International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Revue d'Intelligence Artificielle
Vol. 37, No. 4, August, 2023, pp. 871-879

Journal homepage: http://iieta.org/journals/ria

Secure Route Detection with Multi Level Trust Evaluation Model Using Replicated Auditor Node for Extended Packet Delivery Rate in WSN

Kosaraju Chaitanya[1,2*], Gnanasekaran Dhanabalan[1]

[1] Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai 600062, Tamil Nadu, India
[2] Department of Computer Science and Engineering, Vignan's Nirula Institute of Technology and Science for Women, Pedapalakaluru, Guntur 522005, Andhra Pradesh, India

Corresponding Author Email: kchaitanyaveltech@gmail.com

https://doi.org/10.18280/ria.370406

Received: 13 April 2023
Revised: 16 May 2023
Accepted: 22 May 2023
Available online: 31 August 2023

Keywords:
wireless sensor networks, routing, attacks, trust factor, security attacks, packet loss, Replicated Auditor Node

ABSTRACT

Wireless sensor networks (WSNs) are designed to monitor their surroundings, an application that has been leveraged significantly by advances in the Internet of Things (IoT). However, the susceptibility of wireless systems to errors and malicious attacks remains a challenge. Identity deception, particularly, has emerged as a significant issue, exacerbated by the redundancy of multi-hop routing, leading to potentially damaging attacks on routing protocols. Routing, the method employed in WSNs to disseminate data to base stations, has recently seen the incorporation of trust mechanisms to enhance security and foster cooperation among nodes. Routing decisions are made based on the anticipated trustworthiness of individual nodes. Considering the vulnerability of WSNs to various attacks, secure routing is of paramount importance. In this research, we propose a Multi-Level Trust Evaluation Model using Replicated Auditor Node (MLTEM-RAN) for secure route detection. This model aims at maximizing the packet delivery rate. It takes into account information about each relay node along the path, including the trust value and the current condition of each node. The trust value of a node is defined as the attack probability of the node, which is based on historical behaviors. The node's status, on the other hand, is a composite measure that considers both the node's remaining energy and its distance to the sink node. When compared with existing models, the proposed MLTEM-RAN model demonstrates superior performance in terms of packet delivery rate. This study thus represents a significant step forward in the development of secure and efficient routing strategies for WSNs.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have risen to prominence due to their versatile applications. However, despite their ubiquity, certain applications of WSNs necessitate real-time data delivery with minimal downtime, while others prioritize throughput over latency. Ultimately, the preferred parameters are contingent on application-specific requirements. It is therefore pivotal to have an in-depth comprehension of network architecture and routing protocols that are tailored to the specific needs at hand. Routing, a technique employed for determining the optimal path for data transmission from source to destination, is fraught with challenges given its dependence on network and channel parameters as well as performance measures. In WSNs, data is collected by sensor nodes, and then relayed to the base station. Subsequently, the base station transmits the data to other networks for further processing. This complexity necessitates a robust and flexible approach to routing in WSNs. Given the diversity of potential application requirements, an understanding of the interaction between network architecture, routing protocols, and application needs is essential for the optimal performance of WSNs. This paper aims to contribute to this understanding by proposing a novel routing approach, tailored to the specific needs of the application, and evaluated under realistic network conditions.

1.1 Wireless sensor networks

To keep tabs on things like temperature, air pressure, and humidity levels in the environment, scientists have developed WSNs [1]. The sensors are inexpensive gadgets that carry out a narrow range of sensing tasks. Due to their inexpensive cost, these sensors are often installed in large numbers to keep an eye on a particular occurrence [2]. A sensor node includes components such as a transceiver, microcontroller, external memory, and sensors. The two most common uses are tracking and monitoring [3]. WSNs find widespread use in military settings, in addition to health monitoring and fire detection. Security becomes an important concern because most sensor networks are used in open and unmonitored spaces [4]. Due to the widespread nature of sensor networks, security becomes paramount. The four cornerstones of sensor network security are privacy, authenticity, integrity, and availability. Sensor networks face challenges in areas such as energy, memory, transmission range, fault tolerance, self-organization, and scalability [5].

1.2 Security issues in WSN

There are two primary types of attacks: active and passive. These assaults originate from malicious nodes in wireless networks [6]. Attacks include monitoring and eavesdropping, selective forwarding, hello flood, sybil attack, sinkhole, and wormholes. For safety reasons, a dependable model should properly conserve battery life. The design must be resilient against a wide variety of threats, including eavesdropping, manufacturing, injection, modification, and node capture [7]. Most research into WSN security focuses on key management, secure placement, secure routing, attacks, and prevention. Secure routing is one method of protection against such attacks [8].

Cryptography and authentication, two mainstays of traditional security, can help prevent some forms of assaults [9], but they aren't enough to fend off attacks that target compromised nodes [10]. Once a node has been compromised, it is vulnerable to being ordered to launch attacks against other nodes or the entire WSN [11]. A malicious node might drastically damage the speed of the routing protocol, for instance, luring data from other nodes to itself using various methods, and then dropping all or randomly selected data once it has begun receiving the data [12]. Observing and identifying these nodes is the first step in dealing with them. Given that there is no governing body for WSNs, it is up to the individual nodes to keep an eye out for and report on any suspicious activity [13]. The WSN routing process is shown in Figure 1.

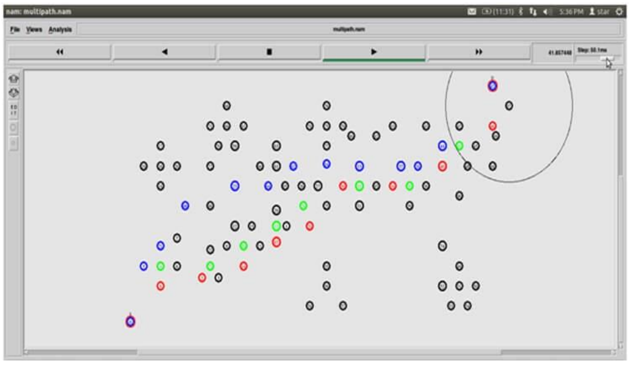

Figure 1. WSN routing process

1.3 Routing in WSN

When it comes to safeguarding WSNs, routing is your best bet. Since the routing protocol is responsible for transporting data to the network's base station, its reliability is crucial in WSNs. This highlights the need of having secure routing that can withstand assaults such as packet dropping or protocol manipulation [14]. In the presence of compromised nodes, multiple secure routing strategies are proposed [15]. Among these methods is building trust, which has been used extensively in research. When figuring out who to trust, it's important to look at how each node has behaved in the past. When doing its routing, it picks only trustworthy nodes and ignores the rest. As trust mechanisms are simple to construct and efficient at detecting compromised nodes [16], they have been the subject of numerous studies aimed at improving network security and cooperation.

Using secure routing in WSN helps locate unattacked nodes. To make matters more complicated, viruses, malwares, etc. can lead nodes to not only behave as if they are reliable and immune from any forms of attacks [17], but also to give the impression that they are actively involved in avoiding all types of threats [18]. There is a chance that standard security processes won't be adequate to deal with the threats we face, thus we need innovative approaches [19]. A promising secured routing solution [20] for WSNs is the employment of software agents to construct safe routes by utilising trustworthy neighbour nodes. Whether or whether a neighbour node may be trusted depends on a number of criteria [21]. Two of the most important are the nodes' wireless connection and the nodes' computing activity.

The misbehaving node may have accurate environmental sensing, but it may move the parameters in the data field before sending it on to its neighbor [22]. Due to inaccurate readings of temperature, pressure, and humidity, the network will incur costs in the form of wasted energy while processing and transmitting the data to the neighbor [23]. If a neighbour node is safe from both categories of threats, we can consider it trustworthy [24]. Traditional security mechanisms are insufficient for the task of safeguarding a wireless channel and the compute activity of a node because they lack intelligent techniques [25]. An intelligent deployment of security mechanism is required to detect such security breaches and make independent decisions [26]. To protect WSNs against the main forms of security breaches [27], auditor node technology to use for monitoring the nodes in the network for secure data transmission. This research proposes a trust factor evaluation at multiple levels by selecting a replicated based auditor node in the network for monitoring all the nodes behavior for improving packet delivery rate [28].

The main challenge in WSN is to detect a secure route that transmists the data efficiently with minimum loss. This paper mainly concentrates on identification of a trusted and secure route in the network [29]. A node called auditor node is selected among the trusted nodes and this node will monitor the behaviour of remaining trusted nodes in the network. This monitoring helps in identification of nodes having malicious properties. Based on the auditor node monitoring information and the trust factor, nodes will be considered in routing table.The introduction section discuss about the background of WSN, issues in WSN and routing process in WSN. The section 2 provides a brief literature review on the routing models and trust evaluation models. Section 3 provides the proposed model and the algorithm for secure route detection. The section 4 depicts the results when proposed model is contrasted with the traditional model. Section 5 provides the conclusion.

2. LITERATURE SURVEY

As opposed to other types of wireless networks, such as mobile ad hoc networks or cellular networks, WSNs present unique challenges when it comes to routing. First, the high cost of maintaining unique identifiers makes it impossible to devise a global addressing system for the installation of an enormous amount of sensor nodes. Many different clustered routing techniques have been created for WSNs in recent years. This work aims to do just that by reviewing and discussing in depth the most important clustering routing methods created for WSNs. The goals of this research is to make a large audience understand the existence and generally good performance of a number of grouping routing techniques in WSNs; to facilitate reading as well as provide an appropriate structure by providing an in-depth taxonomy of routing algorithms; to highlight certain advantages and drawbacks of the algorithms that are suggested with respect to the performance of the various clustering routing techniques in WSN and to assist application designers in identifying alternative so-called best practises for trust route detection.

Security in WSNs is increasingly dependent on research into trust evaluation, which in turn depends on external characteristics and network topology. Trust in WSNs is now evaluated at the node level, but this only ensures the reliability of the next closest node. In this research, Desai and Nene [2] presented a trust evaluation scheme that uses the in-built memory of a node to assess the route's reliability across multiple hops. A multihop trust evaluation mechanism based on the TEAM and TEAP algorithms is proposed in this study. In this paper, the author offered a trust evaluation model for multihop algorithms that combines normative and empirical approaches. With the proposed strategy, both the final destination and intermediate stops along the path may be relied upon.

Two significant issues, security and energy consumption, plague WSNs because of their characteristics of limited resources and dynamic topology. While trust-based solutions are practical today, there are still many threats to consider, such as assaults, excessive energy use, and communication bottlenecks between nodes. As a result, a new trust based secure and energy efficient routing protocol (TBSEER) is proposed in this study by Hu et al. [3]. To counteract black hole, selective forwarding, sinkhole, and hello flood assaults, TBSEER computes a global trust value using an adaptive direct trust value, indirect trust value, and energy trust value. In addition, the volatilization factor and adaptive punishment mechanism are utilized to quickly identify the malicious nodes. In addition, the energy consumption caused by repetitive calculations is reduced because the nodes only need to calculate the direct trust value and the Sink obtains the indirect trust value. Finally, the cluster leaders choose the most secure multi-hop routes using the global trust value, allowing for proactive wormhole attack avoidance.

Robotics, medical equipment, and SDM are just a few examples of the many industrial applications that benefit from the IIoT. While the IIoT holds great promise, there are still a number of obstacles to overcome before it can be fully implemented. These include problems with connectivity, security, privacy, variability, management, and energy efficiency. Some energy-limited nodes have existed in IIoT networks because of the widespread deployment and heterogeneity of the nodes, resulting in a shorter network lifetime. While privacy and security are considered to be key concerns in the design of IIoT, they are seen to be solvable with the implementation of secure routing protocols. A trust-aware multiobjective metaheuristic optimization-based secure clustering with route planning (TAMOMO-SCRP) method is developed in this research by Nagappan et al. [4] for a cluster-based IIoT setting. The bald eagle search (BES) algorithm for clustering and routing processes is the primary emphasis of the given TAMOMO-SCRP method. Maximum energy efficiency and safety are the ends to which the fitness function presented by the TAMOMO-SCRP model is directed. The TAMOMO-SCRP model devises an objective function for efficient clustering by considering four variables: trust level (TL), communication cost (CC), residual energy (RE), and node degree (ND). In addition, the fitness function is used in the route selection process, and it takes into account queue length and link quality.

For the smart city industrial environment, the authenticity and integrity of sensed data at the data collection stage is of the utmost importance. They compromise the reliability of data analysis and the fairness of decision-making. However, for terminals with limited resources, it can be difficult to distinguish attack behaviours from ambient noise and to set up a safe path for data transmission. In this paper, Fang et al. [5] suggested a trust-based security system (TSS) as a solution to these issues. To start, the author at TSS created a trust model that employs a binomial distribution to objectively determine a node's trustworthiness and a third-party recommendation mechanism to increase the reliability of that value. To counter the on-off attack, the author provided a system of trust management. Then, the author stroked a balance between security, transmission speed, and power consumption by designing a secure routing protocol.

Since mobile ad hoc networks (MANETs) do not require preexisting infrastructure to function, they can be rapidly deployed for a variety of uses, including but not limited to: emergency situations, military operations, communications in areas without a radio infrastructure, and special outdoor events. Because of its dynamic, ever-evolving topology and the relative ease with which it may be altered by malicious actors, manet's porous security may be its most serious flaw. Security flaws in MANET have an outsized impact on service quality (QoS). Therefore, the best method to ensure security for MANET is intrusion tracking, which adjusts your system to recognise other violation weaknesses. Detecting intrusions is a vital aspect of providing protections and acting as an additional layer of security against access. A loss of power at a cellular node could affect more than just the node itself; it could also affect its ability to forward packets, which is dependent on the system's overall lifetime. This resulted in the MANETs' routing protocol being institutionalised to its stable optimal choice of this multi-path to boost navigation. Since the topology of such a network is constantly shifting and its resources are limited, providing energy-efficient and secure routing is difficult. Veeraiah et al. [6] proposed a hybrid algorithm, cat slap single-player algorithm (C-SSA), that chooses the optimal leaps in advancing the routing as a means of addressing both energy efficiency and security in MANETs. The cluster heads (CHs) are initially selected using the maximum value of indirect, direct, and recent trust after fuzzy clustering has been applied. Nodes were also found based on their trust threshold value.

The ability to transport both data and power wirelessly at the same time, known as simultaneous wireless information and power transfer (SWIPT), is quickly becoming recognized as a key strategy for extending the operational lifetime of battery-powered wireless sensor nodes. However, existing SWIPT research only evaluated the RF signal from the previous hop's node as a potential source of energy harvesting in multi-hop IoT networks. If the RF signal is weak, the collected energy won't be enough to maintain constant communication. Pavani et al. [7] proposed a novel energy harvesting mechanism that takes into account a number of different sources (MS), including the broadcast energy from a sink, co-channel interference, the RF signal from neighbouring nodes, and the RF signal from the node that immediately preceded it in the hop chain. A novel SWIPT architecture, hybrid SWIPT (H-SWIPT), is proposed to achieve this goal by fusing the time switching (TS) and power splitting (PS) approaches. In addition, a process for selecting routes that makes the best use of energy is implemented to cut down on the overall energy spent. The author performed simulated tests to verify the suggested process and find that H-SWIPT consistently yields more average harvested energy than competing approaches.

Advantages of centralized routing include an improved ability to plan the most efficient route for real-time traffic and a more comprehensive picture of the network as a whole. Researchers' worries about centralized routing have grown in tandem with the popularity of SDN. In this paper, Chai and Zeng [8] suggested a centralized load balancing routing (LBR) scheme for wireless mesh networks that makes use of energy harvesting. When it comes to real-time traffic, LBR can give adaptable and best routes. LBR takes into account queue length, channel condition, energy cost, and energy harvesting to minimize the long-term weighted sum cost including load and energy condition. Using a dynamic programming method, the author took decisions in real time that take into account the state of traffic. Advantages of LBR are shown through simulation.

A new age of underwater surveillance and actuation applications is possible because to underwater wireless sensor networks (UWSN). Due to channel damage, data aggregation and forwarding in this network are severely hindered. An improvement to the routing protocol utilizing the Opportunistic Routing (OR) method is one approach to the data collecting of UWSN. Rahman et al. [9] suggested a new opportunistic routing protocol, NA-TORA, which is based on normalized advancements. To choose the forwarder for the following hop, NA-TORA uses Normalized Advancement rather than predetermined routes (NA). To determine the best forwarding node, the Expected Transmission Count (ETX) and the energy used by the node are factored in. However, if there is a void node in the data forwarding path, the data may not arrive at the intended sink node. To fix this problem, the author added a method to NA-TORA to detect and avoid void nodes and named it NA-TORA with VA. The suggested approach makes use of the angle of transmission adjustment and transmission range extension method to detect void nodes recursively and prevent them from taking part in the data routing process. The new aspect of this work is the way in which a forwarder is chosen, using normalized progress. In addition, the proposed routing protocol can function in either the usual mode of operation (called NA-TORA) or in a special mode designed to avoid empty hops.

Adil et al. [10] proposed a dynamic cluster-based static routing protocol (DCBSRP) that makes use of the ad hoc on-demand distance vector (AODV) routing protocol and the low-energy adaptive clustering hierarchy (LEACH) protocol to create a hybrid routing scheme that makes efficient use of the scarce resources of sensor nodes. The proposed approach employs static routing in the specified clusters using the AODV routing protocol, with the cluster head (CH) nodes being generated dynamically for a predetermined time period. For a set period of time (T), the proposed scheme's static routing condition mandates that all cluster nodes route their data through a single CH node. After a certain amount of time (T), all regular nodes associated with the designated CH are unlocked and can begin campaigning for the CH position throughout the network. Similarly, the CH node closest to the deployed sensor nodes is the one that receives the most route replies (RREPs). The DCBSRP protocol differs in that the newly chosen CH node does not act as a candidate for five cycles and instead behaves like any other node.

The rapid development of wireless communication has allowed for the improvement of wireless MANETs to cover a wide range of domains, including civilian settings, emergency operations, and military concerns. There are a few problems that can arise with source routing in MANETs, such as topology changes that cause links to frequently break and hence increase the need for route discovery. Khudayer et al. [11] improved on-demand source routing protocols by suggesting two mechanisms: a zone-based route discovery mechanism (ZRDM) and a link failure prediction method (LFPM). In contrast to LFPM's goal of preventing route breakages due to node mobility, ZRDM's focus is on regulating the influx of route requests. Network simulation 3 was used to assess the efficiency of the suggested mechanisms in terms of normalized routing load, average end-to-end delay, and packet delivery ratio. Compared to established mechanisms like the dynamic source routing (DSR) protocol, reliable DSR, zone-based DSR, and segment-based DSR, the new methods performed better in experiments.

Both event-driven traffic from sensor nodes to the BS in the form of single-path uni-cast packets and query-driven traffic from the BS to sensors, which better matches multi-casting and generates multi-path traffic, occur in WSNs. Kamarei et al. [12] proposed SiMple, a unified technique for simultaneously routing single and multi-path packets in WSNs. Using a square destination area, SiMple regulates the path multiplicity and the number of nodes in between the starting and ending points. When using single-path routing, SiMple takes into account the line between the source and destination nodes to determine which sensor node is nearest to it and hence best suited to be the packet's next carrier. In this case, SiMple uses a variable number of discontinuous routes, determined by the source node, to send packets in the direction of their final destinations. Asset monitoring applications necessitate the introduction of virtual source nodes, which SiMple provides. Extensive simulation experiments using NS-2 for single- and multi-path packets show that SiMple achieves better performance and uses less energy than the alternative of employing two distinct algorithms to route event and query packets separately.

3. PROPOSED MODEL

Finding a safe and reliable route through the network is the primary focus of this research. From among the trusted nodes, one is chosen to take on the role of auditor node, whose job it is to keep tabs on the actions of the other trusted nodes. With this kind of surveillance, malicious nodes can be isolated and eliminated from the network. Nodes will be evaluated in the routing table based on the trust factor and data gathered from the auditor nodes' monitoring. In order to ensure the fastest possible packet delivery rate, this study offers a Multi-Level Trust Evaluation Model based on a Replicated Auditor Node.

In recent years, WSNs have emerged as a potentially game-changing technology with a wide range of potential uses, including but not limited to monitoring the battlefield, responding to emergencies, monitoring the environment, and keeping tabs on patients' health. Nonetheless, WSNs are susceptible to a wide variety of threats since they are typically placed in a hostile or harsh environment. Capturing sensor nodes in WSNs is simple for attackers, who can then use them to conduct attacks like selective forwarding, wormholes, sinkholes, hello flooding, and Sybil. If the routing protocol is vulnerable, malicious nodes will drop some or all packets, preventing critical information from reaching the sink node. Due to their focus on data transfer, the standard routing algorithms cannot be used in WSNs if malicious nodes are present. In addition, the routing in WSNs is limited by the resources available at the sensor nodes, such as power and processing speed.

The current WSN routing techniques do not provide a sufficient equilibrium between security and energy consumption. Security in these protocols is typically provided by means of encryption and trust mechanisms. While encryption can help WSNs fend off some forms of network attack, the routing protocols that are incorporated with encryption are still susceptible to other forms of network infiltration, leading to increased power consumption. The robustness of these protocols can be increased by utilizing more routing paths; however, building and maintaining these additional routes requires more resources from sensor nodes, such as processing power and memory. Although trust-based routing protocols are resilient to many different kinds of assaults, they incur significant memory and power overhead whenever a trust value is calculated. Current routing methods are usually energy-efficient, therefore they construct a full route between two nodes by gradually adding on to the existing path. The produced paths, however, are not always ideal on a global scale and could fail under malicious attack. As a result, it is challenging for current routing protocols to locate a safe path that respects both security requirements and the limitations imposed by WSNs' limited processing power and battery life.

This research proposes a novel secure routing protocol for WSNs, which can be used even when malicious nodes are present using a multi level trust evaluation model. The trustworthiness and operational status of each relay node along the path are considered by the protocol as it determines the safest route. Each sensor node's trustworthiness is represented as an attack probability, with that value determined based on the node's past communication patterns and the trustworthiness of its immediate neighbors. In order to foresee the sensor node's future actions, it is necessary to know its trustworthiness. Additionally, the sensor nodes' related information can be used to set up a safe path for transmitting data between a pair of sensor nodes, which can successfully minimize interference from malicious nodes. The indirect trust value is used from other nodes in multiple stages to supplement the precision of the direct trust value, since certain sensor nodes may only have partial information.

To increase the reliability of data transmission while hiding the nature of attacks, the proposed safe routing protocol selects a single sensor node at a time. As a result, the following relay node is typically a sensor node that is both closer to the sink node and has a higher residual energy level. Routing, aggregation of data, access control, and intrusion prevention are just some of the newer uses for trust management. Monitoring nearby nodes during transmissions, identifying instances of misbehavior, estimating trust values in light of detection results/recommendations, and spreading trust values and recommendations are all aspects of TM as they pertain to routing. The proposed model framework is shown in Figure 2.

A multi level trust based routing protocol is one where a node takes into account the actions and verification status of a candidate router before making a routing choice. The Trusted Validation metric measures this point of view. From then, trust measures are used to plot a course between the origin and the destination. Trust-based routing is crucial for protecting gathered data, avoiding wasteful resource use, and maintaining network speed. Malicious nodes in a WSN might cause data loss by diverting traffic along erroneous paths or by simply failing to send packets to their intended destination. With a reliable routing system in place, all of the data will be protected during transmission and use, and users have better insight into potential threats. Unfortunately, there are significant flaws in the traditional routing approaches based on trust. While trust-based solutions address the risks associated with wireless networks, they also introduce new dangers that must be carefully considered. This research proposes a multi level trust evaluation Model using Replicated Auditor Node (MLTEM-RAN) for secure route detection that provides maximum packet delivery rate. At regular intervals, the auditor node checks in on the trusted nodes behavior to see if they're ready for the task before any potentially harmful data transmissions take place.

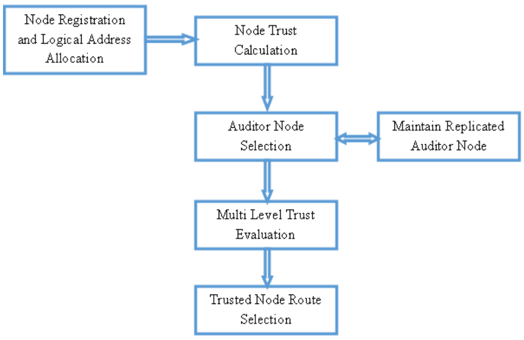
Node Registration and Logical Address Allocation
Node Trust Calculation
Auditor Node Selection
Maintain Replicated Auditor Node
Multi Level Trust Evaluation
Trusted Node Route Selection

Figure 2. Proposed model framework

Algorithm MLTEM-RAN
{
Input: Nodes List {Nset}
Output: Nodes Selected in Routing {Rset}

Step 1: The WSN considers the nodes to establish a network and the nodes in the network will be allocated with a logical address by considering the nodes base address of the nodes registered. The nodes logical address will be allocated that is used for node identity during network communication. The node logical allocation process is performed as:

$$\mathrm{Nodeaddr}[M] = \sum_{n=1}^{M} \frac{\mathrm{nodeaddr}(n)}{\mathrm{Th}} + \mathrm{TimeInst}[\mathrm{Nset}(n)] + \mathrm{getloc}(n) \quad (1)$$

$$\mathrm{NodeLogAddr}[M] = \sum_{n=1}^{M} \frac{\mathrm{Nodeaddr}(n) * \mathrm{rand}(M)}{\max\left(\mathrm{netSize}(M)\right)} + \mathrm{neighborNode}(n) + \mathrm{allocener}(n) \quad (2)$$

Th is the threshold value considered for allocation of logical address, rand() model is used for generating a random umber. netSize() is used to consider the network size.

Step 2: The nodes that are in the part of the WSN will be allocated with a logical address for identity. The malicious nodes also can involve in the network to perform malicious actions in the network. The trust factor is calculated for all the nodes in the WSN and this trust factor plays a key role in the route selection process. The trust factor of all nodes will be calculated as:

$$\begin{aligned}\mathrm{NodeTrans}(\mathrm{Node}[\mathrm{M}]) \\ &= \sum_{n=1} \mathrm{NodeLogAddr}(n) + \max\big(\mathrm{availener}(n)\big) \\ &+ \max\,(\mathrm{PDR}(n))\end{aligned} \qquad (3)$$

$$\begin{aligned}\mathrm{TrustF}(\mathrm{Node}[\mathrm{M}]) \\ &= \sum_{n=1} \max\big(\mathrm{NodeTrans}(n)\big) + \mathrm{NodeLogAddr}(n) \\ &+ \frac{\lambda * \max\,(\mathrm{netSize}(\mathrm{M}))}{\mathrm{len}(\mathrm{NodeLogAddr}(\mathrm{M}))}\end{aligned} \qquad (4)$$

Here λ is the model that considers the computational levels of the nodes in the network. Here len() is used to find the total number of nodes in the network.

Step 3: The auditor selection is performed in the network that has maximum trust factor among the nodes registered. The auditor selection is performed based on the nodes performance that is best. To avoid node or link failures and to avoid delay levels and as the auditor node has to monitor the network performance, the replicated node is also selected for auditor node. The process is performed as:

$$\begin{aligned}&\mathrm{AuditorNode}(\mathrm{M}) \\ &= \sum_{n=1}^{M} \mathrm{NodeLogAddr}(n) \left\{ \begin{array}{c} \displaystyle\sum_{n=1}^{M} \frac{\mathrm{getnode}(n)}{\lambda} + \frac{\max\,(\mathrm{PDR}(n))}{\mathrm{count}(\omega)} + \max\,(\mathrm{PDR}(n)) \\ \text{otherwise NULL} \end{array} \right.\end{aligned} \qquad (5)$$

$$\begin{aligned}\mathrm{Relica}(\mathrm{AuditorNode}[\mathrm{M}]) \\ &= \frac{\left[\min\Big(\mathrm{dist}\big(\mathrm{Node}(\mathrm{N}_{i+1} - \mathrm{N}_i)\big)\Big)\right]}{\max\,(\mathrm{availener}((\mathrm{Node}(n))} \\ &+ \max\big(\mathrm{PDR}(n)\big)\,\{\mathrm{mindist}\big(\mathrm{AuditorNode}(n)\big)\}\end{aligned} \qquad (6)$$

Here ω is the nodes that has high computational power than the remaining nodes.

Step 4: The multi-level trust factor is considered after the auditor node is selected to check the network performance. The multi-level trust factor assessment is performed to remove malicious actions in the network. The multi-level trust factor assessment is performed as:

$$\begin{aligned}\mathrm{FinalTrust}\big(\mathrm{Node}(\mathrm{M})\big) \\ &= \sum_{i=1}^{M} \mathrm{AuditorNode}(\mathrm{PDR}(i)) \\ &- \frac{\min\,(\mathrm{loss}(\mathrm{Node}(i)))}{\omega} \\ &+ \prod_{i=1}^{M} \max\big(\mathrm{PDR}(i)\big) \\ &+ \mathrm{maxavailener}(\mathrm{Node}(i))\end{aligned} \qquad (7)$$

Step 5: The route selection is performed by considering the auditor node evaluation on each node. The nodes whose performance is high is only considered in the routing table. The selected route contains most trusted route that observes maximum packet delivery rate. The route selection process is performed as:

$$\begin{aligned}\mathrm{Troute}\big(\mathrm{LC}(i)\big) &= \sum_{i=1} \max(\mathrm{FinalTrust}(\mathrm{Node}(i))) \\ &- \min\Big(\mathrm{FinalTrust}\big(\mathrm{Node}(i)\big)\Big) \\ &- \max\big(\mathrm{Node}(\omega)\big) \\ &+ \max\,(\mathrm{availenergy}(\mathrm{Node}(i)))\end{aligned} \qquad (8)$$

}

4. RESULTS

Extensive study has been devoted to wireless sensor networking in recent years, and it is now widely accepted as a viable, all-purpose method for a variety of cutting-edge uses, including real-time traffic monitoring, ecological monitoring, and battlefield surveillance. Since these networks handle confidential information, it is crucial that they be protected from threats such node capture, manipulation, eavesdropping, denial of service, and others. In this research, it is shown how wireless sensor networks can benefit from a safe routing technique. The protocol is resistant to attacks in which malevolent nodes drop just some of the packets travelling over a certain route.

Each node in a wireless network instead uses another node in the network as a conduit for its communications with other nodes in the network. Many different secure routing strategies have emerged throughout time to protect WSNs against malicious or self-interested activity. While these routing protocols are useful, their success is mostly dependent on authentication and underlying implementations. Cryptographic procedures, especially the asymmetrically encrypted one, tend to be quite processor and energy-intensive. When it comes to storage, battery life, and processing power, however, low-cost sensor nodes tend to fall short. In WSNs, it is not always feasible to use decentralised authentication and encryption procedures like those used in some routing protocols.

WSN is used in a wide variety of applications because it can gather data in real time from dispersed sensors. This is now possible thanks to the reduction in size, decrease in cost, and increase in sophistication of sensors during recent years. All of these sensors are equipped with wireless interfaces that permit them to exchange data with one another. Routing is crucial to the WSN because it determines the most efficient path for data to travel from one node to another. The study of Wireless Sensor Networks (WSNs) has arisen as a result of recent advances in wireless technology. A WSN is constructed using a large number of low-cost, low-footprint, battery-operated sensor nodes. These senor nodes can be used for a wide variety of purposes, including military applications, climate and ecological monitoring, acoustic collecting information, civic applications, and surveillance. The main limitations of WSN are its processing speed, safety, and power consumption. Due to the limitations of sensor nodes, it is necessary to develop communication protocols that are both energy-efficient and secure. Recently, more effort has been put into studying the complexity of routing in order to ensure the network's cost-effectiveness, security, and dependability.

This research proposes a multi level trust evaluation model using Replicated Auditor Node (MLTEM-RAN) for secure route detection that provides maximum packet delivery rate. The proposed model is compared with the traditional energy-aware and trust-based routing protocol for wireless sensor networks using adaptive genetic algorithm (TAGA). The comparison results are shown clearly that represents that the proposed model performance is high.

The node logical address is the only identifier for a given node across the whole network tree calculated from base address since it represents the node's precise location within the network. Addresses tend to grow in length the further down the network structure a node is placed. The Node Logical Address Allocation Accuracy Levels of the proposed and existing models are shown in Figure 3.

When using the Trusted Node Safety mechanism, network administrator can designate each neighboring node in the routing protocol as internal or external in reference to the particular node of that network map, enforcing stricter security criteria when dealing with certain nodes in the network. The trust evaluation of each node is performed and then based on the trust node a node can be allowed into communication. The Node Trust Evaluation Time Levels of the proposed and existing models are shown in Figure 4.

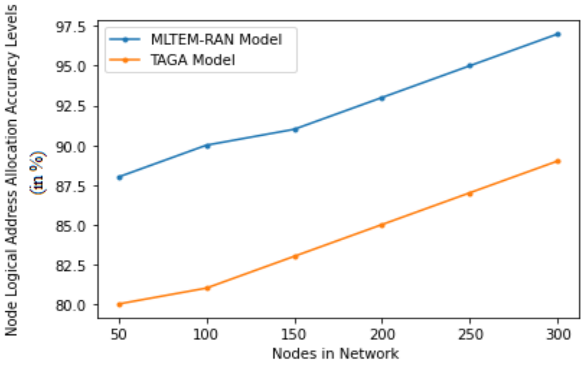

Figure 3. Node logical address allocation accuracy levels

The proposed model selects auditor node in the network based on the trust value. The auditor node monitors all the activities in the network. The auditor is selected based on its performance. The Auditor Node Detection Accuracy Levels of the proposed and existing models are depicted in Figure 5.

The nodes in the WSN, if encountered any issues, then the route link or node failure occurs that results in increased delay. The auditor node which is the important node in the network that monitors all the activities in the network to avoid malicious actions, if failed, then the entire network will be collapsed. To avoid that a Replicated Auditor Node is generated among the remaining trusted nodes. The Replicated Auditor Node Selection Time Levels of the existing and proposed model are represented in Figure 6.

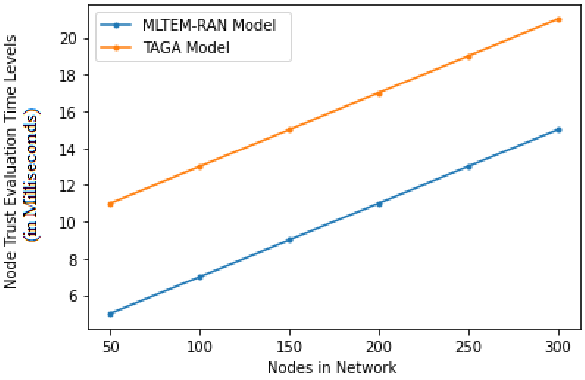

Figure 4. Node trust evaluation time levels

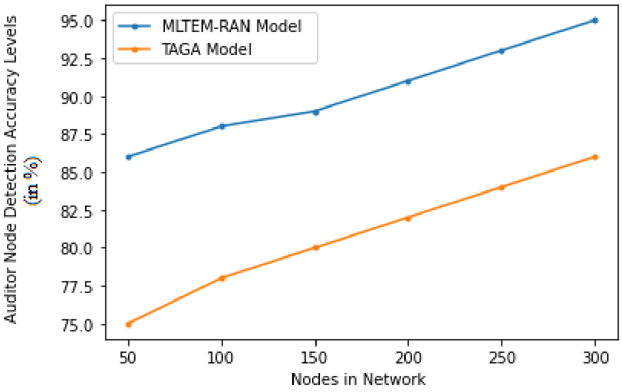

Figure 5. Auditor node detection accuracy levels

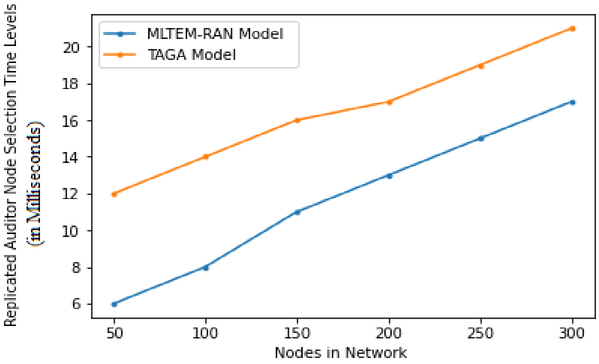

Figure 6. Replicated Auditor Node selection time levels

The proposed model performs multilevel trust evaluation of the nodes involved in data communication. The multi-level trust evaluation helps in avoiding malicious actions in the network with better performance levels. The multi-level trust evaluation accuracy levels of the proposed and existing models are shown in Figure 7.

The purpose of a WSN is to keep gathering information. A wireless sensor node's primary function is to sense and gather data from a certain region, process those data, and then transfer them to a sink where the corresponding application is housed. WSNs are networks of sensors located in different parts of the world that work together to gather and transmit data on environmental conditions. The Trusted Node Route Selection Time Levels of the proposed and traditional models are shown in Figure 8.

A wireless sensor network is a network of sensors that can exchange data wirelessly. Depending on the needs of the application, sensor nodes collect data about the surrounding environment and transfer it to the sink in a single hop or via a series of intermediate nodes. A network's packet delivery rate is defined as the proportion of successfully delivered packets relative to the total number of packets transmitted from a source node to a destination node. Maximum data packet delivery is desired that shows the network efficiency. The Packet Delivery Rate Levels of the proposed and existing models are shown in Figure 9.

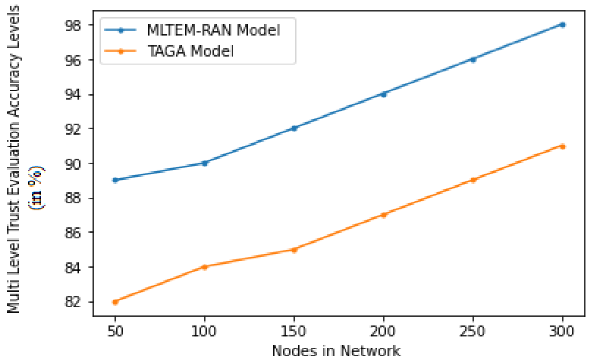

Figure 7. Multi level trust evaluation accuracy levels

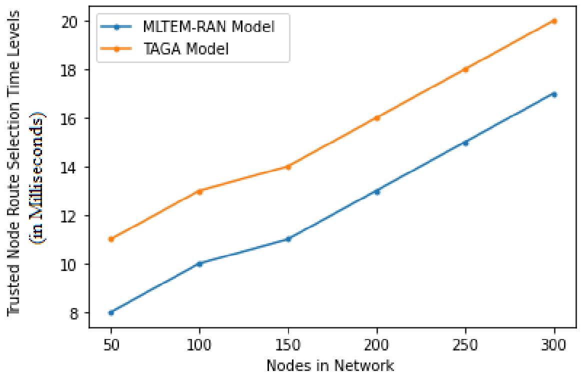

Figure 8. Trusted node route selection time levels

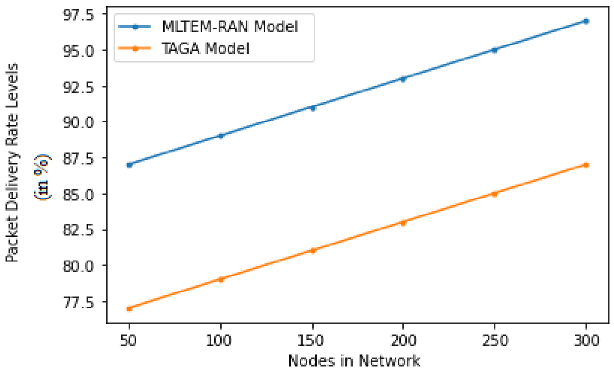

Figure 9. Packet delivery rate levels

5. CONCLUSION

Trust is undeniably crucial when choosing a path. Every node in the network is responsible for keeping track of its neighbouring nodes and rating them on a trust scale. Depending on the chosen routing protocol, there are many methods available for determining a safe routing path and evading a malicious node. A route can be selected at the starting point or at intermediate nodes along the path. When deciding which path to take, a node in a trust-based routing protocol takes into account the auditor node's recent activities and verification status. The security of collected data, the prevention of unnecessary resource consumption, and the preservation of network throughput all depend on trust-based routing. WSN is frequently used to transmit and distribute highly sensitive information in the military and the medical industries. Data loss in a WSN can be caused by malicious nodes taking traffic off-route or simply failing to deliver packets. Unfortunately, trust-based routing methods have serious limitations. While trust-based solutions do mitigate some of the threats associated with wireless networks, they also present their own unique set of challenges. This study presents a Multi-Level Trust Evaluation Model with Replicated Auditor Nodes for Maximum Packet Delivery Rate via Secure Route Detection to address these concerns. The auditor node performs regular audits of the trustworthy nodes' operations and detects any attacks on the network while data is being sent. To be considered safe, a routing system must be impervious to threats such packet erasure, tampering, and disruption. The proposed routing algorithm takes into account the trust measure's properties as well as those of other quality standards for path selection. The proposed model achieves 97% accuracy in packet delivery with the identified route and 98% accuracy in trust node selection that increases the system performance. In future, more parameters like range, life time, aggrgation levels, loss rate, latency rate can be considered along with trust of nodes in route selection and also packet loss can be further reduced with best transmission rate.

REFERENCES

[1] 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

[2] 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

[3] 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

[4] Nagappan, K., Rajendran, S., Alotaibi, Y. (2022). Trust aware multi-objective metaheuristic optimization based secure route planning technique for cluster based IIoT environment. IEEE Access, 10: 112686-112694. https://doi.org/10.1109/ACCESS.2022.3211971

[5] Fang, W., Cui, N., Chen, W., Zhang, W., Chen, Y. (2020). A trust-based security system for data collection in smart city. IEEE Transactions on Industrial Informatics, 17(6):

4131-4140. https://doi.org/10.1109/TII.2020.3006137

[6] Veeraiah, N., Khalaf, O.I., Prasad, C.V.P.R., Alotaibi, Y., Alsufyani, A., Alghamdi, S.A., Alsufyani, N. (2021). Trust aware secure energy efficient hybrid protocol for manet. IEEE Access, 9: 120996-121005. https://doi.org/10.1109/ACCESS.2021.3108807

[7] Pavani, B., Devi, L.N., Subbareddy, K.V. (2022). Energy enhancement and efficient route selection mechanism using H-SWIPT for multi-hop IoT networks. Intelligent and Converged Networks, 3(2): 173-189. https://doi.org/10.23919/ICN.2022.0013

[8] Chai, Y., Zeng, X.J. (2020). Load balancing routing for wireless mesh network with energy harvesting. IEEE Communications Letters, 24(4): 926-930. https://doi.org/10.1109/LCOMM.2020.2969194

[9] Rahman, Z., Hashim, F., Rasid, M.F.A., Othman, M., Alezabi, K.A. (2020). Normalized advancement based totally opportunistic routing algorithm with void detection and avoiding mechanism for underwater wireless sensor network. IEEE Access, 8: 67484-67500. https://doi.org/10.1109/ACCESS.2020.2984652

[10] Adil, M., Khan, R., Ali, J., Roh, B.H., Ta, Q.T.H., Almaiah, M.A. (2020). An energy proficient load balancing routing scheme for wireless sensor networks to maximize their lifespan in an operational environment. IEEE Access, 8: 163209-163224. https://doi.org/10.1109/ACCESS.2020.3020310

[11] Khudayer, B.H., Anbar, M., Hanshi, S.M., Wan, T.C. (2020). Efficient route discovery and link failure detection mechanisms for source routing protocol in mobile ad-hoc networks. IEEE Access, 8: 24019-24032. https://doi.org/10.1109/ACCESS.2020.2970279

[12] Kamarei, M., Patooghy, A., Alsharif, A., Hakami, V. (2020). SiMple: A unified single and multi-path routing algorithm for wireless sensor networks with source location privacy. IEEE Access, 8: 33818-33829. https://doi.org/10.1109/ACCESS.2020.2972354

[13] Abbasian Dehkordi, S., Farajzadeh, K., Rezazadeh, J., Farahbakhsh, R., Sandrasegaran, K., Abbasian Dehkordi, M. (2020). A survey on data aggregation techniques in IoT sensor networks. Wireless Networks, 26: 1243-1263. https://doi.org/10.1007/s11276-019-02142-z

[14] Fang, W., Zhang, W., Chen, W., Pan, T., Ni, Y., Yang, Y. (2020). Trust-based attack and defense in wireless sensor networks: A survey. Wireless Communications and Mobile Computing, 2020: 1-20. https://doi.org/10.1155/2020/2643546

[15] Singh, N.K., Gupta, P.K., Mahajan, V. (2020). Intrusion detection in wireless network of smart grid using intelligent trust-weight method. Smart Science, 8(3): 152-162. https://doi.org/10.1080/23080477.2020.1805679

[16] Ghugar, U., Pradhan, J. (2020). ML-IDS: MAC layer trust-based intrusion detection system for wireless sensor networks. In Computational Intelligence in Data Mining: Proceedings of the International Conference on ICCIDM. Springer Singapore, 2018: 427-434. https://doi.org/10.1007/978-981-13-8676-3_37

[17] Ourouss, K., Naja, N., Jamali, A. (2021). Defending against smart grayhole attack within manets: A reputation-based ant colony optimization approach for secure route discovery in DSR protocol. Wireless Personal Communications, 116: 207-226. https://doi.org/10.1007/s11277-020-07711-6

[18] Moon, J., Lee, S.H., Lee, H., Lee, I. (2019). Proactive eavesdropping with jamming and eavesdropping mode selection. IEEE Transactions on Wireless Communications, 18(7): 3726-3738. https://doi.org/10.1109/TWC.2019.2918452

[19] Wang, K., Yuan, L., Miyazaki, T., Chen, Y., Zhang, Y. (2018). Jamming and eavesdropping defense in green cyber-physical transportation systems using a Stackelberg game. IEEE Transactions on Industrial Informatics, 14(9): 4232-4242. https://doi.org/10.1109/TII.2018.2841033

[20] Sun, Q., Zhang, K., Shi, Y. (2019). Resilient model predictive control of cyber-physical systems under DoS attacks. IEEE Transactions on Industrial Informatics, 16(7): 4920-4927. https://doi.org/10.1109/TII.2019.2963294

[21] Sookhak, M., Tang, H., He, Y., Yu, F.R. (2018). Security and privacy of smart cities: A survey, research issues and challenges. IEEE Communications Surveys & Tutorials, 21(2): 1718-1743. https://doi.org/10.1109/COMST.2018.2867288

[22] Zhu, C., Rodrigues, J.J., Leung, V.C., Shu, L., Yang, L.T. (2018). Trust-based communication for the industrial internet of things. IEEE Communications Magazine, 56(2): 16-22. https://doi.org/10.1109/MCOM.2018.1700592

[23] Li, W., Song, H. (2015). ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems, 17(4): 960-969. https://doi.org/10.1109/TITS.2015.2494017

[24] Meena Kowshalya, A., Valarmathi, M.L. (2017). Trust management for reliable decision making among social objects in the social Internet of Things. IET Networks, 6(4): 75-80. https://doi.org/10.1049/iet-net.2017.0021

[25] Wu, X., Huang, J., Ling, J., Shu, L. (2019). BLTM: Beta and LQI based trust model for wireless sensor networks. IEEE Access, 7: 43679-43690. https://doi.org/10.1109/ACCESS.2019.2905550

[26] Aliady, W.A., Al-Ahmadi, S.A. (2019). Energy preserving secure measure against wormhole attack in wireless sensor networks. IEEE Access, 7: 84132-84141. https://doi.org/10.1109/ACCESS.2019.2924283

[27] Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Khannah Nehemiah, H., Kannan, A. (2019). An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. Wireless Personal Communications, 105: 1475-1490. https://doi.org/10.1007/s11277-019-06155-x

[28] Rajeshkumar, G., Valluvan, K.R. (2017). An energy aware trust based intrusion detection system with adaptive acknowledgement for wireless sensor network. Wireless Personal Communications, 94: 1993-2007. https://doi.org/10.1007/s11277-016-3349-y

[29] Sun, Z., Wei, M., Zhang, Z., Qu, G. (2019). Secure routing protocol based on multi-objective ant-colony-optimization for wireless sensor networks. Applied Soft Computing, 77: 366-375. https://doi.org/10.1016/j.asoc.2019.01.034