IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Adaptive Cryptography Secure Token Approach (ACSTA) For Secure Data Integrity and Authentication Mechanism in Wireless Sensor Network

[1]Mr.S.Prabhu and [2]Dr.C.Chandrasekar,

[1]Research Scholar, Department of Computer Science, Government Arts College, Udumalpet, Tamilnadu, India.

[2]Assistant Professor, Department of Computer Science, Government Arts and Science College for Women, Puliakulam, Coimbatore, Tamilnadu, India.

.

Abstract – The Adaptive Cryptography Secure Token Approach (ACSTA) is introduced in this paper to bolster data integrity and authentication in wireless sensor networks (WSNs). Proposed ACSTA merges adaptive cryptography and secure token-based authentication, utilizing elliptic curve cryptography for dynamic encryption parameter adjustments based on risk assessment. Access tokens are employed for meticulous access control. This synergy enhances data security against threats and unauthorized entry. Through evaluations, ACSTA's prowess in fortifying data integrity and authentication in WSNs is evident. ACSTA stands as a potent solution, countering emerging security challenges and advancing secure communication in WSNs.

Keywords: Adaptive Cryptography, Secure Token Approach, Data Integrity, Authentication Mechanism, Wireless Sensor Network;

1. Introduction

Sensor networks offer solutions for monitoring and tracking events across expansive areas. Deployed in clusters, these networks consist of numerous tiny motes with sensing capabilities. These motes execute simple sensing and processing tasks but truly shine in their cooperative communication abilities. Facilitating message exchange among motes and between motes and base stations is crucial for collecting valuable data. This wireless communication occurs in potentially hostile environments, such as military applications, necessitating robust mechanisms for data integrity, authenticity, and confidentiality. While security solutions for wired and wireless networks are established, the unique context of sensor networks demands tailored approaches due to motes' limited power and processing resources. Over the years, researchers have proposed and tested various algorithms to address these security challenges. However, adapting these algorithms for sensor motes requires redesign or the development of new resource-efficient ones.

Data Integrity

Data integrity stands as a cornerstone in the realm of information security, encompassing the fundamental concept of maintaining the accuracy and consistency. In an era defined by an exponential growth of digital data and its widespread utilization, ensuring data integrity has gained paramount significance. It involves safeguarding data against unauthorized alterations, corruptions, or unintended modifications, thereby preserving its authenticity and trustworthiness. The increasing interconnectedness

of systems, the rise of cloud computing, the pervasive nature of data exchange underlines the critical need for robust data integrity measures. Whether in financial transactions, medical records, critical infrastructure control, or personal communications, upholding data integrity is pivotal to engendering confidence among users, making informed decisions, and fostering the smooth functioning of various sectors in today's technologically driven world.

2. Literature Survey

2.1 Watermarking Approach

Farid Lalem (2016) et.al proposed a new fully distributed watermarking approach for WSNs. This method uses distributed semi-blind watermarking to ensure data integrity and authenticity. Nodes add a fixed watermark to data packets, and receivers verify it by comparing with a locally fixed watermark. Mismatch leads to packet rejection. This approach minimizes payload, complexity, and energy use, demonstrated via Cup Carbon simulation.

2.2 Authentication scheme (RDE) based on a lossless fragile watermarking algorithm

Ding et.al (2015) proposed an authentication scheme (RDE) based on a lossless fragile watermarking algorithm for WSNs. In the source sensor context, a one-way hash function is utilized to create watermark details based on neighboring data, which are then incorporated into said data. The manager node, upon data reception, reconstructs the initial information and conducts reliability checks. An RDE approach enables verification of sensor data via these embedded watermark bits, facilitating accurate restoration of the original data.

2.3 Hash Message Authentication Code (HMAC)

Tiny Hash is using HMAC with Secure Hash Algorithm (SHA-1) for message integrity and authentication. Inspired by TinySec, this framework adopts a hash function over traditional block cipher. Concluding remarks stress the need for a lightweight hash design to balance security and resource constraints in various contexts, ensuring effective and efficient security measures.

2.4 Trust Extended Authentication Mechanism

K.SaiAditya (2014) et.al proposed Transitive Trust Extended Authentication Mechanism in Wireless Sensor Networks. Authenticated nodes in this scheme can authenticate new nodes, creating a cascading network of trust. This decentralized process enhances wireless sensor network (WSN) security and simplifies new node validation. Leveraging transitive trust, the approach provides a scalable and robust authentication framework rooted in established trust among nodes.

3. Proposed Methodology

The Adaptive Cryptography Secure Token Approach (ACSTA) enhances wireless sensor network (WSN) security. ACSTA's adaptive nature recalibrates cryptography in real-time to counter evolving threats. Secure tokens amplify authentication, bolstering node verification. ACSTA seamlessly integrates into WSNs, countering challenges. Notes are secured with token keys, generating unique IDs, encrypted for authentication. Timestamps prevent replay attacks. Randomized token key generation enhances security. Multi-phase user access ensures data integrity. ACSTA offers proactive defense, confidentiality, and trust, establishing a robust security framework for dynamic WSN environments.

3.1 Access Token Lifecycle Management Phase

The Adaptive ECC and Token-based Security Scheme (Adaptive ETSS) algorithm involves procedures for access token lifecycle, including creation, issuance, validation, and management. The gateway node, acting as the network's control center, governs the IoT process. Nodes register, undergo legitimacy checks, and receive token keys generated using SHA-2 hashing. Initiating nodes interact with the gateway, computing unique token key signatures for authentication. This dynamic establishes robust authentication and authorization in the wireless sensor network, with the gateway orchestrating processes from root nodes to end users.

$$T_i \xrightarrow{gateway} Send(t_i K)$$

$$S_i = d_j Q_i + T_{ij}$$

$$A_{Th}(N_i) \xrightarrow{hashing} H\left(S_i \left|\left|T_{ij}\right|\right| N_i\right)$$

Where T_i is the token for node i; K is the selected key for encryption; $S_i$is the source node i; D_i

is the data for node i; Q_i is the qualified metrices for data d_i; T_{ij} is the token belongs to node i and j; A_{Th} is the authentication of node N_i; H is used for hashing the data. The verified nodes along with the authenticated token keys are considered to be the authorized nodes and the user can access the authenticated nodes for accessing the data by undergoing the message decryption process.

Data Integrity Assurance Phase

The Adaptive ECC and Token-based Security Scheme (Adaptive ETSS) prioritizes message integrity and authenticity. Token authentication precedes a secondary security layer for data exchange. Malicious nodes trigger alerts. Elliptic Curve Cryptography (ECC) bolsters transmission, utilizing the Weierstrass function, enhancing security via node coordinates. ECC's curve equation

$$y^2 = x^3 + cx + d\ i$$

Includes parameters x, y, c, and d, defining node-specific coefficients. The discriminant $16(4a^3 + 27b^2) \neq 0$ is crucial. ETSS Node Security accounts for infinity point inclusion in elliptic curve coordinates. Public key computation stems from this infinity point, private key from random numbers at key generator point GK. Security hinges on ECC's complexity and curve equation.

Algorithm: Adaptive ECC and Token-based Security Scheme (Adaptive ETSS) with Encryption and Integrity Protection

Input: Node Ni, Data D
Output: Encrypted and protected data
Step 1: Generate Adaptive ECC Key Pair for Node Ni:
  Step 1.1: Determine adaptive ECC parameters (curve, key length) based on risk assessment.
  Step 1.2: Generate ECC private and public keys for Node Ni.
Step 2: Token Generation and Issuance:
  Step 2.1: Generate an access token for Node Ni using the ETSS.
  Step 2.2: Include appropriate token metadata such as token scope and permissions.
Step 3: Data Encryption and Integrity Protection:
  Step 3.1: Extract the preceding 8-byte succession from Data D.
  Step 3.2: Perform a reverse series operation on the extracted 8-byte series.
  Step 3.3: Use the ECC private key of Node Ni to encrypt and sign the reversed series.
    Step 3.3.1: Apply adaptive encryption parameters based on risk assessment.
Step 4: Token-based Integrity Verification:
  Step 4.1: If data is received, verify the validity of the access token associated with Node Ni.
  Step 4.2: Retrieve the ECC public key of Node Ni from the token metadata.
Step 5: Decrypt and Verify Data Integrity:
  Step 5.1: Decrypt the encrypted series using the ECC public key of Node Ni.
  Step 5.2: Perform the reverse series operation in the decrypted series.
  Step 5.3: Compare the reversed series with the original extracted series to verify data integrity.
Step 6: Access Control and Adaptation:
  Step 6.1: Evaluate the risk level associated with Node Ni based on contextual factors.
  Step 6.2: Determine the required level of access control and adaptation for the data.
    Step 6.2.1: For high-risk scenarios, enforce stricter access control and encryption.
    Step 6.2.2: For low-risk scenarios, allow more lenient access controls.
Step 7: Adaptive Updates:
  Step 7.1: Continuously monitor user behavior, system status, and threat intelligence.
  Step 7.2: Update adaptive parameters (ECC curve, key length, encryption strength) based on real-time risk assessment.
  Step 7.3: Adjust access control and encryption settings as necessary.
Step 8: Logging and Auditing:
  Step 8.1: Log all access attempts, adaptive decisions, and encryption processes.
  Step 8.2: Implement regular auditing to review system behavior and effectiveness.
Step 9: Provide Encrypted and protected data

The algorithm establishes secure communication via adaptive ECC key pairs for nodes (Ni), determining parameters based on risk. ECC private and public keys form the foundation. Tokens encapsulate Ni's permissions, defining secure access. This adaptive ECC integration, with Token-based Security Scheme (ETSS), bolsters network resilience. Data preparation involves 8-byte sequence extraction (D), reverse operation enhancing obscurity, and Ni's ECC private key encryption. Adapted parameters ensure robust encryption. This ensures secure data transmission, safeguarding integrity and authenticity.

$$Let\ EccPrivateKey(Ni) represent\ the$$

$$ECC\ private\ key\ of\ Node\ Ni.$$

$$Let\ ReversedSeries\ represent\ the$$

$$result\ of\ the\ reverse\ series\ operation.$$

$$EncryptedData = EncryptAndSign(ReversedSeries, EccPrivateKey(Ni))$$

After encrypted data reception, the algorithm verifies integrity using Node Ni's access token via ETSS. ECC public key from token metadata is pivotal. Upon valid token confirmation, ECC public key decrypts encrypted series. Reverse series operation aligns series, ensuring data integrity, enhancing communication security.

$$Let\ EccPublicKey(Ni) represent\ the$$

$$ECC\ public\ key\ of\ Node\ Ni.$$

$$DecryptedSeries = DecryptAndVerify(EncryptedData, EccPublicKey(Ni))$$

$$ReversedSeriesAfterDecryption = ReverseSeries(DecryptedSeries)$$

Node Ni's risk assessment guides adaptable access control in the algorithm. High risk enforces stringent measures, low risk opts for permissiveness. Real-time ECC parameter adjustments ensure transparency through logging, audits, and system validation, securing evolving landscapes. The generated public key and the private key are applied with the commutative property and the commutative function states in equation

$$K_{Public}\ (C + D) = K_{Private}(D + K)$$

The source nodes send the public key, and the destination node replies with private key, then the key verification is done by the gateway. If the key matches, then the nodes can be labeled as legitimate and the data transmission is done with the data integrity. If the generated key not matches {(C + D) ≠ (D + K)} then the nodes are proved to be illegitimate and the data transmission ends.

4. Experimental Results

4.1 Packet Delivery Ratio (PDR)

It is the proportion between the number of packets transmitted and received.

No of Nodes	RDE	HMAC	Proposed ACSTA
100	60	72	81
200	62	73	82
300	66	75	84
400	72	78	87
500	75	82	94

Table 1.Comparison Table of Packet Delivery Ratio (PDR)

The comparison table 1 of Packet Delivery Ratio (PDR) addressed the different values of existing (RDE, HMAC) and proposed ACSTA. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 60 to 75 and 72 to 82 and proposed ACSTA values start from 81 to 94. The proposed ACSTA gives the best result.

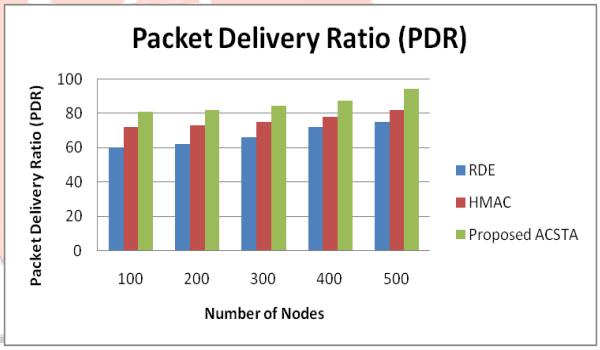

Figure 4.Comparison chart of Packet Delivery Ratio (PDR)

The figure 4 data Packet Delivery Ratio (PDR) describes the different values of existing (RDE, HMAC) and proposed ACSTA. While comparing the existing and the proposed method values are higher than the existing method and No of Nodes in x axis and Packet Delivery Ratio (PDR) in Y axis. The existing values start from 60 to 75 and 72 to 82 and proposed ACSTA values start from 81 to 94. The proposed ACSTA gives the best result.

4.2 Throughput

It denotes that the number of packets successfully received by the receiver.

No of Nodes	RDE	HMAC	Proposed ACSTA
100	52	63	70
200	54	65	74
300	61	68	77
400	64	73	84
500	70	80	90

Table 2.Comparison Table of Throughput

The comparison table 2 of Throughput describes the different values of existing (RDE, HMAC) and proposed ACSTA. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 52 to 70, 63 to 80 and the proposed ACSTA values start from 70 to 90. The proposed ACSTA gives the best result.

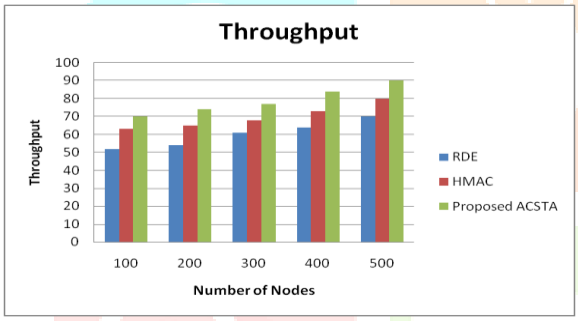

Figure 5.Comparison Chart of Throughput

The figure 5 data Throughput describes the different values of existing (RDE, HMAC) and proposed ACSTA. While comparing the existing and the proposed method values are higher than the existing method and No of Nodes in x axis and throughput in Y axis. The existing values start from 52 to 70, 63 to 80 and proposed ACSTA values start from 70 to 90. The proposed ACSTA gives the best result.

4.3 Average Delay

Average Delay refers to the time it takes for a packet or data to travel from the source node to the destination node in a network

No of Nodes	RDE	HMAC	Proposed ACSTA
100	56	43	32
200	66	63	54
300	74	78	65
400	87	81	71
500	93	85	67

Table 3.Comparison Table of Average Delay

The comparison table 3 of Average Delay describes the different values of existing (RDE, HMAC) and proposed ACSTA. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 56 to 93 and 43 to 85 and proposed ACSTA values start from 32 to 73. The proposed ACSTA gives the best result.

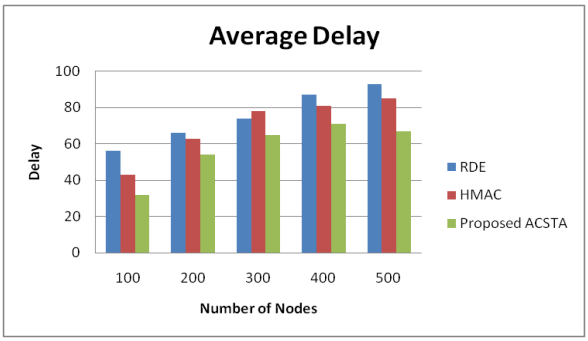

Figure 6.Comparison Table of Average Delay

The figure 6 Average Delay describes the different values of existing (RDE, HMAC) and proposed ACSTA. While comparing the existing and the proposed method values are higher than the existing method and No of Nodes in x axis and Average Delay in Y axis. The existing values start from 56 to 93 and 43 to 85 and proposed ACSTA values start from 32 to 73. The proposed ACSTA gives the best result.

4.4 Remaining Energy

Remaining Energy refers to the amount of energy that is still available or remaining.

No of Nodes	RDE	HMAC	Proposed ACSTA
100	100	100	100
200	82	82	91
300	63	73	82
400	44	61	72
500	20	45	60

Table 4.Comparison Table of Remaining Energy

The table 4 comparison of Remaining Energy describes the different values of existing (RDE, HMAC) and proposed ACSTA. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 100 to 20, 100 to 45 and proposed ACSTA

values start from 100 to 60. The proposed ACSTA gives the best result.

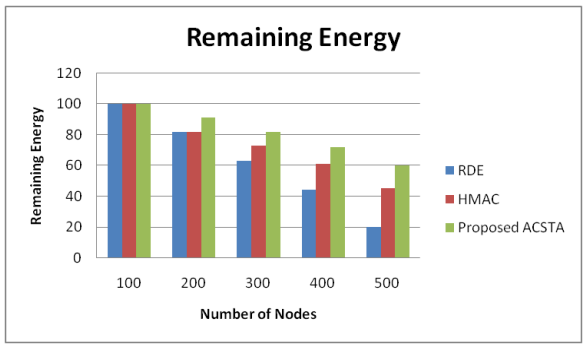

Figure 7.Comparison Chart of Remaining Energy

The figure 7 data Remaining Energy describes the different values of existing (RDE, HMAC) and proposed ACSTA. While comparing the existing and the proposed ACSTA method values are higher than the existing method No of Nodes in x axis and Remaining Energy in Y axis. The existing values start from 100 to 20, 100 to 45 and proposed ACSTA values start from 100 to 60. The proposed ACSTA gives the best result.

5. Conclusion

The Adaptive Cryptography Secure Token Approach (ACSTA) integrates adaptive cryptography with secure token-based authentication, establishing a pioneering framework for robust Data Integrity and Authentication in wireless sensor networks (WSNs). ACSTA's innovation addresses WSN challenges, enhancing security without compromising efficiency. ACSTA stands as a steadfast pillar in the dynamic evolution of WSNs, ushering in a secure and authenticated data communication era.

References

1. Farid Lalem,1 Muath Alshaikh,1 Ahcene Bounceur, ` 1 Reinhardt Euler,1 Lamri Laouamer,2 Laurent Nana,1 Anca Pascu (2016), “Data Authenticity and Integrity in Wireless Sensor Networks Based on a Watermarking Approach”, Proceedings of the Twenty-Ninth International Florida Artificial Intelligence Research Society Conference.
2. Wang, B.; Su, J.; Zhang, Y.; Wang, B.; Shen, J.; Ding, Q.; and Sun, X. 2015. A copyright protection method for wireless sensor networks based on digital watermarking. International Journal of Hybrid Information Technology 8(6):257–268.
3. Qi, X., and Xin, X. 2015. A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization. Journal of Visual Communication and Image Representation.
4. Sindhush, B. S.; Rao, R. K.; and Babu, R. B. 2015. Digital data theft detection using watermarking. Global Journal of Computer Science and Technology 14(9).
5. Sun, X.; Su, J.; Wang, B.; and Liu, Q. 2013. Digital watermarking method for data integrity protection in wireless sensor networks. Int. Journal of Security and Its Applications 7(4):407–416.
6. The Keyed-Hash Message Authentication Code (HMAC). Federal Information Processing Standards Publicatin 198 of the National Institute of Standards and Technology (NIST), 2002 March 6.
7. K.SaiAditya and C.Santwana (2014), “Transitive Trust Extended Authentication Mechanism in Wireless Sensor Networks”, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1828-1832.
8. M. Luo, Y. Luo, Y. Wan, and Z. Wang, “Secure and Efficient Access Control Scheme for Wireless Sensor Networks in the Cross-Domain Context of the IoT,” Security and Communication Networks, vol. 2018, 2018.
9. T. Rault, A. Bouabdallah, and Y. Challal, “Energy efficiency in wireless sensor networks: a top-down survey,” Computer Networks, vol. 67, pp. 104–122, 2014.
10. B. C. Cheng, G. T. Liao, R. Y. Tseng, and P. H. Hsu, “Network lifetime bounds for hierarchical wireless sensor networks in the presence of energy constraints,” Computer Networks, vol. 56, no. 2, pp. 820–831, 2012.