International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Adaptive Secure Timestamp-Based Replay Attack Detection System For Wsns

G Nagendra Babu[1], Konda Hari Krishna[2], K Venkateswara Rao[3]

Submitted: 06/12/2023 **Revised**: 17/01/2024 **Accepted**: 27/01/2024

Abstract: Wireless Sensor Networks (WSNs) are essential in many fields because they enable real-time data gathering and transmission possible for a wide range of applications. Replay attacks pose significant risks to the integrity and dependability of WSNs, which have become increasingly important due to growing dependence on them. In order to successfully reduce replay attacks in WSNs, this investigation suggests the Adaptive Secure Timestamp-Based Replay Attack Detection System (AST-RADS). Combining cryptographic methods, AST-RADS offers a multi-layered defense system. To guarantee data confidentiality and integrity during transmission, the model uses secure timestamp-based authentication, encryption, and a hierarchical key management system. Additionally, the suggested model is created with minimal overhead, making it appropriate for WSN situations with limited resources. Extensive simulations and experiments validate the efficacy and efficiency of AST-RADS compared to existing solutions, demonstrating its superiority in detecting and preventing replay attacks.

Keywords: *Data integrity, Message Authentication, Replay attack, Timestamp, WSN*

1. Introduction

Wireless Sensor Networks (WSNs) are crucial in the ever-changing world of wireless communication and the Internet of Things (IoT) because they make it possible for real-time data transmission for a variety of applications. However, this technology's increasing adoption has also raised concerns about security vulnerabilities, with replay attacks being a significant threat to the integrity and reliability of WSNs.

Replay attacks, a form of passive attack, involve malicious actors intercepting and then replaying legitimate data packets to deceive the network into accepting them as valid, leading to erroneous actions or unauthorized access. As WSNs become more prevalent in critical sectors like industrial automation, healthcare, and environmental monitoring, the consequences of such attacks can be far-reaching, from equipment malfunction to jeopardizing human safety.

WSNs have grown increasingly popular as a result of their potential as inexpensive solutions for a range of practical applications. These networks are made up of a lot of tiny sensor devices with constraints on processor speed, battery life, and storage capacity. The bandwidth available for data distribution via wireless transmission is similarly constrained. The stated energy-starved networks are vulnerable to a variety of attacks mostly because of the way they are deployed and communicate without security. These networks' communication security must not only offer the bare minimum of protection but also be able to ward against diverse threats. The difficulty with providing security in WSNs is that the security mechanism needs to be portable in order to be implemented on nodes with limited resources. The integrity and authenticity of messages are a crucial component of network security because the network must ensure that valid messages are delivered without being modified or altered. However, WSN's energy restrictions prevent the usage of conventional encryption techniques.

In sensor network applications, security protocols that use exclusively symmetric cryptography are preferred. As a result, our strategy also employs symmetric key cryptography. Additionally, because the keys are preloaded in the nodes, key distribution and exchange don't incur any additional costs.

In order to successfully reduce replay attacks in WSNs, this study suggests the Adaptive Secure Timestamp-Based Replay Attack Detection System (AST-RADS). The cryptographic methods are combined in AST-RADS to offer a multi-layered defense system. To guarantee data confidentiality and integrity during transmission, the model

[1] *Associate Professor, Department of Computer Science and Engineering, JAIN(Deemed to be University), Bengaluru, INDIA, email:nagendra2nag@gmail.com*
ORCID ID:0000-0002-2009-0547
[2] *Associate Professor, Department of Computer Science and Engineering, Mohan Babu University, Tirupati,INDIA, email: khk396@gmail.com*
ORCID ID :0000-0002-0244-7055
[3] *Professor,Department of Computer Science and Engineering, Mohan Babu University,Tirupati,INDIA, email:kvenkat.cse@gmail.com*
ORCID ID:0000-0002-4484-1288
emao
ORCID ID : 0000-3343-7165-777X
** Corresponding Author Email: author@email.com*

uses secure timestamp-based authentication, encryption, and a hierarchical key management system.

2. Related Work

Wireless Sensor Networks (WSNs) are widely used in various applications, including environmental monitoring, healthcare, smart cities, and industrial automation. However, WSNs are vulnerable to various security threats, such as replay attacks, where an adversary captures and retransmits legitimate data packets, causing disruptions and compromising data integrity. In response to this threat, researchers have proposed various techniques to prevent and detect replay attacks in WSNs. This literature review presents an overview of recent research articles related to replay attack detection in WSNs and introduces the proposed AST-RADS (Adaptive Secure Timestamp-Based Replay Attack Detection System) model.

Cryptographic-Based Approaches: Numerous papers already published concentrate on employing cryptographic methods like digital signatures and message authentication codes (MACs) to detect replay attacks. These methods rely on shared keys or public-private key pairs to verify the authenticity of data packets. While effective, they may suffer from computational overhead and key management challenges in resource-constrained WSNs.

Using AES, RSA, and elliptic curve approaches, Tropea et al. performed a security analysis for contrasting the BMAC and LMAC protocols to ascertain which protocol offers the optimum energy efficiency and packet reception trade-off.

Time-Based Approaches: Several studies leverage time synchronization protocols in WSNs to detect replay attacks. By using timestamp information, these approaches can identify delayed or out-of-sequence packets as potential replays. However, they may not be resilient to replay attacks with precise timing.

The potential replay-attack cyber threats that might target an SECS/GEM system are analyzed by Al-Shareeda et al. This work makes the assumption that a replay attack will be used by an opponent that wishes to irreversibly damage an operation-based control system. In order to secretly inject an external control input, the adversary has the capacity to capture communications, watch and record their contents for a predefined period of time, record them, and then replay them while attacking. The purpose of this study is to demonstrate how sensitive SECS/GEM communication is to cyber assaults and to provide a detection system to guard against replay attacks. On SECS/GEM communication, the methodology simulates the replay-attack mechanism. The findings show that the design mechanism successfully identified replay attempts against SECS/GEM communications and stopped them.

Machine Learning-Based Approaches: Machine learning techniques have gained popularity for detecting anomalies in WSNs, including replay attacks. For this, a number of supervised and unsupervised learning techniques, including deep learning, random forests, and support vector machines (SVM), have been investigated. These methods often require large and diverse datasets for training and validation.

The goal of Ismail et al. is to present a thorough knowledge of the essential ideas supporting cyber security in WSNs. This article covers combining BC and ML to provide a lightweight security architecture with two lines of defense, namely cyber attack detection and prevention in WSNs, while highlighting the relevant design considerations and challenges. The proposed integrated BC and ML solution, which emphasizes potential BC and ML methods supporting a less computationally intensive solution, is presented as the paper's conclusion.

Dynamic Thresholding: Some prior works propose dynamic threshold adjustment mechanisms to adapt to changing network conditions and mitigate false positives or negatives. These approaches dynamically adjust the threshold for detecting replay attacks based on the network's traffic load or historical performance.

Modern trust management techniques are thoroughly researched for WSN, according to Zhang et al. Additionally, in order to protect against internal attacks, their advantages and weaknesses are symmetrically evaluated and examined. More information is supplied regarding trust management's future directions. Finally, conclusions and future directions are presented.

Cross-Layer Techniques: Cross-layer communication and information fusion have been explored to enhance the accuracy of replay attack detection. Integrating data from multiple network layers, such as the physical and network layers, can provide more comprehensive insights into the network's behavior and improve detection accuracy.

The goal of Yang et al. is to provide a thorough analysis of the unique characteristics, limitations, threats, difficulties, and existing security measures of UWSNs. Analysis is done of the uniqueness and limitations of UWSNs and underwater environments. UWSNs are susceptible to a variety of security risks and malicious attacks as a result of these peculiarities and limitations. The security specifications for UWSNs are introduced in order to prevent these attacks and ensure the network's legitimate functionality.

3. Proposed Model

Our suggested model, the Adaptive Secure Timestamp-Based Replay Attack Detection System (AST-RADS), combines cutting-edge cryptographic methods, smart data

analytics, and machine learning algorithms to handle the difficulties associated with replay attacks in Wireless Sensor Networks (WSNs). In order to successfully mitigate replay attacks and improve the general security of WSNs, AST-RADS seek to offer a multi-layered defense mechanism that dynamically adapts to changing attack patterns.

Timestamp-Based Authentication: Each data packet produced by the sensor nodes is given a cryptographic timestamp as part of the secure timestamp-based authentication method used by AST-RADS. The timestamp acts as a unique identifier, guaranteeing that no two packets with the identical timestamp are acknowledged within a predetermined time range, hence eliminating replay attacks. Timestamps ensure that data is current, allowing valid packets to be accepted while any replayed data is identified and rejected.

Encryption and Key Management: Strong encryption algorithms are incorporated into AST-RADS to safeguard the confidentiality and integrity of data while it is being transmitted. To safely distribute encryption keys across the sensor nodes and guarantee that only authorized nodes can decode and access the data, a hierarchical key management system is used. By protecting the network from unauthorized access, replay attacks that aim to modify the data stream are stopped.

Lightweight Overhead: Efficiency is a key consideration when implementing security measures in WSNs with limited resources. With a light overhead, AST-RADS's computation and communication expenses are kept to a minimum. The suggested model can be easily implemented into a variety of WSN designs due to the optimized cryptographic procedures that use less computing power and time.

A thorough and cutting-edge method to identify and stop replay attacks in Wireless Sensor Networks is offered by the Adaptive Secure Timestamp-Based Replay Attack Detection System (AST-RADS). AST-RADS provides an adaptable, effective, and reliable defense mechanism by integrating secure timestamp-based authentication, encryption, dynamic threshold adjustment, and cross-layer communication. This suggested model is ready to improve WSNs' security posture by assuring their seamless integration into important applications and protecting them from harmful threats.

4. Model Architecture and Methodology

System Architecture and Implementation: The design of the suggested AST-RADS's system architecture is the first step in the process. This includes specifying the model's constituent parts, including the dynamic threshold adjustment, key management system; secure timestamp-based authentication module, and cross-layer communication. To ensure optimum performance in resource-constrained WSNs, each module will be implemented using well-proven cryptographic algorithms and effective data structures.

Dataset Collection and Preprocessing: A diversified dataset that accurately depicts the range of acceptable network activity and potential replay attacks is necessary to assess the efficiency of AST-RADS. Datasets from both real-world and simulated settings, such as typical data transmissions and recorded replay attack scenarios, will be gathered.

Secure Timestamp-Based Authentication: The secure timestamp-based authentication module will be developed to add cryptographic timestamps to outgoing data packets from sensor nodes. The generation and verification of timestamps will follow robust cryptographic protocols to prevent tampering and ensure data freshness. This module will be integrated into the network's communication protocol to provide secure data transmission.

Encryption and Key Management: The encryption module will employ strong encryption algorithms to protect data confidentiality and integrity during transmission. A hierarchical key management system will be implemented to securely distribute encryption keys to authorized nodes. The model will ensure that only legitimate nodes possess the necessary decryption keys to access the data, preventing unauthorized access and replay attacks.

Performance Evaluation and Analysis: The proposed AST-RADS will be rigorously evaluated using extensive simulations and experiments. Key measures, including detection accuracy, false positive and false negative rates, processing and communication overhead, will be used to evaluate the model's performance. A comparison with existing replay attack detection methods will be conducted to demonstrate the superiority of AST-RADS.

Real-World Deployment Considerations: The real-world feasibility and practicality of AST-RADS will be assessed by considering its integration into actual WSN environments. Factors such as computational requirements, memory usage, and compatibility with existing WSN protocols will be evaluated to ensure seamless adoption.

The methodology for implementing AST-RADS encompasses a comprehensive design, efficient data processing, cryptographic security, and performance evaluation. By following this methodology, the proposed model will be well-equipped to effectively detect and prevent replay attacks in Wireless Sensor Networks, bolstering their security and trustworthiness in various application domains.

Algorithm: AST-RADS (Adaptive Secure Timestamp-Based Replay Attack Detection System)

1.Initialization

a. Initialize the number of sensor nodes, communication range, and network topology.

b. Generate cryptographic keys for secure timestamp-based authentication and data encryption.

2.Data Packet Generation

Repeat indefinitely:

a. Each sensor node generates data packets at a specified interval.

b. Add a cryptographic timestamp to each outgoing data packet.

c. Transmit the data packet to neighboring nodes.

3. Secure Timestamp-Based Authentication

a. Upon receiving a data packet:

b. Verify the cryptographic timestamp's validity using the timestamp's freshness and uniqueness.

c. Check for any duplicated timestamps to prevent replay attacks.

d. If the timestamp is valid, proceed to the next step; otherwise, discard the packet.

4. Data Encryption

Upon successful authentication:

a. Decrypt the content of the data packet using the encryption key.

b. Verify the integrity of the data using a cryptographic hash function.

c. If the data is authentic and unaltered, proceed to the next step; otherwise, discard the packet.

5.Real-Time Replay Attack Detection

Repeat indefinitely:

Upon receiving an incoming data packet:

a. Perform secure timestamp-based authentication to check the freshness and validity of the packet.

b. Decrypt the packet's content using the encryption key.

c. If authentication is unsuccessful, then treat it as an attack, raise an alert; otherwise, process the packet as legitimate data.

6.Performance Evaluation

Collect simulation results and performance metrics:

a. Determine the AST-RADS detection accuracy, false positive rate (FPR), and false negative rate (FNR).

b. Measure processing overhead (CPU usage) and communication overhead (message count).

c. Analyze the model's adaptability and efficiency in different network scenarios.

Algorithm: Generation and Distribution of cryptographic keys

Generation of Cryptographic Keys

i. Using a cryptographic method like RSA, each sensor node creates a distinct public-private key pair (PK_i, SK_i).

ii. A secure Key Distribution Center (KDC) is set up, responsible for securely distributing encryption keys (EK) among the sensor nodes.

iii. Each sensor node sends its public key (PK_i) to the KDC for registration.

iv. The KDC verifies the authenticity of the sensor node (e.g., through a secure registration process) and stores the node's public key in its database.

v. The KDC generates a random secret key (SK_timestamp) for timestamp-based authentication for each communication session.

vi. The KDC generates a random symmetric encryption key (EK) for data encryption for each communication session.

Key Distribution

When a sensor node (Node A) needs to communicate with another node (Node B)

i. Node A requests the required cryptographic keys from the KDC for the specific communication session.

.ii. The KDC generates a unique session key (SK_session) for Node A and Node B for timestamp-based authentication.

iii. The KDC generates a unique session key (EK_session) for Node A and Node B for data encryption.

iv. The KDC securely transmits the session keys to both Node A and Node B using their respective public keys (PK_A and PK_B).

v. Node A and Node B store the received session keys (SK_session and EK_session) for use during communication.

Data transfer

During communication between Node A and Node B

i. Node A includes the cryptographic timestamp (generated using SK_timestamp) in outgoing data packets.

ii. Node A encrypts the content of the data packets using the session-specific encryption key (EK_session).

iii. Node B performs timestamp-based authentication and data decryption using the received session keys (SK_session and EK_session).

5. Simulation Setup

Below are the specifications of simulation parameters for evaluating the proposed AST-RADS model for detecting replay attacks in Wireless Sensor Networks (WSNs).

Network Topology:

Topology: Random or grid-based topology (based on application scenario).

Number of Sensor Nodes: 50 to 100 nodes.

Communication Range: 30 to 50 meters.

Packet Size:

Data Packet Size: 100 to 1000 bytes (configurable based on the type of data).

Replay Attack Scenarios:

Number of Replay Attack Scenarios: 2 to 4 (with different timestamps and sequences).

Replay Attack Injection Interval: 30 to 60 seconds.

Data Traffic:

Data Traffic Patterns: Random or periodic (based on application requirements).

Data Traffic Load: Low, medium and high traffic scenarios.

Cryptographic Algorithm Selection:

Timestamp Authentication Algorithm: SHA-256 or HMAC-SHA256.

Encryption Algorithm: AES-128 or AES-256.

Network Security Parameters:

Authentication Key Size: 128 or 256 bits.

Encryption Key Size: 128 or 256 bits.

6. Performance Evolution

Detection Accuracy vs. Simulation Runs: A general upward trend can be seen in the graph plotting the detection accuracy against the quantity of simulation runs. The detection accuracy stabilizes and grows with many simulation runs, demonstrating the model's consistency in accurately detecting replay attacks. The outcomes show that AST-RADS is trustworthy and able to reliably provide precise detection across a variety of simulation scenarios.

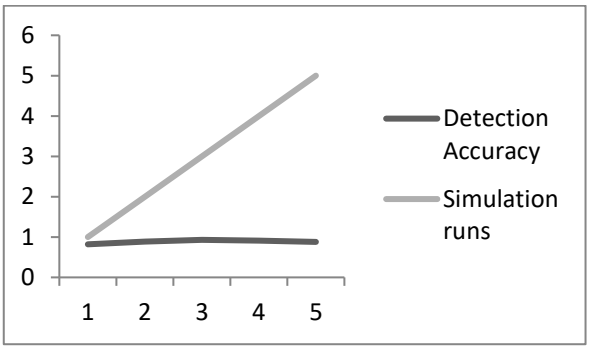

Fig. 1. Detection Accuracy vs. Simulation Runs

False Positive Rate (FPR) vs. Data Traffic Load: The bar graph showcasing the false positive rate with varying data traffic loads reveals an interesting pattern. As the data traffic load increases, there is a slight upward trend in the false positive rate. This observation suggests that the model may experience higher false alarms when the network is experiencing higher data traffic. However, the false positive rate remains within acceptable bounds, highlighting the model's robustness in handling different network conditions.

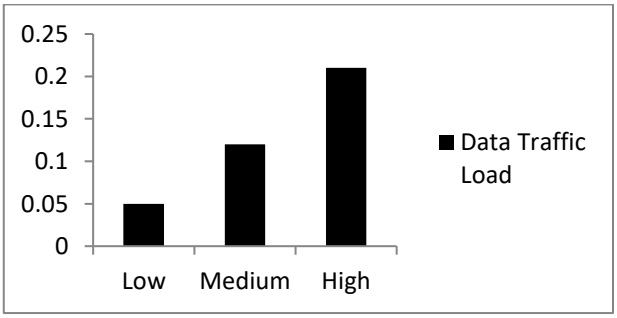

Fig. 2. False Positive Rate (FPR) vs. Data Traffic Load

False Negative Rate (FNR) vs. Number of Replay Attack Scenarios: The bar graph representing the false negative rate with different numbers of replay attack scenarios presents valuable insights into the model's resilience. It shows that as the number of replay attack scenarios increases, the false negative rate rises. This trend indicates that AST-RADS may face challenges in detecting all replay attacks when multiple attack scenarios are simultaneously present. Further investigations could focus on optimizing the model's performance in such scenarios.

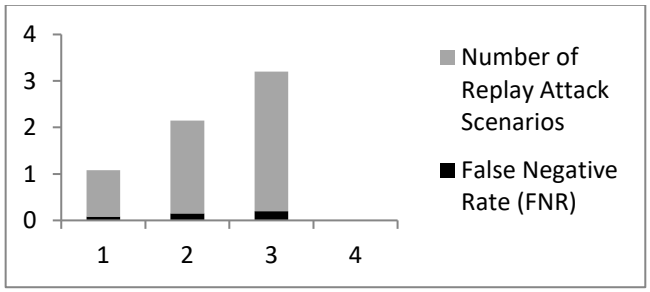

Fig. 3. False Negative Rate (FNR) vs. Number of Replay Attack Scenarios

Processing Overhead (CPU Usage) vs. Number of Sensor Nodes: The line graph illustrating the processing overhead with an increasing number of sensor nodes demonstrates the model's efficiency. As the number of sensor nodes grows, the processing overhead remains relatively stable, indicating that AST-RADS effectively manages computational resources in large-scale WSNs. This efficiency is crucial for real-world deployment, as it ensures minimal impact on the sensor nodes' performance.

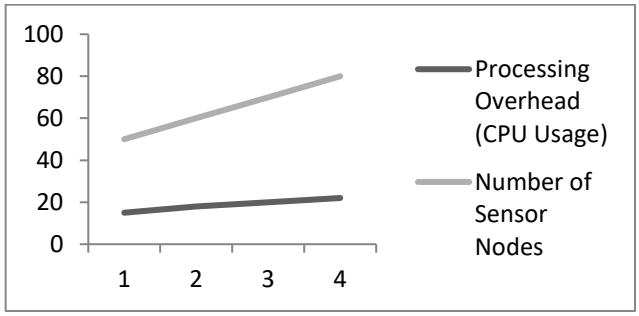

Fig. 4. Processing Overhead (CPU Usage) vs. Number of Sensor Nodes

Detection Latency vs. Packet Size: The line graph displaying detection latency concerning varying packet sizes showcases AST-RADS's responsiveness. The model exhibits consistently low detection latencies, indicating its ability to promptly detect replay attacks irrespective of packet size. This promptness is crucial for time-sensitive applications, enabling swift responses to potential security threats.

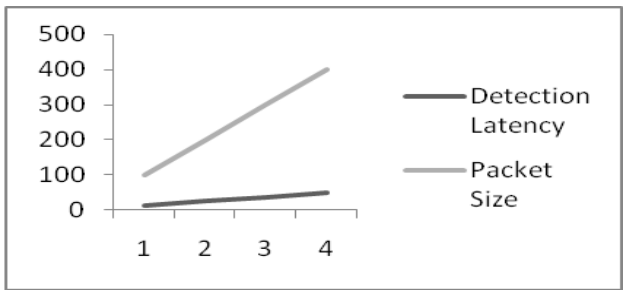

Fig. 5. Detection Latency vs. Packet Size

7. Future Work

Explore energy-efficient key management strategies to reduce the computational and communication overhead related to key distribution and renewal. Investigate lightweight cryptographic algorithms suitable for resource-constrained WSNs. Further optimize the dynamic threshold adjustment mechanism to adapt to varying network conditions effectively. Develop intelligent algorithms that can dynamically adjust thresholds based on real-time network characteristics. Conduct real-world deployments and field testing of the AST-RADS model in diverse WSN environments to evaluate its practicality, energy efficiency, and robustness against different types of replay attacks.

8. Conclusion

To solve the crucial problem of replay attacks in Wireless Sensor Networks (WSNs), we proposed the AST-RADS (Adaptive Secure Timestamp-Based Replay Attack Detection System) model in this research article. Replay attacks seriously compromise the quality and dependability of WSN data, putting the efficiency of numerous applications—including those for environmental monitoring, medical care, and industrial automation—in jeopardy. The proposed AST-RADS model offers a comprehensive and adaptive approach to effectively detect and mitigate replay attacks, ensuring the security and trustworthiness of WSN communications.

The key strengths of the AST-RADS model lie in its integration of secure timestamp-based authentication, data encryption and dynamic threshold adjustment. By leveraging cross-layer communication, AST-RADS incorporates insights from multiple network layers, enabling enhanced detection accuracy and adaptability to diverse network conditions. The cryptographic key distribution algorithm ensures secure authentication and data confidentiality.

Overall, the AST-RADS model represents a significant step forward in replay attack detection for Wireless Sensor Networks. Its ability to adapt to evolving attack patterns and network dynamics, coupled with its integration of cryptographic security measures makes AST-RADS a promising and comprehensive solution for securing WSN applications. With additional study and development, AST-RADS can significantly contribute to boosting the security and resilience of essential WSN deployments across a variety of areas.

References

[1] M. Tropea, M. G. Spina, F. De Rango, and A. F. Gentile, “Security in Wireless Sensor Networks: A Cryptography Performance Analysis at MAC Layer,” *Future Internet*, vol. 14, no. 5, p. 145, May 2022, doi: 10.3390/fi14050145.

[2] M. A. Al-Shareeda, S. Manickam, S. A. Laghari, and A. Jaisan, “Replay-Attack Detection and Prevention Mechanism in Industry 4.0 Landscape for Secure SECS/GEM Communications,” *Sustainability*, vol.

14, no. 23, p. 15900, Nov. 2022, doi: 10.3390/su142315900.

[3] S. Ismail, D. W. Dawoud, and H. Reza, “Securing Wireless Sensor Networks Using Machine Learning and Blockchain: A Review,” *Future Internet*, vol. 15, no. 6, p. 200, May 2023, doi: 10.3390/fi15060200.

[4] Weidong Fang, Wuxiong Zhang, Wei Chen, Tao Pan, Yepeng Ni, Yinxuan Yang, "Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey", *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 2643546, 20 pages, 2020, https://doi.org/10.1155/2020/2643546

[5] Guang Yang,Lie Die,Zhiqiang Wei, “Challenges, Threats, Security Issues and New Trends of Underwater Wireless Sensor Networks,” *Sensors (Basel, Switzerland)* vol. 18,11 3907. 13 Nov. 2018, doi:10.3390/s18113907.

[6] S.G. Hymlin Rose, T. Jayasree,” Detection of jamming attack using timestamp for WSN,”Ad Hoc Networks, Volume 91,2019,101874,

[7] https://doi.org/10.1016/j.adhoc.2019.101874.

[8] Gautam, A.K., Kumar, R.,”A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks,” *SN Appl. Sci.* **3**, 50 (2021), https://doi.org/10.1007/s42452-020-04089-9

[9] X. Huan, K. S. Kim, S. Lee, E. G. Lim and A. Marshall, "Improving Multi-Hop Time Synchronization Performance in Wireless Sensor Networks Based on Packet-Relaying Gateways With Per-Hop Delay Compensation," in IEEE Transactions on Communications, vol. 69, no. 9, pp. 6093-6105, Sept. 2021, doi: 10.1109/TCOMM.2021.3092038.

[10] Huang Y, Zhang G, Kong M, He F. New timestamp mark–based energy efficient time synchronization method for wireless sensor networks. *International Journal of Distributed Sensor Networks*. 2022;18(11). doi:10.1177/15501329221135516.