International Journal of Safety and Security Engineering
Vol. 14, No. 1, February, 2024, pp. 115-123
Journal homepage: http://iieta.org/journals/ijsse

Network Master Node Assessed Trust Factor with Arbitrary Neighbor Assessment for Secure Route Detection in 6G Enabled Wireless Sensor Networks

Pavan Vamsi Mohan Movva*, Radhika Rani Chintala

Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram 522303, India

Corresponding Author Email: pavan.movva@gmail.com

https://doi.org/10.18280/ijsse.140111

Received: 15 May 2023
Revised: 18 January 2024
Accepted: 23 January 2024
Available online: 29 February 2024

Keywords:
wireless sensor network, routing, security, malicious nodes, trust factor, random neighbor evaluation, attacks, data loss

ABSTRACT

The wireless research community has been concentrating on sixth-generation (6G) wireless technology. One of the new paradigms brought forward by 6G is its extensive global coverage, enormous spectrum consumption, sophisticated new applications, and tight security. Nevertheless, current classical computers may lack the computational capability necessary to fully realize such features. Already, major IT firms are investigating quantum computers, which might be used as 6G enablers. A growing number of people are opting for 6G enabled wireless sensor networks (WSNs) due to its potential low cost and broad use. Malicious or self-serving nodes, in addition to broken nodes, can significantly reduce a network's performance. Most trust management schemes come with a powerful tool that can detect unusual node behavior. This research goal is to secure WSNs against malicious attacks that take advantage of the replay of routing information, hence a strong trust based routing model has been devised and built to provide safe routing options for WSNs. This research proposes a Network Master Node assessed Trust Factor with Arbitrary Neighbor Assessment (NMN-TF-ANA) for Secure Route Detection in WSN. The proposed model considers nodes in routing based on trust factor and random neighbor evaluation to achieve secure data transmission. The proposed model when contrasted with existing model achieves better performance in route selection.

1. INTRODUCTION

Wireless sensor networks (WSNs) arise from the deployment of sensor nodes that are small, cheap, and capable of detecting, transmitting, and processing [1]. Temperature, sound, vibration, pressure, mobility, and pollution levels are just some of the physical or environmental factors that these nodes track [2]. All of the acquired data from the monitoring node is transmitted to the user over the Internet. In order to gather sensor field data, a significant number of nodes are put in open in potentially dangerous situations [3]. As a result, all of these nodes work together to keep an eye on things and report any suspicious activity back to the central hub. Node's sensing area and communication range are restricted, thus it must work with other nodes in the network. As a result, node collaboration is crucial to WSN efficiency.

Only little information is known about the specifications of 6G at this time. Nevertheless, it is anticipated that the 6G standards will be finalized by the worldwide standardization organizations by 2030 [4]. 6G will be able to transmit a signal at a human computational capability by 2035, according to work at various research centers. Researchers worldwide have begun to develop a new generation of wireless networks even though 5G is available. Research in the field of wireless communication has largely concentrated on 6G systems. Some of the new paradigms brought about by 6G include worldwide coverage, enormous spectrum utilization, complicated new applications, and robust security [5]. But getting these characteristics to work might necessitate computational capacities beyond what current models are capable of. This is an exciting new direction to investigate since quantum computers employ the characteristics of quantum states to outperform classical computers in specific operations. In order to meet both the very demanding resources and the general goal of optimizing the use of network resources, the next generation of mobile networks, known as 6G, will implement on-demand self-reconfiguration [6]. With Software Defined Networking (SDN), which provides a bird's-eye view of the network, centralized control, and adjustable forwarding rules, this kind of dynamic and flexible network administration is made feasible. 6G networks are notoriously complicated, therefore researchers are looking to AI, SDN, and quantum computing to solve some of the most intractable problems, such optimising routing in these networks [7].

Because of their open and hostile environment, diversified set of critical applications, and open media, WSNs are susceptible to a wide variety of attacks. When confronted with assaults on individual compromised nodes [8], traditional security mechanisms such as authentication and cryptography can only provide partial protection. The entire WSN might be brought down or taken over if a compromised node was commanded to launch attacks against other nodes in the

network [9]. An adversarial node can disrupt the routing protocol in a number of ways. One is by luring data from other nodes to itself. Once it has started receiving data, it can either delete all of it or pick and choose what data to keep. Be on the lookout for these nodes; there's no other way to handle them. Because there is no overarching authority in WSNs, it is the responsibility of each node to detect and report any unusual behavior [10].

Several safe routing methods have been developed over the years to shield WSNs against malicious and selfish conduct [11]. These routing protocols, however, rely heavily on cryptographic primitives and authentication techniques [12] that are inappropriate for use in WSNs [13]. Unfortunately, memory size, energy capacity, and computational capabilities are typically limited on low-cost sensor nodes [14]. It is usually not feasible to use centralized administration for many encryption and authentication schemes in routing protocols [15]. Adversaries may use physical ways to compromise sensor nodes put in an unsupervised region [16]. If the keys are compromised, any security measures taken may be rendered useless. To rephrase, whereas traditional cryptographic primitive-based safe routing protocols can fend off some kinds of external assaults, they can't guard against bad activity on the part of internal nodes [17].

Trust management, which should be a component of WSN security architecture, can fix the issues in handling malicious nodes [18]. A person's level of trust in another is proportional to their confidence in their motives and behavior. Since trust management methods are good at identifying malicious actors and giving information about their future actions, they can be utilized to safeguard routing [19]. In order to ensure a more secure path for data transmission from the source node to the sink node, the results of the trust evaluation are used to select the next-hop node. As a result, various trust-based routing systems have been proposed [20]. The construction of WSN networks and the smooth and transparent replacement of failing or unreliable nodes, as well as the addition or deletion of sensor nodes as the network grows, are both influenced by trust.

However, there are still numerous major issues with the conventional trust-based routing protocols. To begin, although trust-based schemes can mitigate the attacks that naturally occur in wireless networks, they will also introduce some additional hazards that must be carefully considered. Most trust models don't take into account the particularity of trust measurements when building routing protocols, even if they are vastly different from conventional routing metrics like the number of hops, time, or other QoS criteria [21]. Finally, current trust-based routing methods have drawbacks such being tied to a single routing protocol or infrastructure. In other words, if the network's routing protocol is altered, the security methods it employs may no longer function [22]. There are two components to trust evaluation: Trust calculation and trust derivation. Prior trust models mostly focus on the process of trust computation. Actually, the trust information is exchanged frequently in trust derivation to guarantee the precision of trust evaluation, which is the primary cause of the routing procedure's extra work [23]. As a result, creating an effective trust derivation technique is an important challenge for WSN-based network architecture [24]. The WSN routing model is shown in Figure 1.

Various approaches to safeguarding WSNs are laid out, such as Because of their limited radio coverage, wireless sensor nodes frequently have to take roundabout ways to communicate with one another. Important WSN performance parameters, such as lifetime, packet delivery rates, and end-to-end packet latency, are directly affected by the architecture of the routing protocol, which determines the path data is transmitted and delivered along. For WSNs, the routing algorithms account for the precautions taken [25]. Due to the open, scattered, and dynamic nature of WSNs, the routing protocols within them are particularly vulnerable to attacks. Trust computation and trust derivation are the two parts that make up trust evaluation [26]. In earlier iterations of trust models, the trust computation took center stage. In fact, the main reason for the additional work in the routing operation is the frequent exchange of trust information during trust derivation in order to ensure the accuracy of trust evaluation [27]. This emphasizes the significance of developing a reliable technique for deriving trust in WSN-based network architecture [28]. This research proposes a Network Master Node assessed Trust Factor with Arbitrary Neighbor Assessment for Secure Route Detection in WSN. The proposed model considers nodes in routing based on trust factor and random neighbor evaluation to achieve secure data transmission.

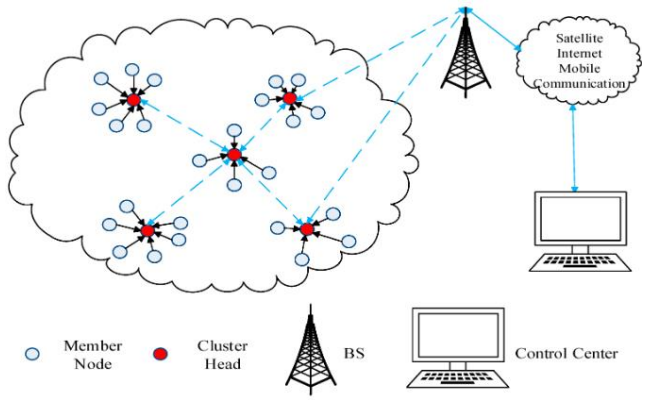

Figure 1. WSN routing model

2. LITERATURE SURVEY

Due to their changing topology and limited resources, WSNs have two major problems: energy consumption and security. Many dangers, such as excessive energy consumption and communication bottlenecks, remain even if trust-based approaches to handling unwanted node behaviors are now feasible. To solve these problems, Hu et al. [1] introduced TbSEERP, a new trust-based secure and energy-efficient routing system. To identify the overall trust value which is protected from black hole, selective forwarding, sinkhole, and hello flood attacks, TbSEERP uses an adaptive direct trust value, an indirect trust value, and an energy trust value. Also, the harmful nodes may be located fast with the help of the volatilization factor and the adaptive punishment mechanism. Nodes just need to compute the explicit trust value, and the Sink gets the indirect trust value, thus there's less energy wasted from repeated calculations. In the end, the cluster heads choose the safest multi-hop routes that actively evade wormhole attacks by utilizing the global trust value.This models experiences high computational complexity that need to be reduced.

Because of their unique working conditions, limited resources, and communication characteristics, wireless sensor

networks face challenges such as energy saving and security improvement in order to prolong the lifetime of the system and guarantee the security of the network. As a result, TAGA was introduced by Han et al. [2] as a trust-based and energy-aware routing approach for WSNs. This approach employs an adaptive evolutionary algorithm to mitigate the network's energy consumption and safeguard it from both generalized and targeted routing attacks. The aggregate trust values are formed by adding the nodes' direct and indirect trust values. This is how TAGA accomplishes this. A new threshold function is provided to select the most effective cluster leaders, which also accounts for the fluctuating global trust levels and residual energy of the nodes. The next step is to use a genetic algorithm that allows you to change the mutation and crossover probability to find the most secure route for the cluster heads.

For wireless mesh networks, Zhao and Srivastava [3] suggests a trust-based opportunistic routing algorithm to solve the problems of low message distribution rate and high network resource use caused by opportunistic network message forwarding. Starting with a comprehensive topology analysis, an opportunistic routing model is created for wireless mesh networks. In order to establish and quantify a new security assessment method based on the trust model, which evaluates the security mechanism and safety danger of communication entities, it is necessary to measure the trust levels of connections and nodes and to construct the trust relationship among nodes. Ultimately, the model's security measurement approach is used to select the node with the highest trust value to participate in the message forwarding process. Prioritizing the node with the highest degree of trust with respect to the destination node as the relay node and allocating the message copy according to the trust degree are necessary steps in designing an opportunistic routing algorithm for wireless mesh networks. This ensures that messages travel in the direction of increasing trust. The model time complexity levels are high that need to be reduced.

Essential to WSNs is the process of routing, which allows data to be transmitted to the network's base stations. The functionality of WSNs can be severely impaired or even destroyed by routing attacks. A dependable routing system is essential for maximizing WSN performance and maintaining secure pathways. Numerous methods have been explored to enhance confidence among routing nodes; a few examples include centralized routing decisions and the use of cryptographic techniques. The difficulty in identifying malicious activity on routing nodes is the main reason why most routing systems are unsuccessful in practice. At the same time, protecting yourself from attacks by malevolent nodes is not an easy task. To overcome these obstacles, Abd El-Moghith and Darwish [4] presented a reliable WSN routing method that combines deep blockchain with MDPs. Within the blockchain network, the Proof of Authority (PoA) method is used to validate the process of node transmission. A deep learning method is employed to select the necessary validation group for proofing by considering the properties of each node. Afterwards, MDPs are employed to ascertain which network node is most suited to serve as a forwarding node, facilitating the secure, efficient, and rapid transfer of messages.

The IoT allows for data sharing and collection by connecting everyday objects to the internet and each other. Everything that can be linked through a network to carry out a certain task is considered to be part of this category. This includes sensors, actuators, telephones, wearables, computers, and anything else. The same holds true for WSNs; they broadcast the data they've collected the moment they identify an occurrence. The Internet of Things (IoT) is extremely open to many different types of attacks, including those that can be transmitted from wireless sensor networks, due to its large size and diversity. Unfortunately, RPL the IPv6 routing protocol for low power and lossy networks which is widely used for IoT networks has its own security flaws caused by its features and functions. Researchers have devised a number of remedies to make sure the routing protocols and networks used by the IoT are secure. Recently, trust-based methods for incorporating security into IoT networks and routing protocols have garnered a lot of attention from academics. The security needs of the IoT system have led to the introduction of numerous trust models in the current literature, including SecTrust, DCTM-IoT, CTRUST, etc. Using the RPL routing protocol, Muzammal et al. [5] investigated various attacks that can be used against IoT networks, including Blackhole, Spoofing, Rank, and others. Additionally, we cover the several methods for reducing threats to secure routing and the significance of trust models in the IoT.

Due to the fact that many elements, such as network architecture and environmental conditions, contribute to WSN security, scientists have been working to refine trust evaluation. Current WSN node-level trust evaluations only take a single hop's worth of a node's reliability into account. Desai and Nene [6] proposed a trust assessment technique for multi-hop scenarios that makes use of a node's internal memory to determine the route's reliability. This work proposes a multihop trust evaluation technique that utilizes the TEAM and TEAP algorithms. Two approaches are proposed for evaluating the reliability of multihop algorithms; one uses normative criteria and the other empirical data. In order to get to a trusted final destination node, the proposed method finds a trustworthy sequence of intermediate nodes.

The functionality of SDWSNs can be compromised by malicious sensor nodes that engage in arbitrary actions like flooding or message dumping. Malicious nodes can lower the network's availability because of in-band communications and the fact that SDWSNs inherently lack secure channels. To aid in the identification of hazards within SDWSNs, the encouragement of node collaboration, and the facilitation of forwarding choices, Bin-Yahya et al. [7] suggested a hierarchical trust management strategy for SDWSNs. Over the numerous levels of the SDWSN architecture, TSW establishes the dependability of the participating nodes and makes it possible to detect malicious behaviors. The author employed complex trust-based computer models to detect a wide range of dangers. The author also suggested distinguishing between control and data traffic using unique trust ratings and attributes to enhance detection performance against attacks targeting the control plane's essential traffic. Lastly, a trust recording mechanism based on acknowledgment was built using some basic SDN control messages. The reliability and accuracy of the trust scores are ensured by using a weighted average technique and developing a dependable trust metric. The delay levels in this mdoels is high.

Trustworthy and reliable data delivery is challenging to achieve with WSNs because of their unique properties and limitations. To provide secure data transmission and alleviate the conflict between energy consumption and security, Yang et al. [8] detailed an evolutionary game-based safe clustering approach for WSNs that employs fuzzy trust evaluation and outlier detection. The initial phase involves implementing a

fuzzy trust assessment method that effectively decreases trust uncertainty and derives trust values from transmission evidences. We provide a K-Means-based outlier detection method for further investigation of the massive amounts of trust values collected via fuzzy trust evaluation and trust recommendation. As a bonus, it shows how different sensor nodes are and how accurate outlier detection is. For sensor nodes to achieve a happy medium between energy savings and security assurance during cluster head elections, the author also presented a safe clustering technique based on evolutionary games. A sensor node that wasn't chosen to lead the cluster can securely choose a new leader when the dangerous nodes are isolated.

Most wireless Internet of Things (IoT) networks that use IPv6 have RPL, the Routing Protocol for Low Power and Lossy Networks, installed. Sybil attacks are dangerous for unmanaged wireless IoT devices that use RPL because a single bad node can take on multiple identities and perform denial-of-service assaults all at once. Numerous approaches have been investigated in an effort to halt Sybils-induced denial-of-service attacks in RPL. Using the received signal strength indicator (RSSI) and a centralized trust system to identify Sybil nodes, Kim et al. [9] presented a new physical identification based trust path routing (PITrust) method. This method was found to improve the detection rate and packet delivery ratio.

These days, most WSN routing protocols aim to do one of three things: lower power consumption, increase service quality, or strengthen network security. Regardless, a broader view of WSNs is required because of the increasing number of applications that require QoS, security guarantees, and the potential to prolong the network's lifetime. The security, reliability, and lifespan of the network are all negatively impacted by the short battery lives of sensor nodes. To address these issues, Rathee et al. [10] presented an ant colony optimization-based QoS aware energy balancing secure routing (QEBSR) algorithm for WSNs. We provide improved heuristics for estimating the total transmission time and the reliability of the nodes in the network. We compare the proposed method to two others that have been utilized before. A distributed energy balancing routing protocol with node-compromised resistance. The complex operations reduces the performance levels. Lighweight operations can be imported to increase the performance levels.

3. PROPOSED MODEL

The proliferation of computers and the Internet has made large-scale network applications a popular topic of research in many disciplines, including engineering, communication, and others. The capability industry may be further upgraded and improved by building a new wireless sensor network and smart communication transmission system. This is a subject that both network and communication academia are currently striving to research. This paper suggests studying intelligent routing algorithms for wireless sensor networks as part of the development of 6G networks. 6G networks are planned to have features including interactive media systems, high-speed telephone, and mapping. 5G telecommunications relies on wireless sensor networks, which offer an active component for communication. In the future, 6G networks will offer ubiquitous, high-speed connectivity for a wide range of devices and applications. Features like increased data rates, decreased latency, wide device connection, and network slicing are all part of their enhanced wireless communication capabilities.

When it comes to long-distance communication or network integration, WSNs can improve their communication capabilities by utilizing the connection infrastructure provided by 5G/6G networks. Achieving long-term and stable connectivity can be challenging with 5G/6G WSNs due to their unique characteristics and requirements. For WSN communication to persist over time, it needs to be energy efficient. The more complicated and faster 5G/6G networks are, the more energy they might potentially consume. In order to reduce power consumption without sacrificing performance, it is crucial to optimize algorithms and create communication protocols that are trusted. When it comes to resources like memory, processing speed, and network throughput, WSNs are known to be stingy.

WSNs are susceptible to a wide variety of attacks, making secure routing all the more important. A novel secure routing method for WSNs is proposed in this research that can operate safely even when malicious nodes are present. The protocol takes into account data like trust value and status for each node along the route. The proposed model considers a master node (MN) for assessing the network nodes trust values based on their performance levels. The status is a hybrid metric that includes the residual energy and distance to the master node, while the trust value is defined as the attack likelihood of the node based on prior packet-forwarding behaviors. As a result, the protocol generates a route that is safe from malicious assaults and optimal in terms of all available data.

Present routing protocols for WSNs do not strike a balance between energy efficiency and security. The sensor nodes would have to use more resources to create and maintain more paths in the event of failures if we increased the number of potential routing paths, which might make the routing protocols more resilient. Due to the memory and processing power needed to calculate trust values, trust-based routing protocols incur high overhead, yet they are resilient to many different kinds of assaults. The majority of current routing algorithms aim to minimize energy consumption, therefore they build a complete connection between any two nodes by incrementally extending the current path. Since the generated roads aren't perfect on a worldwide scale, they might not be able to withstand hostile assaults. Because of this, existing routing protocols have a hard time coming up with a secure route that satisfies both security needs and the constraints of WSNs' processing power and battery life. The WSN routing model is shown in Figure 2.

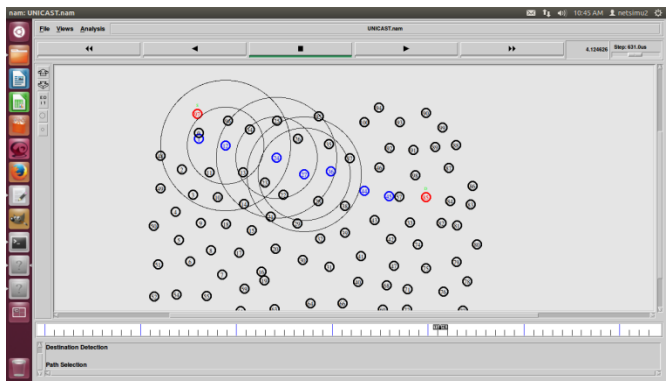

Figure 2. WSN routing model

The term routing describes the procedure by which data in WSNs is distributed to base stations. It is easy to deactivate WSN capability and routing attacks can significantly harm it. Recently, a trust mechanism was introduced to improve node cooperation and security. Nodes are either admitted or excluded from the routing process by the trust mechanism based on their trust value assessment. To secure routing and account for different types of routing attacks, there are several suggestions for trust-based routing protocols. This research demonstrates that the trust value has a direct impact on the route selection methodology. Nodes in a network keeps monitoring on one another and rate one another's trustworthiness. Several distinct methods exist, depending on the routing protocol, for locating a trustworthy routing path and evading a hostile node. It is up to the nodes along the path, or even the one at the beginning, to choose the path. It detects attacks, which is a critical function in trust-building methods. The proposed model framework is shown in Figure 3.

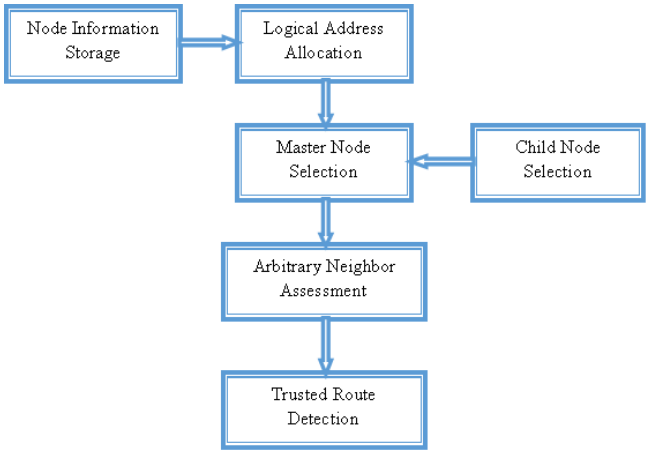

Figure 3. Proposed model framework

Based on the trust level, the next node in the forwarder chain will be chosen. The probability that a node is malicious is factored into the trust metric computation via the trust distribution. The opportunistic routing method takes advantage of the WSN's broadcasting functionality to send data packets across the network whenever the nodes in the connection have them available. The amount of dropped data packets during the data communication process in the WSN is used to assess the likelihood that a sensor node has been compromised or infected. The proposed model considers a switching module between the master node and child node. The master node if failed automatically activates the child node with highest trust factor. The child node will monitor the nodes and analyzes their behaviour. This research proposes a Network Master Node assessed Trust Factor with Arbitrary Neighbor Assessment (NMN-TF-ANA) for Secure Route Detection in WSN. The proposed model considers a master node in the network and this node will monitor all the nodes actions during data transmission. The proposed model along with MN monitoring, considers a trusted and nearby neighbor randomly and considers its trust feedback for the performance analysis.

Input: Nodes List in Network {NodeList}

Output: Trusted Nodes in Route {Troute}

Step-1: The nodes that need to involve in communication or to transmit the data has to provide the node information with the network administrator for involving the network communication and to share details. Every node should have a unique identity in the network and the process of allocation of logical address to the registered nodes is performed as:

$$NLA(NodeList[M]) = \sum_{n=1}^{M} \frac{baseaddr(n)}{netSize(M)} + getloc(X,Y) + maxener(n) + getregTime(n)$$

Here node base address is considered for the logical address generation, X, Y are the location coordinates of a node and the time stamp is considered to fix the node registration time levels for future authentications.

Step-2: The proposed model calculates the trust factor of all the registered nodes in the network and then selects a node as a master node that has highest trust factor than the remaining nodes and that is nearest to all the nodes in the network. The master node in the network will monitor the remaining nodes behavior in the network and can update the trust factors of the nodes. The selection of master node is performed as:

$$dist(n) = \sum_{n=1}^{M} \frac{NLA(n)}{M} + \min\left(\frac{X2(n+1)-X1(n)}{Y2(n+1)-Y1(n)}\right)$$

$$TruF(NodeList[M]) = \prod_{n=1}^{M} \text{maxPDR(n)} + \tau(n) + \text{maxavailener(n)} + \text{minlossrate(n)} + mindist(n)$$

$$MN[M] = NLA(n) + \frac{maxPDR(n)}{totpkts(M)} + maxPDR(n)$$

$$\sum_{n=1}^{M} \begin{cases} MN \leftarrow NLA(n) \; if \; (maxPDR(n) \; and \; maxener(n)) \\ recalculate \qquad\qquad Otherwise \end{cases}$$

Here maxPDR reflects the maximum packet delivery rate of a node considered and τ is the model that calculates the computational capabilities of a selected node and nodes having maximum energy levels are considered.

Step-3: In WSN, because of limited battery power, any node can be removed from the network at any time. If master node selected has any issue, then the entire network will be collapsed. In order to avoid network crash and delay, when a master node is selected, a child node will be considered for the master node that maintains all the data available with the master node. The child node selection is performed as:

$$CN(MN[M]) = \sum_{n=1}^{M} setNode(N) + maxPDR(n) + \max\big(TruF(n)\big) + maxavailener(n)$$

$$\begin{cases} CN \leftarrow NLA(n)! = MN \; and \; if\big(maxPDR(n)\big) and \; maxener(n)) \\ recalculate \qquad\qquad Otherwise \end{cases}$$

Step-4: The arbitrary neighbor trust feedback is also considered for considering a node in the routing process. The nodes in the route will be finalized only after considering the trust feedback of master node and arbitrary neighbor node. The arbitrary node selection and trust feedback assessment is performed as:

$$ArbNode[M] = \prod_{n=1}^{M} \frac{NLA(n)+NLA(n+1)}{M} + \min\big(dist(n, n+1)\big) + \max\left(TruF(n)\right) + getrand(n) \begin{cases} rand! = MN \; and \; CN \\ recalculate \;\; otherwise \end{cases}$$

Step-5: The trusted route is identified by considering the master node feedback and arbitrary neighbor node trust

feedback and the final routing table updation is performed as:

$$Troute(LC(i)) = \sum_{n=1} MN(maxTruF(n)) + ArbNode(maxTruF(n)) + \min(dist(n, n+1)) + maxener(n)$$

4. RESULTS

WSNs have gained immense appeal due to their adaptability, which has led to their implementation in a wide variety of industries. The majority of these fields depend on unattended sites for measuring and recording environmental data such as atmospheric pressure, wind velocity, temperature, vibrations, humidity, and so on. Due to the typically unattended nature of these locations, malicious assaults on the sensor nodes are quite likely. As a result, the integrity of the data gathered and transmitted by the WSN is at risk, and the physical security of sensor nodes is compromised. Over time, several protocols have been established to ensure the safe collection and transfer of data via the internet. Due to their inefficient use of crucial sensor node resources, classical protocols are not considered to be very successful in the context of WSN. However, these protocols typically assume, incorrectly, that all nodes on the network would be cooperative and forthright when data is transmitted.

The scalability of node to node connections in 6G WSN is anticipated to be improved in 6G networks compared to earlier networks. If a network can scale to support more users and devices without compromising performance, it is considered as scalable. Increased data rates, decreased latency, and huge connection will define the 6G networks. Their characteristics make them ideal for WSN nodes communication. Devices can communicate with each other through nodes in the networks automatically. Consideration of scalability should be made in order to accommodate the increasing number of node connections in 6G networks.

Scalable networks will be more important as the amount of network connections grows. Because of the widespread deployment of 6G networks and the vast number of devices they support, a greater number of nodes will be able to connect to the network, meeting the requirements of applications like the IoT. By making sure consumers have a regular and dependable connection to the network, scalability will also aid in improving the user experience. As a result, cutting-edge wireless network applications like transportation, smart cities, and industrial automation may become possible. Wireless sensors and the IoT have worked together with several real-time settings to gather and process physical data. In order to provide high data coverage and service quality, this work introduces a reliable routing system that makes use of 6G networks in WSN. To begin, the suggested protocol sets up a routing procedure by means of a simulated annealing trust method. This model offers a risk-aware security system by avoiding uncertainties in the network and ensuring dependable session-oriented communication with network edges among linked nodes.

Due to the emergence of more complicated use cases, the number of WSN devices has multiplied by ten in recent years. The increasing expansion of WSNs necessitates measures to protect them from various security risks. In a WSN, devices can communicate ad hoc and the network's setup can be altered dynamically, without requiring any prior infrastructure. A reliable routing system is essential for efficiently navigating WSNs due to their dynamic nature. Despite the proliferation of WSN routing algorithms, most of them struggle to scale to very large-scale settings. This study presents a novel multi-path routing method that prioritizes the use of the most trustworthy nodes when making decisions. To establish the reliability of each node, we look at its trustworthy metrics. In order to establish these measures, the nodes' threshold values are utilized. This research proposes a Network Master Node assessed Trust Factor with Arbitrary Neighbor Assessment (NMN-TF-ANA) for Secure Route Detection in WSN. The proposed model is compared with the traditional Trust Based Secure and Energy Efficient Routing Protocol (TbSEERP) for Wireless Sensor Networks. The proposed model exhibits better performance levels when contrasted with t eh traditional model.

The nodes registered in the network need to be allocated with a number or an address for further communication. The proposed model maintains the node information and allocates a logical address for the nodes as a unique value for communicating with other nodes. The Node Logical Address Allocation Time Levels of the proposed and existing models are shown in Figure 4.

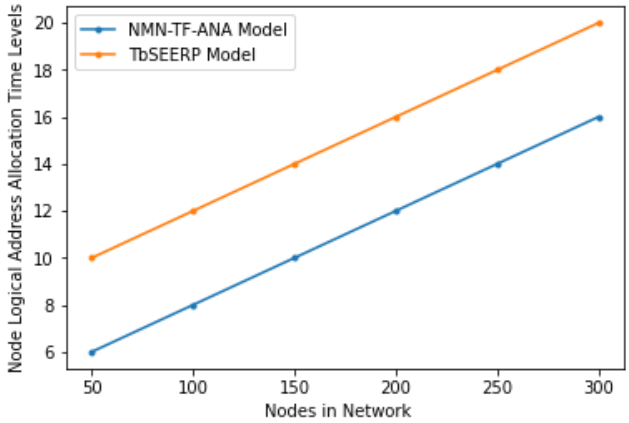

Figure 4. Node logical address allocation time levels

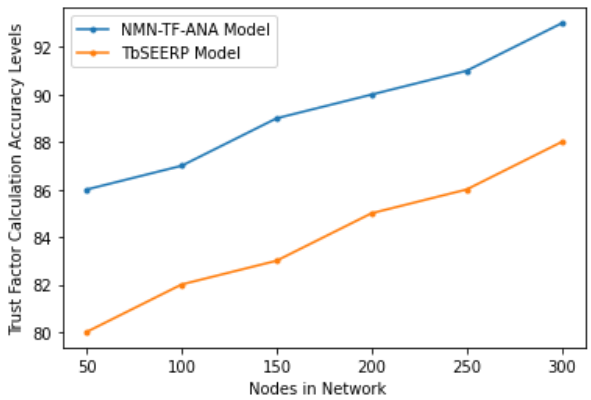

Figure 5. Trust factor calculation accuracy levels

A novel technique for safe packet routing is trust, defined as the degree to which one may rely on another node to carry out an operation or set of actions. Any node in the network can determine a node's reliability by looking at its transaction history with its neighbors. QoS parameters such as data packets and control packets forwarded, data rate, power consumption, dependability, etc. are displayed and used to assess a node's level of trust. The trust factor of a node is used

to identify the node type as normal or malicious. The Trust Factor Calculation Accuracy Levels of the proposed and existing models are shown in Figure 5.

The proposed model considers Master Node among the trusted nodes in the network. The master node will monitor the entire network and the behavior of the nodes will be assessed. The Master Node Selection Accuracy Levels of the proposed and traditional models are shown in Figure 6.

The proposed model calculates the nodes trust factor of all the nodes in the WSN and then a node that is nearby is arbitrarily selected and the feedback is considered for a node. The Arbitrary Neighbor Selection Time Levels of the existing and proposed models are shown in Figure 7.

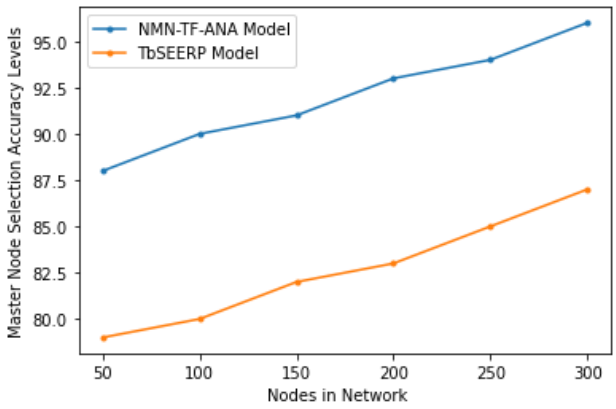

Figure 6. Master node selection accuracy levels

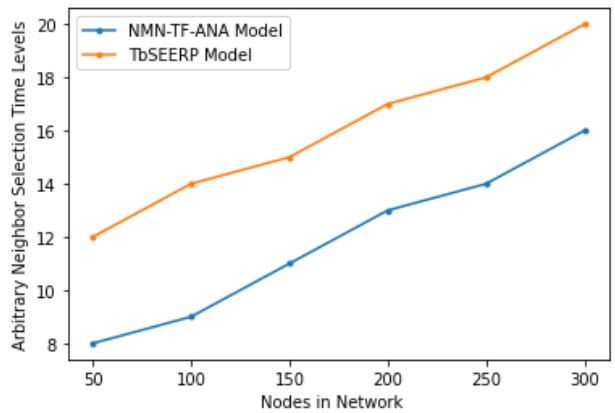

Figure 7. Arbitrary neighbor selection time levels

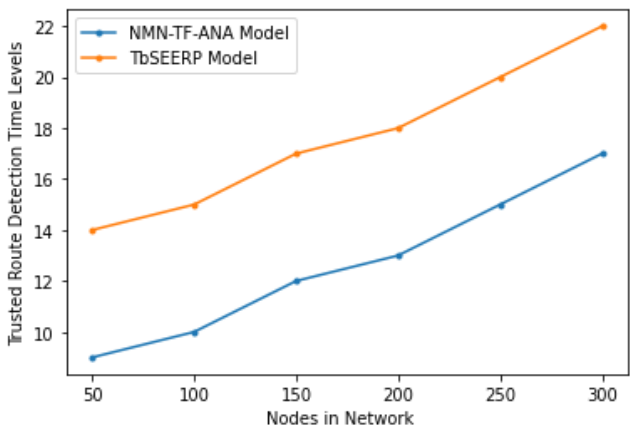

Figure 8. Trusted route detection time levels

The Trusted Route Detection is performed by considering only trusted nodes that are accessed by considering the nodes trust factor and arbitrary node trust factor along with the MN node evaluation. The trusted route helps in secure data transmission in the WSM. The Figure 8 shows the Trusted Route Detection Time Levels of the existing and proposed models.

It is the job of secure network architectures in WSN to protect route discovery from being disrupted by malicious attempts at tampering with the network's routing infrastructure. The Trusted Route Detection Accuracy Levels of the proposed and existing models are shown in Figure 9.

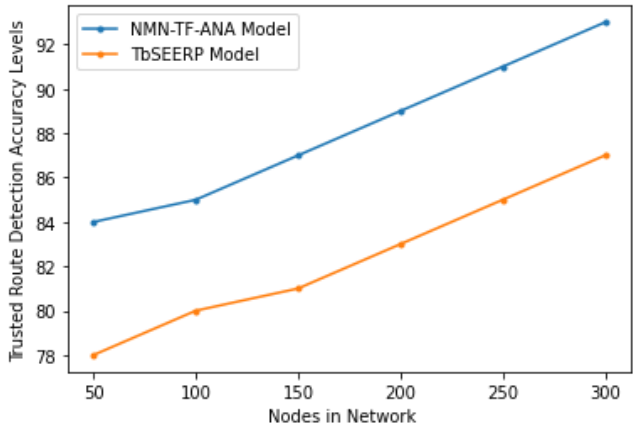

Figure 9. Trusted route detection accuracy levels

5. CONCLUSION

To meet performance goals that were too ambitious for 5G networks to achieve, new standards will be set by 6G mobile network technology. The need for a highly intelligent network, with extremely low latency, extremely fast network connection speeds, and the ability to handle a large number of different linked applications are major factors in this. Over time, 5G's ability to bring together different types of business advancements with communication platforms will bring to light the areas where 5G's performance falls short of expectations. More and more, WSNs are being used in mission-critical environments. Because of their meager resources, they are susceptible to several security risks. To get around this problem, WSNs will use a trust-based dynamic security and routing motif in 6G environment. The next forwarder node can be selected by the routing mechanism based on these reliable criteria. The opportunistic routing mechanism in WSN is well-suited to trust-based techniques because of this feature. A major improvement to WSN network design is going to be required to meet the demands of future applications. 6G networks outperform 5G networks in terms of capacity, latency, and data transfer rate. This model uses 6G networks environment, covering all the bases: the new architectural modifications that make up 6G networks and the most important characteristics of these networks for best route selection.The suggested protocol is an attempt to guarantee the security of data transport from source node to destination node by utilizing trust-based techniques with opportunistic routing. The proposed protocol calculates a trust metric and assigns it to each node in the forwarder list that the routing protocol chooses. Calculating a node's trust factor is necessary for trust-based techniques to be applicable in opportunistic routing. The

significance of the offered protocol is proven in the face of enormous network traffic, and it is not dependent on the placement of any particular node. Trust contributes to the prevention of black holes and the reinforcement of information network safety by actively producing a broad variety of discovering routes to quickly detect and gain node trust. It is the most significant invention of its type. The algorithm checks each network node to see if it is legitimate or malicious before allowing it to participate in routing. This research proposes a Network Master Node assessed Trust Factor with Arbitrary Neighbor Assessment for Secure Route Detection in WSN. The proposed model achieves 98.2% trusted route detection accuracy for secure data transmission. In future, optimization models can be applied to the routing model for still enhancing the accuracy levels and parameters for trust calculation also can be extended for better performance levels.

REFERENCES

[1] 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. https://doi.org/10.1109/ACCESS.2021.3075959

[2] 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. https://doi.org/10.1109/ACCESS.2022.3144015

[3] Zhao, Y., Srivastava, G. (2021). A wireless mesh opportunistic network routing algorithm based on trust relationships. IEEE Access, 10: 4786-4793. https://doi.org/10.1109/ACCESS.2021.3138370

[4] Abd El-Moghith, I.A., Darwish, S.M. (2021). Towards designing a trusted routing scheme in wireless sensor networks: A new deep blockchain approach. IEEE Access, 9: 103822-103834. https://doi.org/10.1109/ACCESS.2021.3098933

[5] Muzammal, S.M., Murugesan, R.K., Jhanjhi, N.Z. (2020). A comprehensive review on secure routing in internet of things: Mitigation methods and trust-based approaches. IEEE Internet of Things Journal, 8(6): 4186-4210. https://doi.org/10.1109/JIOT.2020.3031162

[6] Desai, S.S., Nene, M.J. (2021). Multihop trust evaluation using memory integrity in wireless sensor networks. IEEE Transactions on Information Forensics and Security, 16: 4092-4100. https://doi.org/10.1109/TIFS.2021.3101051

[7] Bin-Yahya, M., Alhussein, O., Shen, X. (2021). Securing software-defined WSNs communication via trust management. IEEE Internet of Things Journal, 9(22): 22230-22245. https://doi.org/10.1109/JIOT.2021.3102578

[8] Yang, L., Lu, Y., Yang, S. X., Zhong, Y., Guo, T., Liang, Z. (2021). An evolutionary game-based secure clustering protocol with fuzzy trust evaluation and outlier detection for wireless sensor networks. IEEE Sensors Journal, 21(12): 13935-13947. https://doi.org/10.1109/JSEN.2021.3070689

[9] Kim, J.D., Ko, M., Chung, J.M. (2022). Physical identification based trust path routing against sybil attacks on RPL in IoT networks. IEEE Wireless Communications Letters, 11(5): 1102-1106. https://doi.org/10.1109/LWC.2022.3157831

[10] Rathee, M., Kumar, S., Gandomi, A.H., Dilip, K., Balusamy, B., Patan, R. (2019). Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks. IEEE Transactions on Engineering Management, 68(1): 170-182. https://doi.org/10.1109/TEM.2019.2953889

[11] Javaid, N. (2022). A secure and efficient trust model for wireless sensor IoTs using blockchain. IEEE Access, 10: 4568-4579. https://doi.org/10.1109/ACCESS.2022.3140401

[12] Kavitha, A., Reddy, V.B., Singh, N., Gunjan, V.K., Lakshmanna, K., Khan, A.A., Wechtaisong, C. (2022). Security in IoT mesh networks based on trust similarity. IEEE Access, 10: 121712-121724. https://doi.org/10.1109/ACCESS.2022.3220678

[13] Gao, H., Liu, C., Yin, Y., Xu, Y., Li, Y. (2021). A hybrid approach to trust node assessment and management for vanets cooperative data communication: Historical interaction perspective. IEEE Transactions on Intelligent Transportation Systems, 23(9): 16504-16513. https://doi.org/10.1109/TITS.2021.3129458

[14] Kumbhar, F.H., Shin, S.Y. (2020). DT-VAR: Decision tree predicted compatibility-based vehicular ad-hoc reliable routing. IEEE Wireless Communications Letters, 10(1): 87-91. https://doi.org/10.1109/LWC.2020.3021430

[15] Lakshman Narayana, V., Lakshmi Patibandla, R.S.M., Pavani, V., Radhika, P. (2023). Optimized nature-inspired computing algorithms for lung disorder detection. In: Raza, K. (eds) Nature-Inspired Intelligent Computing Techniques in Bioinformatics. Studies in Computational Intelligence, vol 1066. Springer, Singapore. https://doi.org/10.1007/978-981-19-6379-7_6

[16] Fang, W., Zhang, W., Yang, W., Li, Z., Gao, W., Yang, Y. (2021). Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks. Digital Communications and Networks, 7(4): 470-478. https://doi.org/10.1016/j.dcan.2021.03.005

[17] Thangaramya, K., Kulothungan, K., Indira Gandhi, S., Selvi, M., Santhosh Kumar, S.V.N., Arputharaj, K. (2020). Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN. Soft Computing, 24: 16483-16497. https://doi.org/10.1007/s00500-020-04955-z

[18] Narayana, V.L., Sujatha, V., Sri, K.S., Pavani, V., Prasanna, T.V.N., Ranganarayana, K. (2023). Computer tomography image based interconnected antecedence clustering model using deep convolution neural network for prediction of COVID-19. Traitement du Signal, 40(4): 1689-1696. https://doi.org/10.18280/ts.400437

[19] Thahniyath, G., Jayaprasad, M. (2022). Secure and load balanced routing model for wireless sensor networks. Journal of King Saud University-Computer and Information Sciences, 34(7): 4209-4218. https://doi.org/10.1016/j.jksuci.2020.10.012

[20] Hamouid, K., Othmen, S., Barkat, A. (2020). LSTR: Lightweight and secure tree-based routing for wireless sensor networks. Wireless Personal Communications, 112: 1479-1501. https://doi.org/10.1007/s11277-020-07111-w

[21] Mathapati, M., Kumaran, T.S., Muruganandham, A. (2020). Secure routing scheme with multi-dimensional trust evaluation for wireless sensor network. Journal of

Ambient Intelligence and Humanized Computing, 12(6): 6047-6055. https://doi.org/10.1007/s12652-020-02169-7
[22] Fang, W., Zhang, W., Chen, W., Liu, Y., Tang, C. (2020). TMSRS: Trust management-based secure routing scheme in industrial wireless sensor network with fog computing. Wireless Networks, 26: 3169-3182. https://doi.org/10.1007/s11276-019-02129-w
[23] Narayana, V.L., Bharathi, C.R. (2023). Efficient route discovery method in MANETs and packet loss reduction mechanisms. International Journal of Advanced Intelligence Paradigms, 25(1-2): 129-140. https://doi.org/10.1504/IJAIP.2023.130818
[24] Fang, W., Zhu, C., Chen, W., Zhang, W., Rodrigues, J.J. (2018). BDTMS: Binomial distribution-based trust management scheme for healthcare-oriented Wireless Sensor Network. In 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, pp. 382-387. https://doi.org/10.1109/IWCMC.2018.8450403
[25] Tang, L., Lu, Z., Fan, B. (2020). Energy efficient and reliable routing algorithm for wireless sensors networks. Applied Sciences, 10(5): 1885. https://doi.org/10.3390/app10051885
[26] Raoof, A., Matrawy, A., Lung, C.H. (2018). Routing attacks and mitigation methods for RPL-based Internet of Things. IEEE Communications Surveys & Tutorials, 21(2): 1582-1606. https://doi.org/10.1109/COMST.2018.2885894
[27] Ghaleb, B., Al-Dubai, A.Y., Ekonomou, E., Alsarhan, A., Nasser, Y., Mackenzie, L.M., Boukerche, A. (2018). A survey of limitations and enhancements of the ipv6 routing protocol for low-power and lossy networks: A focus on core operations. IEEE Communications Surveys & Tutorials, 21(2): 1607-1635. https://doi.org/10.1109/COMST.2018.2874356
[28] Adewuyi, A.A., Cheng, H., Shi, Q., Cao, J., MacDermott, Á., Wang, X. (2019). CTRUST: A dynamic trust model for collaborative applications in the Internet of Things. IEEE Internet of Things Journal, 6(3): 5432-5445. https://doi.org/10.1109/JIOT.2019.2902022