©2022 International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies

ISSN 2228-9860 eISSN 1906-9642 CODEN: ITJEA8

International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies

http://TuEngr.com

# An End-to-End Security Aware WSN Approach with Localization & Authentication and Data Exchange Security

**R Priyanka[1*], K Satyanarayan Reddy[2]**

[1]*Department of Information Science and Engineering, Cambridge Institute of Technology, Bangalore, Affiliated to VTU, Belagavi, INDIA.*

[2]*Cambridge Institute of Technology North Campus Bangalore, Affiliated to VTU, Belagavi, INDIA.*

**Corresponding Author (Tel: +919606694391, Email: priyanka.89.r@gmail.com).*

**Paper ID: 13A7N**

**Volume 13 Issue 7**

Received 15 January 2022
Received in revised form 15 May 2022
Accepted 23 May 2022
Available online 30 May 2022

**Keywords:**
WSN; Security; Localization; ECDH; RSA; Cryptography.

## Abstract

The demand for sensor Network-based communication has increased due to its wide range of applications. Reliability of data collection is a challenging task in these networks. There are two concerns about sensor placement. First, attackers may target the localization process to manipulate estimated positions. Second, because sensor nodes may get hacked, Base Station (BS) might not be able to trust the positions provided by sensor nodes. Researchers have proposed two techniques to address these two issues: secure localization and location verification. Routing in WSN is considered because it facilitates the transmission of data from any source node to the destinated nodes. Routing attacks have the potential to disrupt and degrade WSN functionality. Numerous experiments, including cryptographic approaches and centralized routing, have been done to enhance confidence between routing nodes. However, the generally utilized message transmission approaches are unsuitable in reality because of the difficulties they face in accurately recognizing hostile node activity. This study focuses on introducing a combined method where secure node localization, node authentication, and secure data exchange via cryptography are presented. The comparative analysis shows that the proposed approach can prevent a greater number of internal and external attacks when compared with state-of-art techniques.

**Disciplinary**: Computer Science & Engineering.

©2022 INT TRANS J ENG MANAG SCI TECH.

## Cite This Article:

Priyanka, R., Reddy, K. S. (2022). An End-to-End Security Aware WSN Approach with Localization & Authentication and Data Exchange Security. *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies, 13*(7), 13A7N, 1-15. http://TUENGR.COM/V13/13A7N.pdf DOI: 10.14456/ITJEMAST.2022.140

# 1 Introduction

The growth of compact, low-cost devices known as sensors has been boosted by technological advancement. The detected data is then transmitted to a chosen destination called a sink node or a base station [1]. WSNs (Wireless Sensor Networks) [2] comprise a hefty count of sensory devices that function together to observe a specific region. This network class has grown in popularity [3] due to its broad applicability in various domains, such as military, industrial, and domestic applications.

Generally, the WSNs are deployed for specific purposes. Due to this condition, WSN faces several challenges related to its management. Similarly, it faces several challenges such as limited computation capacity, decentralized task processing, scalability, efficient deployment, the communication range of nodes and routing, etc. [4 -6]. In light of these WSN problems, if we receive data without knowledge of the source's location in any of the applications mentioned above, the data has no meaning or is simply meaningless. As a result, localization (data source location estimate) is an essential aspect of WSN or IoT [7-8]. The most straightforward technique to determine a node's position is the Global Positioning System (GPS) [9]. However, it makes the network expensive, making it unsuitable for situations when a large number of sensors are required. Satellite communication, on the other hand, needs additional energy and processing capacity [10-11]. WSN solutions, on the other hand, need to be somewhat reliable, energy-conservative, and resilient. These approaches may be broadly divided into two groups, i.e., range-based and range-free localization. Since their inception, a constant battle between the two groups has existed [12, 13, 14].

The information acquired by the nodes in the WSNs is transferred to the destination node either directly or indirectly through other sensor nodes. [18]. As a result, a direct or one-hop connection for transmitting data to the sink nodes isn't possible. The nodes distributed across longer distances rely on the assistance of other sensor nodes to route their data packets to the target node [19]. This challenge may be handled by establishing a cluster of sensor nodes, selecting a cluster head (CH), and routing data through the CHs [20-23].

This research focuses on the challenges mentioned above in WSNs and introduces novel key management, authentication, and cryptography-based approaches to secure the node information and protect the data. The main contribution of the proposed method is as follows:

- To study existing protocols that claim the secure communication and localization in sensor networks
- To develop a secure node localization scheme by using a Hash mechanism
- To incorporate node authentication and data encryption along with a third-party verifier to ensure full-fledged security in the network.

For the rest of the article, section II consists of a literature survey on existing techniques of security provisioning in WSN, section III discusses the proposed key management, authentication,

and cryptography model, and section IV presents the outcome of this approach along with security analysis. Lastly, section V discusses the research conclusion.

## 2 Literature Review

In this section, a brief description of various techniques related to minimizing energy consumption by utilizing energy proficient schemes in WSN is presented Al Mazaideh et al. [5] developed a multi-hop routing algorithm with the help of compressive sensing and genetic algorithm. Similar to this, Adnan et al. [15] created clustering-based multi-hop routing with the help of fuzzy logic. Based on the clustering concept, Rezaeipanah et al. [28] presented a new approach where clusters are re-formed during the multi-hop routing procedure to ensure minimum energy consumption, minimum delay, and maximum packet delivery. In [29], Arora et al. discussed two types of cluster communications, inter and intra.

The authors developed Energy-efficient Balanced Multi-Hop Routing Scheme (EBMRS). Rajaram et al. [30] adopted a fuzzy logic approach for routing and load balancing in WSN. Moreover, this approach presents a 3-tier multi-hop optimized routing scheme. Hamzah et al. [25] used fuzzy logic for CH selection, where fuzzy rules are designed based on residual energy, position suitability, node deployment strategy, and distance from the base station. Yong et al. [31] developed tree-based multi-hop routing to optimize energy consumption.

Shyjith et al. [32] suggested an optimization-based approach for optimal and dynamic cluster head selection for WSN. Lastly, the outcome of this approach is measured in terms of energy and network lifespan. Qabouche et al. [33] presented hybrid energy coherent static routing protocol to extend the lifespan of WSN. Koyuncu et al. [34] considered agricultural monitoring using WSN and adopted the Deterministic Energy-Efficient Clustering (DEC) protocol and modified it by combining a multi-tier model.

Qureshi et al. [35] also focused on the application of WSN in agriculture and introduced Gateway Clustering Energy-Efficient Centroid (GCEEC) routing protocol. The gateway node is responsible for packet transmission to the base station. Xu et al. [36] explored the existing routing scheme of WSNs and identified that optimization schemes could be a promising solution to prolong the network lifespan. This scheme adopts the ant colony optimization algorithm to lessen power depletion. Han et al. [37] presented WPO-EECRP, weight, and parameter optimization for WSN.

## 3 Method

The current literature has revealed several drawbacks in WSNs in terms of network security. Several schemes have been introduced, but achieving remarkable energy efficiency while maintaining security remains tedious. Thus, a combined system to handle secure localization while maintaining a secure data exchange is presented in this work.

The complete model includes the following phases:

**Securing the location information**: in this stage, we use the Hash generation mechanism to anonymize the location of the localized sensor node by concealing it through Hash. It prevents location spoofing.

**Cluster formation and cluster head selection**: for this stage, we use our previous methodology [43], which considers the node's remaining energy, and distance from BS to elect the CH.

**Secure data exchange**: in this stage, the cluster members communicate with their corresponding cluster head. Before communication, the participating nodes are authenticated, and the message is encrypted and transmitted to CH.

**Secure communication between CH and FN**: in this stage, the cluster head node identifies its forwarder node (next cluster head) as the relay node towards the base station. In this stage, three security tasks are performed: authentication of CHs, verifying the message with third-party authority, and encrypting the message.

After processing through these stages, the data is received at the base station. The overall architecture of the proposed system is presented in the given figure.

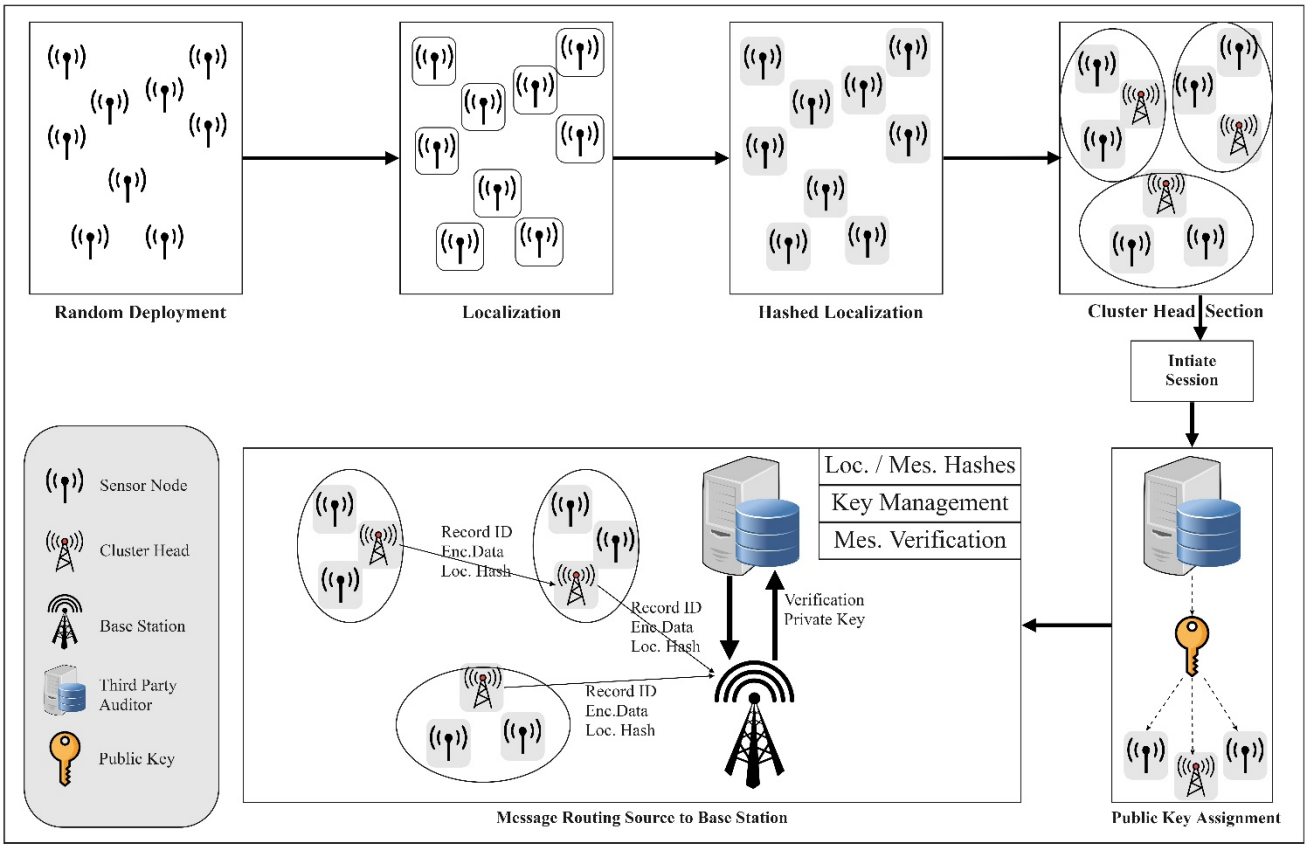


**Figure 1:** Proposed secure WSN architecture

As per the proposed model architecture Figure 1, at first, the sensor nodes are arbitrarily installed in the network grid; further, the localization process takes place where the locations of each node are identified. Subsequently, the locations are anonymized using the SHA-256 hashing(DS) technique. The cluster head selection takes place based on distance and energy parameters. Upon setup, before initiating any transaction, a session is created, and a shared public key is disseminated to all the nodes by the Third-Party Auditor (TPA). Next, the sensor nodes' data packets containing information like record ID, encrypted message, and location hash are forwarded to the intra-cluster CH. CH routes the packets inter-cluster to the forwarding node or the Base

Station. Finally, the base station sends the packet to TPA for message authenticity check and receives a private key from TPA upon successful verification.

## 3.1 Hash Operation

To protect the sensor node location, we adopt the SHA-256 hashing technique for the generation of the nodes' location hashes and messages. Below some sample outcomes are presented:

Input: This is a WSN

Hash: B908AA0529D7D119B7FA58177463B69EF9F9CADA48E71F0F77E0527A30783455

Input: (92.5, 89.3)

Hash: 82E9EB1D16207A3D0D2419819FCFE1FC0A385FC953F78077E4D9BA98C166FDA1

## 3.2 ECDH Key Exchange for Data Exchange

According to DH key exchange, give $g^u$ and $g^v$ where $u$ and $v$ are randomly extracted from $\{1, \dots, |G|\}$ then it becomes difficult to compute $g^{uv}$. In some cases, the adversary may be able to extract some part but this makes the adversary weak to extract the information. However, we adopt the ECDH key exchange to increase security because ECDH is an anonymous key agreement scheme. This approach enables data exchange between two communicating nodes which are having an elliptic curve public-private key pair. These key pairs are used to establish secret sharing over an insecure WSN communication channel. The ECDH mechanism follows the working of classical DH key exchange except that it replaces modular exponentiations and adopts ECC point multiplication. Property of EC points can be defined as

$$(a * G) * b = (b * G) * a \qquad (1).$$

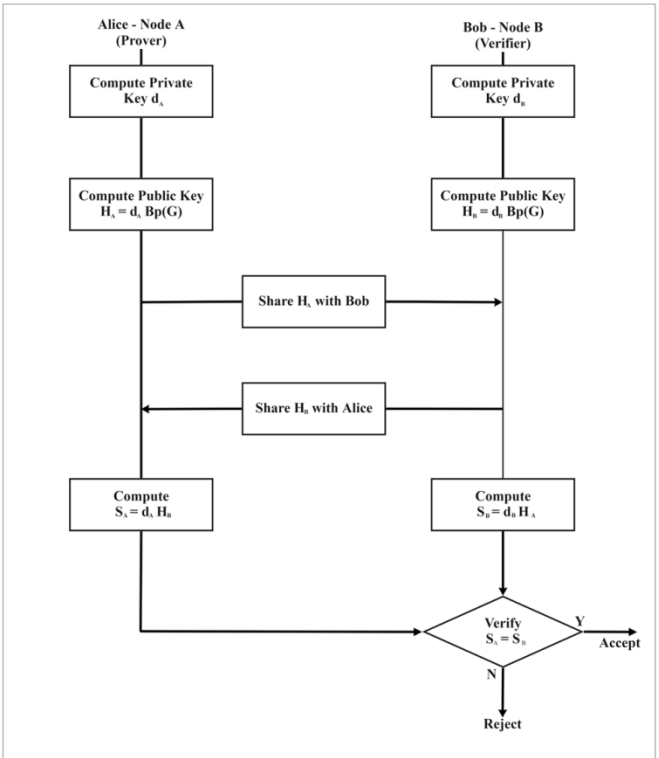


**Figure 2:** ECDH key exchange

Figure 2 depicts the ECDH key exchange model, which consists of two communicating nodes as node A and node B. Node A is denoted as Alice which is a "Prover" entity and node B is denoted by Bob which is a "Verifier" entity.

The overall procedure of ECDH is depicted in Figure 2, as follows:

Step 1: Setup phase: node A and node B chose a point $E$ over $F_p$ which contains a common base point as $B_p(G)$ which is an element of $F_p$.

Step 2: node A generates the private as $d_A$ and performs point multiplication to obtain the public key as $H_A = d_A\, B_p(G)$ and node A transmits this info $H_A$ to node B.

Step 3: node B also generates the private key as $d_B$ and generates the pubic key $H_B = d_B B_p(G)$. This info is sent to node A.

Step 4: these public keys $H_A$ and $H_B$ are exchanged between node A and node B

Step 5: node A (Alice) computes $S = d_A\, H_B$ by applying point multiplication.

Step 6: node B (Bob) computes $S = d_B\, H_A$ by applying point multiplication

step 7: shared secret $S$ is common for both nodes as $S = d_A H_B = d_A \left(d_B B_p(g)\right) = d_B \left(d_A B_p(G)\right) = d_B H_B$

## 3.3 RSA Cryptography

Cryptography has a pivotal role in the secure provisioning of a sensor network to ensure secure information exchange among nodes. In this stage, we adopt the RSA-based cryptography model. The RSA cryptography scheme performs modular exponentiation operation, and the size of the modulus is used to determine the security strength of the cipher. To generate the key, it uses two random prime numbers, and their product is computed

$$n = pq \tag{2}.$$

Further, $\phi(n)$ is used to define the number of integers that are smaller than $n$ and prime to $n$. If $n$ is the product of these small prime numbers then the $\phi$ can be stated as

$$\phi(n) = (p-1)(q-1) \tag{3}.$$

Further, a random number $e$ is selected such that $e$ and $\phi(n)$ are the primes, next, an integer $d$ is computed in such a way that it is the inverse of $e$ *modulo* $\phi(n)$, this can be expressed as

$$\gcd\left(e, \phi(n)\right) = 1 \tag{4},$$

$$d = 1\, mod\, \phi(n) \tag{5}.$$

The public key is $\{e, n\}$ and the private key is denoted as $\{d, n\}$. Based on modulo operations, it performs an encryption and decryption process which helps to generate the cipher text and decipher text as

$$c = s^e mod\, n \tag{6},$$

$$s = c^d mod\, n \tag{7}.$$

The operation $c = s^e mod\ n$ is used to perform the encryption whereas $s = c^d mod\ n$ denotes the decrypted data. Below given figure 3 depicts the overall algorithm of RSA cryptography.

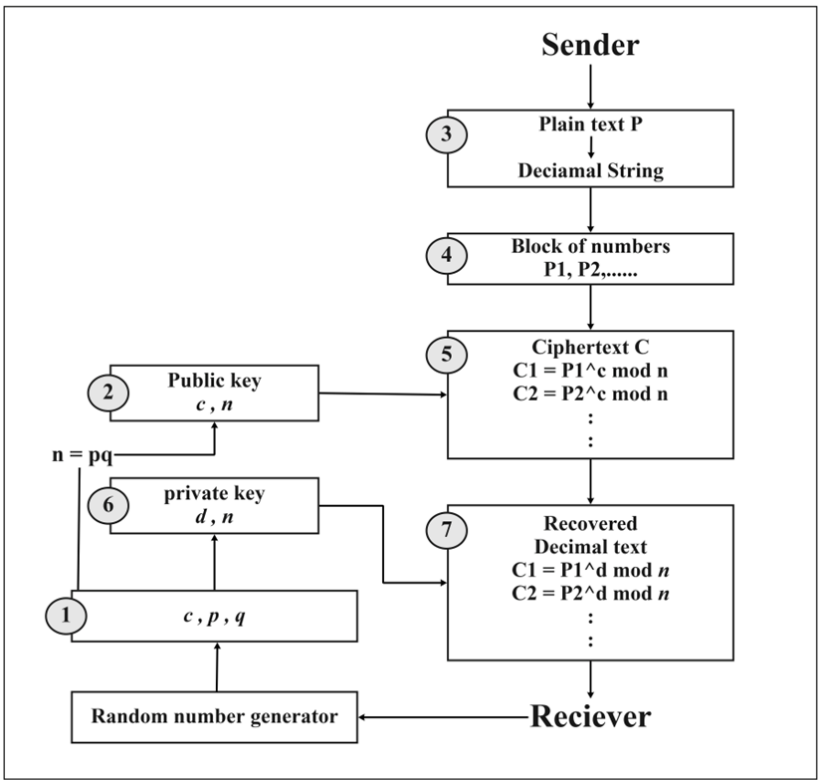


**Figure 3:** RSA cryptography

## 4 Result and Discussion

The outcome of the projected secure localization and data exchange approach is validated by comparing the obtained performance with various state-of-the-art algorithms. The complete system is implemented using the MATLAB simulation tool. Below given table 1 depicts the environment configuration of the simulation.

**Table 1:** Simulation parameters

| Parameter | Value |
|---|---|
| Network Area | 100x100m2 |
| Number of nodes | 100 |
| Packet size | 4000/bits |
| $\epsilon_{mp}$ | 0.0013pj/bit/m4 |
| $\epsilon_{fs}$ | 10pj/bit/m2 |
| $E_{elec}$ | 50nJ/bit |
| Initial energy | 0.5J |
| Hash algorithm | SHA-256 |

The efficacy of the proposed approach is evaluated by calculating the detection accuracy of the malicious node. The attained outcome is contrasted against the existing technique as mentioned in [29]. The detection accuracy is computed by finding the ratio of nodes identified and the total nodes count. It is expressed as

$$Acc = \frac{Identified\ Nodes}{Total\ Nodes} \times 100 \quad (8).$$

For this experiment, we consider two scenarios; in the first step, we vary the number of malicious nodes during deployment and measure the detection accuracy. In the second stage, we change the ratio of beacon nodes and measure the detection performance.

Figure 4 depicts the detection accuracy performance for a varied number of malicious nodes. In this experiment, we have varied malicious nodes from 5 to 30.

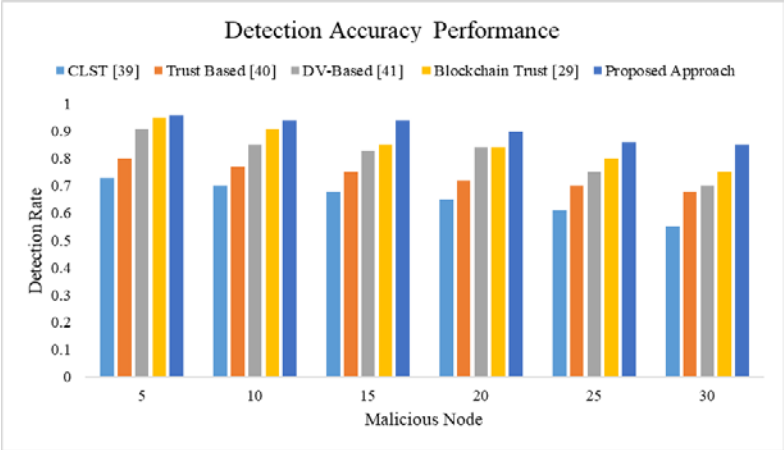


**Figure 4:** Detection accuracy performance

According to this experiment, the average detection rate is obtained as 65.33%, 73.66%, 81.33%, 85.11%, and 90.83 by using the CLST [39], Trust-Based [40], DV-Based [41], Blockchain Trust [29], and the proposed approach, respectively. The increase in the count of malicious nodes affects detection accuracy performance. Below given figure 5 depicts the detection accuracy performance for diverse no. of beacon nodes. The total count of beacon nodes is between 5-30 nodes.

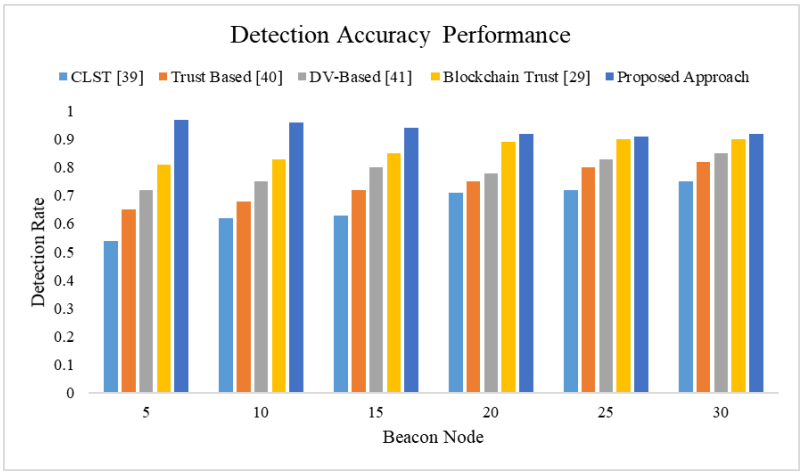


**Figure 5:** Detection accuracy performance for varied beacon node

Through the experimentation, average detection accuracy is attained as 66.16%, 73.66%, 78.83%, 86.33%, and 95.66% using CLST [39], Trust-Based [40], DV-Based [41], Blockchain Trust [29], and proposed techniques, respectively.

Further, we evaluate the efficacy of the proposed secure routing method by assessing its effect on network lifetime. For this experiment, we vary the malicious nodes count in the n/w;

therefore, as the no. of malicious nodes increases, it causes energy drain attacks by message replaying and degrades performance by various means. The attained outcomes are compared with the existing techniques mentioned in [42]. Figure 6 depicts the network lifetime efficiency as depicted below.

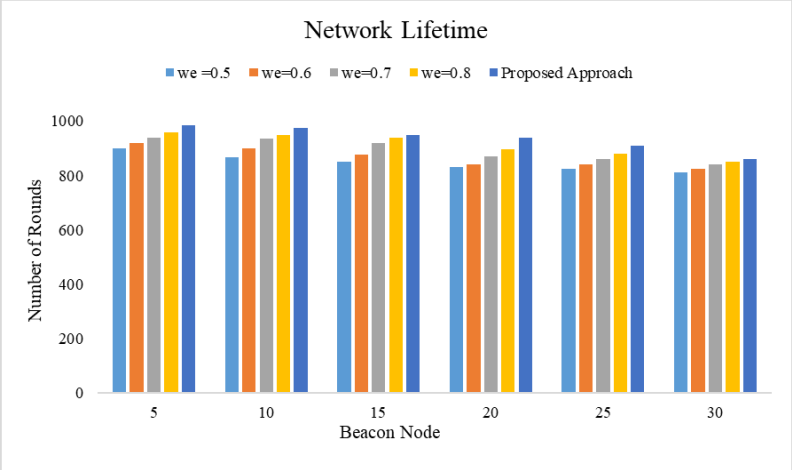


**Figure 6:** Network lifetime performance

As per the experimentation, the average network lifetime performance results are obtained as 847 rounds, 867 rounds, 894 rounds, 912 rounds, and 936 rounds using the existing routing technique [42] and the proposed method.

## 4.1 Security Analysis

Here, the security analysis of the proposed approach is presented and compared with the existing security protocols for WSN communication.

### 4.1.1 Message Replay Attack

Consider that an attacker may acquire access to a sensor node by replaying a message issued by a legitimate user node. The sensor node dismisses messages that come after a specific threshold equivalent to the maximum communication duration from a valid user node to the sensor node. As a result, the proposed system is resistant to replay assaults. Therefore, incorporating the time stamp during information exchange and authenticating between nodes helps prevent message replay attacks.

### 4.1.2 Man-In-The-Middle (MITM) Attack

An attacker attempting a MITM attack intercepts and forges authentication messages to influence communication among genuine entities, then re-transmits those messages to prove to them that they have direct contact with each other. This technique uses authentication and encryption to safeguard all authentication messages sent between network entities. However, without knowing these unique values, the attacker cannot counterfeit the verification message. As a result, this technique is safe from MITM.

### 4.1.3 Flooding Attacks

The attacker transmits multiple HELLO packets while attempting to drain n/w battery power in this attack. The sensory nodes receive and share data to the dynamically allocated CH in the n/w topology in our technique, and the base station maintains data flow. To transmit data, the base station authenticates each node. As a result, our approach is unaffected by the 'Hello' flood assault. Similarly, because the data from a sensor node is transmitted via a selected CH, it doesn't get affected by the flooding attack.

### 4.1.4 Denial of Service Attack

Here, the attacker transmits the junk data packets and uses maximum n/w capacity to block the services and avert the system user's service accessibility. This type of attack gets solved by dynamically altering the CH node after each transmission round. Furthermore, an acknowledged message delivered by the BS aids in preventing such threats.

Table 2 presents the comparative analysis where various security attributes are considered to prove the robustness of the proposed approach for multiple attacks.

**Table 2:** Security analysis: resiliency to various attacks

| Security Feature | [13] | [19] | [14] | Proposed approach |
|---|---|---|---|---|
| User anonymity | ✓ | ✓ | ✓ | ✓ |
| Mutual Authentication | ✓ | ✓ | ✓ | ✓ |
| Subsequence Authentication | × | × | × | ✓ |
| Forward secrecy | × | × | ✓ | ✓ |
| Desynchronization attack | × | × | ✓ | ✓ |
| Smart card loss attack | × | × | × | ✓ |
| Replay attack | ✓ | ✓ | ✓ | ✓ |
| Impersonation attack | ✓ | ✓ | ✓ | ✓ |
| MITM attack | ✓ | ✓ | ✓ | ✓ |
| Insider attack | ✓ | ✓ | ✓ | ✓ |

According to this analysis, we conclude that the proposed method is capable of preventing various types of attacks on the network.

## 4.2 Comparative Analysis

This subsection presents a comparative study where the proposed (GT-PSO[43] and security-aware routing) model is compared. The obtained performance is evaluated against existing methods. Figure 7 depicts the comparative analysis in terms of packet delivery performance.

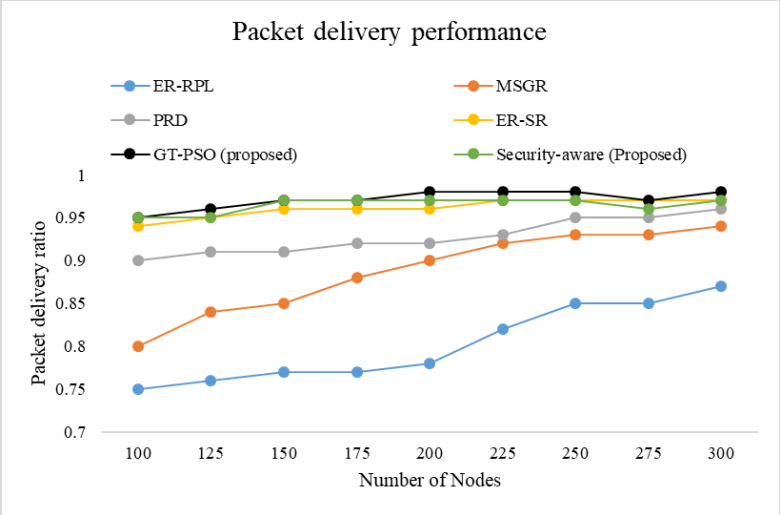


**Figure 7:** Packet delivery performance

The obtained results are compared against the existing scheme. The average packet delivery results are attained as 0.80, 0.88, 0.92, 0.96, 0.97, and 0.96 using ER-RPL, MSGR, PRD, ER-SR, GT-PSO (proposed), and Proposed (security) techniques, respectively.

Further, we extended this experiment and measured the network lifetime performance. The proposed approaches GT-PSO and security-aware routing techniques [43] help achieve better network lifetime performance. The proposed security-aware system achieves better network lifetime performance because it mitigates the energy drain attacks, thus maintaining a better network lifetime.

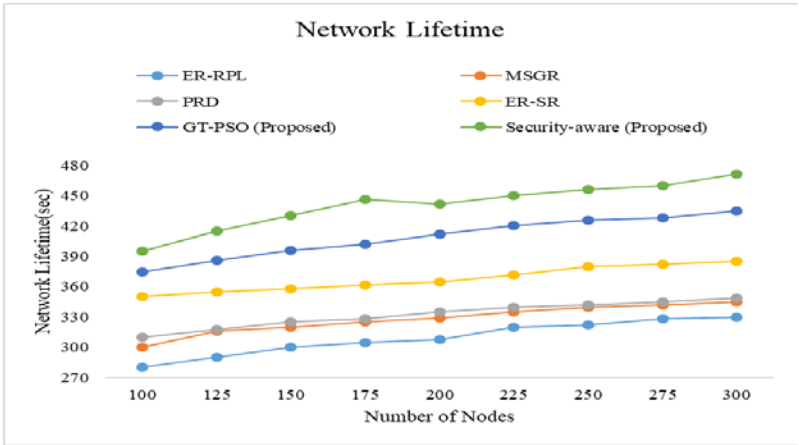


**Figure 8:** Network lifetime performance

The obtained Network lifetime efficiency is presented in the above figure 8, which shows a significant improvement in network lifetime using the proposed schemes. The performance result is obtained as 310, 333, 368, 409, and 441 using ER-RPL, MSGR, PRD, ER-SR, GT-PSO (Proposed), and Security-aware (Proposed), respectively.

In the next step, we measure the performance by varying the network size and the corresponding number of rounds.

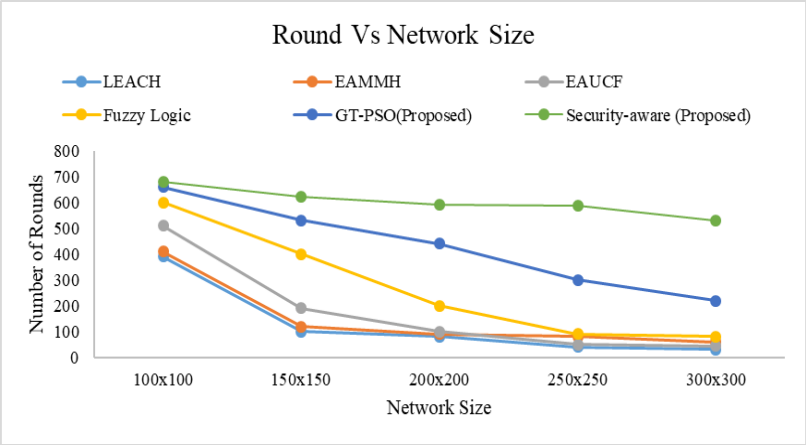


**Figure 9:** Number of rounds vs network size

# 5 Conclusion

An intrusion prevention framework for secure wireless sensor network localization and routing (WSN) is provided. The primary goal is to extend the network's life, increase data dependability, and protect the network from harmful assaults. Most energy-saving systems concentrate on static sensor nodes and use a greedy algorithm for data routing. However, due to unprotected routes, such solutions are not possible. To overcome the issues, a novel combined approach considers secure node localization, node authentication, and data encryption before transmission is introduced to ensure security. The comparative analysis proves the robustness of the proposed method for various types of attacks.

# 6 Availability of Data and Material

Data can be made available by contacting the corresponding author.

# 7 Acknowledgment

The authors thank the management of Cambridge Institute of Technology, Bangalore for their constant support throughout this research.

# 8 References

[1] Gorgich, S., & Tabatabaei, S. (2021). Proposing an energy-aware routing protocol by using a fish swarm optimization algorithm in WSN (wireless sensor networks). Wireless Personal Communications, 119(3), 1935-1955.

[2] Nabavi, S. R., Eraghi, N. O., & Torkestani, J. A. (2021). WSN routing protocol using a multi-objective greedy approach. Wireless Communications and Mobile Computing, 2021.

[3] Khalifa, B., Al Aghbari, Z., & Khedr, A. M. (2021). A distributed self-healing coverage hole detection and repair scheme for mobile wireless sensor networks. *Sustainable Computing: Informatics and Systems*, *30*, 100428.

[4] Mahajan, H. B., & Badarla, A. (2021). Cross-layer protocol for WSN-assisted IoT smart farming applications using a nature-inspired algorithm. Wireless Personal Communications, 121(4), 3125-3149.

[5] Tripathy, B. K., Jena, S. K., Reddy, V., Das, S., & Panda, S. K. (2021). A novel communication framework between MANET and WSN in an IoT-based smart environment. *International Journal of Information Technology*, *13*(3), 921-931.

[6] Al-Mashhadani, M. A., Hamdi, M. M., & Mustafa, A. S. (2021). Role and challenges of the use of UAV-aided WSN monitoring system in large-scale sectors. In *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)* (pp. 1-5). IEEE.

[7] Lv, Y., Liu, W., Wang, Z., & Zhang, Z. (2020). WSN localization technology is based on a hybrid GA-PSO-BP algorithm for indoor three-dimensional space. *Wireless Personal Communications*, *114*(1), 167-184.

[8] Zhu, Y., Yan, F., Zhao, S., Xing, S., & Shen, L. (2021). On improving the cooperative localization performance for IoT WSNs. *Ad Hoc Networks*, *118*, 102504.

[9] Saad, E., Elhosseini, M., & Haikal, A. Y. (2018). Recent achievements in sensor localization algorithms. *Alexandria engineering journal*, *57*(4), 4219-4228.

[10] Khriji, S., El Houssaini, D., Kammoun, I., Besbes, K., & Kanoun, O. (2019). Energy-efficient routing algorithm based on localization and clustering techniques for agricultural applications. *IEEE Aerospace and Electronic Systems Magazine*, *34*(3), 56-66.

[11] Zhang, L., Yang, Z., Zhang, S., & Yang, H. (2019). Three-dimensional localization algorithm of WSN nodes based on RSSI-TOA and single mobile anchor node. *Journal of Electrical and Computer Engineering*, *2019*.

[12] Shahra, E. Q., Sheltami, T. R., & Shakshuki, E. M. (2020). A comparative study of range-free and range-based localization protocols for wireless sensor network: Using cooja simulator. In Sensor Technology: Concepts, Methodologies, Tools, and Applications (pp. 1522-1537). IGI Global.

[13] Lu, Y., Li, L., Peng, H., & Yang, Y. (2016). An energy-efficient mutual authentication and key agreement scheme preserving anonymity for wireless sensor networks. *Sensors*, *16*(6), 837.

[14] Xiong, L., Peng, D., Peng, T., Liang, H., & Liu, Z. (2017). A lightweight anonymous authentication protocol with perfect forward secrecy for wireless sensor networks. *Sensors*, *17*(11), 2681.

[15] Chen, J., Sackey, S. H., Anajemba, J. H., Zhang, X., & He, Y. (2021). Energy-efficient clustering and localization technique using genetic algorithm in wireless sensor networks. *Complexity*, *2021*.

[16] Cao, Y., & Wang, Z. (2019). Improved DV-hop localization algorithm based on dynamic anchor node set for wireless sensor networks. *IEEE Access*, *7*, 124876-124890.

[17] Jondhale, S. R., Maheswar, R., & Lloret, J. (2022). Target Localization and Tracking Using WSN. In Received Signal Strength Based Target Localization and Tracking Using Wireless Sensor Networks (pp. 21-48). Springer, Cham.

[18] Yun, W. K., & Yoo, S. J. (2021). Q-learning-based data-aggregation-aware energy-efficient routing protocol for wireless sensor networks. *IEEE Access*, 9, 10737-10750.

[19] Jung, J., Kim, J., Choi, Y., & Won, D. (2016). Anonymous user authentication and key agreement scheme based on a symmetric cryptosystem in wireless sensor networks. *Sensors*, *16*(8), 1299.

[20] Nguyen, N. T., Le, T. T., Nguyen, H. H., & Voznak, M. (2021). Energy-efficient clustering multi-hop routing protocol in a UWSN. *Sensors*, *21*(2), 627.

[21] Aydin, M. A., Karabekir, B., & Zaim, A. H. (2021). Energy-efficient clustering-based mobile routing algorithm on WSNs. *IEEE Access*, *9*, 89593-89601.

[22] Khan, T., & Singh, K. (2021). TASRP: a trust-aware secure routing protocol for wireless sensor networks. International Journal of Innovative Computing and Applications, 12(2-3), 108-122.

[23] Jerbi, W., Cheikhrouhou, O., Guermazi, A., Boubaker, A., & Trabelsi, H. (2021, June). A Novel Blockchain Secure to Routing Protocol in WSN. In 2021 IEEE 22nd International Conference on High-Performance Switching and Routing (HPSR) (pp. 1-6). IEEE.

[24] Nguyen, T. N., Le, V. V., Chu, S. I., Liu, B. H., & Hsu, Y. C. (2021). Secure localization algorithms against localization attacks in wireless sensor networks. *Wireless Personal Communications*, 1-26.

[25] Misra, S., & Ojha, T. (2021). SecRET: Secure range-based localization with evidence theory for underwater sensor networks. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, 15(1), 1-26.

[26] Xie, N., Chen, Y., Li, Z., & Wu, D. O. (2021). Lightweight Secure Localization Approach in Wireless Sensor Networks. *IEEE Transactions on Communications*, *69*(10), 6879-6893.

[27] Prashar, D., Rashid, M., Siddiqui, S. T., Kumar, D., Nagpal, A., AlGhamdi, A. S., & Alshamrani, S. S. (2021). SDSWSN—A Secure Approach for a Hop-Based Localization Algorithm Using a Digital Signature in the Wireless Sensor Network. *Electronics*, *10*(24), 3074.

[28] Wang, C., Luo, J., Liu, X., & He, X. (2021). Secure and Reliable Indoor Localization Based on Multi-Task Collaborative Learning for Large-Scale Buildings. *IEEE Internet of Things Journal*.

[29] Kim, T. H., Goyat, R., Rai, M. K., Kumar, G., Buchanan, W. J., Saha, R., & Thomas, R. (2019). A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks. *IEEE Access*, *7*, 184133-184144.

[30] Yuan, Y., Huo, L., Wang, Z., & Hogrefe, D. (2018). Secure APIT localization scheme against Sybil attacks in distributed wireless sensor networks. *IEEE Access*, 6, 27629-27636.

[31] Arshad, A., Hanapi, Z. M., Subramaniam, S., & Latip, R. (2021). A survey of Sybil attack countermeasures in IoT-based wireless sensor networks. Peer J Computer Science, 7, e673.

[32] Bhatt, S., & Ragiri, P. R. (2021). Security trends in Internet of Things: A survey. *SN Applied Sciences*, *3*(1), 1-14.

[33] Kwon, D., Yu, S., Lee, J., Seung, S., & Park, Y. (2021). WSN-SLAP: Secure and lightweight mutual authentication protocol for wireless sensor networks. *Sensors*, *21*(3), 936.

[34] Hajian, R., & Erfani, S. H. (2021). CHESDA: continuous hybrid and energy-efficient secure data aggregation for WSN. The Journal of Supercomputing, 77(5), 5045-5075.

[35] Qureshi, S. G., & Shandilya, S. K. (2021). Novel fuzzy-based crow search optimization algorithm for secure node-to-node data transmission in WSN. Wireless Personal Communications, 1-21.

[36] Gulganwa, P., & Jain, S. (2021). EES-WCA: energy-efficient and securely weighted clustering for WSN using a machine learning approach. International Journal of Information Technology, 1-10.

[37] Mehmood, G., Khan, M. S., Waheed, A., Zareei, M., Fayaz, M., Sadad, T., ... & Azmi, A. (2021). An efficient and secure session key management scheme in a wireless sensor network. Complexity, 2021.

[38] Qazi, R., Qureshi, K. N., Bashir, F., Islam, N. U., Iqbal, S., & Arshad, A. (2021). Security protocol using elliptic curve cryptography algorithm for wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*, *12*(1), 547-566.

[39] Han, G., L. Liu, J. Jiang, L. Shu, and J. J. P. C. Rodrigues. (2016). A collaborative secure localization algorithm based on trust model in underwater wireless sensor networks. *Sensors*, 16(2), 229.

[40] Gaber, T., S. Abdelwahab, M. Elhoseny, and A. E. Hassanien. 2018. Trust-based secure clustering in WSN-based intelligent transportation systems. *Comput. Netw.*, 146, 151–158.

[41] Das, B. B., and S. K. Ram. (2016). Localization using beacon in wireless sensor networks to detect faulty nodes and accuracy improvement through DVHop algorithm,'' in *Proc. Int. Conf. Inventive Comput. Technol., (ICICT)*, 1, 1–5.

[42] Rathee, M., Kumar, S., Gandomi, A. H.; Dilip, K., Balusamy, B., Patan, R. (2019). Ant Colony Optimization Based Quality of Service Aware Energy Balancing Secure Routing Algorithm for Wireless Sensor Networks. *IEEE Transactions on Engineering Management*, 1–13.

[43] Priyanka R, K. S. Reddy. (2022). GT-PSO- An Approach For Energy Efficient Routing in WSN. *International Journal of Computer Science & Network Security (IJCSNS)*, 22(4), 17-26.

**Priyanka R** is a Research Scholar at Cambridge Institute of Technology, Bangalore affiliated with VTU Belgaum. Her research focus is on the area of Wireless Sensor Networks. She holds a B.E. degree in CSE from Visvesvaraya Technological University and an M.Tech degree in CSE from the Visvesvaraya Technological University. Her interests include Operating Systems, Software Engineering, Storage Area Networks, Design and Analysis of algorithms, Object-Oriented Modelling and Design, System Software, Object-Oriented Programming, and Computer networks.

**Dr. K. Satyanarayan Reddy** is Principal, Cambridge Institute of Technology North campus, Bangalore, Karnataka State, India. He received his M.Sc. & M.Phil. (Mathematics) Degrees from Nagpur University, Maharashtra State, and M. Tech. (CSE with specialization in Computer Applications) from Indian School of Mines (now IIT (ISM)), Dhanbad, Jharkhand. He received a Ph.D. (Computer Science) degree from the School of Science & Technology, Dept. of Computer Science at Dravidian University, Kuppam, AP, India. His areas of research are High-Speed Networks, Data Communications, Network Security, Wireless Sensor Networks, Big Data, and Artificial Intelligence.