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

An Energy Efficient Master Auditor Node with Trust Based Secure Routing in Wireless Sensor Networks

D. Murli Krishna Reddy[1], R. Sathya[2], V.V.A.S. Lakshmi[3]

Submitted: 24/04/2023 **Revised**: 26/06/2023 **Accepted**: 06/07/2023

Abstract: Wireless Sensor Networks (WSN) has risen in popularity as a result of the pervasiveness of communication networks and the convenience of transmitting and collecting information through these networks. Its widespread adoption can be attributed to the fact that these networks can be used in any setting without the need for costly and time-consuming environmental monitoring and engineering. To counteract malicious activity on individual nodes, trust-based approaches have recently emerged as a promising option. Implementing a reliable reputation system is the standard method used to provide trust-aware routing. When it comes to modelling the information on the behavior of nodes in a manner that accurately reflects various sources of this information, a good rating technique is essential in WSN reputation systems. Routing can be easily attacked, which can severely reduce the performance of WSNs. As most routing attacks originate from compromised nodes, conventional security mechanisms like cryptography and authentication are insufficient to counter them on their own. In order to strengthen safety and collaboration between nodes, a trust mechanism was recently implemented. The trust mechanism in routing either excludes or includes nodes in the routing procedure based on the predicted trust value. The proposed model considers a master auditor node (MAN) from the available trusted nodes that monitor the entire network analyzing each node behavior. This research proposes an Energy Efficient Master Auditor Node with Trust based Secure Routing (EE-MAN-TbSR) in Wireless Sensor Networks for trusted route selection for secured data transmission. The proposed model when contrasted with the existing models performs better in trusted route selection avoiding malicious actions in the network.

Keywords*: *Wireless Sensor Network, Trust Factor, Trusted Node, Malicious Actions, Node Behavior, Master Node, Energy Efficiency, Data Transmission.

1. Introduction

Wireless Sensor Networks arise from the incorporation of sensor nodes that are small, inexpensive, and capable of detecting, communicating, and processing [1]. These nodes keep tabs on things like temperature, noise, vibration, pressure, motion, and pollution all around the place. The data from the monitored objects are transmitted to a central station [2], where they are compiled and made available to the user via the web. In order to collect sensor field data, a significant number of nodes must be put in open, potentially dangerous areas [3]. This vast network of nodes works together to keep monitoring things and report any suspicious activity back to the central hub. Due to its restricted sensing region and communication range, the node must act in conjunction with other nodes in the network [4]. That's why it's so important for the nodes in a WSN to work together for optimal performance [5].

There are many ways in which a WSN can be compromised due to its unique characteristics. These include the network's open and hostile environment, its open medium, and the wide range of critically vital applications it supports [6]. Although cryptography and authentication, two staples of traditional security, can help, they are insufficient in the face of attacks on individual nodes. If a node has been compromised [7], it can be ordered to conduct attacks against other nodes in the network, which could

potentially bring down or take control of the entire WSN [8]. A malicious node can use various techniques to draw data from other nodes to itself, and then, once it has begun receiving the data, it can drop all or arbitrarily selected pieces of data, severely impacting the routing protocol's efficiency [9]. The only effective method of dealing with such nodes is to constantly keep monitoring them.

The many methods suggested to secure WSNs introduce routing as one approach. Routing is a crucial protocol for WSNs since it handles data delivery to the base station [10]. Thus, it is crucial to have secure routing that can withstand packet manipulation and disruption attempts. Several strategies are offered to secure routing, particularly in the face of hacked nodes [11]. Trust establishment is one such technique that has been implemented in numerous studies. Establishing trust allows us to identify reliable and unreliable nodes by analyzing their track records of behavior and performance [12]. In its routing operations, it chooses only reliable nodes and avoids the rest [13]. Trust mechanisms are widely studied to increase network

1 Research Scholar in CSE Department Annamalai University Chidambaram,Tamil Nadu, India
2 Assistant professor in CSE Department Annamalai University Chidambaram,Tamil Nadu, India
3 Professor &HOD in CSE(AI&ML), Narasaraopet Engineering College, Narasaraopet, Andhra Pradesh India
** Corresponding Author Email: murali.aucse32@gmail.com*

security and cooperation because they are easy to implement and very effective at detecting compromised nodes. The WSN nodes communication is shown in Figure 1.

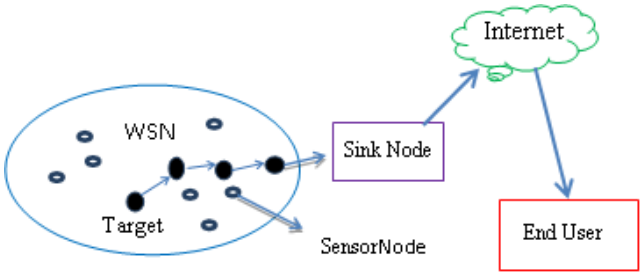

Fig 1: WSN Communication

Managing trust is essential for spotting authorized malevolent, selfish, and compromised nodes. It has been extensively researched in a variety of network settings, including P2P networks [14], grid and ubiquitous computing, and others. The truth, however, is that sensor nodes have fewer resources and other unique characteristics [15], heightening the importance and difficulty of trust management for WSNs. Thus far, studies into WSNs' trust management techniques have concentrated on evaluating the nodes' trustworthiness improving the networks' security and robustness [16]. Some real-world uses of this technique are the route, data integration, and cluster head selection [17].Trust management in WSNs is difficult despite the success of some existing ways in boosting the security of other networks [18]. In this research, an efficient algorithm is proposed that consider a master auditor node for monitoring all the nodes in the network. Initially, each node calculates its own trustworthiness and the trustworthiness of its neighbors by taking into account a wide range of trust variables, as well as the security level of the network, the link between nodes. Packet received, sent, strictness, delivery, consistency, availability, etc. are all examples of trust elements [19]. The integrated trust value of a node is generated by integrating the trustworthiness of numerous neighbor nodes using the auditor node feedback [20].

While trying to protect a WSN, trust and reputation-based approaches have proven to be more robust against attacks from malicious nodes [21]. An alternative to traditional cryptographic methods, trust-based security relies instead on established relationships between parties. In the context of wireless communication networks, trust can be thought of as the confidence one has in the activities of other nodes [22]. The use of trust-based schemes allows for more accurate prediction of node behavior based on historical data, and aids in the making of more informed decisions when attempting to identify suspicious node activity [23]. As a further point, the security architecture of a sensor network is well suited to trust-based solutions. Like the human behavior model, trust in WSN allows two nodes to communicate with one another based on the level of trust that has been built up between them over time [24]. If new information becomes available, the trust level must be adjusted accordingly. Because trusted nodes don't operate together with untrusted ones, trust-based solutions boost network performance [25].

Many trust models and secure routing methods have been presented in recent years. Nonetheless, many of the current schemes have flaws. Most trust-based routing methods, for starters, ignore the limited energy reserves of trusted nodes and instead prioritize selecting the most trustworthy neighbors [26]. Second, most methods are susceptible to substantial network overheads due to the regular exchange of a large volume of information. A malicious node may use this information flow to launch a false reporting attack, in which it spreads fake information in an effort to lower the trust rating of a trustworthy node [27]. Third, high-powered hardware platforms with an abundance of storage, battery life, and processing power are the primary focus of trust-based routing systems developed for networks [28]. Due to the distributed nature of WSNs and the limited capabilities of individual sensor nodes, these solutions are inapplicable not their current form. Finally, the dynamic identification of packet forwarding misbehavior due to malfunctioning or congested nodes is not given enough thought. The routing simulation in WSN is shown in Figure 2.

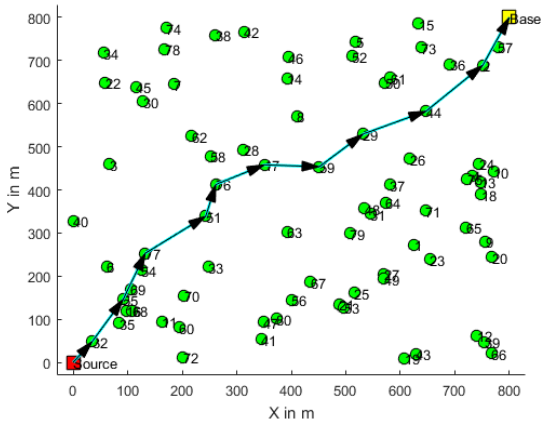

Fig 2: WSN Routing Model

Energy consumption, routing overhead, interference, delay, etc. are only few of the numerous network variables that are affected by the number of hops and the distance between hops. If the number of hops is too high, energy consumption can be lowered, but this comes at the expense of increased end-to-end latency and control overhead [29]. Due to the long-distance wireless communication nature, if the hop number is too little, the latency will be very minimal but the energy consumption will be quite high [30]. Consequently, in order to achieve both energy reduction and energy balancing, it is necessary to calculate

an ideal hop number with sufficient individual distances. The proposed model considers a master auditor node from the available trusted nodes that monitor the entire network analyzing each node behavior. This research proposes an Energy Efficient Master Auditor Node with Trust based Secure Routing in Wireless Sensor Networks for trusted route selection for secured data transmission.

2. Literature Survey

Wireless sensor networks have issues such as improving energy efficiency and effective interventions to extend the lifetime of the network and guarantee the security measures because of their working settings, restricted resources, and communication characteristics. So, in order to minimize the energy usage caused by data transmission and to protect against conventional routing assaults and particular trust attacks, an energy-aware and trust-based routing algorithm for wireless sensor networks employing adaptive evolutionary algorithm named TAGA is developed by Han et al. [2]. To achieve this goal, TAGA builds the nodes' global trust values from their direct trust values while accounting for volatilization and adaptive penalty factors, and from their indirect trust values using the filtering processes.

WSNs have two primary challenges to overcome: security and energy consumption, which arise from the features of restricted resources and dynamic topology. Although trust-based solutions are practical today, many threats, including excessive energy consumption, communication congestion, and a wide range of malicious node actions, persist. Hu et al. [3] presented a novel trust based safe and energy efficient routing protocol (TBSEER) as a means of addressing these issues. Moreover, the energy consumption caused by repetitive calculations is reduced because the nodes only need to compute the direct trust value and the Sink obtains the indirect trust value. Lastly, the cluster leaders choose the most secure multi-hop routes using the global trust value, allowing for proactive wormhole attack avoidance.

Most of the existing routing protocols for WSNs are concerned with either maximizing network lifetime or ensuring a minimum level of service availability and reliability. Yet, a more all-encompassing perspective on WSNs is required, as many applications demand QoS and security guarantees in addition to the necessity to extend the network's lifetime. Because sensor nodes have finite energy resources, a compromise must be struck among network longevity, quality of service, and security. In this article, Rathee et al. [4] proposed a QoS aware energy balancing secure routing (QEBSR) algorithm for WSNs that uses ant colony optimization to overcome these concerns. The author offered more accurate heuristics for determining both the total transmission time and the node trustworthiness along the route. The author evaluated the suggested algorithm in comparison to two others: distributed energy balanced routing and energy efficient routing with node compromised resistance.

The routing mechanism is crucial in WSNs because it facilitates the transfer of information to the network's foundation. The functionality of WSNs can be severely compromised or even destroyed by routing attacks. Security in routing and high performance in WSNs depend on a reliable routing system. In response to these challenges, Abd El-Moghith et al. [5] proposed a trusted routing approach that integrates deep blockchain and Markov Decision Processes (MDPs) to improve the safety and effectiveness of routing in WSNs. The Proof of Authority (PoA) technique is implemented within the blockchain network to verify the node transmission process. To identify the requisite validation group for verification, a deep learning approach is employed that takes into account the characteristics of each node. Next, an MDP is utilized to select a trustworthy forwarding node that can safely and efficiently convey the messages.

Mobile ad hoc networks (MANETs) are a type of wireless network that can be deployed quickly and does not require any preexisting infrastructure. This makes them ideal for use in situations such as emergency situations, natural disasters, military operations, and special events that take place outside. Security is a major concern in MANET because of the network's adaptability and dynamic topology, which leaves it vulnerable to a wide variety of attacks. They include eavesdropping, rerouting, and software modifications. Problems with security in MANET have become so pervasive that they have outweighed concerns about the network's quality of service (QoS). So, the best method to provide security for MANET would be intrusion tracking, which adjusts your system to recognize other violation weaknesses. Identifying intrusions is an essential component of providing security and acts as an additional line of defence against unauthorized entry. The dynamic topology and limited resources of this type of network make it difficult to provide energy-efficient and secure routing. Veeraiah et al. [6] proposed a trust-based secure energy-efficient navigation in MANETs using the hybrid algorithm, cat slap single-player algorithm (C-SSA), which picks the best leaps in advancing the routing, to deal with the energy efficiency and security issues.

While building routing protocols for Internet of Things (IoT) applications utilizing multihop networking, it is important to take into account not just the usual concerns of energy efficiency, but also the varying needs of security, heterogeneity, and scalability. Energy Efficient Multi-Level Secure Routing (EEMSR) is proposed by Zhan et al. [7] as a method for ensuring the safety of IoT networks while also conserving energy. A cluster-based multihop

routing protocol is used to cut down on the excessive communication overhead brought on by the scalability of IoT networks, which is a realistic approach given that clustering is a viable means of energy conservation.

In wireless mesh networks, packets are transmitted using a multi-hop architecture and are handled by a number of mesh clients organized in a mobile infrastructure. The effectiveness of routing protocols is vital to the connectivity and throughput of nodes in mesh networks, hence their influence is substantial. Connecting billions of units and achieving quick coverage at low network cost has pushed the Internet of Things (IoT) and mesh clients closer together in recent years. If the clients of a mesh network are mobile, however, the data routing via intermediary nodes has a significant impact on the network's performance and latency. Additionally, the Internet's vastness makes it possible for a hostile node to become a member of the mesh network, compromising the integrity of the information being sent. Because of this need, Haseeb et al. [8] suggested a robust and trusted scheme (RTS) for IoT-based mobile mesh networks to ensure secure and private communication and data transfer. To begin, the suggested approach provides a secure data routing among mobile mesh clients, routers, and gateway devices according to network parameters and measurements of wireless channels.

Reducing power consumption is a major area of study for wireless sensor networks. Using the clustering technique effectively allows for power savings. Nevertheless, most existing clustering algorithms perform each round of clustering using a fixed cluster head election procedure, which results in inappropriate nodes continually being elected as cluster heads, which quickly depletes node energy and shortens the lifespan of the network. Hou et al. [9] offered an Energy-saving Fuzzy Clustering Routing method (EFCR) for wireless sensor networks by dividing the clustering process into two distinct phases, Clustering Type1 and Clustering Type2, and executing each phase in turn at intervals determined by a predetermined threshold.

3. Proposed Model

WSN has seen a meteoric rise in its widespread use in recent years. WSN applications are bound by the limited set of computer resources owned by the sensor nodes and the security considerations of data communication in the WSN. Researchers are actively working into the topic of routing in WSN to find ways to enhance the capabilities of WSN. Until date, energy-effective routing has been a substantial challenge to overcome. A protocol for data transmission is necessary among nodes of a WSN to select a path for data transfer through the network. The power consumption of a WSN can be reduced by using one of the many energy-efficient data transfer protocols that can be set up to distribute the energy load among all nodes. The uncontrolled nature of wireless networking in WSN, coupled with the limited capabilities of individual nodes, makes ensuring security and privacy difficult.

Trust-based techniques have been shown to be more secure against internal node assaults in WSNs. New solutions for the routing security of WSNs can be found with the use of a trust-based scheme, which can be used to forecast the behavior of nodes based on past observations and to identify an effective decision based on the behavior of a suspect node. Yet, there are limitations to the conventional trust-aware based routing protocols as well, such as excessive energy consumption and a dearth of attack types. In addition, the paths whose extensive trust value is based on hops may be inadequate for message transmission because the paths with a greater comprehensive trust value have more hops. As taking part in secure routing cooperation is predicated on nodes' trust values, the latter will more often than not be chosen as the relay node in the routing path. The primary trust value, secondary trust value, volatilization factor, and remaining energy of a node are used to determine the comprehensive trust level, and the node is regarded to be untrustworthy if the overall trust value is less than the predefined threshold. The proposed model framework is shown in Figure 3.

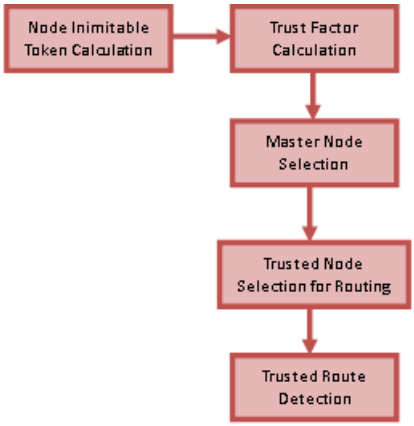

Fig 3: Proposed Model Framework

The suggested trust mechanisms rely heavily on the master auditor node mechanism to underpin their learning component. Connected nodes within radio range of one another can employ the master node function to keep monitoring the nodes in the network. The node which has the best trust value and better performance rate can be selected as MAN node that evaluates each node behavior and performance and provided feedback to update the route. A trust estimation's precision is directly affected by the learning component's output, which is used as an input. This highlights the significance of precise detection of malicious nodes. As every node in the network can commence routing establishment by broadcasting an RREQ message, the sink may receive several RREQs equal to the number of link tables, where r is the total

number of links. This research proposes an Energy Efficient Master Auditor Node with Trust based Secure Routing (EE-MAN-TbSR) in Wireless Sensor Networks for trusted route selection for secured data transmission.

Algorithm EE-MAN-TbSR

{

Input: Nodes Set {Nset}

Output: Trusted Route List {TRLset}

At first, all the nodes in WSN are added as registered members of the network. An inimitable token will be assigned to each node in the network. All of the verified nodes in the network will be given the same Inimitable token for easy identification of nodes during communication. The process of assigning Inimitable tokens are performed as

$$RegNode[N] = \sum_{i=1}^{N} \frac{nodephID(i)}{netsize(N)} + \frac{getTI(i)}{Th} * maxPrime(i) + allocener(i)$$

Here nodephID is the nodes physical address and netsize() is the network node handling capacity, maxPrime() is the maximum prime number considered during node registration and allocated energy is considered.

Inimitable tokens will be assigned to nodes that have registered with the network, with the trust factor taking into account the node's past data transfer rate and traffic capacity. In order to decide whether or not to include a node in the routing process, its trustworthiness is determined. The trust factor estimates the node consideration in routing. The trust factor calculation is performed as

$$TrustFactor[N] = \prod_{i=1}^{N} \frac{maxPDR(i)}{\delta} + availener(i) + getmax\big(\tau(i)\big) + Th$$

$$TrFac[N] = \prod_{i=1}^{N} \max\big(TrustFactor(i, i+1)\big) + RegNode(i) + Th$$

Here δ is the total packets generated in the network, τ is the computational complexity calculation model and Th is the threshold value in trust factor calculation.

The trusted nodes will be considered in the data transmission process and among the trusted nodes, the best trusted node having minimum energy consumption, highest trust factor, high computational capabilities will be considered as the Master Auditor Node (MAN). The MAN node will monitor all the remaining trusted nodes to check their behavior during active state. The MAN node selection is performed as

$$Inode[N] = \sum_{i=1}^{N} \frac{mindist((Y2 - Y1) + (X2 - X1))}{netsize(N)} + mindist(i)$$

$$MAN[N] = \sum_{i=1}^{N} \frac{maxPDR(N)}{netsize(N)} + \max\big(availener(i)\big) + \max\big(TrFac(i)\big) - \min\big(TrFac(i)\big) + \tau(i)$$

The MAN node feedback processing and trust factor consideration is performed to select the nodes to involve in routing process. The node selection process is performed as

$$NSelec[N] = \prod_{i=1}^{N} \frac{TrFac\big(MAN(i)\big)}{\tau(i, i+1)} + \frac{\max\big(PDR(i, i+1)\big)}{\delta(i)} * \sum_{i=1}^{N} mindist(i) + Th$$

The MAN node will analyze the nodes frequently and the trust factor consideration is performed and the final route will be selected for data transmission. The routing table finalization process is performed as

$$Trou(MAN[N]) = \sum_{i=1}^{N} max\big(NSelec(i, i+1)\big) * \prod_{i=1}^{N} \lim_{i \to N} \left(\delta(i) + \frac{\tau}{i}\right)^2 + \frac{maxPDR(i, i+1)}{\delta} - minloss(i) + \frac{setneigh(i, i+1)}{netsize(i)}$$

}

4. Results

A WSN is a network of several sensor nodes, typically placed in outlying locations. Many types of sensors are installed on the sensor nodes. As a result of the wide variety of sensor nodes, WSNs can be used in numerous contexts, from the medical to the military to the agricultural to the domestic. Despite widespread use, WSNs struggle with the usual suspects such low power, slow processing, little memory, and slow communication. These factors all contribute to a decline in sensor network performance and a shorter lifespan. As time goes on, WSNs will become increasingly significant. Few uses of wireless sensor networks, despite their widespread use, necessitate real-time data delivery with as little downtime as feasible. For a number of uses, throughput is more critical than latency. Which parameter is preferred depends entirely on the needs of the application. The ability to understand and implement a network's underlying structure

and routing protocol is crucial, and this understanding must be tailored to each individual application.

Routing is a crucial process in WSNs and must be handled with care. Getting data from the sensor nodes to the base stations requires a routing mechanism. This paper's primary concern is with the routing protocol, which varies with use case. When combined with the higher energy required to run the network, the routing issue drastically shortens the lifespan of the system. As a result, many different routing protocols have been created in an effort to reduce the network's overall power consumption and extend its useful life. This research proposes an Energy Efficient Master Auditor Node with Trust based Secure Routing (EE-MAN-TbSR) in Wireless Sensor Networks for trusted route selection for secured data transmission. The proposed model is compared with the traditional Adaptive QoS and Trust-Based Lightweight Secure Routing (AQoS-TLSR) Algorithm for WSNs. The proposed model achieves better accuracy in selection of best trusted route.

The proposed model initially maintains nodes information in the network so that they can be easily recognized in data transmissions. The Inimitable tokens are allocated for each node in the network. The Node Inimitable Token Allocation Accuracy Levels of the existing and proposed models are shown in Table 1 and Figure 4.

Table 1: Node Inimitable Token Allocation Accuracy Levels

Nodes in the Network	Models Considered	
	EE-MAN-TbSR Model	AQoS-TLSR Model
50	94	50
100	94.6	100
150	95	150
200	95.6	200
250	96.3	250
300	97.2	300

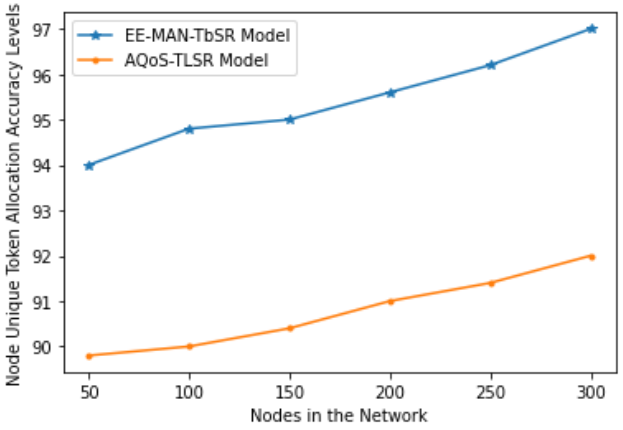

Fig 4: Node Inimitable Token Allocation Accuracy Levels

The WSN model considers trusted nodes and the communication is performed only among the trusted nodes that are marked in green color. The WSN nodes that are certified as trusted nodes by the MAN node only will be considered as finalized nodes that are involved in the routing process. The WSN trusted node simulation model is shown in Figure 5.

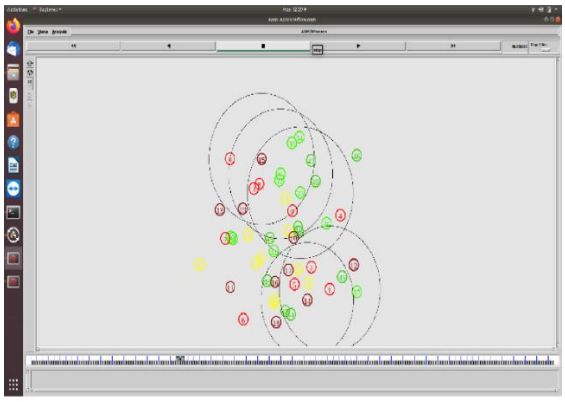

Fig 5: WSN Trusted Node Simulation

Trust factor is a value assigned to nodes in the network based on their behavior in the network. Packet delivery rate, energy consumption, computational capabilities are the parameters used to identify the node behavior. Using a node's trustworthiness in carrying out activities in QoS characteristics is a novel approach for ensuring packet security. Based on its past transaction history, a node's credibility can be assessed by any other node in the network. The Table 2 and Figure 6 represents the Trust Factor Calculation Time Levels of the existing and proposed models.

Table 2: Trust Factor Calculation Time Levels

Nodes in the Network	Models Considered	
	EE-MAN-TbSR Model	AQoS-TLSR Model
50	14.2	50

100	14.5	100
150	14.8	150
200	16.2	200
250	16.4	250
300	16.8	300

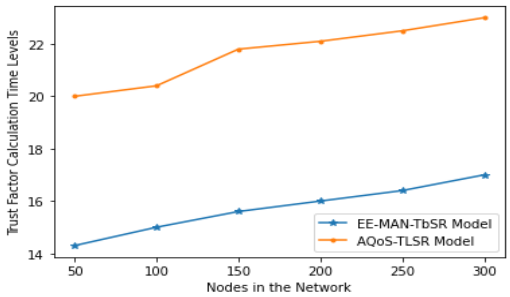

Fig 6: Trust Factor Calculation Time Levels

The proposed model considers the MAN node from the trusted nodes in the network. The MAN node will monitor the entire network for the nodes behavior during data transmission. The Table 3 and Figure 7 represents the Master Auditor Node Selection Time Levels of the proposed and traditional models.

Table 3: Master Auditor Node Selection Time Levels

Nodes in the Network	Models Considered	
	EE-MAN-TbSR Model	AQoS-TLSR Model
50	14.3	50
100	14.5	100
150	14.9	150
200	16.1	200
250	16.2	250
300	16.4	300

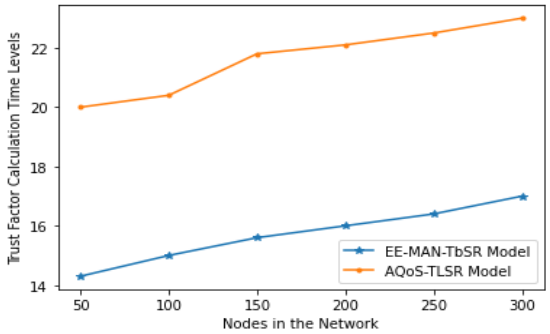

Fig 7: Master Auditor Node Selection Time Levels

During data transmission, there is a possibility of attackers nodes to perform malicious actions in the network. The MAN node will frequently monitor the nodes behavior during data transmission. The Master Auditor Node Selection Accuracy Levels of the proposed and traditional models are shown in Table 4 and Figure 8.

Table 4: Master Auditor Node Selection Accuracy Levels

Nodes in the Network	Models Considered	
	EE-MAN-TbSR Model	AQoS-TLSR Model
50	91	50
100	93	100
150	93.6	150
200	94.5	200
250	95	250
300	96	300

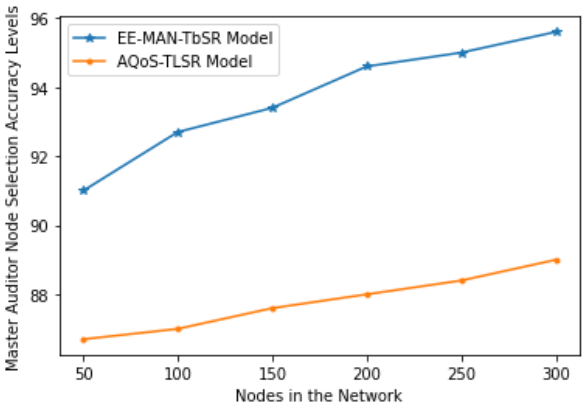

Fig 8: Master Auditor Node Selection Accuracy Levels

Routing is a crucial process in WSNs and must be handled with care providing security. In order to establish communication between the sensor nodes and the access points, a routing strategy is required to transmit the data between them securely. The proposed model based on the trust factor identifies the route in a short time. The Table 5 and Figure 9 represents the Trusted Node Route Selection Time Levels of the proposed and existing models.

Table 5: Trusted Node Route Selection Time Levels

Nodes in the Network	Models Considered	
	EE-MAN-TbSR Model	AQoS-TLSR Model
50	8	50

100	8.5	100
150	10	150
200	10.3	200
250	10.9	250
300	11	300

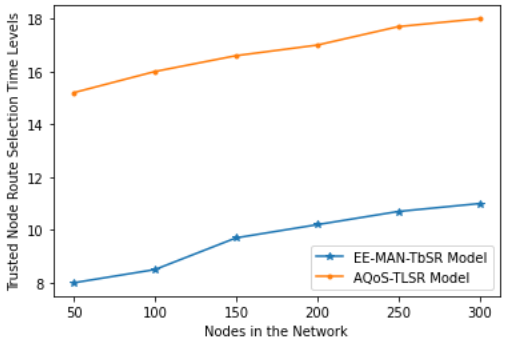

Fig 9: Trusted Node Route Selection Time Levels

In WSNs, data distribution to base stations is accomplished through a process known as routing. It is easy to disable and drastically degrade the performance of WSNs via routing attacks. As most routing attacks originate from compromised nodes, traditional security mechanisms like cryptography and authentication are unable to counter them on their own. In order to strengthen safety and collaboration between nodes, a trust mechanism was recently implemented. The routing process uses an estimated trust value to choose which nodes to include or exclude. The Trusted Route Selection Accuracy Levels of the proposed and traditional models are shown in Table 6 and Figure 10.

Table 6: Trusted Route Selection Accuracy Levels

Nodes in the Network	Models Considered	
	EE-MAN-TbSR Model	AQoS-TLSR Model
50	94.6	50
100	95	100
150	95.4	150
200	96	200
250	97.5	250
300	98.2	300

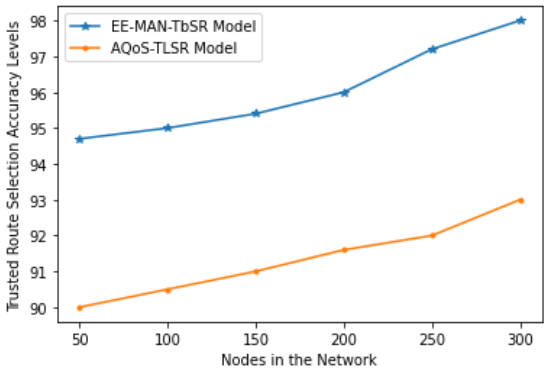

Fig 10: Trusted Route Selection Accuracy Levels

When comparing the number of packets transmitted from a source node to a destination node in a network to the number of packets actually received, packet delivery ratio is calculated. The maximum possible number of data packets must be delivered to the receiver. The Table 7 and Figure 11 depicts the Packet Delivery Rate Levels of the existing and proposed models.

Table 7: Packet Delivery Rate Levels

Nodes in the Network	Models Considered	
	EE-MAN-TbSR Model	AQoS-TLSR Model
50	96	50
100	96.5	100
150	97	150
200	97.5	200
250	98	250
300	98.4	300

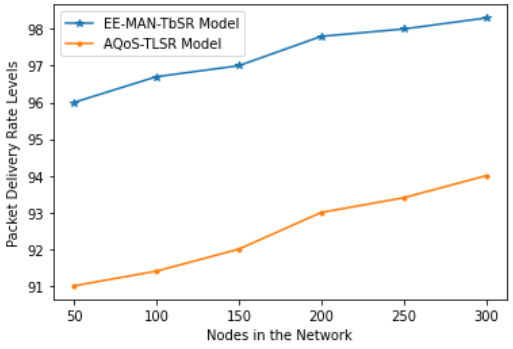

Fig 11: Packet Delivery Rate Levels

5. Conclusion

WSNs are characterized by opportunistic transmission, sparse connection, and regularly shifting network

architecture among its nodes. Without end-to-end connectivity, WSN routing uses a store carry-and-forward method, in which messages are relayed via a series of intermediate nodes utilizing opportunistic encountering, leading to significant end-to-end latency. For WSNs, a dynamic trust management approach for handling malevolent and opportunistic misbehaving nodes is proposed in this research. Transmitting data reliably and efficiently while accounting for the unpredictable behavior of nodes is difficult. To address this issue, this research presented a trust based secure routing protocol with master auditor node. This research proposes an Energy Efficient Master Auditor Node with Trust based Secure Routing in Wireless Sensor Networks for trusted route selection for secured data transmission this method aids in the selection of a trustworthy and power-saving path, both of which are crucial to the sustainability of WSN networks. The proposed architecture makes it possible to zero in on the optimal trust setting for trust aggregation, where subjective trust is most in line with objective trust for each trust feature. The routing function used gives equal weight to trust, energy, and hop counts, allowing for the selection of nodes that are reliable, economical, and fast. The MAN node will frequently identify the nodes behavior and the trust factor based final route is updated. The proposed model achieves 98.2% accuracy in trusted route selection for secure data transmission. In future, optimization techniques can be integrated with the trust-based routing models and cluster auditors can be selected for the better performance levels.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Pathak, I. Al-Anbagi and H. J. Hamilton, "An Adaptive QoS and Trust-Based Lightweight Secure Routing Algorithm for WSNs," in IEEE Internet of Things Journal, vol. 9, no. 23, pp. 23826-23840, 1 Dec.1, 2022, doi: 10.1109/JIOT.2022.3189832.

[2] Y. Han, H. Hu and Y. Guo, "Energy-Aware and Trust-Based Secure Routing Protocol for Wireless Sensor Networks Using Adaptive Genetic Algorithm," in IEEE Access, vol. 10, pp. 11538-11550, 2022, doi: 10.1109/ACCESS.2022.3144015.

[3] H. Hu, Y. Han, M. Yao and X. Song, "Trust Based Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks," in IEEE Access, vol. 10, pp. 10585-10596, 2022, doi: 10.1109/ACCESS.2021.3075959.

[4] M. Rathee, S. Kumar, A. H. Gandomi, K. Dilip, B. Balusamy and R. Patan, "Ant Colony Optimization Based Quality of Service Aware Energy Balancing Secure Routing Algorithm for Wireless Sensor Networks," in IEEE Transactions on Engineering Management, vol. 68, no. 1, pp. 170-182, Feb. 2021, doi: 10.1109/TEM.2019.2953889.

[5] A.A. A. E. -M. And and S. M. Darwish, "Towards Designing a Trusted Routing Scheme in Wireless Sensor Networks: A New Deep Blockchain Approach," in IEEE Access, vol. 9, pp. 103822-103834, 2021, doi: 10.1109/ACCESS.2021.3098933.

[6] N. Veeraiah et al., "Trust Aware Secure Energy Efficient Hybrid Protocol for MANET," in IEEE Access, vol. 9, pp. 120996-121005, 2021, doi: 10.1109/ACCESS.2021.3108807.

[7] Y. Zhang, Q. Ren, K. Song, Y. Liu, T. Zhang and Y. Qian, "An Energy-Efficient Multilevel Secure Routing Protocol in IoT Networks," in IEEE Internet of Things Journal, vol. 9, no. 13, pp. 10539-10553, 1 July1, 2022, doi: 10.1109/JIOT.2021.3121529.

[8] K. Haseeb, I. Ud Din, A. Almogren, N. Islam and A. Altameem, "RTS: A Robust and Trusted Scheme for IoT-Based Mobile Wireless Mesh Networks," in IEEE Access, vol. 8, pp. 68379-68390, 2020, doi: 10.1109/ACCESS.2020.2985851.

[9] J. Hou, J. Qiao and X. Han, "Energy-Saving Clustering Routing Protocol for Wireless Sensor Networks Using Fuzzy Inference," in IEEE Sensors Journal, vol. 22, no. 3, pp. 2845-2857, 1 Feb.1, 2022, doi: 10.1109/JSEN.2021.3132682.

[10] W. Fang, W. Zhang, W. Yang, Z. Li, W. Gao and Y. Yang, "Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks", *Digit. Commun. Netw.*, vol. 7, no. 4, pp. 470-478, Nov. 2021.

[11] K. Thangaramya, K. Kulothungan, S. I. Gandhi and M. Selvi, "Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN", *Soft Comput.*, vol. 24, no. 21, pp. 16483-16497, Apr. 2020.

[12] V. Gomathy, N. Padhy, D. Samanta, M. Sivaram, V. Jain and I. S. Amiri, "Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks", *J. Ambient Intell. Hum. Comput.*, vol. 11, no. 11, pp. 4995-5001, Feb. 2020.

[13] G. Thahniyath and M. Jayaprasad, "Secure and load balanced routing model for wireless sensor networks", *J. King Saud Univ.-Comput. Inf. Sci.*, Oct. 2020.

[14] K. Hamouid, S. Othmen and A. Barkat, "LSTR: Lightweight and secure tree-based routing for

wireless sensor networks", *Wireless Pers. Commun.*, vol. 112, no. 3, pp. 1479-1501, Jan. 2020.

[15] M. Rathee, S. Kumar, A. H. Gandomi, K. Dilip, B. Balusamy and R. Patan, "Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks", *IEEE Trans. Eng. Manag.*, vol. 68, no. 1, pp. 170-182, Feb. 2021.

[16] M. Mathapati, T. S. Kumaran, A. Muruganandham and M. Mathivanan, "Secure routing scheme with multi-dimensional trust evaluation for wireless sensor network", *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 6, pp. 6047-6055, Jun. 2021.

[17] Jiang N, Xu D, Zhou J, Yan H, Wan T, Zheng J (2020) Toward optimal participant decisions with voting-based incentive model for crowd sensing. Inf Sci 512:1–17

[18] Li J, Wang X, Huang Z, Wang L, Xiang Y (2019) Multi-level multisecret sharing scheme for decentralized e-voting in cloud computing. J Parallel DistribComput 130:91–97

[19] Liu Z, Wang L, Wang X, Shen X, Li L (2019) Secure remote sensing image registration based on compressed sensing in cloud setting. IEEE Access 7:36516–36526

[20] Sengupta J, Ruj S, Das Bit S (2018) An efcient and secure directed difusion in industrial wireless sensor networks. In: Proceedings of the 1st international workshop on future industrial communication networks, pp 41–46

[21] Sengupta J, Ruj S, Bit SD (2019) End to end secure anonymous communication for secure directed difusion in IoT. In: Proceedings of the 20th international conference on distributed computing and networking, pp 445–450

[22] Wang X, Zhang Y, Gupta BB, Zhu H, Liu D (2019) An identity-based signcryption on lattice without trapdoor. J UCS 25(3):282–293

[23] Ye Z, Wen T, Liu Z, Fu C (2019) An algorithm of trust-based secure data aggregation for wireless sensor networks. J Northeastern Univ 12:98–110

[24] W. Fang, W. Zhang, W. Chen, Y. Liu and C. Tang, "TMSRS: Trust management-based secure routing scheme in industrial wireless sensor network with fog computing", *Wireless Netw.*, vol. 26, no. 5, pp. 3169-3182, Sep. 2020.

[25] A.B. Feroz Khan and G. Anandharaj, "A cognitive energy efficient and trusted routing model for the security of wireless sensor networks: CEMT", *Wireless Pers. Commun.*, vol. 119, no. 4, pp. 3149-3159, Apr. 2021.

[26] X. Yu, F. Li, T. Li, N. Wu, H. Wang and H. Zhou, "Trust-based secure directed diffusion routing protocol in WSN", *J. Ambient Intell. Hum. Comput.*, pp. 1-13, Nov. 2020.

[27] P. A. Patil, R. S. Deshpande and P. B. Mane, "Trust and opportunity based routing framework in wireless sensor network using hybrid optimization algorithm", *Wireless Pers. Commun.*, vol. 115, no. 1, pp. 415-437, Jun. 2020.

[28] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi and A. Kannan, "QoS aware trust based routing algorithm for wireless sensor networks", *Wireless Pers. Commun.*, vol. 110, no. 4, pp. 1637-1658, Feb. 2020.

[29] M. Hajiee, M. Fartash and N. OsatiEraghi, "An energy-aware trust and opportunity based routing algorithm in wireless sensor networks using multipath routes technique", Neural Process. Lett., vol. 53, no. 4, pp. 2829-2852, Aug. 2021.

[30] J. Jasper, "A secure routing scheme to mitigate attack in wireless adhoc sensor network", Comput. Secur., vol. 103, Apr. 2021.

[31] W. Fang, W. Zhang, W. Chen, J. Liu, Y. Ni and Y. Yang, "MSCR: Multidimensional secure clustered routing scheme in hierarchical wireless sensor networks", EURASIP J. Wireless Commun. Netw., vol. 2021, no. 1, pp. 1-20, Jan. 2021.

[32] Q. Zhang, X. Liu, J. Yu and X. Qi, "A trust-based dynamic slicing mechanism for wireless sensor networks", Proc. Comput. Sci., vol. 174, pp. 572-577, Oct. 2020.

[33] T. Yang, X. Xiangyang, L. Peng, L. Tonghui and P. Leina, "A secure routing of wireless sensor networks based on trust evaluation model", Proc. Comput. Sci., vol. 131, pp. 1156-1163, Oct. 2018.

[34] Q. Shi, L. Qin, Y. Ding, B. Xie, J. Zheng and L. Song, "Information-aware secure routing in wireless sensor networks", Sensors, vol. 20, no. 1, pp. 165, Dec. 2019.

[35] N. Sun and Y. Lu, "A self-adaptive genetic algorithm with improved mutation mode based on measurement of population diversity", Neural Comput. Appl., vol. 31, no. 5, pp. 1435-1443, May 2019.

[36] J. Xu, L. Pei and R.-Z. Zhu, "Application of a genetic algorithm with random crossover and dynamic mutation on the travelling salesman problem", Proc. Comput. Sci., vol. 131, pp. 937-945, May 2018.

[37] Mr. Kunal Verma, Mr. Dharmesh Dhabliya. (2015).

Design of Hand Motion Assist Robot for Rehabilitation Physiotherapy. International Journal of New Practices in Management and Engineering, 4(04), 07 - 11. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/40

[38] Kawale, S., Dhabliya, D., & Yenurkar, G. (2022). Analysis and Simulation of Sound Classification System Using Machine Learning Techniques. 2022 International Conference on Emerging Trends in Engineering and Medical Sciences (ICETEMS), 407–412. IEEE.

[39] M. Joseph, L. ., & Fredrik, E. J. T. . (2023). Protecting Information Stored Inside the Cloud with A New CCA-EBO Protocol Designed on Hive Technology. International Journal on Recent and Innovation Trends in Computing and Communication, 11(4s), 40–49. https://doi.org/10.17762/ijritcc.v11i4s.6305