DOI: 10.21917/ijct.2023.0424

FUZZY BASED OPTIMIZATION FOR IMPROVING THE TRUST SCORE IN MANETS

K. Karunambiga[1], M. Sathiya[2], S. Bhaggiaraj[3] and K.C. Rajheshwari[4]
[1]*Department of Computer Science and Engineering, Karpagam Institute of Technology, India*
[2]*Department of Information Technology, Karpagam Institute of Technology, India*
[3]*Department of Information Technology, Sri Ramakrishna Engineering College, India*
[4]*Department of Computer Science and Engineering, Sona College of Technology, India*

Abstract

In this paper, research develop a method for identifying abnormal behavior based on two inputs: the trustworthiness of the user, as well as the reliability of the recommendations that they make. Specifically, research look at the reliability of the user recommendations. The next thing that needs to be done is to calculate the node general trust value in order to determine if there has been any kind of malicious attack. This will show whether or not the node has been compromised in any way. It is conceivable that this could lessen the amount of power that is needed for the communication that takes place between different networks. Additionally, it demonstrates that the model is better able to utilize the evaluation results of the common neighbor nodes to synthesize the confidence value when fewer nodes are deployed in the network. This is demonstrated by the fact that fewer nodes are deployed in the network. The reliability of the trust assessment improves while the number of trusts for which recommendations are made decreases.

Keywords:

Fuzzy Optimization, Trust, Score, MANETs, Direct Trust

1. INTRODUCTION

When the wireless transmission ranges of two nodes in a MANET overlap with one another, the result is that the overlapping nodes are instantaneously able to communicate with one another [1]. In the event that the ranges do not overlap, the nodes in question will have no choice but to depend on the services of other nodes in order to relay their messages. A MANET is a network that can develop whenever there is a need for it, without the requirement for established connections or other permanent nodes [2].

Nodes, neighbors, and third parties who are not immediately involved in a situation can all play a role in establishing trust. The confidence of a node neighboring nodes is determined by a recommendation or feedback system, and the trust of the network as a whole is determined by an impartial third-party making use of the experiences, recommendations, and expertise of the network constituent nodes [3].

The quality of the services that a node in the network provides determines the individual trust number that node receives. In the setting of trust computation, direct computation mechanisms include a node own experience as well as its feedback about a target node. In contrast, indirect computation mechanisms include acquiring information from other nodes [4].

Direct computation mechanisms include a node own experience as well as its feedback about a target node. As part of a hybrid technique, calculations are carried out that combine both direct and indirect approaches [5].

The dependability of each component in a network is dependent on the dependability of the other components, networks are extremely essential. Techniques of trust computation require a significant number of resources in order to re-compute the degree of confidence held by each node with regard to the target node [6]. In contrast to traditional networks, MANETs, are mobile and require a significantly lower quantity of resources to function effectively.

Therefore, the implementation of re-computational trust techniques results in the addition of labor that is not strictly necessary for the operation of these systems [7]. This overhead is kept to a minimal by trust propagation strategies, which do so by calculating the trust value only once, as opposed to doing so at each node. These strategies keep the trust value at a consistent level across the network. The computed confidence value is then broadcast to other nodes, and the recommendations of surrounding nodes are taken into consideration before making any final decisions [8].

A technique is required to estimate the correct value of trust at the requested node because there may be numerous paths with different values by which the confidence of a target node is propagated to the requester node. As a result of this, a method is required to estimate the correct value of trust at the requested node [9]-[11]. As a result of this, a technique is necessary in order to estimate the appropriate value of trust at the node that was requested.

One strategy that can be used to help in arriving at an accurate evaluation of the necessary level of assurance is known as the trust aggregation procedure. Dedicated paths, the shortest distance between the source and the target, highly trusted nodes in the path of trust propagation, probability, trust table and such concepts are the details upon which the different methods for aggregating trust depend. Trust aggregation is a computationally challenging task that must be managed by nodes with appropriate resources [12].

If a node trust score is ambiguous or if there is a discrepancy between the node claimed trust score and its actual trust score, the trust prediction mechanism may be able to assist with the calculation of the node confidence. When determining whether or not to place confidence in a node, the actions that node has taken in the past are taken into consideration whenever it is possible to do so.

2. PRELIMINARIES

2.1 COMMUNICATION TRUST

After N attempts at establishing contact between sensor nodes j and i, research are going to make the assumption that the sum of the total number of successful attempts (Sc_{ij}) and the total number of unsuccessful attempts (Fc_{ij}) will be equal to N i.e. $Sc_{ij} + Fc_{ij} = N$. This is the assumption that research are going to

make. In order to determine whether or not something can be relied upon, research make use of the beta distribution model.

If research assume that node *i* is responsible for maintaining the picture of node *j* in communications, then research can represent the current expectation of the variable $Rc_{ij} = \beta(Sc_{ij},Fc_{ij})$. This will allow us to express Rc_{ij} as an equation. The current anticipation of the variable Rc_{ij} is denoted by the value Rc_{ij}.

$$E\left(Rc_{ij}\right) = E\left(\beta\left(Sc_{ij}, Fc_{ij}\right)\right) = \frac{Sc_{ij}}{Sc_{ij} + Fc_{ij}} \tag{1}$$

Let say, for the sake of this discussion, that the confidence in the subsequent communication, which is Tc_{ij}^{t} from now on, was productive. The trust expectation Tc_{ij}^{t} in the succeeding communication is described as follows, taking into account the fact that trust is the subjective anticipation by an individual of the outcome of a statistical distribution representing reputation between two nodes. This is due to the fact that confidence can be defined as an individual subjective anticipation of the outcome.

$$Tc_{ij}^{t} = \frac{1 + Sc_{ij}}{1 + Sc_{ij} + Fc_{ij}} \tag{2}$$

2.1.1 Message Trust:

Due to the fact that WSNs are set up with the sole intention of acquiring a particular message, its verification is of the uttermost importance. The calculations of confidence that are carried out by the message trust model make use of the beta distribution model. This model is applied in the context of the authentication of identities and the verification of data.

At the beginning of the process of setting up a network, each node will run a random algorithm in order to generate a one-of-a-kind authentication number, which is also referred to as an ID. This suggests that each node has two identifiers - the node ID and the arbitrary integer ID' - the former of which is the node ID. These identifiers are what are used to create a one-of-a-kind name for the object.

A data set is maintained in an array by the leader of the cluster, who receives the information from each member of the cluster along with its own unique identifier and an additional identification symbol, which is abbreviated as ID'. The leader of the cluster also keeps track of an additional identification symbol. The base station would then store both of these identifiers after receiving them from the cluster leader, who would transmit both their ID and their ID' to the base station.

During the time that data is being transferred, members of the cluster will communicate with the leader of the cluster by sending him or her messages. The head of the cluster then makes a comparison between the ID' that is stored in the array and the source ID that was received; if the findings are the same, research presume that the identity authentication was successful. In the event that the findings are not the same, on the other hand, research will presume that authentication was not successful.

A Sybil attack is a form of identity attack in which numerous forged identifiers for the same node are sent to a receiver. This technique can uncover Sybil attacks, which are able to uncover them. Dictionary attacks are yet another form of identity theft that can be discovered with the help of this technique. Our approach, on the other hand, makes use of a random function to generate IDs in order to provide the cluster master with the ability to distinguish between genuine and spoofed nodes.

The data verification byte is generated by a one-way hash function based on the data, which makes it impossible to reverse. The data is extracted by the recipient from the message that it has received, and then the data is re-authenticated using the same one-way hash function. If the byte value that is generated is identical to the one that was used for identity authentication, then research consider the authentication to have been successful. If the value of the byte that is generated is different from the one that was used for identity authentication, then the authentication was not successful.

Tc_{ij}^{t} is the trust expectation of identity authentication, and it is computed in a manner that is comparable to that of Tc_{ij}^{t}, where Si ij is the number of times sensor node j has successfully authenticated with sensor node *i*, and Fi_{ij} is the number of times it has failed to do so.

Tc_{ij}^{t} is then compared to Ti_{ij}^{t}, which is the current successful trust expectation of identity authentication. The results of this comparison are then compared to the present successful trust expectation for identity authentication, which is denoted by Tc_{ij}^{t}.

$$Ti_{ij}^{t} = \frac{1 + Si_{ij}}{1 + Si_{ij} + Fi_{ij}} \tag{3}$$

If research make the presumption that Sd_{ij} represents the total number of successful data verifications and Fd_{ij} represents the total number of unsuccessful data verifications, then the anticipated number of successful data verifications in the future, Td_{ij}^{t}, can be computed by using these two numbers. This is because Sd_{ij} represents the total number of successful data verifications and Fd_{ij} represents the total number of unsuccessful data verifications.

$$Td_{ij}^{t} = \frac{1 + Sd_{ij}}{1 + Sd_{ij} + Fd_{ij}} \tag{4}$$

The tm_{ij}^{t} is the trust in the next message. When calculating tm_{ij}^{t}, research make use of the following formula, which is founded on the principles of probability statistics and takes into consideration the fact that authenticating one identity and verifying one data are two separate processes.

$$tm_{ij}^{t} = Ti_{ij}^{t} \times Td_{ij}^{t} \tag{5}$$

2.1.2 Energy Trust:

Research makes use of the first-order radio model that is described in LEACH in order to calculate the amount of power that is lost in WSNs during the transmission and receiving of messages. This is done because the conservation of energy is of utmost importance in these kinds of networks. The following formula is used to determine the quantity of electricity that must be present at node *j* in order for a communication to be sent from that node:

$$E_{j}^{s} = lE_{elec} + l\varepsilon_{amp}d^{2} \tag{6}$$

where E_{elec} - energy dissipation for transmission and reception, and ε_{amp} - amplification factor to transmit a message of *l* bits over a distance *d*.

The following equation is used to determine Node *j* energy consumption upon message reception. When it comes to the organization of the clusters that make up WSNs, the dissipation of the cluster leader is caused by the reception of messages sent by other nodes that make up the cluster. This is because the leader of the cluster is the node that receives the most messages. These communications have been sent from various other participants of the cluster. The dissemination of broadcast messages from the cluster leaders is the primary contributor to the scattering of members, which occurs when members leave the cluster. (Since this utilization is relatively low, research disregarded it in the model of our energy trust.

$$E_j^r = E_{elec} * l \tag{7}$$

This spending of resources is represented by E_{aj}, and its mathematical representation is Eq.(8), where E_{DA} is the amount of energy required to aggregate a single bit of data. In addition, the supervisor of the cluster consumes energy in order to aggregate the data contributed by the other members of the cluster.

$$E_j^a = E_{DA} * l \tag{8}$$

where E_{DA} - energy consumption while a single bit data is aggregated.

The anticipation of the energy trust The ratio of theoretical energy consumption to actual energy consumption is what determines the value of the te_{ij}^t field for node *j*, which is kept by node *i* in compliance with the energy trust model. It is taken as given that the theoretical energy consumption, which is represented by E_j^{tc}, and the actual energy consumption, which is represented by E_j^{ac}, are one in the same. In order to determine Te_{ij}^t in a manner that will result in $0 \leq Te_{ij}^t \leq 1$, the following formula is used:

$$Te_{i,j}^t = \frac{\min\left(E_j^{tc}, E_j^{ac}\right)}{\max\left(E_j^{tc}, E_j^{ac}\right)}$$

$$E_j^{ac} = E_j^{a-res} - E_j^{a-res'} \tag{9}$$

where

N - cluster members,

E_j^{a-res} - residual energy prior communication,

$E_j^{a-res'}$ - residual energy after a certain communication.

3. PROBLEM STATEMENT

In this section, research develop a system for reducing congestion and improving network quality of service in MANETs, a type of dynamic network that is heavily attacked and presents a significant challenge to improving network performance.

Within the context of this suggested trust management methodology, enhancing the trust assessment scheme and strengthening the safety of mobile ad hoc networks with the assistance of random repeat trust is one of the goals of the approach.

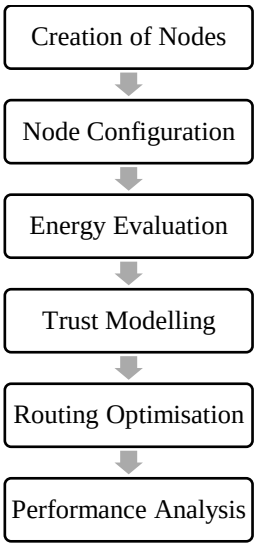

Fig.1. Trust Management Flow Model

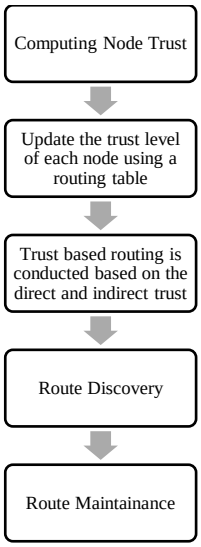

Fig.2. Trust Computation

As in Fig.1, the network gives rise to nodes, each of which is distinguished by a singular identification and is connected to a particular rate of motion. A data transmission is used to investigate the energy assessment that is taking place between the nodes while the energy confidence steps are being carried out. This investigation is conducted while the energy confidence steps are being carried out.

In order to improve the effectiveness of the proposed technique, the random-repeat-trust strategy is put into practice. This is done in order to develop direct and indirect trust computation in order to evaluate trust value for each node by observing node activity and getting trust value from the assessment of neighboring nodes.

This develops direct and indirect trust computation in order to evaluate trust value for each node. The ultimate goal of this evaluation is to identify malicious attacks and to modify the

routing table so that it takes into account the most recent information that is presently available.

A performance study is carried out making use of enhanced quality of service metrics including packet delivery ratio, delay, routing overhead, and detection ratio.

4. PROCESS FOR TRUST COMPUTATION

The Fig.2. provides an illustration of the technique for computing the trust. An explanation of the method that is utilized in order to determine the degree to which a node can be relied in the following Eq.(10):

$$T_{i,j}(t) = W_1 T_{i,j}^{d}(t) + W_2 T_{i,j}^{r}(t) \quad (10)$$

4.1 UPDATE THE NODE TRUST

If the trust-based paradigm that is utilized in MANETs is not routinely maintained and communicated, it will eventually break apart and cause MANETs to fail. It is possible for one to become disconnected from the present group for a variety of reasons, such as the malfunctioning of a link on one of the nodes, an unanticipated occurrence, or the intention to reduce energy consumption. One of the nodes may also intentionally disconnect from the group.

Before being able to forward packets to a particular neighbor node based on its behavior and Quality of Service (QoS) parameters, the sender must first establish the trust value for that particular neighbor node based on the activities that they have both participated in together. In the event that this condition is not met, the sender will be unable to forward messages.

Research suggests a trust-based model in which node levels of confidence are periodically updated following the passage of a predetermined amount of time at regular intervals. This model would be implemented in a way that would allow for periodic updates. It is not difficult to recognize the malicious networks and promptly set up new pathways that are safe and travel to their final destinations.

The steps that need to be taken in order to bring the routing database up to speed with the relationships of new nodes, which you can view here. The subsequent step involves applying the subsequent algorithm in order to compute the overall degree of confidence in the neighbors:

$$N_T = W_1 CFR + W_2 DFR + W_3 E_{Res} + W_4 L_Q + W_5 C_Q \quad (11)$$

An equation can be used to describe the relationship that exists between the total number of data packets that a node has successfully forwarded and the total number of data packets that should have been forwarded. (8). This equation also describes the relationship between the total number of control packets that should have been forwarded and the number of control packets that were successfully forwarded by a node. It is possible to find a solution: $W_1+W_2+W_3+W_4+W_5+W_6=1$ by using the weights W_1, W_2, W_3, W_4 and W_5 in that order.

$$0 \leq W_1\ W_2\ W_3\ W_4\ W_5\ W_6 \leq 1 \quad (12)$$

The technique that was carried out is the only object that has the potential to decide the weight values. In order to provide users with greater flexibility in prioritizing their activities, the QoS settings and MANET applications have been made more restrictive. While this was going on, the actions of neighboring node peers had an impact on how trustworthy they were perceived to be. The confidence threshold was effective in differentiating the trustworthy nodes from the malicious nodes in the network. The routing table is constantly kept up to date with the most recent routing information in order to facilitate the process of building the most effective and risk-free (secure) paths that are possible. This is done in order to protect the network from potential threats. This is done because nodes that are of poor quality and behave in a dishonest manner are marked as malicious.

4.2 TRUST BASED QOS ROUTING

The term confidence in quality of service, abbreviated as QoS, refers to the probability that a specific communication network node transmitted the messages or data precisely as it was intended to do so. The nodes of energy are taken into consideration in the process of establishing the dependability of QoS. The amount of energy that is available at a node is extremely important for the performance of tasks that are connected to quality of service, such as preprocessing and fundamental routing. The movement patterns of a node are what determine its standard of service and trust connectivity, which is another name for its capacity for data-sharing with other nodes in the network.

This is connected to the trust-based ordering of the quality of service, and the words threshold, direct trust degree, and indirect trust degree are all pertinent here. The node that is at the beginning of the chain is required to consult its routing database in order to identify the gateway for the node that is the intended recipient of the data before any data can be transmitted. This must be done before any data can be transmitted.

After a reliable entrance point has been established, data may then be transferred to the location that is ultimately intended for it. If this is not the case, the source node will initiate the process of route discovery by transmitting RREQ packets, which contain a request for a path to the destination node. This will begin the process of finding a route to the destination node.

If the routing table of an intermediate node includes a distrusted node that was determined to be malicious during the process of updating the node trust, then the next hop of the intermediate node will be determined as if it were the destination node for the duration of the routing process. This determination will be made as if the intermediate node were the destination node.

This occurrence takes place when a malicious node is present in the routing database of an intermediate node. The component in question is removed after its original implementation has been completed. The method for finding routes caused the intermediate node to perform this action in order to locate a reliable node to connect to as the next hop in the route. This action was required because the technique for finding routes.

The trust-based quality-of-service routing in MANET should be pursued during the route setup process. This routing method makes use of the recommended method of the Trust Computation Approach for optimized routing. This is something that can be accomplished with the assistance of route optimization. Following the discovery of the final node, the sender node was able to quickly recover its route reply (RREP) through the use of trusted hops. In the event that the seed node delivers more than one RREP, the route that delivers the highest destination sequence

number is selected, and the seed node is promoted to the position of a trusted node in the routing tree. The information is transmitted to the final node using the Random Repeat Trust Approach, which is a trust-based quality of service routing technique. In the event that it is not feasible to establish a data transmission route that is reliable, the processing phases will be carried out multiple times.

4.3 ROUTE DISCOVERY

The first RREQ messages contained the introduction of three new elements; these were the malicious node address, the necessary path trust, and the reverse route trust. The number one is where one should begin when gaining confidence in going rearward. Before the router can send out the RREQ packet, it must first join a multicast group that does not have an incorrect route. This is a prerequisite for sending out the packet. After the RREQ has been transmitted, the message will proceed in the opposite direction in order to reach the responder node as quickly as possible.

The upstream nodes serve as an indicator of which nodes are the most easily approachable. The fact that the reply was closed, on the other hand, provides a strong indication that this server is situated further downstream. The reliability of the node that either initiated the transmission of the message or actually transmitted it is appraised by the node that actually received the message in question.

After the results of a comparison between the trust value of the route and that of the pertinent node have been tallied, the value of the reverse path will be changed to reflect whichever of the two was determined to have a lower score. On the other hand, the RREQ message will not be transmitted if the trust value of the node is lower than the minimal necessary route confidence. This can happen if, for example, the node has a lower level of path reliability.

The RREP messages that are originally transmitted contain an expanded version of one field. If there are n different locations that make up the route that is chosen, then you can use this formula to determine how trustworthy the route as a whole is on average. The algorithm can be broken down as follows:

$$A_{TV} = \frac{\sum_{k=1}^{n} T_v}{n} \tag{13}$$

Each node along the route has a trust value, which is denoted by T_v and can be accessed by clicking on that node. The member of the multicast group who was provided the RREQ is the one who is responsible for sending the RREP back to the server that sent it. This must be done in order for the process to continue.

After the information has been received by the sending node, the sending node will determine the most efficient way to communicate the information on to the subsequent node. It is possible for there to be more than one active route between the parent node and the destination node, despite the fact that there should be no more than one active route in this direction.

The method that is normal for AODV order that the winner must be chosen based on which one is the shortest, and this is how the competition is conducted. Then, having confidence in one another is the single most important action that can be done. The node at its ultimate destination will always select the path that has the highest possible average trust rating in order to guarantee the confidentiality of the data while it is being transmitted.

This is done to keep the data safe. Any node that has not yet received the message will, before activating the path that has received the message, first clear the route from its memory, and then activate the path. This process will continue until all nodes have received the message.

4.4 ROUTE MAINTENANCE

Each individual participant in a multicast group is accountable for the upkeep of their own individual routing table. After composing an address array into a single array that contains all of the malicious nodes, one should then place the address array in a multiplex routing table once the address array has been compiled. When both the formation of the group and the beginning of data transmission have been completed, the upstream node will be in a position to observe the forward actions carried out by the downstream node.

If the upstream node arrives that the downstream node is being malevolent, then it will unicast an RREQ message to the group leader. It is expected that the address of the malicious node will be included in this communication. The communication is first delivered to the group commander, and the captain is also the one who sends the group RREP message in response. The cluster head sends out a hello communication that is transmitted throughout the entirety of the network. The address of the node that has been compromised can be found within this communication.

The completion of the message processing, the malicious address will be added to the routing directory that is maintained by the server that is currently receiving it. After this malicious server has been removed from the multicast group, it will be possible for the remaining participants to reestablish the group and reconnect. The renegade node will not be able to rejoin the group until it has successfully restored its multicast routing table. Until then, it will be unable to participate. After the Threshold time parameter has run its course and reached its endpoint, the routing database will be reloaded, and the confidence value will be reset to 0.5.

4.5 TRUST BETWEEN NODES

A trustworthy relationship is one in which one node recommends another on the basis of first-hand experience or information. Direct observations made between every pair of nodes and recommendations made to *i* about *j* are two crucial elements in the construction of confidence.

4.5.1 Direct Trust Evaluation:

Developing confidence in one ability to interact directly with others requires building a strong foundation of interpersonal relationships. When a node *i* has a high degree of trust in the node *j* that is its neighbor, it indicates that the node i has been able to keep an eye on the node *j* through direct interactions in the past without the need for any mediation from other nodes. This is because the node *i* has been able to keep an eye on the node *j* without the need for any other nodes. The answer to the following equation will indicate the degree to which is direct:

$$T_n^d(i,j)=\begin{cases}T_o^d(i,j)+RF & if\ ST>0\\ T_o^d(i,j)-PF & if\ FT>0\end{cases} \quad (14)$$

The initial degree of confidence, denoted by T_o^d, is compared to the percentage of successful routes, denoted by *ST*, and the percentage of unsuccessful routes, denoted by *FT*, over the course of some amount of time. *ST* stands for successful routes, and *FT* stands for unsuccessful routes.

A reward factor (*RF*) will be awarded to a node if that node has completed a positive number of transactions successfully, and a punishment factor will be awarded to that node if it has completed a positive number of transactions unsuccessfully.

RFs and PFs are both referred to as reward and punishment factors, respectively. As a result, $0 \le PF \le RF \le 1$, while $RF + PF = 1$. Every node in the network has the same number associated with the principal direct trust degree that they have been given.

4.5.2 Indirect Trust Evaluation:

The term indirect trust degree refers to the level of confidence that is bestowed upon a node or collection of nodes on the basis of the recommendations and evaluations offered by other nodes in the network.

The degree to which two nodes, i and k, have comparable judging and recommending abilities to some neighbor node in their trust relationship is expressed by the similarity between those two nodes. This neighborhood node reliability should be evaluated on a case-by-case basis.

A greater similarity level between two nodes i and k indicates that those nodes have the same opinion of and the same ability to recommend that specific node. This is one factor that goes into determining the degree to which a node can be trusted.

For the purpose of determining the degree of indirect confidence, one can use the following expression, which is based on Eq.(15):

$$T^r(i,j)=\frac{\sum_{k\in m} T^d(i,j)*s(i,k)}{\sum_{k\in m} s(i,k)} \quad (15)$$

where *m* - nearest common neighbors with most similarity.

The method that is being described here has a threshold value of 0 as its lowest possible value; the important practical field determines what value should be used for the threshold $\tau \ge 0.6$.

4.5.3 Estimation of the Total Trust:

The total trust assessment takes into account not only the level of trust between nodes but also the level of trust between nodes and RSUs when determining the degree to which the behavior of a node can be relied upon to be accurate. This is done in order to ensure that an accurate evaluation can be carried out. Regardless of whether or not an RSU is present, every node in the network is capable of calculating a total confidence value for every adjacent node j that is within its communication range.

The $T(i,j)$ represents this all-encompassing assessment of conviction in the given information. Nodes are periodically granted historical confidence as well as the in-segment trust of all nodes that are a part of the same segment in order to deter dishonesty and protect the integrity of the network. Nodes are able to acquire an accurate picture of their immediate environment as well as the environment further around them as a result of this.

Even if a node is not in close proximity to an RSU, it is still able to evaluate the other nodes in its immediate neighborhood by looking at the RSU most recent reports as well as the RSU trustworthiness in both direct and indirect ways. This allows the node to make an assessment of the other nodes in its immediate vicinity.

The significance factor can be computed as follows:

$$T(i,j)=\left(1-\frac{t_1}{t_2}\right)\left[\alpha T_n^d(i,j)+\beta T^r(i,j)\right]+\left(\frac{t_1}{t_2}\right) \quad (14)$$

where t1 is the time at which the report was received, t2 is the time at which the calculation is being performed, and t1/t2 is the ratio of the two periods. Because of this, one is able to calculate the level of trustworthiness that can be placed in a particular automobile. Because both and are considered to be weighted variables, the computations show that $\alpha + \beta = 1$. This is because $\alpha > \beta$ and are both considered to be weighted variables.

5. EXPERIMENTAL ANALYSIS AND DISCUSSION

In order for a node to be considered normal, the success rates of its communication, message (including identification and data), and energy interaction must be higher than 80%. On the other hand, the success rates of a node that is behaving abnormally will be lower than 80%.

Research build the system in such a way that all normal nodes will unfailingly have a trust grade of three or higher, whereas all unnormal nodes will, with the exception of the first round, always have a trust grade of less than three. This is to ensure that the system functions as intended. The simulation parameters are given in Table.1.

Table.1. Simulation Parameters

Parameter	Value
Nodes Distribution	Random
Network Coverage	(0, 0) ~ (100, 100) m
Base Station Location	(50, 100) m
Nodes	200
Node initial energy	1 J
E_{DA}	50 nJ/bit
E_{elec}	50 nJ/bit
ε_{amp}	10 pJ/bit/m^2
Broadcast packet	200 bits
Data packet	4000 bits

Table.2. Accuracy of Detection of Various Attacks

Approach	Probe (%)	DoS (%)	R2L (%)	U2R (%)
SVM Trust	97.66	97.32	83.94	85.66
ANN Trust	96.12	95.12	80.12	84.96
Fuzzy Trust	80.55	95.55	95.15	92.75

At the 10th round, it is assumed that a node is continuously under attack from blackholes, data attacks, selfish behavior, and on-off attacks; these attacks have an approximate attack rate of 50% and are intended to disrupt communication, messages, energy, and mixtures, respectively.

In this situation, it is believed that a node is being subjected to a continuous attack from blackholes, data attacks, selfish behavior, and on-off attacks. After 10 rounds have been completed, the node presently possesses a trust value and its score is given in Fig.3.

Despite their high sensitivity to malicious attack, they do not demonstrate the tolerance of our technique to abnormal environments, so additional observation is required. This is the reason why there is a requirement for additional observation.

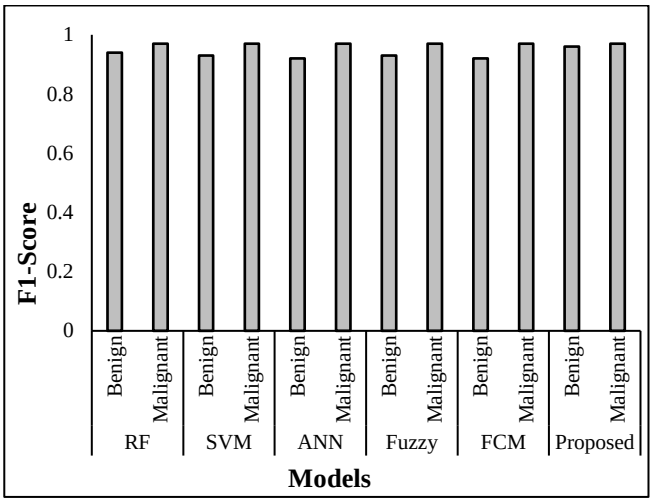

Fig.3. F1-Score

Even if a node has been subjected to repeated attacks, which have resulted in a decrease in its trust rating, and consecutive rounds have passed, it is not completely impossible for the node to be removed from the network.

6. CONCLUSION

In order to accomplish sensitivity to numerous attacks, the method builds mathematical models for the communication factor, the message factor, and the energy factor. These factors can influence the confidence value of sensor nodes. Because of this, the method can be vulnerable to numerous types of attacks. In the end, research calculate the ultimate trust cloud while giving as much weight as feasible to the recommendation trust cloud. This makes the network more resistant to the effects of unexpected occurrences, making it more reliable.

REFERENCES

[1] R. Sabitha, V. Anusuya and V. Saravanan, "Network Based Detection of IoT Attack Using AIS-IDS Model", *Wireless Personal Communications*, Vol. 98, pp. 1-24, 2022.

[2] N. Khandelwal and S. Gupta, "A Review: Trust based Secure IoT Architecture in Mobile Ad-hoc Network", *Proceedings of International Conference on Applied Artificial Intelligence and Computing*, pp. 1464-1472, 2022.

[3] V. Thirunavukkarasu, and P. Prakasam, "Cluster and Angular based Energy Proficient Trusted Routing Protocol for Mobile Ad-Hoc Network",*Peer-to-Peer Networking and Applications*, Vol. 15, No. 5, pp. 2240-2252, 2022.

[4] J. Singh and S. Sakthivel, "Energy-Efficient Clustering and Routing Algorithm Using Hybrid Fuzzy with Grey Wolf Optimization in Wireless Sensor Networks", *Security and Communication Networks*, Vol. 2022, pp. 1-13, 2022.

[5] Y. Wang and L.C. Kho, "Towards Strengthening the Resilience of IoV Networks-A Trust Management Perspective", *Future Internet*, Vol. 14, No. 7, pp. 202-215, 2022.

[6] J. Kuriakose and A.K. Bairwa, "EMBN-MANET: A Method to Eliminating Malicious Beacon Nodes in Ultra-Wideband (UWB) based Mobile Ad-Hoc Network", *Ad Hoc Networks*, Vol. 140, pp. 103063-103076, 2023.

[7] S. Ayed and L. Chaari, "Blockchain and Trust-Based Clustering Scheme for the IoV", *Ad Hoc Networks*, Vol. 140, pp. 103093-103108, 2023.

[8] Y.H. Robinson, V. Saravanan and P.E. Darney, "Enhanced Energy Proficient Encoding Algorithm for Reducing Medium Time in Wireless Networks", *Wireless Personal Communications*, Vol. 119, pp. 3569-3588, 2021.

[9] N. El Ioini and C. Pahl, "Trust Management for Service Migration in Multi-Access Edge Computing Environments", *Computer Communications*, Vol. 194, pp. 167-179, 2022.

[10] M. Kandasamy and A.S. Kumar, "QoS Design using Mmwave Backhaul Solution for Utilising Underutilised 5G Bandwidth In GHz Transmission", *Proceedings of International Conference on Artificial Intelligence and Smart Energy*, pp. 1615-1620, 2023.

[11] N.M.M. Hiraide and N. Yoshida, "Trust Management in Growing Decentralized Networks", *Journal of Computations and Modelling*, Vol. 12, No. 3, pp. 1-12, 2022.

[12] J. Kundu and S. Pal, "Trust-Based Efficient Computational Scheme for MANET in Clustering Environment", *Proceedings of International Conference on Mathematical Modeling and Computational Science*, pp. 305-314, 2022.