Trust Based Security Model for Intrusion Detection in Wireless Sensor Networks

A.B. Hajirabe[1], D. Saravanan[2], C. Jayapratha[1], S. Parasuraman[3], A. Manimaran [3]

[1]Department of Computer Applications, KarpagaVinayaga College of Engineering and Technology, Madhuranthagam - 603 308, Tamil Nadu, India.
[2]Department of Mathematics, KarpagaVinayaga College of Engineering and Technology, Madhuranthagam - 603 308, Tamil Nadu, India.
[3]Department of Electronics and Communication Engineering, KarpagaVinayaga College of Engineering and Technology, Madhuranthagam - 603 308, Tamil Nadu, India

Abstract

To offer robust security throughout network communication, Two Stage Security Node Authentication (TSSNA) is proposed for Wireless Sensor Networks (WSN). In terms of data privacy and genuine communication, this enhances security. Everynode that enters into the networkshould get registered withBase Station (BS)here since the nodes distributed over the network should interact with one another in a secured environment. Choosing trustworthy nodes during the preliminary stage involves removing malicious nodes from the communication process. This is carried out through node contact ratio which is determined using direct trust and recommended trust. The secondary stage uses an asymmetric random key generator to produce the keys for the chosen trustworthy nodes and fully excludes the unfairness nodes from the process of communication. The suggested TSSNA system has the capacity to identify malicious node operations, to offer high level security, and to withstand various security threats. The proposed approach provides better delivery rates with high key matching ratio, as demonstrated by simulation results.

Keywords: Node Contact Ratio, Pseudorandom key generator, Node Authenticity, Trust Computation, Sign verification.

1. Introduction

The most popular type of sensor node for sensing and transmitting infrastructure reports in recent years has been a wireless one. This sensor node typically comprises of a small number of inexpensive, low-capacity, and low-power resources [1]. Target tracking, civil and military activities, monitoring of the healthcare system, and atmospheric surveillance represent a few of the use-case areas of WSN. The deployed sensor nodes constantly scan their immediate environment and transmit updated sequences to the controller or base station over a single hop or multiple hops. Massive numbers of sensor nodes are installed in WSNs in order to maintain the network's security because of how easily an attacker could bring erroneous data into the system and manipulate the external environment [2].

Every node in a sensor system must first be authorized by the Base Station in order to receive actual-time information from the nodes that are collecting data. By doing this, unauthorised access from the nodes and by the nodes can be avoided. All types of sensors are capable of producing different types of data with varying security levels in situations like mission-critical or combat applications. Authentication ensures that the data came from the approved node or source and verifies the identity of the connected node [3]. To improve network efficiency, confidentiality of information, reliability, and trustworthiness must be guaranteed.

2. Related Works

To secure the network, a number of encryption and verification techniques were suggested. For the purpose of comparison, a few protocols were addressed below.

In order to swiftly identify and acquire nodal trust and hence increase the data route security, ActiveTrust actively creates a number of monitoring routes. This is one of the efficient conventional strategies for avoiding black holes. The ActiveTrust method, which can fully utilize the energy in non-hotspots to build as various detection routes as necessary to meet the specified safety and energy proficiency, is more significant since it provides the development and distribution of detection routes [4]. Each node uses its range of transmission to find its neighbour node and establish the network's integrity. The Lightweight Dynamic User Authentication System [5] is a well-known authentication scheme that was designed for the WSN to protect against replay and counterfeit attacks. Three phases make up this system: registration, authentication, and authorization. Registration requires a username and password; once registered positively, a query is submitted by the user with a set time limit. The user must go through the enrolment process to begin a new cycle if the predefined time runs out as a result of any delays, either internal or external to the user.

A detailed summary of WSNs and a categorization of WSN attacks based on the protocol stack levels were discussed [6]. Below are eleven common attackers' attack detection techniques for the purpose of measuring WSN security. A key component of security measurement is the detection of security anomalies using security data extraction methods. In maintaining the WSN security without affecting its system presentation, Data Aggregation (DA) in conjunction with a security measure can offer a better option [7].

In order to highlight the application scenarios and security mechanisms of transmission schemes, a thorough analysis of Secure DA (SDA) in WSNs was conducted, along with comparisons and discussions of its security objectives. Comparative evaluations of security plans that classify SDA procedures into five groups based on various security objectives were looked at. An effective and scalable technique for establishing and maintaining the keys amongst sensor nodes was developed [8]. With this approach, each sensor node has a key cache table to keep track of the keys. These key caching checks to see if a key pair already exists between nodes and confirms by comparing the key to the access point.The movable sensors should be authorized to new adjacent nodes and a credential should really be generated for protected communication to ensure a high level of security. In heterogeneous WSN, a password-based client admission control [9] system with functionality authentication was developed. To retrieve the data from the network in this case, the user must possess the appropriate key and matching set of attributes. Using a collision-resistant hashing algorithm with a statistical approach, the security is examined.

Reciprocated verification and session-key conformance are used in the lightweight user authentication process for WSNs [10]. To demonstrate the resistance over same, very few conventional techniques and typical attacks are deployed. The secrecy, authenticity, authentication protocols, and session key creation of this method have all been demonstrated. Security Cooperation Collection Tree Protocol (EASMR AND TSEER) scheme [11] is a security coordination paradigm that preserves a trustworthy environment and separates malfunctioning nodes. This technique uses coupled factors influence for synchronisation and topological control. The networks synchronized by constraining the amount of targets and utilising weights.The node topology control's behaviour is evaluated using a simplistic computation of the temporal synchronisation values between nearby nodes. By routinely modifying the coupling conditional probability, the network energy usage is decreased. To make security decisions and accurately distinguish among assault nodes and inactive nodes, the coupling coordination threshold was defined.

Certificate-based pair-wise key generation [12] was suggested for implementing a strong privacy safeguarding key for data public transportation. Together with hybrid keys, symmetric key cryptosystem is employed. Elliptic Curve Cryptography (ECC) is used to incriminate the certificates used for the derivation of linked pair-wise keys. The nodes are positioned in a secure area, and secure key generation using a lightweight encryption algorithm [13] was developed. Secured communication between nodes uses two-way authentication. A system called Authenticated Anonymous Secure Routing (AASR) [14] is used to stave off powerful attacks. For protecting nodes from misinterpreting a real intent process, a secured authentication message is generated using the cryptography of onion based routing approach. However this method suffers with huge transmission delay while processing the information. The analyses of the sensors' results are utilised to identify the malicious nodes and predict their activities during attacks. The information gain trust model is used to study the authentication process [15].

Physical Layer Secure Key Generation (PL-SKG) approach [16] was suggested to minimise the quantity of key material needed for device deployment. ECC keys are used to safeguard the data and stop it from leaking to neighbourhood enemies.Energy Aware and Secure Multi-hop Routing (EASMR) protocol [17]. A conceal sharing mechanism was employed to increase network security and performance in terms of energy efficiency. Three factors are taken into account in this situation: initially the network is divided into inner and outer zones; foremost, nodes are organized into clusters based on locality proximity and the information is secured using a selective encryption method; and third, a statistical analysis is conducted to mitigate packet forwarding inadequacies. Trust based Secure and Energy Efficient Routing (TSEER) protocol was proposed [18-21] to compute comprehensive trust values for nodes. This incorporates trust values such as direct trust values, indirect trust values and energy trust values that can withstand from selective forwarding attack, black hole attacks, etc. Malignant nodes are identified vastly by using the thermal decomposition factor and adaptable consequence process.

3. Proposed work:TSSNA

To ensure robust security throughout data transmission, the Two Stage Security Model for Node Authentication (TSSNA) is developed. In terms of data privacy and genuine communication, this enhances security. Each node is issued with a credential after registration with BS in this proposed scheme since nodes distributed over the network should interface with each other in a stable manner.

Choosing trustworthy nodes during the preliminary stage involves removing malicious nodes from the routing communication process by computing the node contact ratio. The secondary step fully eliminates the malicious nodes from the transmission process and uses an asymmetric random key generator to generate keys for the chosen trustworthy nodes.

(i) Trust Node Selection – Stage 1:

Calculation of Node Contact Ratio(N_{CR}) supports in identifying the reliable nodes in the network. For determining whether nodes are present within the communication range, N_{CR} is calculated using the message requesting the route (RR_Msg) and route reply (RP_Msg) packet message (Rp_Msg) that were sent to one another. Based on the ratio of unsent RPwith respect to the number of obtained RRand sent RPto the specific node the N_{CR} is estimated. Equation 1 calculates the N_{CR}.

$$N_{CR} = \left(\frac{RR - (1 - RP)}{RP} \right) * 100 \quad (1)$$

Hybrid evaluation of trust, which considers both direct trust as well as probability of recommended trust, is performed on the node once the N_{CR} has been calculated. It is calculated using

the node's interactions value. The node is classified as an aggressor node if the weight of the interactions is lower. The computed node interaction values that are supplied to the source nodes' neighbours are used to calculate the probability of recommending trust, which gauges the node accuracy.

a. Direct Trust: The first step in computing the node's direct trust level is to use the packet routing protocol. The trust accuracy of acquired t1 and t2 for the respective analysis of node; each node keeps the trust significance level of t1. The node "M" transmits the packet to "N" with nodes trust level "t1," and node "N" transmits the message to "X" is t2 (0, 1),the nodes are trustable with the value 'DT(1)' only if the significance value t1 = t2. Once the node 'A' has been calculated "DT(A)"and retains the DT valuation of DT(1), the node "A" is added to the list of trustable nodes. If the DT ratio does not match, as in the case of node t1!=t2, the node "A" retains the trustable value of "0," i.e. DT(0) (0). Figure 1 shows the representation of direct trust. Equation 2 is used to calculate the direct trust accuracy for nodes.

$$DT(\mathrm{X})_{M,N} = \frac{M\_TransData' \rightarrow N}{N_{data} + DropData' \rightarrow X} \quad (2)$$

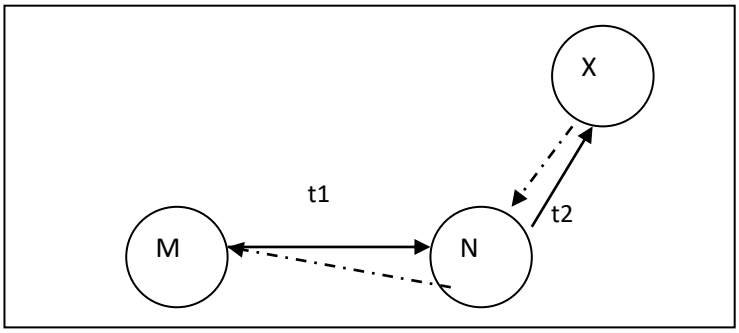

Figure 1: Direct Trust Model

Recommended Trust (RT): The weighted Dempster-Shafer trustworthiness ratio between both the nodes is used to calculate the correctness of the suggested trust. Let's consider that nodes 'M' and 'N' are neighbours and that they are denoted by the notation Y_{AB}. The proportions of recommending trust evaluation for node 'N' is then calculated at node 'M' utilizing equation 3.

$$R_{TM}^{N}(t) = \sqrt{\frac{\sum_{y \in Y_{AB}} D_T{}^{N}(\mathrm{t}) - D_{T^{N}}^{Y}(\mathrm{t})^2}{|Y_{MN}|}} \quad (3)$$

The recommended trust ratio for nodes within the source node's transmission range is calculated using the direct trustworthiness of the node. As a result, by combining the direct trust level with the current security values, the suggested trust value for each node is obtained. In this case, RT is determined using equation 4 because 'A' reflects the direct trust results calculated for the nearest neighbours and 'B' indicates the recommended trust given for the nearest neighbours.

$$R_{TM}^{N}(T) = (1 - D_{TM}^{N}(\mathrm{t})) \times \frac{\sum_{i \in Y_{AB}} (A_i \wedge B_i)}{N_i} \quad (5)$$

In this case, "n" stands for the total number of recommended trust values. Therecommendation of trust value of node "Z" in relation to its neighbouring nodes "A" and "B" is shown in Figure 2. As a result, by combining the trust values for nodes 'P', 'Q', and 'R' received through 'A' and 'B', the recommendation trust for node 'Z' may be determined.

(ii) Key Generation Process – Stage 2:

Private keys are generated for each of the chosen hubs after the clusters' trustworthy nodes have been chosen. In order to determine the node authenticity N_{Ai}, BS also produces anodesurreptitious number A_n and for each node the private key is evaluated in relation to their ID. Any authorized node that is available in the network will be able to access the data if the node's private key is made as public. As a result, the equivalent private key match along with the key validates the signature and certifies that the node is legitimate and accessible by authorized nodes.

The Certificate Authority (CA) issues certificates once the nodes' validity has been established through token verification. When a new node joins into the network system and is designated as the router, the node needs to have a legitimate identity. The node cannot continue processing the input without sign authority. When the validity of the nodes has been established (N_{Ai}, S_{Id}(key)), the two nodes can communicate to one another. Then the nodes are verified during the key generation phase in order to protect against impersonation and deception attacks. The secret key Mk is created by the random key generator and used in the message encryption procedure. Each communication has a shared authentication MAC key, or "K" which guards against hostile nodes changing the message.

The BS begins the authentication procedure after getting the authorization message, using a token identification system, and then confirms the node's eligibility for access. The message encoding procedure is completed once the certificate for the legitimate nodes is given. The algorithm for hashing of the encryption approach using a shared authentication secret is used for encryption of the communication from the recipient's network. Then the M_k is sent to the destination along with valid sign $\{N_{ai}, Id(K_i)\}$ which is included in header field of the encrypted message.

$$M_{(A,B)} = E_{msg} \,||\{\mathrm{N_{ai}}, \mathrm{S_{Id}(key)}\} \tag{3}$$

Consequently, the trust ratings collected by both DT and RT are used to evaluate the node stabilization function. The specific node is assigned to the Trustee Node (TN) list if both DT and RT of the nodes are determined to be identical. If the node trustee value appears to be changed as a result, the node is designated as aMalevolentNode (MN) and eliminated from the routing table. The consequent trustworthy node created using DT and RT values are shown in Table 1.

Table 1: Resultant Nodes

D_T	R_T	Consequent Value
0	0	TN
0	1	MN
1	0	MN
1	1	TN

Algorithm for TSSNA:

Step 1: Initial

*Step2:*Deploy ‘N’ number of nodes;

*Step3:*Once entered register with BS;

→ ***Apply preliminary stage security***

*Step 4:*Evaluate N_{CR} using RR & RP

Step 5: Compute D_T&R_T

Step 6: If obtained D_T& $R_T$are of same value

Step 7: Elect as TN else add in MN list

→ ***Apply Secondary Stage Security***

Step 8: Generate Keys for TN using pseudo random key generator ‘A_n’

*Step 9:*Set ‘S’ and ‘D’ node for transmitting data.

Step 10: Check S_{Id} for verifying node.

Step 11: Do node validation {N_{ai}, S_{Id}(key)}

Step 12: If S_{Id}(key) matches then process transmission

*Step 13:*Secured data is forwarded else discard

Step 14: End

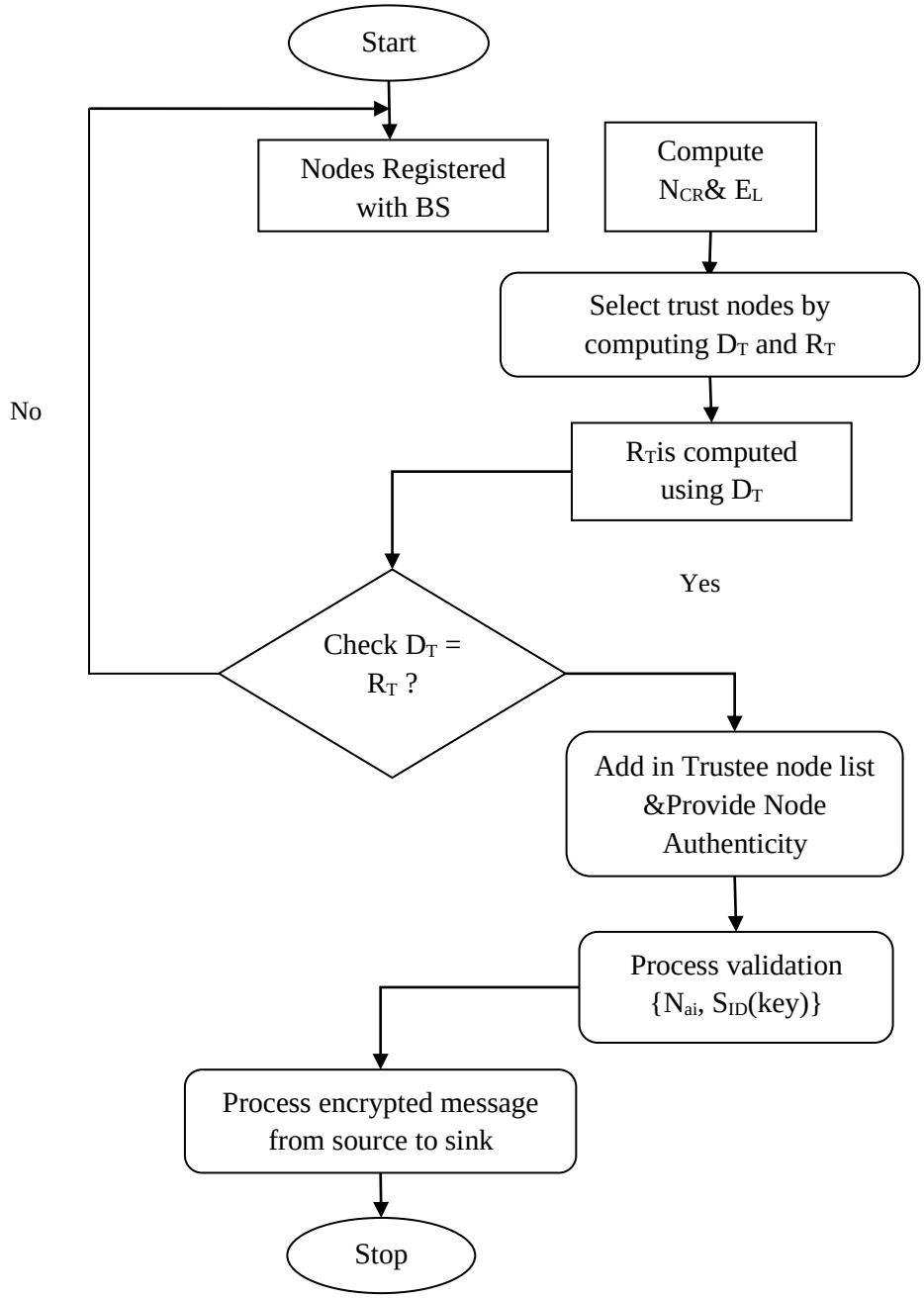

Figure 3: Flowchart for TSSNA Algorithm

4. Performance Evaluation

Using the Network Simulator tool, the TSSNA system's efficiency is evaluated. (NS2). It is a C++ and Object-Oriented Tool Command Language open source computer language. A network with 150 nodes and a 1000x1500 m2 area is used to evaluate the suggested TSSNA mechanism. Five parametric assessments are used in the simulation analysis, including the packet delivery rate, energy remaining, delay, and key matching ratio.

Table 2: Parameters and its Value

Parameter	Value

Channel Type	Wireless Channel
Network Interface Type	WirelessPhy
Number of Nodes	125
Simulation Time	80 sec
MAC Type	802.11
Traffic Model	Constant Bit Rate (CBR)
Communication Range	250metres
Data_Rate	11Mbps

Delivery Rate (DR): The term "Packet Delivery Rate" (PDR) refers to the accelerated rate at which data packets generated by CBR source are actually sent over the receiver. This measure demonstrates how effectively data is delivered over the network. The following equation (4), in which T stands for time taken and n represented for the network's node density provided.

$$PDR = \frac{\sum_{0}^{n} Successful\ Pkts\_Delivered}{Time} \quad (6)$$

Average Transmission Delay: Queuing delay is also included in the definition of packet transmission delay, which is the length of time it takes for a packet to travel from one node terminal to another. This measure calculates the proposed methodology routing policy's success rate. Equation 7 gives the data forwarding delay, where n represents the total amount of nodes.

$$Transmit_{Delay} = \frac{\sum_{0}^{n} Pkt\ rcvd\ time - Pkt\ sent\ time}{n} \quad (7)$$

Mismatch-Key Ratio: The fundamental statistic to identify fake private keys produced by malicious nodes that get mismatched when linked with BS is known as the Key Mismatch Ratio (KMR). KMR is defined as the relationship between different secret key bit counts and the overall key bit count produced for signature verification.

Leftover Energy: The node's remaining energy level present at current instant timeis referred to as leftover energy. In other terms it can also be defined as; it can be assessed by comparing the higher energy that the node has used and the energy that is still in the node.

A figure 4, 5, 6 and 7 describes the data delivery rate, leftover energy, transmission delay and KMRfor the proposed TSSNAand conventional EASMR and TSEER protocols.

The proposed strategy is compared to the conventional techniques EASMR and TSEER, in consequence the TSSNA method has higher packet rate of delivery at the recipient end. When compared to the EASMR and TSEER schemes, the suggested scheme's delivery rates are better by 23.4%.

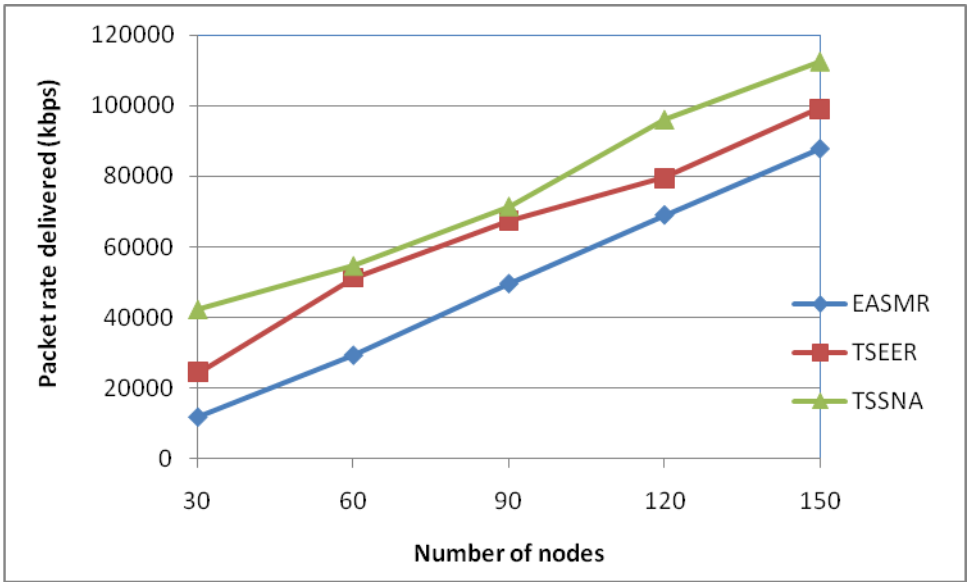

Figure4: Data Delivery Rate

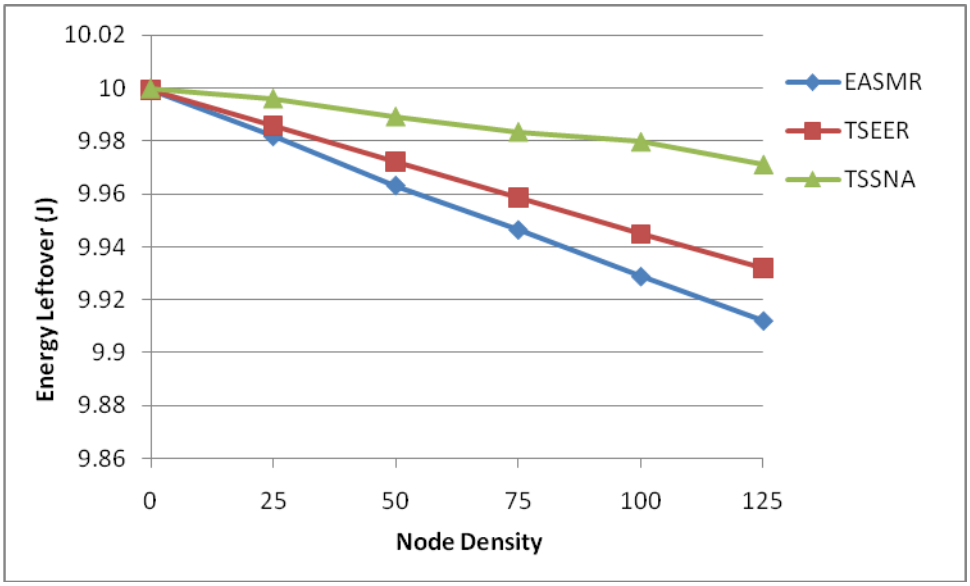

Figure5: Leftover Energy level in nodes

The node's remaining energy is calculated by taking the difference between the node's current energy level and its starting energy level. Figure 5 shows the graphical representation of energy leftover level for both proposed and conventional schemes. It is proved that the nodes in the proposed TSSNA network expend lesser energy than the conventional EASMR AND TSEER schemes.

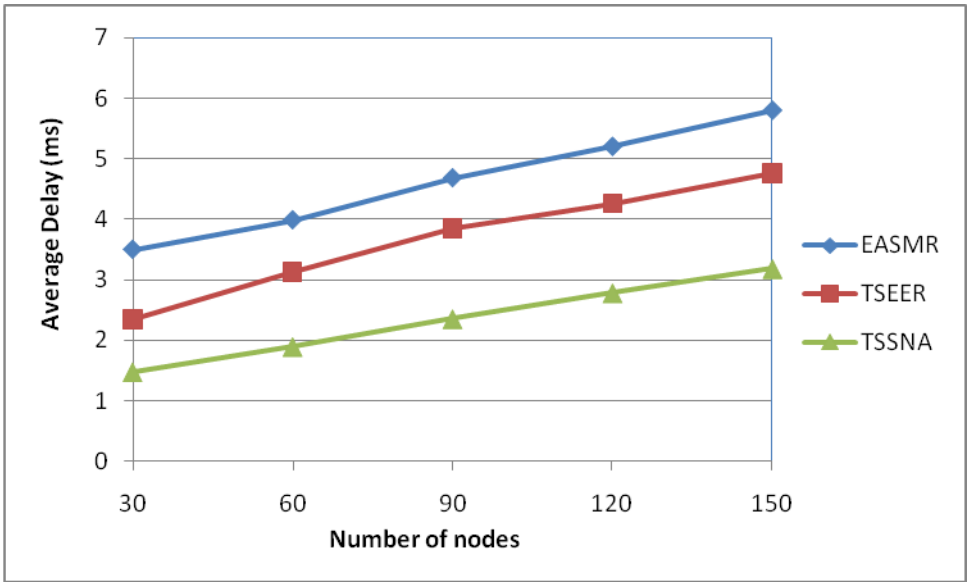

Figure6: Transmission Delay

Figure 6 depicts the delay for the proposed and typical schemes. It is demonstrated clearly that the proposed scheme TSSNA outperforms over the conventional protocols such as EASMR AND TSEER in terms of average data transmission delay.

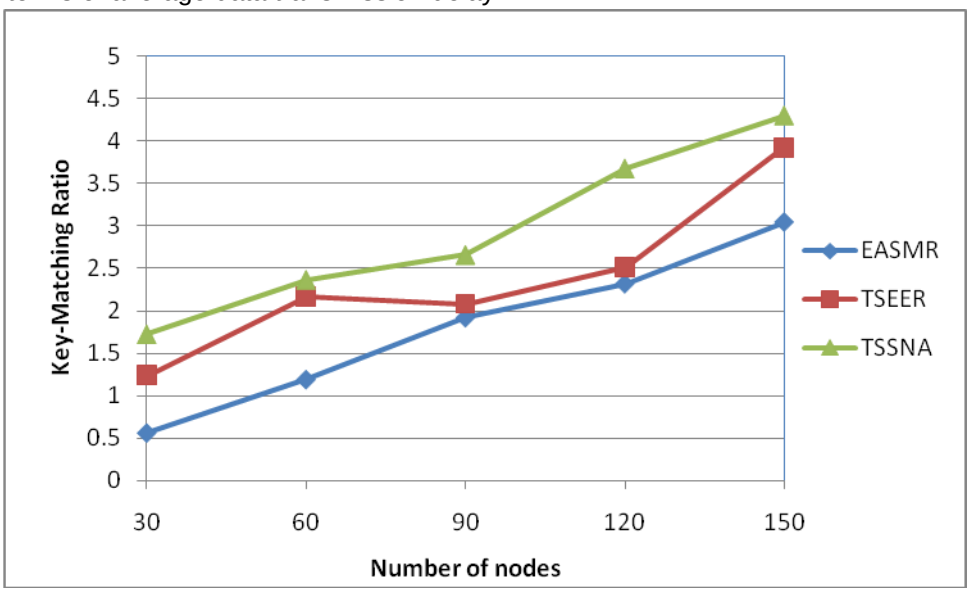

Figure 7: Matching-Key Ratio

Figure 7 provides information on KMR for the TSSNA scheme and the conventional schemes considered here. It can be seen and deduced from the graph that the proposed scheme TSSNA has a higher key-matching ratio than the conventional protocols EASMR AND TSEER.

Conclusion:

TSSNA is proposed for WSN to improve the robustness and reliability of the network. In terms of data privacy and scalable communication, this TSSNA enhances the security measures. This scheme undergoes two stage security levels by selecting trusted nodes and adding security key to the nodes present in the trusted route. Choosing trustworthy nodes during the preliminary stage involves removing malicious nodes from the communication process. This is carried out through node contact ratio which is determined using direct trust and recommended trust. The secondary stage uses an

asymmetric random key generator to produce the keys for the chosen trustworthy nodes and fully excludes the unfairness nodes from the process of communication. The suggested TSSNA system has the capacity to identify malicious node operations, to offer high level security, and to withstand various security threats. The proposed approach provides better delivery rates with high key matching ratio, as demonstrated by simulation results.

References

1. Kocakulak, M., & Butun, I. (2017, January). An overview of Wireless Sensor Networks towards internet of things. In 2017 IEEE 7th annual computing and communication workshop and conference (CCWC) (pp. 1-6).
2. Riaz, M. N., Buriro, A., & Mahboob, A. (2018). Classification of attacks on wireless sensor networks: A survey. *International Journal of Wireless and Microwave Technologies*, *8*(6), 15-39.
3. Dhamodharan, U. S. R. K., & Vayanaperumal, R. (2015). Detecting and preventing sybil attacks in wireless sensor networks using message authentication and passing method. *The Scientific World Journal*, *2015*.
4. Liu, Y., Dong, M., Ota, K., & Liu, A. (2016). ActiveTrust: Secure and trustable routing in wireless sensor networks. IEEE Transactions on Information Forensics and Security, 11(9), 2013-2027. "
5. Cheikhrouhou, Omar, Anis Koubaa, Manel Boujelben, and Mohamed Abid. "A lightweight user authentication scheme for wireless sensor networks." In ACS/IEEE International Conference on Computer Systems and Applications-AICCSA 2010, pp. 1-7. IEEE, 2010.
6. Xie, H., Yan, Z., Yao, Z., & Atiquzzaman, M. (2018). Data collection for security measurement in wireless sensor networks: a survey. *IEEE Internet of Things Journal*, *6*(2), 2205-2224.
7. Liu, X., Yu, J., Li, F., Lv, W., Wang, Y., & Cheng, X. (2019). Data aggregation in wireless sensor networks: from the perspective of security. *IEEE Internet of Things Journal*.
8. Y. Qiu, J. Zhou, J. Baek, and J. Lopez, “Authentication and key establishment in dynamic wireless sensor networks,” *Sensors*, vol. 10, no. 4, pp. 3718–3731, 2010.
9. Jokhio, S. H., Jokhio, I. A., & Kemp, A. H. (2013). Light-weight framework for security-sensitive wireless sensor networks applications. *IET Wireless Sensor Systems*, *3*(4), 298-306.
10. Chatterjee, S., & Das, A. K. (2015). An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks. *Security and Communication Networks*, *8*(9), 1752-1771.
11. Liu, Z., Liu, W., Ma, Q., Liu, G., Zhang, L., Fang, L., & Sheng, V. S. (2019). Security cooperation model based on topology control and time synchronization for wireless sensor networks. *Journal of Communications and Networks*, *21*(5), 469-480.
12. Porambage, P., Kumar, P., Schmitt, C., Gurtov, A., & Ylianttila, M. (2013, December). Certificate-based pairwise key establishment protocol for wireless sensor networks. In *Computational Science and Engineering (CSE), 2013 IEEE 16th International Conference on* (pp. 667-674). IEEE.
13. Jokhio, S. H., Jokhio, I. A., & Kemp, A. H. (2013). Light-weight framework for security-sensitive wireless sensor networks applications. *IET Wireless Sensor Systems*, *3*(4), 298-306.
14. M. Abdelhakim, L. E. Lightfoot, J. Ren, and T. Li, “Distributed detection in mobile access wireless sensor networks under byzantine attacks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 4, pp. 950–959, 2014.
15. Shen, H., & Zhao, L. (2013). ALERT: an anonymous location-based efficient routing protocol in MANETs. *IEEE Transactions on Mobile Computing*, *12*(6), 1079-1093.
16. Moara-Nkwe, K., Shi, Q., Lee, G. M., & Eiza, M. H. (2018). A Novel Physical Layer Secure Key Generation and Refreshment Scheme for Wireless Sensor Networks. *IEEE Access*, *6*, 11374-11387.
17. 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.

18. Hu, H., Han, Y., Yao, M., & Song, X. (2021). Trust based secure and energy efficient routing protocol for wireless sensor networks. *IEEE Access*, *10*, 10585-10596.
19. Uma Sankar G, **Saravanan D**, (2018), Single Objective for an Integer Partial Flexible Open Shop Scheduling Problem Using Developed Ant Colony Optimization, International Journal of Mechanical and Production Engineering Research and Development (IJMPERD) ISSN(P): 2249-6890; ISSN(E): 2249-8001 Vol. 8, Issue 3, Jun 2018, PP 1121-1132.
20. Vilma Roseline J, **Saravanan D**, (2019), Crossover and Mutation Strategies applied in Job Shop Scheduling Problems, Journal of Physics: Conference Series (JPCS), 1377 (2019) 012031 doi:10.1088/1742-6596/1377/1/012031Conference Proceedings.
21. Vilma Roseline J, **Saravanan D**, (2022), Hybrid Backward Production Scheduling for Manufacturing Systems, *Indian Journal of Natural Sciences, ISSN: 0976 – 099, Vol.13, Issue 75, PP 51559-51568*