International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/220733 Volume 10, Issue 2, March – April (2023)

RESEARCH ARTICLE

# Energy-Efficient Trust and Quarantine-Based Secure Data Transmission in Wireless Sensor Networks

S. Shanmuga Priya
Department of Computer Science, Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore, Tamil Nadu, India.
charanmum@gmail.com

N. Shanmuga Priya
Department of Computer Applications, Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore, Tamil Nadu, India.
spriyanatrajan@gmail.com

Received: 29 July 2022 / Revised: 12 February 2023 / Accepted: 23 February 2023 / Published: 29 April 2023

**Abstract – Wireless Sensor Networks (WSN) are comprised of a significant amount of sensors that are dispersed to acquire data regarding a certain region. The sensor nodes are self-contained and create an ad-hoc inter-communication topology with one another. On the other hand, sensors are limited by their limited resources for managing energy, storing data, communication, and computing power. The hacked nodes make the information more susceptible to security issues. The safety of an unreliable network is a source of concern for researchers. To reduce energy consumption and provide secure communication this research work aims to present an energy-efficient secure data transmission system for WSNs that use the trust concept to detect and prevent data compromise while providing high performance. The proposed method comprises two main steps: First, it presents a new data security scheme that includes data confidentiality and integrity. Second, use the trust concept for analyzing the quality of data links for secure transmission and quarantine nodes and edges based on the trust value. The outcomes of the simulation showed that the suggested protocol increases the effectiveness of network lifetime and energy usage.**

**Index Terms – WSN, Energy-Efficient, Trust, Encryption, Data Transmission, Security.**

## 1. INTRODUCTION

The wireless sensor network (WSN) field is being explored by a wide range of applications, including defense, medical, and farming, to watch and obtain physical data [1]. To collect information on a regular interval or incident basis, the sensor nodes are placed randomly or uniformly. End-users employ wireless broadband channels to obtain the requisite information from the base station over the Internet [2]. Although sensor nodes are crucial in various academic and industrial domains, their effectiveness is limited by several factors. Battery, storage, transport, and computations are a few restrictions of WSN. With these aspects, the main pressing issue for various applications is improving the energy effectiveness of WSNs while maintaining rapid data delivery [3].

Due to their dispersed nature, WSNs are susceptible to a variety of threats that cause network latency and data loss [4]. Furthermore, WSNs have high data sensitivities, permitting the intruder to steal data from the sensors [5] invisibly. For instance, the attacker can interrupt sent packets by severing the connection between the transmitter and the receiver, creating a false node with a homogenous identity to the genuine node, or changing the communication direction. As a result, implementing security in WSN is critical to maintaining the network's integrity. However, because of the minimal available energy and the significant energy consumption throughout data communication, integrating security in WSN can be difficult. Therefore, the quantity of transmission overhead should be decreased to lengthen the network's life span and devote energy to security implementation [6].

Data integrity and confidentiality are the two main security criteria for WSN. In network security, information secrecy is a critical need. Therefore, this criterion is taken into account initially in any network security solution for communication devices. Any WSN's confidentiality must take into account the following factors.

- The data collected by the sensors must not be shared with its neighbors or any other node. Because the data in some apps is very sensitive and protected, releasing it might jeopardize the network's goals.
- WSN nodes convey highly sensitive information in various applications, such as security keys and distribution; making channels safe in the WSN is critical.

RESEARCH ARTICLE

- Some sensor-related data, such as IDs and security keys, etc., is stored in encrypted form in sensors. Thus, it is possible to keep it safe against passive attackers as well as traffic analysis.

### 1.1. Problem Statement

If data packets are encrypted with secure keys, adversaries will be unable to read or steal data. Still, they will be able to append false data or hazardous scripts to the data. For example, a malicious node could add junk or alter the data in information packets. These altered data can't be used on the network, which can be dangerous for network connectivity. As a result, information reliability ensures that any data received has not been tampered with during communication. When building a security solution for WSN, the following constraints are taken into account.

Lightweight: The security technique must utilize the least amount of usage of resources and actions due to the resource limitations of the sensor network.

Distributed: The network's sensors are all interconnected, making any node vulnerable to attack at any time. Decentralized security solutions must be designed. If one portion of the security algorithm fails, it won't have an impact on the network.

Reactive: The defense system should respond to network changes. Because sensor networks are dynamic and operate in real-time contexts, solutions must adapt to these conditions and respond favorably to security risks that arise unexpectedly.

Fault-Tolerant: The communication channel between the sensors is insecure and untrustworthy. The capacity to detect and recover from these defects is required for wireless communications. Therefore, these flaws must be taken carefully and included in the security solution.

### 1.2. Objectives

The objectives of this research are as follows:

- To provide the data confidentiality, integrity, lightweight, and fault-tolerant based security solution for WSN.
- To develop the energy-efficient secure data transmission system for WSNs
- To use the trust concept to detect, prevent data compromise, and provide high performance.

### 1.3. Contributions

The proposed method comprises two main steps:

- It presents a new data security scheme that includes data confidentiality and integrity.
- The trust concept is used for analyzing the quality of data links for secure transmission and quarantine nodes and edges based on the trust value.

### 1.4. Paper Structure

Section 2 reviews various securities and routing schemes' related work. Then, the proposed secure data transmission method is described in section 3. Section 4 examines the performance of the suggested work. Section 5 concludes the research work.

## 2. RELATED WORK

Haseeb et al. [7] describe a safe routing method that improves energy efficiency while also providing multi-hop information protection against malevolent acts. It uses lightweight operations for safe communication with limited resources. It assesses the statistical investigation for a specific association to recognize congestion, resulting in reduced routing interruption and retransmission.

Binu et al. [8] developed a unique heuristic-based energy-efficient routing algorithm for WSNs, to lower energy usage and packet drop ratio. However, there are no security measures included in this strategy to deal with malicious attacks. Furthermore, in network-wide routing, the value of wireless connectivity to the sink node is disregarded, resulting in repeated route re-discoveries and data retransmissions.

Al Hayajneh et al. [9] developed a unique security protocol for WSNs based on cooperative communication, intending to increase performance, robustness, and data reliability in the face of cyberattacks. It includes an information safety MAC technique with a hashing algorithm for message reliability verification and a basic key distribution method for network entry authentication. Thus, it increases network security, but it's only suitable for a few sensors, and transmission speed isn't considered.

Haseeb et al. [10] present a safe and energy-aware heuristic approach for WSN, intending to optimize the routing approach with an intelligent judgment against rogue nodes. It improves network performance by using remaining power, hop count to BS, and connection reliability parameters to optimize data routing and transmission reliability.

An efficient, secure routing algorithm for WSN environments is described in [11] that is successfully immune to IP spoofing and ensures the detection of proper connectivity information over an untrusted network. Kumar et al. [12] offer a new secure multipath routing technique for secure communication in military heterogeneous WSNs. It takes advantage of a cryptographic algorithm to discover trusted neighbors and set up several secure pathways for data transmission. This protocol features an effective key management method that increases network security while also improving performance.

**RESEARCH ARTICLE**

An energy and trust-based routing strategy for wireless sensor networks is proposed by Han et al. [13] utilizing an adaptive evolutionary algorithm. To defend against various attacks, increase the speed at which the attackers can be located, and choose secure and energy-efficient routes, it defends against both common routing attacks and particular trust attacks. Lai and Wang [14] investigate the issue of WSN broadcast data dispersion in IoT systems. A new protocol is suggested, which increases the data transmission's reliability and effectiveness. Finally, Qiu et al. [15] offer a routing protocol for WSN that supports various traffic models and is assessed on real-world testbeds to achieve shorter communication time.

A secure routing method [16] is presented to increase the information arrival rate and communication latency while considering the restricted ability for recognizing malevolent nodes and power. Elhoseny et al. [17] suggested a new ECC based on a generic method for determining the best network layout and homomorphic encryption to secure data transfer. The communication overflow and latency caused by the new network structure's broadcast message are the work's key limitations. Another source of overhead and power usage is ECC, which is not suited for use in WSNs since it necessitates a high level of processing capabilities in the sensors.

Anitha et al [18] propose a Fuzzy Trust Based Energy Aware Balanced Secure Routing Algorithm for addressing the problems of multi-hop communication. It enhances the network's security requirement and guarantees data protection over multi-hop communication-based networks. It minimizes communication overhead. In [19], a safe routing strategy for block-chained WSNs is proposed. Using public and private blockchains, the sensor and aggregator nodes are verified. After the sensor nodes have been authenticated, the trust values of the sensors are calculated based on transmission, response time, and data forwarding. The high trust scores nodes are regarded as legitimate and other nodes are regarded as malicious.

Kalidoss et al. [20] offer a secured Quality of Service (QoS) routing approach that relies on reliance and power modeling to improve WSN performance. To calculate trust value, confidence modeling employs a validation technique with a key-based protection method. It describes a cluster-based routing system where the cluster head is selected using QoS measurements and trust ratings. The final path was chosen based on trust, power, and the number of hops.

Bangotra et al., [21] suggested a new routing approach that relies on trust. The factors used to determine trust is honesty in data packet transmission, truthfulness in response, and energy consumption. In [22], a unique hybrid fitness function is presented about a power-aware trust routing scheme. The two primary parts of this algorithm are to choose trustworthy nodes based on a threshold and then to choose proactive nodes from nodes to carry out routine. It makes use of a multi-hop cluster transmission method along with the multipath routes method. The advantages and disadvantages of the related work are shown in Table 1.

Table 1 Related Work Summary

| Ref | Methodology | Advantages | Disadvantages |
|---|---|---|---|
| [7] | A multi-hop routing protocol with energy awareness and security that use a private sharing method. | With the secret sharing approach, secure data communication from CH to BS. It offers a simple key for the IoT-based WSN. | The CHs near the BS uses more energy, which causes energy holes to emerge nearby and shortens the network lifetime. |
| [8] | A new, energy-efficient WSN routing approach based on a heuristics model. | It significantly decreases both power usage and the packet flow ratio. | Based on node characteristics, routing performance is inefficient, and data integrity and privacy may be at risk. |
| [9] | Cooperative communication is used in a unique security mechanism for WSNs. | It increases network security, offers data protection, and ensures data reliability against cyber-attacks. | It is suitable when there are few sensor nodes, and routing performance is disregarded. |
| [10] | A secure and energy-conscious heuristic-based routing strategy for WSN. | The network throughput is improved. It lessens network failures. | The energy effectiveness of the network desires to be increased. |
| [13] | Trust-based routing using a genetic algorithm | It reduces packet loss and increases network energy efficiency. | Need to improve the security routing |
| [17] | A new encryption scheme based on homomorphic and elliptic curve | It improves the network | High computational complexity and need more energy for the |

**RESEARCH ARTICLE**

| | | | |
|---|---|---|---|
| | cryptography (ECC) has been developed. | performances | decryption process |
| [20] | Energy-efficient routing protocol with QoS awareness. | It provides better communication and increases packet delivery ratio, network lifetime, and protection | The main issue is uncertainty. |
| [21] | Routing protocol with intelligence and security based on trust. | It provides enhanced network performance. | QoS requirement is not met for mission-critical data, and large-capacity data cannot be processed. |

## 3. SECURE DATA TRANSMISSION

The complete explanation of the suggested work is discussed in this section. This method was created for low-constraint sensors to enhance network performance in energy usage, data delivery, and security. The two primary phases of this scheme are data confidentiality with integrity and trust-based routing. The proposed method uses lightweight encryption and a signature-based scheme for data confidentiality and integrity in the first phase. Secure and efficient routing based on the trust and quarantine scheme is the second phase. The sample network model with the workflow of the suggested approach is shown in Figure 1.

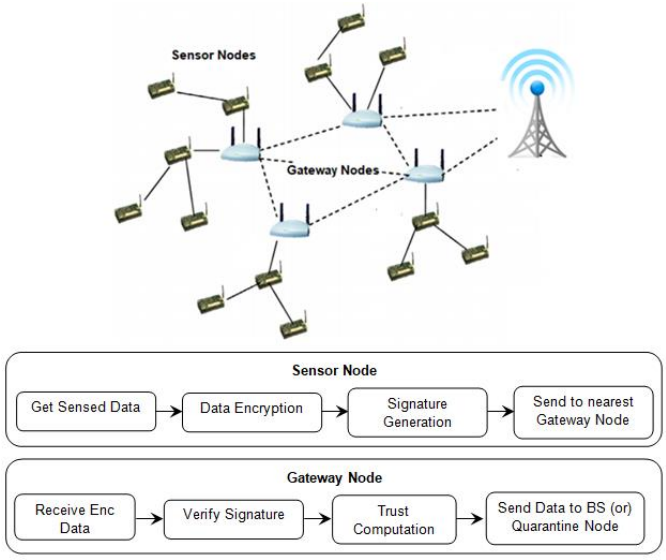


Figure 1 Network Model and WorkFlow

### 3.1. Data Confidentiality and Integrity

Data confidentiality in WSN is one of the most crucial requirements in sensitive WSN applications since it prohibits illegitimate parties from obtaining data. A sensor node shouldn't communicate environmental data to nearby neighbors. The data that the nodes collect may be very confidential, particularly in military applications. Moreover, nodes in a variety of applications must use wireless transmission to send extremely private data (key distribution) to other sensor nodes. Moreover, malevolent nodes must be prevented from accessing routing data to prevent data abuse and performance degradation on the network. Due to these difficulties, it is crucial to offer a secure communication route for data transfer in WSNs. The conventional approach for preserving data privacy involves encrypting data with a secret key.

Data confidentiality can stop malicious nodes from accessing data, but it cannot stop unauthorized people from altering the data. The integrity of the data makes sure that it is not altered while being transmitted. A malevolent node can break the network by interfering with the message. Additionally, the messages could be interrupted during transmission even in the absence of a malevolent node. To ensure data integrity, message authentication codes or cyclic codes are necessary. The method for encrypting data is described in Algorithm 1.

Input: Sensed Data (SD)

Output: Encrypted Data ($ED_1$), $ED_2$,

Step1: $ED_1 = AES\_Enc(SD)$

Step2: $h_1 = h(ED_1)$

Step3: num = numeric _bits($h_1$)

Step4: alpha = alpha_bits($h_1$)

Step5: if num % 2 ==0 then

Step6: WB = num[1] || alpha[1] || num[2] || alpha[2] || num[3] || alpha[3]

Step7: Else

Step8: WB = num[1] || num[2] || num[3] || alpha[1] || alpha[2] || alpha[3]

Step9: $ED_2 = h_1 \oplus WB$

Step10: $h_2 = h(ED_2)$

Step11: $Enc\_Msg = (ED_1, h_1, ED_2, h_2)$

Step12: Send to nearest Gateway node

Algorithm 1 Data Encryption

**RESEARCH ARTICLE**

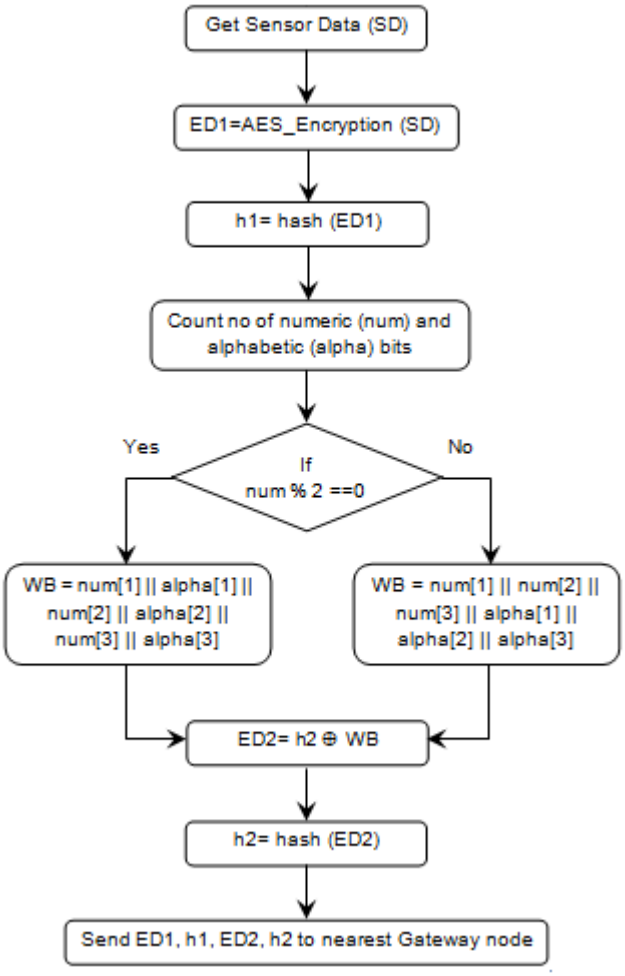


Figure 2 Flowchart of Data Encryption Process

Initially, the sensed data is encrypted using the AES algorithm (equation (1)).

$$ED_1 = AES\_Encryption(SD) \quad (1)$$

It is a symmetric key ciphertext algorithm. There are several symmetric-key algorithms like DES, 3DES, RSA, AES, and blowfish [23]. Each algorithm has its advantages and disadvantages. This paper selects the AES algorithm because it provides high data confidentiality and integrity [24]. Then, using equation (2), get the hash value of the encrypted data. The hash function is a method for encrypting communications into a digital signature of a fixed digit in such a way that it is difficult to decode the data from the encoded value, and the following conditions can be met [25]:

- h() creates fixed-length encoded digits for any size of the data.
- Generating g = h(m) from a given m is simple. On the other hand, generating m = $h^{-1}$(g) from a given g is impossible.
- Finding h(m) = h(g) given m and g can be computationally infeasible.

$$h_1 = hash(ED_1) \quad (2)$$

After finding the hash value of encrypted data, separate the numeric and alphabetic bits. For example, if the hash value is '1E6947AC7FB3A9529A9726EB692C8CC5' then num=' 16947739529972669285' and alpha = 'EACFBAAEBCCC'. Generate WB based on the numeric bits (num).

$$ED_2 = h_1 \oplus WB \quad (3)$$

Using equation (3), apply the xor operator to generate $ED_2$ and generate the hash value of $ED_2$. Send the encrypted message {$ED_1$, $h_1$, $ED_2$, $h_2$} to nearest gateway node. Figure 2 shows the flowchart of the data encryption process.

Table 2 shows the working example:

Table 2 Data Encryption Working Example

| Operation | Result |
|---|---|
| Input (SD) | Secret Message |
| $ED_1$=AES_Enc(SD) | O2a4XYR3DnnZ8o6lWRsBXQ== |
| $h_1$ = h($ED_1$) | 27a36b878af0fa790f9bb6ecf9bb7995 |
| num = numeric _bits($h_1$) | 18 |
| alpha = alpha_bits($h_1$) | 14 |
| WB = num[1] \|\| alpha[1] \|\| num[2] \|\| alpha[2] \|\| num[3] \|\| alpha[3] | 2a7b3a |
| $ED_2 = h_1 \oplus WB$ | 001001 |
| $h_2$ = h($ED_2$) | 1fccb567a44880e8665b7cb9d0f97271 |
| Output | $ED_1$, $h_1$, $ED_2$, $h_2$ |

3.2. Trust-Based Data Transmission

A trust management scheme is incorporated into WSNs to safeguard them from possible threats and identify trustworthy nodes from vulnerable nodes [26]. Trust models are initially used in e-commerce platforms to recognize trustable respondents. The assessment of node confidence is related to the historical performance of distrustful nodes and recommendations from reliable neighbors, and it is more effective to identify hacked nodes in networks. The historical behaviors of suspicious nodes are computed based on their past successful and unsuccessful data transmission. Trust-based routing solutions are offered to improve network security based on such rationale. The most important aspect for the period of the design stage of associated techniques is

RESEARCH ARTICLE

how to choose the best secure routing intermediate nodes based on trust levels. Furthermore, some trust-aware models incorporate energy consumption distances from neighbors to sink nodes or many links into secure routing assessment to access improved secure paths [27].

To build a robust and responsive routing system, trust management models can be used as efficiently as feasible in WSN. A variety of methodologies and methods for calculating the trust value of sensor nodes and the resulting value may then be used in a variety of ways to discover a secure routing route. Algorithm-2 explains trust-based data transmission.

Input: Enc_Msg ($ED_1$, $h_1$, $ED_2$, $h_2$)

Output: Enc_Msg is transmitted to BS or Node Quarantine

Step1: $HT_1 = h(ED_1)$

Step2: $HT_2 = h(ED_2)$

Step3: if ($HT_1$== $h_1$ and $HT_2$ ==$h_2$) then

Step4: SignTrust = 1

Step5: else

Step6: SignTrust = 0

Step7: Compute CommTrust = $\frac{SC+1}{SC+UC+\varepsilon}$

SC = Successful communication between node and gateway

UC = Unsuccessful communication between node and gateway

ε = random number between 0 to 1

Step8: If (SignTrust==1 and CommTrust ≥ 0.5)

Step9: Send Enc_Msg to BS

Step10: Else if SignTrust ==1 and CommTrust < 0.5

Step11: Analyze previous node transmission

Step12: Else

Step13: Quarantine Node for a certain time

Algorithm 2 Data Transmission

In algorithm-2, two types of trust values are computed: signature trust (SignTrust) and communication trust (CommTrust). The signature trust is computed based on the verification of the hash value of encrypted messages. It can be calculated using equation (4)

$$SignTrust = \begin{cases} 1, & if\ HT_1 == h_1\ and\ HT_2 == h_2 \\ 0, & Otherwise \end{cases} \quad (4)$$

The communication trust levels calculated among nodes are based on their cooperation in transmitting network messages to other nodes. Communication trust is the main important aspect to consider when determining the trustworthiness of an individual node in a trust assessment. It determines whether or not the target node will act normally in the future, and the trust computation procedure is rapidly sufficient to conserve node energy. The commTrust can be computed using equation (5)

$$commTrust = \frac{SC+1}{SC+UC+\varepsilon} \quad (5)$$

Based on the computed node trust value, the gateway node decides for transmitting the data. If the signTrust value is zero, then the node is in quarantine mode. The word quarantine is more popular because of covid-19. In the case of illness dissemination in plants, it is standard practice to kill any susceptible hosts near an affected one. In the case of personal infections, quarantining asymptomatic individuals who have had contact with an infected node is a common strategy [28]. Similarly, in the case of a network, the quarantine technique entails removing all infected nodes from the system and all of their susceptible neighbors. Figure 3 shows the flowchart of Data Transmission.

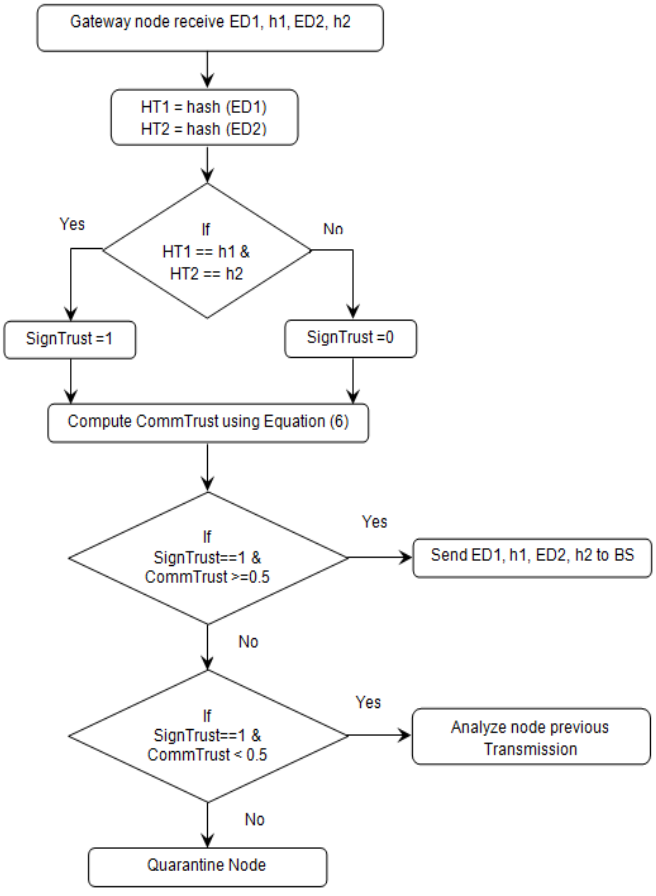


Figure 3 Flowchart of Data Transmission Process

RESEARCH ARTICLE

The communication trust value is decreased when increasing the number of nodes. Figure 4 shows the trust value. When increasing the number of nodes the significant number of malicious nodes is increased so it reduces the packet transmission.

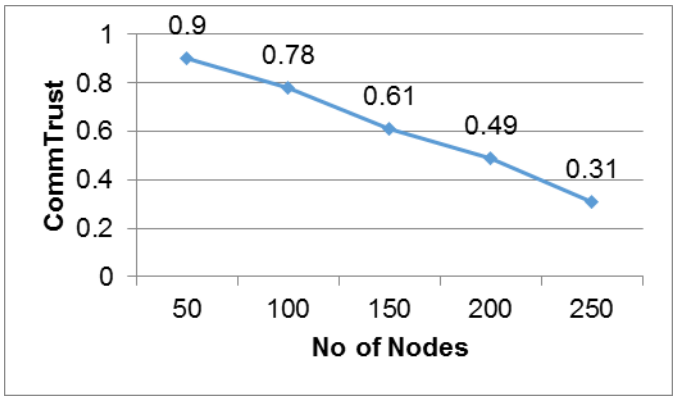


Figure 4 No of Nodes Vs CommTrust

## 4. SIMULATION RESULT

The proposed secure data transmission model is developed and assessed using MATLAB (R2014b) with the recommended experimental setup. In this study, 100 nodes are arbitrarily dispersed in the area of 100 × 100m. The simulation setup is shown in Table 3.

Table 3 Simulation Parameter

| Parameter | Settings |
|---|---|
| Area | 100m x 100m |
| Node Deployment | Random |
| Number of Nodes | 100 |
| Node Initial Energy | 2J |
| Data Packet Size | 64 bytes |
| Control Packet Size | 16 bytes |
| Transmission Range | 25m |
| Base Station Location | 50, 50 |

The proposed work and some existing work are compared in terms of network lifespan, energy consumption (EC), network throughput (NT), packet delivery ratio (PDR), and packet loss ratio (PLR). The BS is located at the coordination of (50, 50). All of the nodes' transmission ranges are set to 25 m. The node's initial energy level is 2J.

The performance of the suggested work was evaluated with SecTrust-RPL [29], EATMR [30], and SEHR [10].

### 4.1. Throughput

It is calculated as the number of packets received in a specific amount of time, and packet delivery is then acknowledged. The throughput is calculated using equation (6)

$$Throughput = \frac{N_r}{T} * 100 \quad (6)$$

Here T is the simulation period and Nr is the total sum of all the nodes.

The throughput comparison for the different numbers of nodes is shown in Figure 5. According to the results of the experiments, the SecTrustRPL achieves 84%, SEHR 92%, EATMR 90% and the proposed approach achieve 95% throughput. Furthermore, the suggested technique uses a cryptography hash method to find the connection reliability value and finds the majority trustworthy communication path for information forwarding, resulting in increased network throughput. The proposed approach increases throughput by 12.19% and 5.74% compared to SecTrustRPL and EATMAR for 100 nodes.

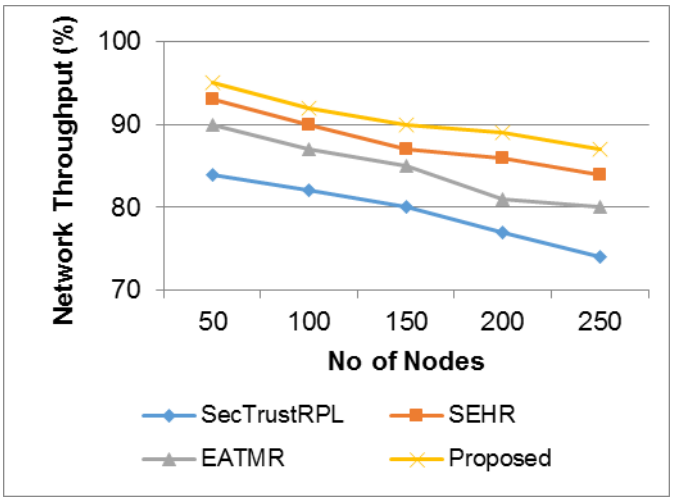


Figure 5 Throughput Comparison

### 4.2. Packet Loss Ratio

The packet loss ratio is the percentage of lost packets to the total packets sent. The packet loss can be computed using (7)

$$PLR = \frac{N_{tp} - N_{rp}}{N_{tp}} \times 100 \quad (7)$$

Here $N_{tp}$ indicates the count of transmitted packets and $N_{rp}$ indicates the count of received packets. Figure 6 shows the packet loss comparison.

The proposed approach decreases the packet loss ratio compared to other methods. When an increasing number of nodes the packet loss ratio is also increased. The proposed approach decreases packet loss by 33.3% and 18.18% compared to SecTrustRPL and SEHR for 100 nodes.

RESEARCH ARTICLE

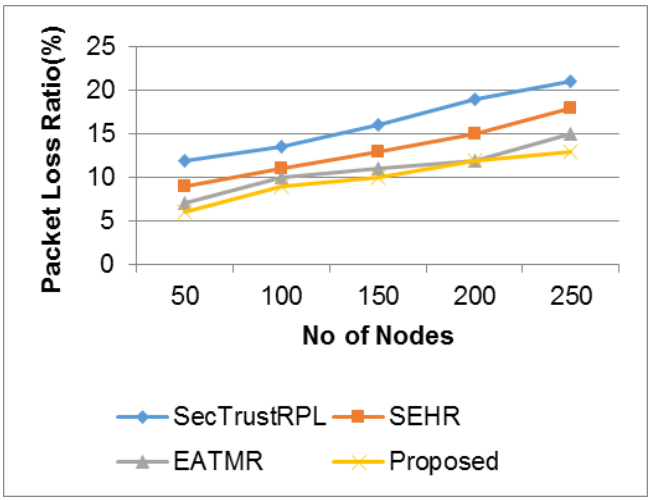


Figure 6 Packet Drop Ratio Comparison

4.3. Delay

The mean time between when the source delivers a packet and when it is successfully received at the intended destination is referred to as network delay. The delay is calculated by taking into account the data packets' propagation and queuing delays. The end-to-end delay for the different numbers of nodes is shown in Figure 7. The proposed approach decreases packet loss by 29.93% and 23.07% compared to SecTrustRPL and EATMR for 100 nodes.

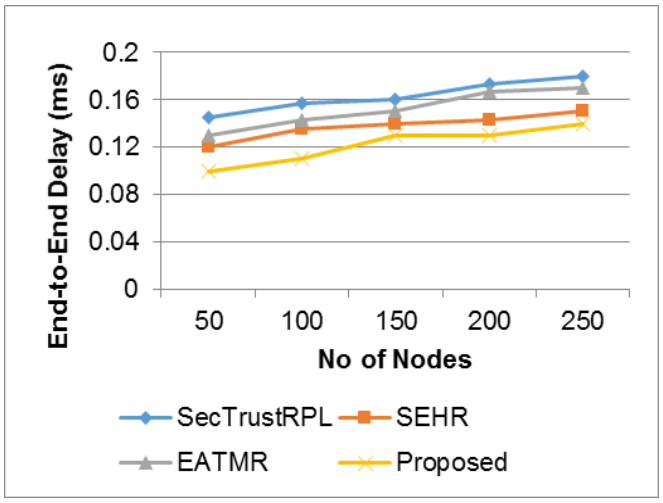


Figure 7 End-to-End Delay Comparison

4.4. Energy Consumption

The energy consumption for the different numbers of nodes is shown in Figure 8.

The suggested technique employs the hash function in the assessment of link reliability, which eliminates various data re-routing methods and reduces transmission link interference. The proposed approach decreases energy consumption by 33.3% and 15.78% compared to SecTrustRPL and SEHR for 100 nodes.

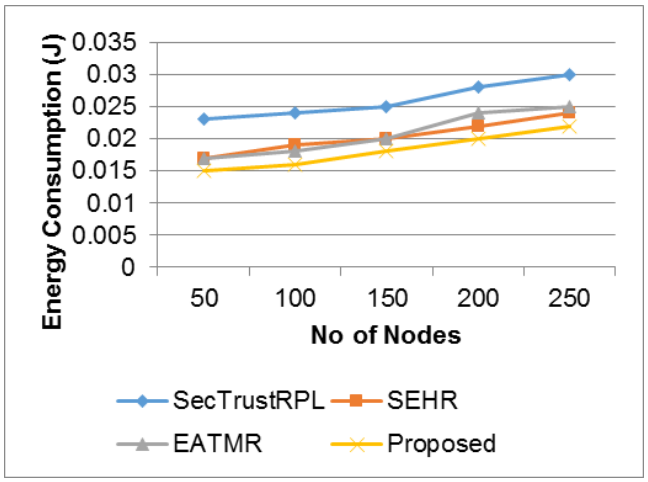


Figure 8 Energy Consumption Comparison

4.5. Packet Delivery Ratio

It is calculated by dividing the total number of packets transmitted by the source node by the total number of packets that were collected at the destination. It can be calculated using equation (8)

$$PDR = \frac{N_{rp}}{N_{tp}} \times 100 \quad (8)$$

Figure 9 shows the comparison of packet delivery ratio for different number nodes.

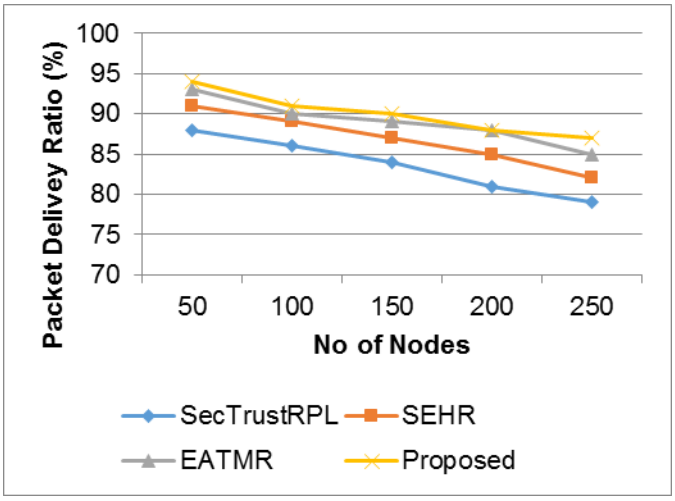


Figure 9 Packet Delivery Ratio Comparison

The proposed have high packet delivery compared to other approaches. The proposed approach increases the packet delivery ratio by 5.81% and 2.24% compared to SecTrustRPL and SEHR.

**RESEARCH ARTICLE**

## 5. CONCLUSION

WSNs, which are built for time-critical applications, are widely used in the commercial world. In tactical and hostile situations, yet, WSN has restricted resources to utilize. Security has been a top priority for WSN protocols because of how widely deployed such a network is and how important it is to maintain security. For identification and authentication, a variety of countermeasures have been proposed, including some based on cryptography. While using a public key encryption approach has shown to be useful in the past, it is computationally expensive. This research work presents an energy-efficient secure data transmission system for WSNs that use the trust concept to detect and prevent data compromise while providing high performance. This research focuses on crucial variables like energy usage and safe data delivery, which are necessary restrictions for WSN transmission to be dependable and trustworthy. The counter-mode encryption technique improves data security by being lightweight, simple, and unpredictable. The simulation outcome demonstrates that the suggested protocol performs better in terms of security and energy consumption than other earlier protocols.

## REFERENCES

[1] Liu, X., Qiu, T., & Wang, T. (2019). Load-balanced data dissemination for wireless sensor networks: A nature-inspired approach. IEEE Internet of Things Journal, 6(6), 9256-9265.
[2] Rimal, B. P., Maier, M., & Satyanarayanan, M. (2018). Experimental testbed for edge computing in fiber-wireless broadband access networks. IEEE Communications Magazine, 56(8), 160-167.
[3] Fernandez-Prieto, J. A., Cañada-Bago, J., & Gadeo-Martos, M. A. (2019). Wireless acoustic sensor nodes for noise monitoring in the city of linares (Jaén). Sensors, 20(1), 124.
[4] Ávila, K., Sanmartin, P., Jabba, D., & Gómez, J. (2022). An analytical survey of attack scenario parameters on the techniques of attack mitigation in WSN. Wireless Personal Communications, 1-32.
[5] Iqbal, U., & Mir, A. H. (2022). Secure and practical access control mechanism for WSN with node privacy. Journal of King Saud University-Computer and Information Sciences, 34(6), 3630-3646.
[6] Nels, S. N., & Singh, J. A. P. (2020). Analysis of data aggregation methods and related issues in Wireless Sensor Networks. Control and Cybernetics, 49(4), 419-446.
[7] Haseeb, K., Islam, N., Almogren, A., Din, I. U., Almajed, H. N., & Guizani, N. (2019). Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs. IEEE Access, 7, 79980-79988.
[8] Binu, G. S., & Shajimohan, B. (2020). A novel heuristic based energy efficient routing strategy in wireless sensor network. Peer-to-Peer Networking and Applications, 13, 1853-1871.
[9] Al Hayajneh, A., Bhuiyan, M. Z. A., & McAndrew, I. (2020). A novel security protocol for wireless sensor networks with cooperative communication. Computers, 9(1), 4.
[10] Haseeb, K., Almustafa, K. M., Jan, Z., Saba, T., & Tariq, U. (2020). Secure and energy-aware heuristic routing protocol for wireless sensor network. IEEE Access, 8, 163962-163974.
[11] Huang, D. C., Chu, Y. Y., Tzeng, Y. K., Chen, Y. Y., & Chen, W. M. (2019). Secure routing for WSN-based tactical-level intelligent transportation systems. Journal of Internet Technology, 20(4), 1013-1026.
[12] Kumar, K. A., Krishna, A. V., & Chatrapati, K. S. (2017). New secure routing protocol with elliptic curve cryptography for military heterogeneous wireless sensor networks. Journal of Information and Optimization Sciences, 38(2), 341-365.
[13] Han, Y., Hu, H., & Guo, Y. (2022). Energy-aware and trust-based secure routing protocol for wireless sensor networks using adaptive genetic algorithm. IEEE Access, 10, 11538-11550.
[14] Lai, X., & Wang, H. (2018). RNOB: Receiver negotiation opportunity broadcast protocol for trustworthy data dissemination in wireless sensor networks. IEEE Access, 6, 53235-53242.
[15] Qiu, Y., Li, S., Li, Z., Zhang, Y., & Yang, Z. (2017). Multi-gradient routing protocol for wireless sensor networks. China Communications, 14(3), 118-129.
[16] Liu, X., Liu, A., Wang, T., Ota, K., Dong, M., Liu, Y., & Cai, Z. (2020). Adaptive data and verified message disjoint security routing for gathering big data in energy harvesting networks. Journal of Parallel and Distributed Computing, 135, 140-155.
[17] Elhoseny, M., Elminir, H., Riad, A., & Yuan, X. (2016). A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption. Journal of King Saud University-Computer and Information Sciences, 28(3), 262-275.
[18] Anitha, R., Bapu, B. T., Kuppusamy, P. G., Partheeban, N., & Sasikumar, A. N. (2022). FEBSRA: Fuzzy Trust Based Energy Aware Balanced Secure Routing Algorithm for Secured Communications in WSNs. Wireless Personal Communications, 125(1), 63-86.
[19] Awan, S., Javaid, N., Ullah, S., Khan, A. U., Qamar, A. M., & Choi, J. G. (2022). Blockchain based secure routing and trust management in wireless sensor networks. Sensors, 22(2), 411.
[20] Kalidoss, T., Rajasekaran, L., Kanagasabai, K., Sannasi, G., & Kannan, A. (2020). QoS aware trust based routing algorithm for wireless sensor networks. Wireless Personal Communications, 110, 1637-1658.
[21] Bangotra, D. K., Singh, Y., Selwal, A., Kumar, N., & Singh, P. K. (2022). A trust based secure intelligent opportunistic routing protocol for wireless sensor networks. Wireless Personal Communications, 127(2), 1045-1066.
[22] Hajiee, M., Fartash, M., & Osati Eraghi, N. (2021). An energy-aware trust and opportunity based routing algorithm in wireless sensor networks using multipath routes technique. Neural Processing Letters, 53(4), 2829-2852.
[23] Patil, P., Narayankar, P., Narayan, D. G., & Meena, S. M. (2016). A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. Procedia Computer Science, 78, 617-624.
[24] Wahid, M. N. A., Ali, A., Esparham, B., & Marwan, M. (2018). A comparison of cryptographic algorithms: DES, 3DES, AES, RSA and blowfish for guessing attacks prevention. Journal Computer Science Applications and Information Technology, 3(2), 1-7.
[25] Zhou, C., Zhu, G., Zhao, B., & Wei, W. (2006, November). Study of one-way hash function to digital signature technology. In 2006 International Conference on Computational Intelligence and Security (Vol. 2, pp. 1503-1506). IEEE.
[26] Fang, W., Zhang, W., Chen, W., Pan, T., Ni, Y., & Yang, Y. (2020). Trust-based attack and defense in wireless sensor networks: a survey. Wireless Communications and Mobile Computing, 2020, 1-20.
[27] Sun B, Li D (2017) A comprehensive trust-aware routing protocol with Multi-attributes for WSNs. IEEE Access, vol. 6, pp. 4725–4741
[28] Strona, G., & Castellano, C. (2018). Rapid decay in the relative efficiency of quarantine to halt epidemics in networks. Physical Review E, 97(2), 022308.
[29] Airehrour, D., Gutierrez, J. A., & Ray, S. K. (2019). SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. Future Generation Computer Systems, 93, 860-876.
[30] Yin, H., Yang, H., & Shahmoradi, S. (2022). EATMR: an energy-aware trust algorithm based the AODV protocol and multi-path routing approach in wireless sensor networks. Telecommunication Systems, 81(1), 1-19.

**RESEARCH ARTICLE**

Authors

Mrs. S. Shanmuga priya is working as an Assistant Professor and Head in Computer Science Department at Shiri Kumaran College of Arts and Science, Karamadai, Coimbatore, India. She has 16 years of experience in teaching field. She is currently pursuing her Ph.D in Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore, Tamil Nadu, India. She is proficient in Framing of Curriculum, Regulations and syllabus for Undergraduate and Postgraduate degree programmes. She is heading as a Coordinator for Placement Cell in her College.Her area of interests includes Wireless Sensor Networks, Artificial Intelligence and the Internet of Things.

Dr. N. Shanmugapriya, presently working as an Associate Professor and Head , Department of Computer Applications(PG), Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore. She has 20+ years of experience in teaching; Academic oriented Administration and research in Computer Science Field. She published more than 25 Journals in various National and International Journals. She has completed a UGC Minor Research project related to her research work. She is proficient in preparing proposals for funding agencies, Affiliation process, Framing of Curriculum, Regulations and syllabus for Undergraduate and Postgraduate degree programmes. She is heading as a Coordinator for Software Development Cell and Intellectual Property Rights Cell in her College. She is a active Member in Association of Computer Machinery (ACM), and Computer Society of India (CSI). She has been playing the role of Reviewer for various International Journals and External PhD Thesis Assessor. Her area of research fields includes Speech Enhancement, Artificial Intelligence, Machine Learning and Robotics. She has recently filed a patent related to Mobile sensors.

**How to cite this article:**

S. Shanmuga Priya, N. Shanmuga Priya, "Energy-Efficient Trust and Quarantine-Based Secure Data Transmission in Wireless Sensor Networks", International Journal of Computer Networks and Applications (IJCNA), 10(2), PP: 156-165, 2023, DOI: 10.22247/ijcna/2023/220733.