International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/217706 Volume 9, Issue 6, November – December (2022)

RESEARCH ARTICLE

A Competent Intelligence Modeling for Trust-Based Security Scheme in Mobile Ad Hoc Network

K. Vijay Anand
Department of Computer Science, SNMV College of Arts and Science, Coimbatore, Tamil Nadu, India.
vijayanandphd123@gmail.com

G. Abel Thangaraja
Department of Computer Technology, Sri Krishna Adithya College of Arts and Science, Coimbatore, Tamil Nadu, India.
abeltraja@gmail.com

Received: 25 September 2022 / Revised: 19 November 2022 / Accepted: 23 November 2022 / Published: 30 December 2022

Abstract – Mobile Ad Hoc Network (MANET) is one of the rising wireless configurations which have self-organizing wireless mobile nodes and adaptive network connectivity. Because of its dynamic nature and constantly changing topology, security is a critical issue for MANET. So, a trust-based secure energy-efficient routing protocol has been suggested in MANET which predicts the node's trust level based on the static threshold value to detect malicious nodes and choose the best paths for data transfer. But, this threshold might not be ideal regarding identification accuracy and Packet Loss Ratio (PLR). To solve this issue, a highly suitable trust level must be estimated according to the node parameters like mobility, Node Degree (ND), etc. Hence, this article proposes an adaptive Trust Threshold (TT)-aware secure energy-efficient protocol by considering the network parameters to adaptively choose the TT. The TT in this protocol is adjusted dynamically at each node based on the different network factors. Initially, these various network variables are determined for all nodes. After that, an Artificial Neural Network (ANN) classifier learns such parameters to identify the TT, which aids in predicting the node's trust level. Further, malicious and benign nodes are discovered properly based on their trust level. At last, the simulation results exhibit that the proposed protocol achieves 92.1% accuracy while deploying 300 nodes compared to the other protocols.

Index Terms – MANET, Security, Data Transfer, Trust-Aware Routing, Energy Efficiency, Adaptive Trust Threshold, ANN.

1. INTRODUCTION

Mobile Ad Hoc Network (MANET) is a modern communication technology wherein nodes connect using peer-to-peer data transmission and multi-hop pathways. It is possible to run it without the need for a static base station or mobile network access. As a result, MANET may be used for a broad variety of applications in scenarios, such as military surveillance, rescue activities, and so on [1]. Each node in a MANET must rely on the other node to transmit packets, necessitating the deployment of a precise cooperation strategy for data transfer from hop to hop until reaching an intended destination via routing protocols. MANET's major characteristics are interactivity, topology modifications, and cost constraints.

Because of the adaptability of MANET, nodes are more vulnerable to a wide range of attacks. The dependability of MANET is harmed as a result of node misbehavior. To overcome this problem, trustworthy routing protocols must be developed, which is a more complex and challenging procedure in MANET [2]. Both trustworthy and untrustworthy nodes can share data or resources. Because one node has no prior knowledge of the others, the inherent flexibility of self-organized MANET raises security concerns. As a result, only reliable nodes have access to resources, and trust among unknown nodes must be determined.

Ad Hoc On-demand Distance Vector (AODV) [3, 4] and Dynamic Source Routing (DSR) [5] are the 2 most frequent routing methods used in MANET transmission. These protocols are the foundation for the idea that every node is entirely trustworthy and will always act cooperatively. However, this makes the network more susceptible to routing failures caused by non-cooperative disruptive nodes. The use of Trust-based Routing Schemes (TRSs) looks to be a viable solution to this problem [6]. The possibility of varied aspects for confidence evaluation brings up a wide variety of research opportunities. This inspires the authors to contribute by developing and implementing the TRSs in the AODV framework [7].

One of the most fundamental aspects of MANET is trust, which helps clients to deal with uncertainty and unpredictability. Because of computation cost needs and individual node autonomy, trust assessment and control are highly complex considerations in MANET. In a MANET, an unstable node might represent a substantial hazard and reduce information efficiency [8, 9, 10].

As a result, examining a node's confidence level improves the security with which an operator interacts with that node. The confidence assessment is used to defend malicious nodes from the routing path during data transfer. To recognize and separate mischievous nodes, many trust-based security approaches that are deeply integrated with misconduct recognition approaches were developed. In these approaches, each node calculates and retains a trust value regarding another node [11, 12]. Those trust ranges have been evaluated with the static TT, which was the node’s maximum acceptable misconduct. A node was called trustworthy when it effectively transmits a specified proportion of incoming packets by the underlying network protocol standard.

From this perspective, a trust-based secure power-effective routing [13] was developed in MANETs by the Cat Slap Single-player Algorithm (C-SSA) to improve security and energy efficacy. Initially, the CHs were estimated by the fuzzy grouping scheme combined with the maximum trust values of each node. Then, malicious nodes were identified and neglected from the routing path between the origin node and target node based on the fixed threshold value. Moreover, the optimum routes were decided by the C-SSA that depends on the deliberate target attribute and different parameters: ability, throughput, and transmission of the route. On the other hand, because each node in a MANET encounters varied network parameters, including movement and ND, a fixed TT might not be optimum regarding identification accuracy and PLR.

Typically, these trust-based security systems assess a node's trustworthiness in the range between 0 and 1 with 0.5 being the most widely used threshold. But, limited communication regions and rapid movement result in limited contact durations among nodes. Because node activity in MANETs may vary fast, it is challenging to establish an adequate trust level for mischievous node identification, which performs well in every case. The fixed TT leads to a significant number of false positives and a poor rate of malicious node identification. When the TT is set very minimum, the false positives were large because mischievous nodes were discarded from the route earlier. When the TT is set very maximum, the false positives were less, yet some nodes were allowed to engage in the path because many nodes would be perceived as mischievous nodes. Further, a sophisticated malicious node can adjust its misbehaving strategy by the preset TT to circumvent identification. As a result, a highly appropriate trust level must rely on node parameters [14].

Therefore in this manuscript, an adaptive TT-aware secure energy-efficient protocol is proposed that considers the network parameters to adaptively choose the TT. In this protocol, the TT is adapted locally at each node based on various node parameters including ND, mobility, etc. First, these different network parameters are computed for each node that exists in the network. Then, such computed values of each parameter are learned by the ANN to find the TT which helps to predict the node’s trust level. According to the trust level of nodes, the malicious and normal nodes are detected appropriately.

The rest of the portions of this paper are prepared as follows: The recent work linked with the secure and reliable routing protocols for MANETs is presented in Section 2. Section 3 explains the presented protocol, whereas Section 4 demonstrates its efficacy. Section 5 summarizes this paper and suggests its possible improvement.

2. RELATED WORK

An Evolutionary Self-Cooperative Trust (ESCT) method [15] was designed, which relies on a trusted range for circumventing various routing disruption assaults. The trust data was exchanged by the mobile nodes and the received data was analyzed using their cognitive decision. Also, the malicious entities were removed by evolving the cognition of each node adaptively. But, its energy consumption was still high in contrast with the DSR protocol.

Doss et al. [16] developed a new method called precise recognition and mitigation of jellyfish attack in MANET using a Support Vector Machine (SVM). The trusted nodes decided to transfer the data based on the hierarchical trust analysis property of nodes. But, the detection rate was degraded while increasing the number of nodes.

Paul et al. [17] designed a Multi-Attribute Trust Evaluation and Management (MATEM) to guarantee secure, reliable, and pervasive transfer over a hostile delay-tolerant network. In this model, the trust conditions such as risk and cooperativeness were introduced for merging the suspected and social behavior of nodes. The estimates of uncertainty and mean data forwarding delay were applied for quantifying the inherent risk involved in delay tolerant network data transfer and guaranteeing Quality-of-Service (QoS) demands in routing in a hostile atmosphere. But, it has a fixed threshold for determining trust values.

Merlin and Ravi [18] developed a new Trust-based Energy-Aware Routing (TEAR) protocol to prevent black holes through the dynamic creation of multiple discovery paths and provide a highly secure path by determining the node trust. The multi-discovery paths were created by fully using the energy in non-hotspots to increase energy efficacy and require information path confidentiality. But, it has a high communication overhead.

Elhoseny and Shankar [19] concentrated on clustering the nodes by an energy-efficient routing strategy and selecting the optimal Cluster Head (CH) by the Modified Discrete Particle

Swarm Optimization (MDPSO). Also, a secured routing protocol and a signcryption framework were employed which encrypts the digital sign to enhance the secrecy of the data transfer in MANET. But, it needs backup routing to achieve reliable security while path failure occurs.

Luong et al. [20] presented a novel Flooding Attacks Detection Algorithm (FADA) for MANETs depending on the K-Nearest Neighbor (KNN) algorithm. It was focused on the path-finding history data of all nodes to obtain the analogous features and behaviors of nodes belonging to similar classes to decide whether a node was malevolent or not. Also, a novel Flooding Attacks Prevention Routing Protocol (FAPRP) was designed by combining FADA and the standard AODV protocol.

Zhao et al. [21] developed an Exponential-based Trust and Reputation Evaluation System (ETRES) to analyze the node's behaviors and describe the exponential distribution of the node's trust. The node's trust was used to find trustworthy nodes and defend the malicious nodes. Besides, the entropy concept was applied to estimate the ambiguity of direct trust, and the belief term was restated to adjust the node's trust. But, it needs to identify compromised nodes effectively and increase network security.

Suganthi et al. [22] designed a novel Trust-based Efficient energy-balanced Routing (TER) protocol that selects the intermediate forwarding nodes to increase the network efficiency. The efficient factor was determined based on the remaining energy, distance, occupied buffer space, and the node speed to select the adjacent as successive hop. But, the throughput was not high if the number of nodes was high.

Kumar and Devi [23] developed a routing method to enhance MANET security by isolating the attacked nodes. First, all nodes were assigned with maximum trust. Then, the trust level of all nodes was maintained based on their adjacent node's trust level. Based on the variation in the trust level, the malicious nodes were identified. But, the PLR was high while the percentage of malicious nodes was high.

Sirajuddin et al. [24] developed a Trust-Based Secure Multipath Routing (TBSMR) protocol to improve MANET efficiency. In this protocol, different aspects such as congestion control, PLR reduction, suspected node identification, and secure data sharing were considered to enhance the QoS of MANET. But, security was not effective which needs cryptographic algorithms for further enhancement.

Mahamune and Chandane [25] developed an Efficient TRS (ETRS) to prevent misbehaving nodes and establish confidential transmissions in MANET. This ETRS was applied to offer explicit diagnosis to each intermediary node participating in the network transmission, to prevent the distribution of fake data deliberately prepared by suspected nodes, and to define a certain category of trusted path control scheme upon identification of the suspected node. But, the average time needed to transmit data between the origin node and target node was high while the node's mobility was high.

3. PROPOSED MODELLING

In this section, the proposed protocol is described briefly. The secure energy-efficient routing guarantees that information is successfully delivered between the origin and the target nodes. The schematic representation of an adaptive TT-based secure energy-efficient hybrid routing in MANET is shown in Figure 1.

Initially, the MANET is created using N number of nodes. After that, fuzzy clustering is performed to split the entire network into different clusters. Then, the CH for each cluster is chosen by the highest ranges of direct, indirect, and current trust. Moreover, the malicious node is detected by the adaptive threshold value. This adaptive threshold value is determined by using the ANN model which learns the different network parameters including the percentage of route alterations, ND, connectivity, node stability, mobility, residual power, pause time and mean neighborhood trustworthiness. When the trust of a given node is greater than the adaptive threshold range, it is termed a benign node; or else, it is termed a malicious node. The identified malicious node is avoided from the routing path between the origin node and target nodes to transfer the data packets. Further, the hybrid C-SSA is applied to decide the optimal routes depending on the delay, throughput, and route connectivity to reduce PLR.

3.1. Network Model

In this study, the MANET is constructed as a graph $G(V,E)$ in which V indicates the collection of nodes and E denotes the collection of links,$E \subseteq V \times V$. Consider that each node has a homogeneous communication range r_0. The wireless link $(i,j) \in E$ when the Euclidean distance D_E between nodes i and j is less than r_0. For 2-hop connectivity of i, the sub-graph $G_i$is considered which has only the 1-hop and 2-hop adjacent of i. This is described by equation (1).

$$2hop(i) = \{w \in V, k \in V: (i,k) \in E \wedge (k,w) \in E\} \qquad (1)$$

Also, consider that the adaptive TT range is $\xi \in [0,1]$ whereas 0 is the minimum and 1 is the maximum. Besides, the adversarial model is considered which consists of malevolent nodes that might discard, change or infuse data. In this study, consider that a trust-based malicious node identification and mitigation protocol is applied at each node to identify malicious nodes. The malicious identification protocol can induce the dynamic TT selection algorithm while a malicious node is identified. It is essential to observe that the TT ξ and the reliability of all adjacent are limited to all nodes, defining that every node will determine these values independently.

The strategy for determining TT is completely dispersed and so various nodes may contain distinct perceptions of similar adjacent. Therefore, the malicious node is secluded from the route to specify a solution for all nodes.

3.2. Determination of Network Parameters

3.2.1. Network Density (ND)

It refers to the number of nodes in the 1-hop vicinity. Consider i and its degree at an interval t, represented as $\delta_i(t)$ with r_0 is described as $\left|\left\{j \in V_i : D_{E_{(t)}}(i,j) \le r_0\right\}\right|$. The ND $\delta = 0$ is secluded, i.e. it includes no adjacent; so, the least ND, $(min(\delta_i))$ is 0. Additionally, the node involves the highest ND $(max(\delta_i))$ when each node in the MANET is directly linked to i. The TT is directly proportional to the ND. All nodes consider the ND in its 1-hop vicinity when calculating the TT. The greater the number of nodes in the 1-hop vicinity, the greater the TT value, and vice versa. In particular, if an origin node contains a greater number of different 1-hop nodes from which to choose forwarding nodes, it may handle higher TT values while reducing the probability of network clustering.

When a malevolent node m is prevented from the route, i leftovers interacted with the system, ensuring the tradeoff between identification accuracy and PDR.

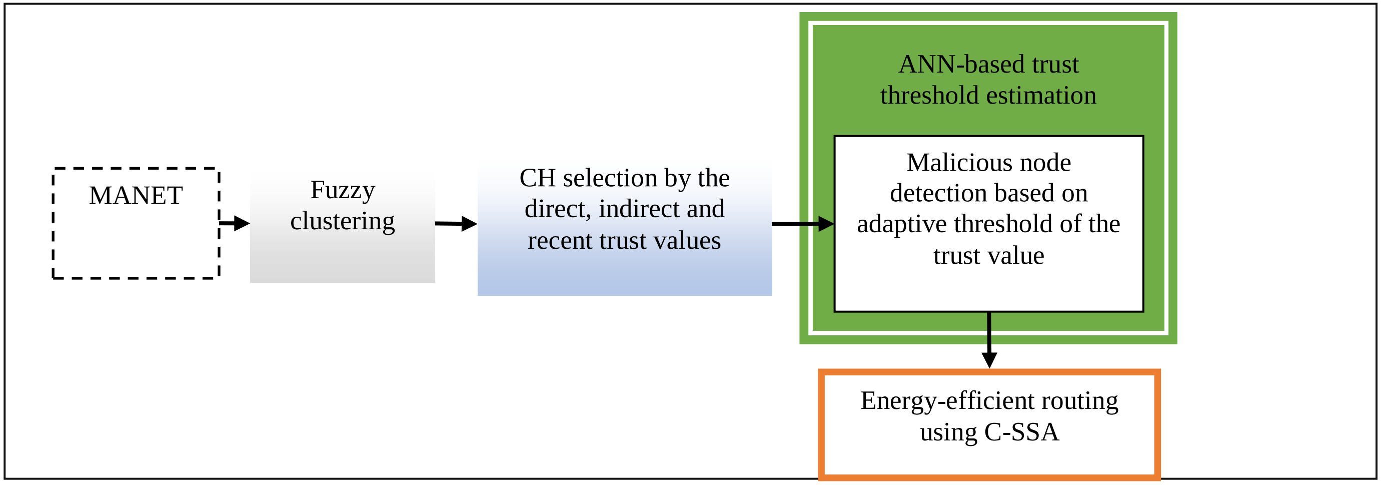
MANET
Fuzzy clustering
CH selection by the direct, indirect and recent trust values
ANN-based trust threshold estimation
Malicious node detection based on adaptive threshold of the trust value
Energy-efficient routing using C-SSA

Figure 1 Adaptive Trust Threshold-based Malicious Node Detection and Hybrid Routing Protocol for MANET

3.2.2. 2-Hop Connectivity

In this protocol, the 2-hop connectivity $(\tau_{(i,k)})$ at i for a certain direct adjacent k is defined as the number of nodes w in a 2-hop vicinity, which are simply accessible via k, described by equation (2).

$$\tau_{(i,k)} = \{w \in 2hop(i): (i,k) \in E_i \wedge (k,w) \in E_i \wedge (\nexists p \in 1hop(i), p \neq k: (i,p) \in E_i \wedge (p,w) \in E_i)\} \quad (2)$$

The least 2-hop connectivity of the node $(min(\tau_i))$ regarding a certain 1-hop adjacent k is 0 and is defined as the reality that no 2-hop node is accessible simply via that node. On the other hand, the highest 2-hop connectivity $(max(\tau_i))$ of the node regarding the shortest adjacent k is $|2hop(i)|$, referring that each 2-hop adjacent of i are simply accessible through k. The 2-hop connectivity is measured to guarantee the network connectivity before preventing the malevolent node from the route.

3.2.3. Percentage of Path Alterations

The network structure and the vicinity of the individual nodes modify regularly because of node mobility. The node can compute the node mobility in its vicinity by determining the vicinity percentage of path modifications. The greater the movement, the higher the system topology varies and so the greater the percentage of modification in the node vicinity.

The rate of change in a neighborhood is considered to determine the TT. The percentage of link modifications at i is determined by the percentage of path modification at i rather than considering the mean percentage of path modifications in the entire system as in equation (3):

$$\eta_i = \lambda_i + \mu_i \quad (3)$$

Each fresh node, which visits i's communication region produces a fresh connection to i. So, the number of fresh nodes in the vicinity of i is equal to the overall path arrival rate at i (λ_i) for each period $[t-1, t]$ as in equation (4):

$$\lambda_i(t) = \left\{j \in V_i, D_{E_{(t-1)}}(i,j) > r_0 \wedge D_{E_{(t)}}(i,j) \le r_0\right\} \quad (4)$$

Likewise, the link failure rate μ defines the overall amount of nodes traveling out of i's communication range for $[t-1, t]$ and is represented in the equation (5):

$$\mu_i(t) = \left\{ j \in V_i, D_{E_{(t-1)}}(i,j) \leq r_0 \wedge D_{E_{(t)}}(i,j) > r_0 \right\} \quad (5)$$

By substituting equations (4), (5), (3), the rate of link modification at i as $\eta_i = |\lambda_i| + |\mu_i|$. The minimum potential η_i, $(min(\eta_i))$ for i at t is 0, defining that there is no fresh appearance of nodes and no path failures due to no movement of nodes. Likewise, the highest potential $\mu_i, (max(\mu_i))$ for i at t is given if each direct adjacent travel out of the communication range, and the highest λ_i, $(max(\lambda_i))$ is equivalent to the failure ratio. The highest η_i, $(max(\eta_i))$ is devised as $max(\lambda_i(t)) + max(\mu_i(t)) = 2 \cdot \delta_i(t)$.

3.2.4. Mean Neighborhood Reliability

In trust-based protection strategies, all nodes handle the trust list to observe the trust of another node; so, the mean neighborhood reliability is simply determined. In this protocol, the entries of this list for all adjacent are determined via forecasting the proportion of data properly transmitted through that adjacent in a sliding window W of the most current examined conducts. Every node considers the mean reliability of the nodes, i.e. the complete trust status of the nodes in its 1-hop vicinity as equation (6):

$$mean\_\varphi_i = \frac{1}{n} \sum_{a=1}^{N} \varphi_a \quad (6)$$

In equation (6), N denotes the overall amount of nodes in the 1-hop neighborhood. Observe that the highest neighborhood reliability $(max(\varphi_i))$ is equivalent to 1 when the least neighborhood reliability $(min(\varphi_i))$ is 0.

3.2.5. Node Mobility and Stability

The node mobility is determined by considering the random waypoint model. Based on this model, each node randomly chooses the position as its target. Then, it moves towards this target with a fixed velocity decided regularly and randomly from $[0, Vt_{max}]$. Upon reaching the target, the node stops for an interval called pause time $(Pause\ time)$. So, the stability factor of a node i is determined as equation (7):

$$SF_i = {}^{Pause\ time}/_{Vt_i} \quad (7)$$

In equation (7), Vt_i is the relative velocity of the node with respect to the origin node and $(0 \leq Vt_i \leq Vt_{max})$, where Vt_{max} is the maximum allowable velocity for each node.

3.2.6. Residual Power

It is the remaining battery power of the node at a specified interval.

3.3. Adaptive Trust Threshold Prediction using ANN

Once all the network parameters for each node are computed, these are fed to the ANN to learn and detect the node's behavior as benign or malicious. The ANN has three different units as shown in Figure 2: an input, the hidden, and the output units. Normally, to adjust the weights until the error is less, the back-propagation learning algorithm is used.

The training set $\{(x_1, y_1), \ldots, (x_n, y_n)\}$ consists of input parameters and desired TT values. If the input (X_i) is given to the ANN, the ANN produces an output (O_i), which may be different from the target $(\hat{y}_i)$. The considered network parameters are initially fed to the input unit and its outcomes are linked to the hidden unit. This is described by equation (8)

$$H_i = \sum_{i=1}^{n} w_i X_i + b \quad (8)$$

In equation (8), w_i is the weight value of the input unit and X_i is the input network parameters value and b is the bias. The ANN's hidden unit is characterized using the tan-sigmoid transfer function as equation (9):

$$f(H_i) = \frac{2}{1+e^{-2H_i}} - 1 \quad (9)$$

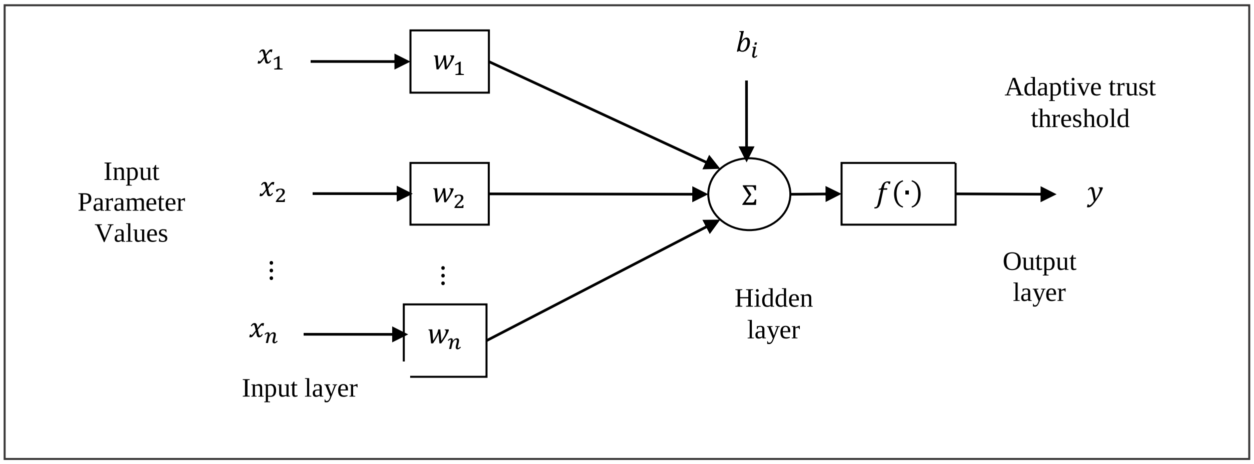

Figure 2 Architecture of ANN for Adaptive Trust Threshold Prediction

At last, the ANN's output unit is represented by equation (10).

$$o_i = f(\sum_{i=1}^{n} w_h Y_i + b) \tag{10}$$

In equation (10), o_i is the range of output neurons, $f(x)$ is the transfer function and w_h is the hidden unit's weight. The range of output neurons is a value of TT which compares the node's trust values to identify their behavior as malicious or normal. The goal of ANN learning is to minimize the error between the real and required outputs. The error value is computed as equation (11):

$$\text{Error} = \frac{1}{2}\sum_{i=1}^{n}(o_i - \hat{y}_i)^2 \tag{11}$$

Thus, the ANN is trained to adaptively predict the TT for malicious node identification. Once the malicious nodes are identified, they are excluded from the routing path and the best stable routing paths are chosen by the C-SSA to achieve effective data transfer with a minimum packet loss. The algorithm for the proposed protocol called ANN-C-SSA is presented in Algorithm 1.

```
Input: $N$ number of nodes
Output: Malicious or normal node
1. Create the network using $N$ number of nodes;
2. Cluster the nodes based on fuzzy clustering;
3. Choose the CH for each cluster by determining the trust values of all nodes;
4. Determine the percentage of route alterations, ND, connectivity, node stability, mobility, residual power, pause time and mean neighborhood trustworthiness for each node;
5. Train the ANN model to predict the adaptive TT value;
6. Compare the adaptive TT and node's trust value to identify the malicious and normal nodes;
7. If the trust of a given node is larger than the adaptive threshold range, then the considered node is called non-malevolent;
8. If the trust of a given node is less than the adaptive threshold range, then the considered node is called malevolent;
9. Seclude the malicious node from the routing path;
```

Algorithm 1 for Proposed ANN-C-SSA Protocol

The algorithm 1 describes the process of the ANN-C-SSA protocol. In Step 1, the network is created by N number of nodes. Step 2 performs the fuzzy clustering and Step 3 selects the CH for each cluster based on the trust values of each node. In Step 5, different network parameters of each node are calculated. Step 6 applies the ANN model for predicting the adaptive TT value. Step 6-Step 8 compares the adaptive TT value with the node's trust value to identify malicious and normal nodes. Step 9 removes the identified malicious node from the routing path for data transmission.

4. RESULTS AND DISCUSSION

This part analyzes the efficiency of the presented protocol called ANN-C-SSA by simulating it in Network Simulator version 3 (NS3.33). Also, its efficiency is compared with the existing trust-aware routing protocols such as TEAR [18], ETRES [21], ETRS [25], and C-SSA [13]. The comparison is conducted in terms of different metrics such as Packet Delivery Ratio (PDR), End-to-End Delay (E2D), Packet Loss Ratio (PLR), energy consumption, throughput, false positives, and detection rate. Table 1 provides the considered simulation parameters.

Table 1 Simulation Parameter

Parameters	**Values**
Topology area	1400×1400m^2
Number of nodes	200
Number of attackers	15
Channel type	Wireless
Antenna type	Omni-directional
Link layer type	Link layer
Radio propagation scheme	Two-ray ground
Queue category	Drop tail
MAC type	MAC802.11
Mobility model	Random waypoint
Protocol type	AODV
Node mobility	10-60m/sec
Transmission range	250m
Initial energy	16.5J
Packet size	512bytes/packet
Traffic type	Constant bit rate
Simulation time	300sec

4.1. Packet Delivery Ratio (PDR)

It is the proportion of a quantity of data properly received by the target node to the quantity of data transmitted from the origin node.

Figure 3 illustrates the Packet Delivery Ratio (PDR) (in %) achieved by the TEAR, ETRES, ETRS, C-SSA, and ANN-C-

SSA-based routing protocols under a varying number of nodes. It indicates that the Packet Delivery Ratio (PDR) achieved by the ANN-C-SSA algorithm is greater than all other protocols for identifying the malicious nodes in the network during data transfer. For the case of 200 nodes in the network, the Packet Delivery Ratio (PDR) of ANN-C-SSA is 11.09% higher than the TEAR, 7.81% higher than the ETRES, 5.08% higher than the ETRS, and 2.7% higher than the C-SSA.

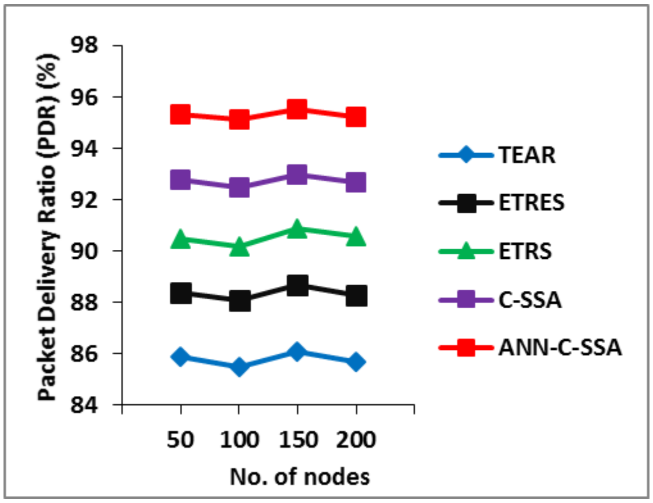

Figure 3 Packet Delivery Ratio (PDR) vs. No. of Nodes

4.2. End-to-End Delay (E2D)

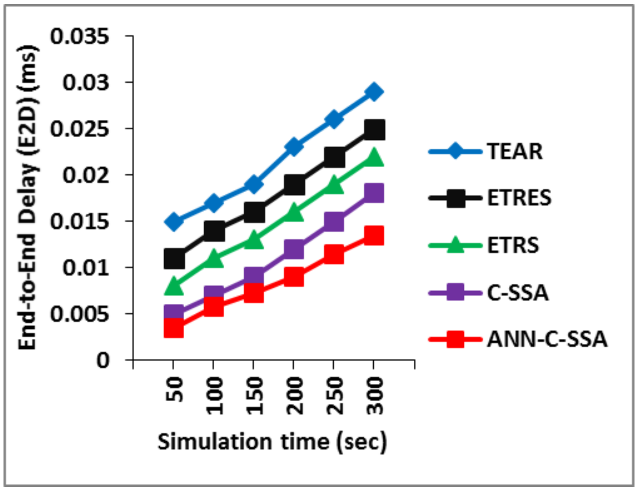

Figure 4 End-to-End Delay (E2D) vs. Simulation Time

It is the mean interval required by the data packets transmitted from the origin node to the target nodes. Figure 4 depicts the End-to-End Delay (E2D) (in ms) achieved by the TEAR, ETRES, ETRS, C-SSA, and ANN-C-SSA-based routing protocols under varying simulation time (in sec). It observes that the End-to-End Delay (E2D) obtained by the ANN-C-SSA algorithm is less than all other protocols to detect and prevent malicious nodes. If the simulation period is 300sec, the End-to-End Delay (E2D) of ANN-C-SSA is 53.45% less than the TEAR, 46% less than the ETRES, 38.64% less than the ETRS, and 25% less than the C-SSA.

4.3. Packet Loss Ratio (PLR)

It is the proportion of data discarded via malicious nodes to the overall quantity of data sent. Figure 5 portrays the Packet Loss Ratio (PLR) (in %) achieved by the TEAR, ETRES, ETRS, C-SSA, and ANN-C-SSA-based routing protocols under a varying number of nodes. It analyzes that the Packet Loss Ratio (PLR) obtained by the ANN-C-SSA algorithm is less than all other protocols to detect and prevent malicious nodes. For example, if there are 200 nodes in the network, the Packet Loss Ratio (PLR) of ANN-C-SSA is 66.43% less than the TEAR, 58.97% less than the ETRES, 48.94% less than the ETRS, and 34.25% less than the C-SSA.

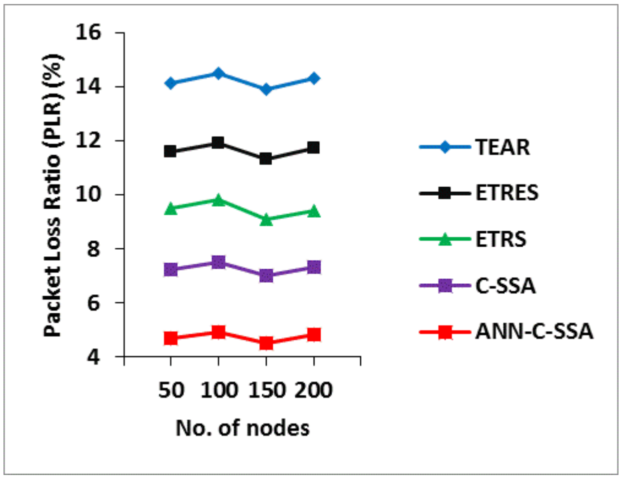

Figure 5 Packet Loss Ratio (PLR) vs. No. of Nodes

4.4. Energy Consumption

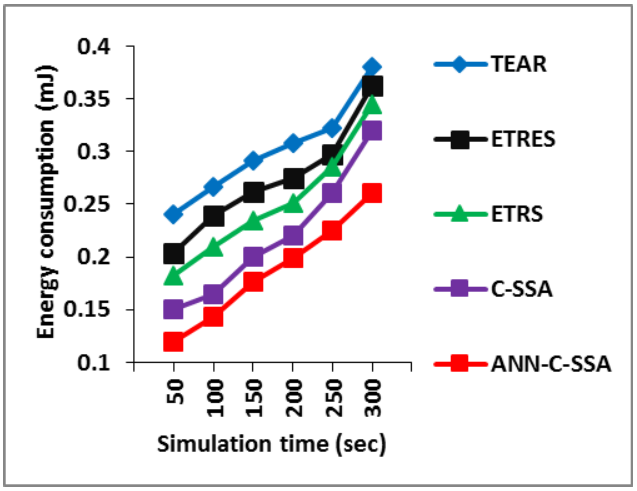

Figure 6 Energy Consumption vs. Simulation Time

It is the fraction of the mean depleted energy at every node to the primary energy at nodes. Figure 6 portrays the energy consumption (in mJ) achieved by the TEAR, ETRES, ETRS, C-SSA, and ANN-C-SSA-based routing protocols under varying simulation times (in sec). It observes that the energy consumption obtained by the ANN-C-SSA algorithm is less than all other protocols to detect and prevent malicious nodes. If the simulation period is 300sec, the energy consumption of ANN-C-SSA is 31.32% less than the TEAR, 28.1% less than the ETRES, 24.35% less than the ETRS, and 18.44% less than the C-SSA.

4.5. Throughput

It defines the average of bits accepted by the target per second. Figure 7 depicts the throughput (in bits/sec) achieved by the TEAR, ETRES, ETRS, C-SSA, and ANN-C-SSA-based routing protocols under a varying number of nodes. It observes that the throughput obtained by the ANN-C-SSA algorithm is greater than all other protocols to detect and prevent malicious nodes in the network. For example, if there are 200 nodes in the network, the throughput of ANN-C-SSA is 69.87% greater than the TEAR, 43.18% greater than the ETRES, 17.73% greater than the ETRS, and 9.92% greater than the C-SSA.

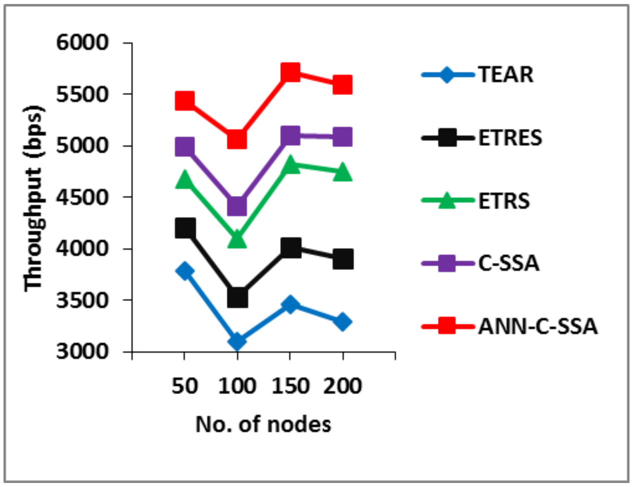

Figure 7 Throughput vs. No. of Nodes

4.6. False Positives

It refers to the fraction between the trusted nodes identified as malevolent and the overall amount of trusted nodes. Figure 8 shows the PLR (in %) achieved by the TEAR, ETRES, ETRS, C-SSA, and ANN-C-SSA-based routing protocols under a varying number of nodes. It analyzes that the PLR obtained by the ANN-C-SSA algorithm is less than all other protocols to detect and prevent malicious nodes. For example, if there are 200 nodes in the network, the PLR of ANN-C-SSA is 26.92% less than the TEAR, 20.83% less than the ETRES, 17.39% less than the ETRS, and 11.63% less than the C-SSA.

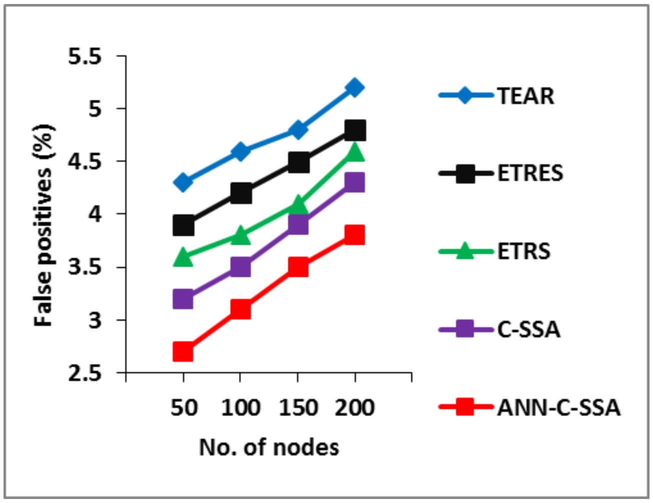

Figure 8 False Positives vs. No. of Nodes

4.7. Detection Rate

It is the ratio of malevolent nodes identified to the sum amount of malevolent nodes. Figure 9 portrays the detection rate (in %) achieved by the TEAR, ETRES, ETRS, C-SSA, and ANN-C-SSA-based routing protocols under varying simulation times (in sec). It observes that the detection rate obtained by the ANN-C-SSA algorithm is higher than all other protocols to detect and prevent malicious nodes. If the simulation period is 300sec, the detection rate of ANN-C-SSA is 7.34% higher than the TEAR, 5.62% higher than the ETRES, 4.66% higher than the ETRS, and 3.6% higher than the C-SSA.

According to these analyses, it is observed that the ANN-C-SSA protocol realizes the maximum network performance because of identifying and mitigating the malicious nodes from the data transmission using their trust values compared to the other protocols.

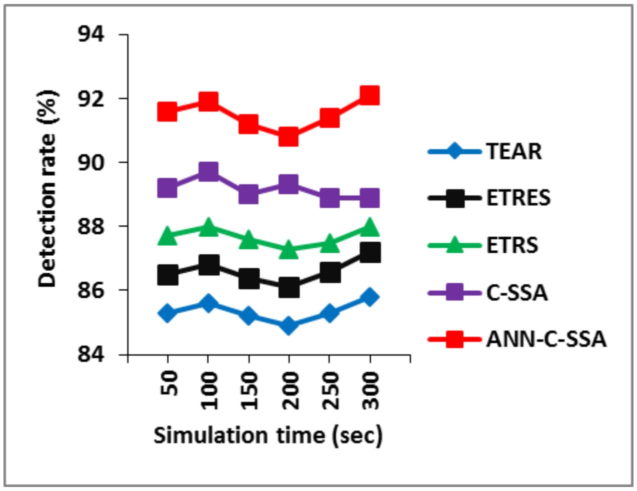

Figure 9 Detection Rate vs. Simulation Time

5. CONCLUSION

In this study, an adaptive TT-aware secure energy-efficient protocol was presented which enhances the detection and mitigation of malevolent nodes in MANET. At first, the network was clustered and the corresponding CHs were chosen based on the trust management scheme. Then, different parameters were calculated for each node in the network and utilized to train the ANN for predicting the adaptive TT value. By comparing the predicted TT and node's trust values, the malicious and normal nodes were identified. Moreover, the malicious nodes were discarded from the route and the most stable path was chosen by the C-SSA for effective data transfer. Finally, the simulation results proved that the proposed protocol has a detection rate of 92.1% for 300 nodes compared to the other protocols. On the other hand, the conflicting behaviour attacks were not recognized and prevented, which also impacts the network performance. So, future work will focus on the detection and mitigation of conflicting behaviour attacks based on trust along with various network parameters.

REFERENCES

[1] N. Raza, M.U. Aftab, M.Q. Akbar, O. Ashraf, M. Irfan, "Mobile ad-hoc networks applications and its challenges", Communications and Network, vol. 8, no. 3, 2016, pp. 131-136.

[2] N. A. M. Saudi, M. A. Arshad, A. G. Buja, A. F. A. Fadzil, R. M. Saidi, "Mobile ad-hoc network (MANET) routing protocols: a performance assessment", In Proceedings of the Third International Conference on Computing, Mathematics and Statistics, Springer, Singapore, 2019, pp. 53-59.

[3] T. K. Saini, S. C. Sharma, "Recent advancements, review analysis, and extensions of the AODV with the illustration of the applied concept", Ad Hoc Networks, vol 103, 2020, pp.1-20.

[4] M. I. Talukdar, R. Hassan, M. S. Hossen, K. Ahmad, F. Qamar, A. S. Ahmed, "Performance improvements of AODV by black hole attack detection using IDS and digital signature", Wireless Communications and Mobile Computing, 2021, pp 1-13.

[5] R. Menaka, J. M. Mathana, R. Dhanagopal, B. Sundarambal, "Performance evaluation of DSR protocol in MANET untrustworthy environment" , In IEEE 6th International Conference on Advanced Computing and Communication Systems, 2020, pp. 1049-1052.

[6] W. Alnumay, U. Ghosh, P. Chatterjee, "A Trust-Based predictive model for mobile ad hoc network in internet of things", Sensors, vol.19, no.6, 2019 , pp 1-14.

[7] Usman, A. B., Gutierrez, J. Toward trust based protocols in a pervasive and mobile computing environment: A survey. Ad Hoc Networks, 81, 2018, 143-159.

[8] R. J. Cai, W. C. W. Tan, P. H. J. Chong, "An overview of trust-based routing design under adversarial mobile ad hoc network environment", Wireless Personal Communications, vol. 96, no.3, 2017 , pp. 3923-3946.

[9] A. Sharma, E. S. Pilli, A. P. Mazumdar, P. Gera "Towards trustworthy internet of things: a survey on trust management applications and schemes", Computer Communications, vol .160, 2020, pp .475-493.

[10] R. K Chahal, N. Kumar, S. Batra, "Trust management in social internet of things: a taxonomy, open issues, and challenges", Computer Communications, vol. 150, 2020, pp. 13-46.

[11] H. Xu, H. Si, H. Zhang, L. Zhang, Y. Leng, J. Wang, D. Li, "Trust-based probabilistic broadcast scheme for mobile ad hoc networks", IEEE Access, vol. 8, 2020 , pp. 21380-21392.

[12] D. Zhang, C. Gong, K. Jiang, X. Zhang, T. Zhang, "A kind of new method of intelligent trust engineering metrics (ITEM) for application of mobile ad hoc network", Engineering Computations, 2019 , pp.1617-1643.

[13] N.Veeraiah, O. I.Khalaf, C. V. P. R. Prasad, Y. Alotaibi, A. Alsufyani, S. Alghamdi, N.Alsufyani, "Trust aware secure energy efficient hybrid protocol for MANET", IEEE Access, 2020, pp. 120996-121005.

[14] S. Gurung, S. Chauhan, "A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET", Wireless Networks, vol. 25 no.4, 2019, pp. 1685-1695.

[15] R. J. Cai, X. J. Li, P. H. J. Chong, "An evolutionary self-cooperative trust scheme against routing disruptions in MANETs", IEEE Transactions on Mobile Computing, vol.18, no.1, 2018, pp .42-55.

[16] S. Doss, A. Nayyar, G. Suseendran, S. Tanwar, A. Khanna, P. H. Thong, "APD-JFAD: accurate prevention and detection of jelly fish attack in MANET", IEEE Access, vol 6, 2018, pp.56954-56965.

[17] B.Paul, S.Biswas, S.Nandi, S.Chakraborty, "MATEM: A unified framework based on trust and MCDM for assuring security, reliability and QoS in DTN routing", Journal of Network and Computer Applications, 2018, pp.104, 1-20.

[18] R. T. Merlin, R. Ravi, "Novel trust based energy aware routing mechanism for mitigation of black hole attacks in MANE", Wireless Personal Communications, vol. 104, no. 4, 2019, pp.1599-1636.

[19] M.Elhoseny, & K.Shankar, "Reliable data transmission model for mobile ad hoc network using signcryption technique", IEEE Transactions on Reliability, vol. 69, no. 3, 2019, pp.1077-1086.

[20] N. T. Luong, T. T. Vo, D.Hoang, "FAPRP: A machine learning approach to flooding attacks prevention routing protocol in mobile ad hoc networks",Wireless Communications and Mobile Computing, 2019, pp.1-17.

[21] J.Zhao, J. Huang, N.Xiong, "An effective exponential-based trust and reputation evaluation system in wireless sensor networks", IEEE Access, vol .7, 2019, pp.33859-33869.

[22] R. Suganthi, I. Poonguzhali, J. Navarajan, R. Krishnaveni, N. N. Saranya, "Trust based efficient routing (TER) protocol for MANETS", Materials Today: Proceedings, 2021.

[23] G. S. Kumar, P. R. Devi, "A novel proactive routing strategy to defend node isolation attack in MANETS", Materials Today: Proceedings, 2021.

[24] M. Sirajuddin, C. Rupa, C. Iwendi, C. Biamba, "TBSMR: a trust-based secure multipath routing protocol for enhancing the QoS of the mobile ad hoc network", Security and Communication Networks, 2021, pp.1-9.

[25] A. Mahamune, M. M. Chandane, "An efficient trust-based routing scheme against malicious communication in MANET", International Journal of Wireless Information Networks, 2021, pp.1-18.

Authors

K.Vijay Anand completed B.Sc. in Physics (1996) from Manonmaniam Sundaranar University, Thirunelveli, and a Master of Computer Applications (1999) from Bharathiar University, Coimbatore. He completed his M.Phil. in Computer Science with a specialization in Network Security in the year 2008 from Manonmaniam Sundaranar University. Thirunelveli. He is currently pursuing a Ph.D. in Computer Science at Bharathiar University, Coimbatore. He is presently working as Associate Professor at SNMV College of Arts and Science, Coimbatore. He is having 23 years of teaching experience and 3 years of research experience. His research interests include Network Security, Wireless Sensor Networks, Cloud Computing, and Neural Networks.

RESEARCH ARTICLE

Dr. G. Abel Thangaraja, M.C.A., M.Phil., Ph.D., Assistant Professor of the Department of Computer Technology at Sri Krishna Adithya College of Arts and Science, Coimbatore. He has been awarded a Doctoral degree by Bharathiar University in the year 2015; he completed his MCA at Anna University. 15 years of Teaching & Research experience during which he has also acted as a senate member of Bharathiar University, ICT Co-coordinator, and Examcell Convenor. He completed a funded project worth Rs.1,00,000 by TNSCST in the year 2015. Supervising 4 research scholars, and his research interests include Bigdata, Data Mining, and published research papers in reputed peer-reviewed journals and presented in various seminars and conferences.

How to cite this article:

K. Vijay Anand, G. Abel Thangaraja, “A Competent Intelligence Modeling for Trust-Based Security Scheme in Mobile Ad Hoc Network”, International Journal of Computer Networks and Applications (IJCNA), 9(6), PP: 736-745, 2022, DOI: 10.22247/ijcna/2022/217706.