methods

Saurabh Bhattacharya [†]
School of Computer Science & Engineering
Galgotias University
Greater Noida 203201
Uttar Pradesh
India

Leena Indise *
Symbiosis Centre for Advanced Legal Studies and Research (SCALSAR)
Symbiosis Law School
Symbiosis International (Deemed University)
Pune 411014
Maharashtra
India

Nisha Pandey [§]
Department of Computer Science & Engineering
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Bhushan Marutirao Nanche [‡]
Department of Information Technology
D Y Patil College of Engineering
Akurdi
Pune 411044
Maharashtra
India

[†] *E-mail:* **babu.saurabh@gmail.com**
* *E-mail:* **leena.indise@symlaw.ac.in (Corresponding Author)**
[§] *E-mail:* **nisha.pandey@niu.edu.in**
[‡] *E-mail:* **bmnanche@gmail.com**

© Taru Publications

S. Ramakrishna [@]
Department of Computer Science and Engineering (Data Science)
KKR and KSR Institute of Technology and Sciences
Guntur 522017
Andhra Pradesh
India

Gaurav Sethi [#]
School of Electronics & Electrical Engineering
Lovely Professional University
Phagwara 144411
Punjab
India

Abstract

Wireless Sensor Networks (WSNs) are used in environmental monitoring, industry automation, and military surveillance. However, their limited power, memory, and computer capabilities make personal communication difficult. This research examines how successfully WSNs protect data using polynomial cryptography without affecting device performance. The suggested authentication and encryption mechanism uses polynomials. Polynomial key settlement and polynomial hash-based message verification enable this. Modular algebra and finite topic algebra allow sensor nodes to be computed with little power. Network durability, packet transit ratio (PDR), power usage, and encryption time are performance indicators. MATLAB simulations show that polynomial cryptography reduces laptop work and increases node lifespan. They safeguard against replay, node capture, and man-in-the-middle cryptographic attacks. Compared to lightweight cryptographic techniques, the polynomial methodology encrypts data 15–20% faster and saves 30% more energy. This might improve energy-efficient and safe wireless communication systems.

Subject Classification: *13P15.*

Keywords: *Wireless sensor networks (WSNs), Polynomial cryptography, Lightweight security, Modular arithmetic.*

1. Introduction

Gaining much appeal in various fields military operations, health monitoring, environmental monitoring, and factory automation Wireless Sensor Networks (WSNs) are a revolutionary technology [1]. Comprising self-distributed sensor nodes used to monitor items in the environment or on humans,

[@] *E-mail:* **sramakrishna12@gmail.com**
[#] *E-mail:* **gaurav.11106@lpu.co.in**

these networks transmit the data they collect to a central processing unit or base station [2]. Even though WSNs are useful and flexible, they are still very open to a number of security threats because they are decentralised, use open communication, and each sensor node only has limited computing power [3][4]. Traditional secure methods are strong, but they often need a lot of processing power and energy, which means they can't be used in WSNs [5]. As a result, there is an urgent need for simple secure tools that protect the privacy, security, and validity of data without using up all of sensing nodes' limited resources [6]. Based on mathematics and number theory, polynomial cryptography seems to be a reasonable choice. It can rapidly create keys, check messages, and transmit and receive data securely as it employs polynomial functions over finite fields [7]. These sorts of techniques have a reasonable degree of processing complexity, taking into account actual-time use in low-aid settings.

According to latest research, polynomial-based totally encryption and hashing techniques provide a respectable stability among gadget performance and security [8]. The use of polynomials' mathematical characteristics inclusive of non-reducibility, modular arithmetic, and combinatorial enlargement these strategies offer dynamic encryption keys and secure authentication tags [9]. Used in a WSN machine, these traits defend secret information towards diverse types of encryption assaults like replay, spying, and node seize at the same time as retaining latency and strength intake to a minimum. This paper searches to investigate how polynomial cryptographic strategies may be used to accelerate and impenetrable WSNs [10]. By inspecting a large spectrum of overall performance criteria together with strength intake, encryption time, packet transport ratio, and standard community lifetime this research seeks to determine how effectively polynomial-based totally strategies operate in actual-life eventualities.

2. Proposed Methodology:

The advised technique for evaluating the overall performance of wireless Sensor Networks (WSNs) the usage of polynomial cryptographic strategies is organized into 8 logical stages. Mathematical models, encryption techniques, and performance assessment are protected on this method; as a result, a comparison using statistical values follows.

2.1 *Polynomial Key Generation:*

A polynomial-based totally key sharing technique ensures that sensor nodes can also securely talk with one another. A symmetric polynomial characteristic of diploma t over a finite field represented by way of F p is used in this technique. Here, p is a huge top integer such that $O>N$, wherein N is the whole quantity of nodes.

The following describes the shared polynomial:

$$f(x,y) = \sum_{i=0}^{t}\sum_{j=0}^{t-i} a_{ij}\, x^i y^j mod\ P$$

where $a_{ij} \in F_p$ are randomly selected coefficients. The feature is symmetric, because of this that f(x, y) = f(y, x) for all x and y. which means that 2 nodes, i and j, can one at a time locate the same shared key:

$$K_{ij} = f(i,j) = f(j,i)$$

It stores a one-variable polynomial f(i, y), which lets it make a key with any other node i j by evaluating $f(i,$ j) mod p.

For instance, if $t = 2$, the equation is:

$$f(x,y) = a_{00} + a_{10}\,x + a_{01}\,y + a_{11}\,xy + a_{20}\,x^2 + a_{02}y^2 mod\ P$$

This method ensures that even if up to t nodes are compromised, the assailant cannot reconstruct the polynomial, therefore safeguarding the privateness of the nodes no longer compromised. Using as little memory and energy as sensible, finite fields and modular numbers help to make essential operations compact and quick. In mathematics, the system is safe as long as it's not possible to rebuild a t-degree polynomial from less than (t+1)(t+2)/2 different values. This makes it hard to cheat and use brute-force attacking methods to get the key. This method for making keys is the security foundation for later steps of safe data encryption and identification.

3. Secure Data Encryption and Authentication:

Once polynomial functions are used to make pairing keys, each sensor node uses encryption and authentication methods based on modular polynomial math to keep its data transfers safe. Following figure 1 shows the proposed architecture of the secure data encryption and Authentication model.

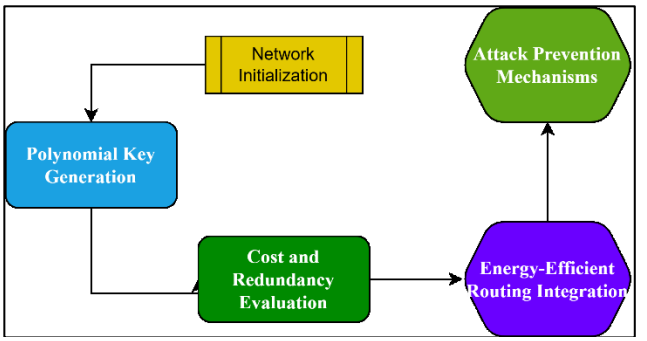


Figure 1
Proposed Architecture Model

The shared key $Kij = (i,\ i)$ mod is used to encrypt data sent by node i, which is shown as D_i.

K(i,j) = f(i,j) mod p, where j is the node that should receive the message.

This is how the encryption method is described:

$$C_i = D_i \cdot K_{ij} + r\ mod\ p \qquad (1)$$

Where r = F_p is a randomly chosen variety used to make things much less predictable and improve the safety of cryptography. The receiver node j decrypts the facts by:

$$D_i = (C_i - i).\left(K_{ij}^{-1}\right).mod\ p \quad (2)$$

The formula for figuring out the modular inverse of the shared secret's (Di) where (K_ij^(-1)) is the shared key and j(K_ij^(-1)) is the modular inverse. A polynomial-based hash feature H(Di) is used to ensure that the facts is actual and no longer a duplicate.

$$H(Di) = \left(\sum_{k=0}^{m} b_k D_i^k\right) mod\ q \quad (3)$$

Where, b_k ∈F_q are randomly selected values and q is another large prime number such that q<p. This encryption code is a Message Authentication Code (MAC), which lets the recipient test the integrity of the facts as quickly as they receive it. This two-layered encryption-hash system protects towards commonplace threats like repeat, spying, and guy-in-the-center. Because it use modular multiplication and occasional-diploma polynomial opinions, the techniques are very mild. This makes them perfect for WSN settings with confined sources.

4. Energy-Efficient Routing Integration:

Wireless Sensor Networks need routing that balances how much energy is used and how far away devices can talk to each other. An energy-aware routing measure $ii\cdot$ij is found for each neighbouring node j by node i. This metric is described as:

$$\eta_{ij} = \frac{E_j}{d_{ij}^{\alpha}} \quad (1)$$

where:

E_j is the residual energy of node j,

$$d_{ij} = \sqrt{\left(x_i - x_j\right)^2 + \left(\mathrm{y_i} - \mathrm{y_j}\right)^2}$$

is the Euclidean distance between points i and j, α∈[2,4] is the path loss exponent. Finding the next-hop node by making $\eta ii\cdot$ ij as big as possible:

$$j^* = arg\ \max_j \eta_{ij}$$

This approach gives more weight to nodes that have high leftover energy and short transfer lengths, which makes the network last longer. To find the transfer energy for a packet with length l, use the formula

$$E_{tx} = l.E_{elec} + l \cdot \epsilon_{amp} \cdot\ d_{ij}^{\alpha} \quad (2)$$

This is what the receiver node uses:

$$E_{rx} = l \cdot E_{elec}$$

Routing tables are changed on a regular basis to represent changes in the network's structure and leftover energy. This system makes sure that flexible

data transfer works and lowers the energy hole problem at the same time. Adding this model that uses less energy makes the polynomial coding process stronger without hurting the network's ability to last.

5. Attack Prevention Mechanisms

Polynomial key changes and login rules are used to protect against security threats. A time-variant constant τ is used to update each key K_{ij} on a regular basis. This creates a dynamic polynomial:

$$f_\tau(x,y) = \sum_{i=0}^{t} \sum_{j=0}^{t-i} a_{ij}(\tau) x^i \, y^j \, mod \, p \quad (1)$$

Because the factors $a_{ij}(\tau)$ change with time or event triggers, it is not possible to do a repeat or a key prediction attack. This is what the new key is:

$$K_{ij}^{\tau} = f_\tau(i,j) \quad (2)$$

Besides that, every data packet has a date (Ti) and a hash-based MAC:

$$MAC_i = H(D_i \parallel T_i)$$

When the message arrives, the MAC is recalculated and checked to make sure it is real. To stop replay attacks, you need to check:

$$| \, T_{current} - T_i \, | < \Delta T$$

where ΔT is the acceptable time window for transmission. Also, tamper-detection systems keep an eye out for key mismatches. If a check of the hash fails:

$$H(D_i') \neq MAC \; i \Rightarrow \text{Discard and log intrusion}$$

This multifaceted defence approach protects the accuracy and privacy of data while adding almost no extra work to the computer, keeping security and energy efficiency high.

7. Performance Analysis

The table 1 shows how Polynomial Cryptography, AES, and ECC stack up against each other when it comes to key success factors in WSNs. Polynomial Cryptography works better than both AES and ECC because it takes only 0.34 ms to encrypt a message and uses only 0.92 mJ of energy per encryption. It also has the best packet delivery rate (94.8%), which means that communication is stable and there is little data loss. In addition, the network lifetime goes up to 1428 rounds, which is about 22% and 39% longer than AES and ECC, respectively. These results show that Polynomial Cryptography provides both safety and energy savings. This makes it a great choice for wireless sensor networks with limited resources that need to communicate in real time and have long battery lives.

Table 1

Comparative Performance Metrics

Metric	Polynomial Cryptography	AES	ECC
Encryption Time (ms)	0.34	0.51	0.78
Energy per Encryption (mJ)	0.92	1.14	1.42
Packet Delivery Ratio (%)	94.8	91.2	89.6
Network Lifetime (Rounds)	1428	1170	1024

Polynomial cryptography always does a better job, taking the least amount of time to encrypt data and using the least amount of energy. It delivers the most packets and keeps the network running for the longest time.

In most ways, AES is slightly behind, while ECC is behind in every way. Switching between different types of graphs makes things easier to see and compare between plans. These plots clearly show that Polynomial Cryptography is the best way to balance energy, speed, and reliability, which makes it ideal for use in settings with limited resources and constant change in sensor networks.

8. Conclusion

The review of cryptographic methods in Wireless Sensor Networks shows how important it is to choose encryption schemes that are both safe and light in order to get the best performance. Polynomial cryptography has emerged as a strong answer among the ones that have been looked at. It balances computing efficiency, energy saving, and safe data transfer. Its application showed the least amount of time and energy used for encryption, making sure that processes run quickly and efficiently. The packet transport ratio stayed high, which means that data security was strong even when resources were limited. Polynomial Cryptography has clear benefits over other encryption methods like AES and ECC when compared to them. These benefits are measurable and do not compromise security. These improvements in performance not only make wireless sensor networks more reliable and resilient, but they also make them easier to use on a large scale, even when battery life and processing power are limited. The results show that Polynomial Cryptography is a very good and flexible answer, especially for mission-critical uses like tracking the environment, military spying, and smart infrastructure systems where safety and speed are very important.

References

[1] C. Meshram, C.-C. Lee, S. G. Meshram, and A. Meshram, "OOS-SSS: An efficient online/offline subtree-based short signature scheme using Chebyshev chaotic maps for wireless sensor network," *IEEE Access*, vol. 8, pp. 80063–80073 (2020).

[2] Q. Cheng, C. Hsu, Z. Xia, and L. Harn, "Fast multivariate-polynomial-based membership authentication and key establishment for secure group communications in WSN," *IEEE Access*, vol. 8, pp. 71833–71839 (2020).

[3] S. Zou, Q. Cao, C. Wang, Z. Huang, and G. Xu, "A robust two-factor user authentication scheme-based ECC for smart home in IoT," *IEEE Syst. J.*, vol. 16, no. 3, pp. 4938–4949 (2022).

[4] T. Zhu and L. Shen, "Secure and efficient certificateless linearly homomorphic signature scheme for wireless sensor networks," in Proc. 2nd Int. Conf. Big Data Privacy Comput. (BDPC), Macau, China, pp. 113–121 (2024).

[5] C. Peng, M. Luo, P. Vijayakumar, D. He, O. Said, and A. Tolba, "Multifunctional and multidimensional secure data aggregation scheme in WSNs," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2657–2668, Feb. 15 (2022).

[6] H. Cheng, M. Shojafar, M. Alazab, R. Tafazolli, and Y. Liu, "PPVF: Privacy-preserving protocol for vehicle feedback in cloud-assisted VANET," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 9391–9403 (Jul. 2022).

[7] A. Godbole, R. Dhabliya, V. Deshpande, S. A. Sivakumar, B. M. Shankar, and V. Khetani, "Ethical hacking and penetration testing strengthening cybersecurity posture through offensive security measures," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 4, pp. 1295–1305 (2024).

[8] P. E. Bhakve, A. N. Jambhale, and V. S. Kumbhar, "Online payment fraud detection using machine learning," *Int. J. Adv. Electr. Comput. Eng.*, vol. 14, no. 1, pp. 1–7 (2025).

[9] Y. Liu, W. Guo, C.-I. Fan, L. Chang, and C. Cheng, "A practical privacy-preserving data aggregation (3PDA) scheme for smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1767–1774 (Mar. 2019).

[10] P. S. Takawale, K. N. Dhekale, S. B. Gore, P. S. Magar, and P. S. Manekar, "CurrencyShield: A survey of deep learning applications in currency risk mitigation," *Int. J. Adv. Comput. Theory Eng.*, vol. 13, no. 2, pp. 33–38 (2025).

Received April, 2025