Journal of Education for Pure Science- University of Thi-Qar
Vol.13, No.3 (Sept.2023)
Website: jceps.utq.edu.iq Email jceps@eps.utq.edu.iq

DOI: http://doi.org/10.32792/utq.jceps.10.01.01

Affective Approach for Routing Attack Detection for Ad- hoc Mobile Networks Based on Trust Model

Intisar N. manea [1], Intisar.neamah@stu.edu.iq

Lubna Najah Rasoul [2]

[1] Department of Acoounting Techniques, Thi-Qar technical College, Southern Technical University, Thi-Qar Iraq,

[2] Directorate General of Education in Thi Qar, Iraq lubna.n.rasol@utq.edu.iq,

Received 16/7/2023, Accepted 16/8/2023, Published 21/9/2023

Abstract:

The mobile adhoc network is highly dependent on the energy parameter of the mobile nodes, it suffers from different threats wich target the service performance of thed network. The packets transferred through intermediate nodes are subject to attack and the routing informationhas become a subject for malicious threats. In this paper a trust model is presented based on the computation of different parameters to improve the performance of intrusion detection in mobile adhoc network. The trust model computes the direct trust between different agents. Similarly the method computes the indirect trust which is propagated by the direct trust which is computed between third party. The method monitors the network and stores the logs about the data packet being forwarded. At each time when a node has a packet it performs neighbor discovery and route discovery. Then for each route the method compute the trust weight and each intermediate node has been verified for its location factor. Based on trust weight computed the method selects an efficient forwarding neighbor to send the data packet.Finally the method computes the recommendation trust between different agents to perform intrusion detection. Using all these measures the method performs intrusion detection on the mobile adhoc network.

Keywords: Routing Attack Detection, Trust Model, Ad hoc Mobile Networks

1. Introduction

A collection of mobile nodes that are dynamically connected to one another via a wireless media is known as a mobile ad hoc network (MANET). When a packet is sent from the source to the destination in the network, there are numerous security and performance measures that are lacking. Given that it is a growing methodology globally. Further derivations include the VANET, iMANET,

and SPANs. Many researchers have proposed various MANET models, however each of them has one flaw that can either be categorized as security or performance [1].

This paper introduces the recommendation trust verification model. The method performs trust verification in two ways. One in the direct trust method which uses the previous transmission details to verify the trust. The method verifies the trust using a third party. The cluster manager performs the third party trust verification and produces a better performance in secure routing.

2. Literature Review

Various reputation and trust models have been put out in recent years to improve security in MANETs and allow nodes to assess their neighbors either directly or through recommendations from other nodes in the network. The issue of dishonest suggestions has received considerable attention in the proposed models, but finding efficient solutions to minimize or lessen its impact is still a challenge for MANETs.

Buchegger and Boudec [2] handles the issue of dishonest suggestion using personal experience method. The received recommendations are subjected to a deviation test, and those that surpass the cutoff point are disregarded. Based on the outcomes of the deflection test, the reputation value of the suggestion node is updated. The only information transmitted between nodes is the negative recommendation, which the model cannot stop from being published [3].

Propose CORE model, which only accepts positive recommendations from others, write Michiardi and Molva [4]. As a result, the system's efficiency may suffer since nodes cannot share negative network experiences with those who are acting inappropriately.

Additionally, because it leaves room for misbehaving nodes to coordinate and receive unfairly high ratings, CORE cannot be resilient to ballot-stuffing attacks. For self-policing mobile ad hoc networks, Wang et al. [5] propose a trust-based incentive model to mitigate the influence of erroneous recommendation on the accuracy of trust value. The effectiveness of the methodology is not evaluated against particular attacks like disparaging remarks, though.

Propose RFSTrust, a trust model based on fuzzy recommendation similarity, which is presented to quantify and evaluate the trustworthiness of nodes, write the authors in [6]. To assess the node-to-node recommendation linkages, they employ similarity theory. That is, the evaluation between the two nodes is more constant the more similar the evaluating and recommending nodes are to one another. When selfish nodes attack, only one specific scenario is taken into account in this model; other assaults relating to recommendation are not examined to see how well it performs.

In [7], Soltanali et al. suggest a trust paradigm to promote inter-node collaboration through direct observation and recommendation. This model solely takes into account a node's most recent opinion, which is sent to a reputation manager system at the conclusion of each interval. Only taking into account the most recent opinion is not insightful enough to detect changes in a node's behavior, such as in an on-off attack [8].

Li et al. in [9] add a confidence value in their evaluation by combining two values: trust and confidence into a single value termed trustworthiness in an effort to boost the honesty of applying recommendations. They use the trustworthiness rating to give recommendations weight, giving more weight to recommended nodes with higher trustworthiness values. This work does not take into

account collusion attacks that result in fraudulent suggestions, which may result in improper evaluation of the recommendations that were given [10]. Using an additional parameter known as an acceptability threshold (in relation to the confidence level), Hermes [11] is a recommendation-based trust model. In order to verify that sufficient observations of the behavior of participating nodes have been acquired, the concept of acceptability is applied in the computation of recommendation. However, choosing acceptability involves making a trade-off between getting a more precise trustworthiness value and the time needed to get it. Pedro B. et al. [12] propose the recommendation exchange protocol (REP) to enable nodes to submit and receive recommendations from nearby nodes. It presents the idea of mature relationships based on the length of time nodes have been acquainted. Long-term associate recommendations are given more weight than recommendations from short-term associates. The length of the relationship is the only characteristic used to determine the maturity of the relationship. In [13], Yu et al. suggest using a clustering technique to separate reliable recommendations from unreliable ones. By choosing the cluster with the most suggestions as the most reliable, they apply the majority rule. They put their concept to the test against various assaults, including defamation and vote-rigging. However, majority rule might not be effective since some nodes might band together to launch an attack and not be truthful in their assessments of other nodes.

3. Mobile Ad hoc Networks

Adhoc has two definitions-the first is "imprompt" or "using what is on hand," while the other is "for one specific reason." Unconnected wireless mobile nodes that establish a temporary network without a stable transportation network are called mobile ad-hoc nodes. The mobile nodes linked by wireless links that are free to move a routers at the same time [14].

MANETS were sponsored by DARPA and known as "small package radio networks" in the early 1970s. These initial systems were built by BBN Technologies and SRI Global for tests. Jerry Burchfield, Robert Kahn, and Ray Tomlinson, subsequently famous for TENEX, the Internet, and email, were experimenters. The fact that these early packet radio systems existed before the Internet and contributed to the development of the distinctive Internet Protocol suite is interesting to note. The Survivable Radio Network (SURAN) project was a part of a DARPA experiment that was conducted later in the 1980s. With the introduction of affordable 802.11 radio cards for a personal computer in the mid-1990s, a third wave of academic activity was already underway [15].

JTRS and NTDR are two examples of current MANETS that are designed largely for military utility. The alternative method simply manages wireless device traffic within a single local "cloud" of devices. Each node sends and receives data, but does not route any information among the systems in the network. However, several IEEE ad-hoc networks are combined into MANETS using higher-level protocols [16,17].

Figure 1 is an example of an ad hoc network design without a predetermined topology. Each mobile node in this network performs the dual roles of host and router, passing packets to other mobile nodes that might not be directly within wireless transmission range of any given node. Because all nodes can roam and can join via dynamic network topologies, the wireless non-infrastructure network does not have a fixed router [18, 19].

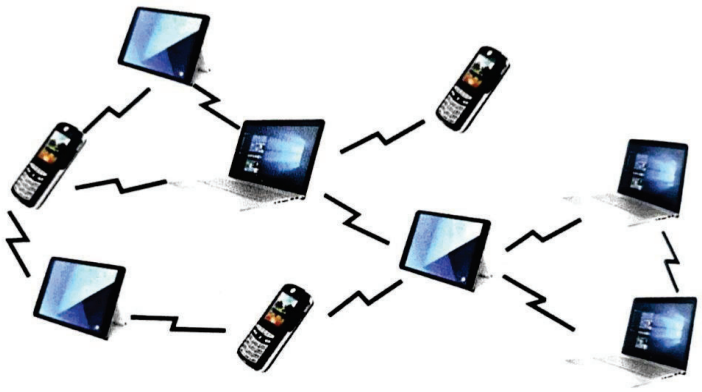


Figure 1 AdHoc network

4. Security in MANET

In MANET, physical security is barely present. The two types of attack are active attack and passive attack. Passive attacks, which include eavesdropping and in-sequence reveal, are the most frequent sanctuary problems. Active attacks include data alteration by viruses, Trojans, and worms, as well as service failure. Other glaring issues with mobile adhoc networks include channel and node sensitivity, complicated black holes, and Byzantine wormhole attacks. Attacks that could introduce inaccurate routing information and network traffic redirection that results in ineffective manufacturing routing are further security concerns. There are several ways to lessen the impact of these attacks, including the use of digital signatures and prior trust connections, safe direction-finding utilizing public and private keys to obtain a documentation authority, and many others [20].

Due to the extremely dynamic nature of ad-hoc networks and in opposition to the need to function effectively on too little funding, counting network bandwidth and the CPU dispensation capacity, memory, and battery power of each entity node in the network, secure informal network routing protocols are challenging to design. Existing self-conscious ad hoc network routing protocols are typically greatly optimized to extend new routing quickly when circumstances change, necessitating a faster and more frequently shared routing protocol barrier between nodes than what a typical network would require. Expensive and challenging security measures may slow down or thwart such associations of routing in sequence, which will reduce routing efficiency. They may also consume extraneous complex or node resources, which will create numerous new opportunities for potential Denial-of-Service attacks from end to end routing protocols [20].

5. Proposed Model to Filter Dishonest Recommendation Attacks

The mobile adhoc network consists of number of nodes and each node has no restriction in their mobility and no limit for their speed. Each node can perform source routing as they select their own way of forwarding the data pocket. The nodes of the mobile adhoc network perform cooperative data transmission. The route discovery process is first carried out by the source node to determine the options for getting to the destination. When the delay is greater, the route finding is done at each phase of the data transfer. The route request is sent by the source node to its neighbors, and it is then sent to all other nodes in the network. A node with the link creates the route reply to the so node

when it receives the request packet. The source node receives numerous route replies from its neighbors in a similar manner.

It can determine the list of routes that are available based on the route requests it receives from its neighbors. The source node chooses the best path to take while transmitting data to the destination node. The network accomplishes routing based on a variety of factors; for instance, if the network uses shortest path routing, it chooses the route with the fewest hops possible. The source node delivers the data packet through the first neighbor toward the distinction after choosing the route. The source node believes the chosen path to be the shortest one. If there are no malicious nodes on the route, it receives acknowledgement as soon as feasible and transmits data at the highest throughput. Real-world conditions, however, are more complicated since there might be a hostile node in an intermediate site who is engaged in various routing assaults.

This section analyses different routing attacks possible presents a solution for them. Figure 2 shows the A model of the network topology containing 21 numbers of nodes. The source node has been marked as 1 and the destination node is 10.

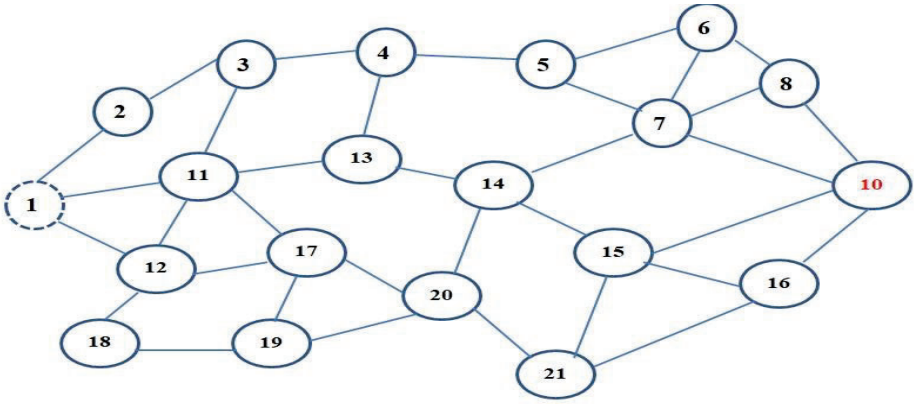


Figure 2 A model of the network topology

There are several intermediate nodes along the route that the source node found. The source node looks to confirm the effectiveness of the intermediary nodes in data transfer after determining the path. Not every node on the route would use the exact routing and would participate in various attacks. Verifying the reliable nodes is hence more crucial. In this scenario, the source node would gather data regarding the transmission that the intermediate node was participating in.

The source node would generate a control message to collect the transmission details of each intermediate node to collect the strategy of the nodes. The source node would expect the transmission involved, number of transmissions performed successfully, the average latency occurrence and number of drops occurred and so on.

If there is a malicious node while collecting the information about the intermediate nodes, it would send false information and strategy about the other nodes in an intension to select it as the forwarding route. The first neighbor would also send false information about the transmission involved and so on.

The neighbor node would send false information about the possible residual energy on the other way. Each node loses some energy at each transmission but when the neighbor node claims the energy it would send wrong information about the energy parameter. Similarly the route identified in

the previous routing would have a link failure. However, if the source node chooses the same route for data transmission, the intermediate node would conceal the connection failure when the verification is carried out. This causes the network to experience packet drops or greater delay.

The trust of the nodes is measured based on various parameters and there are a number of methods used to verify the trustworthiness of the nodes.

5.1. Trace Based Trust Management

To check whether a node in a mobile ad hoc network can be trusted, the following transmission trace is employed. The general block diagram of a trace-based trust management system is shown in Figure 3.

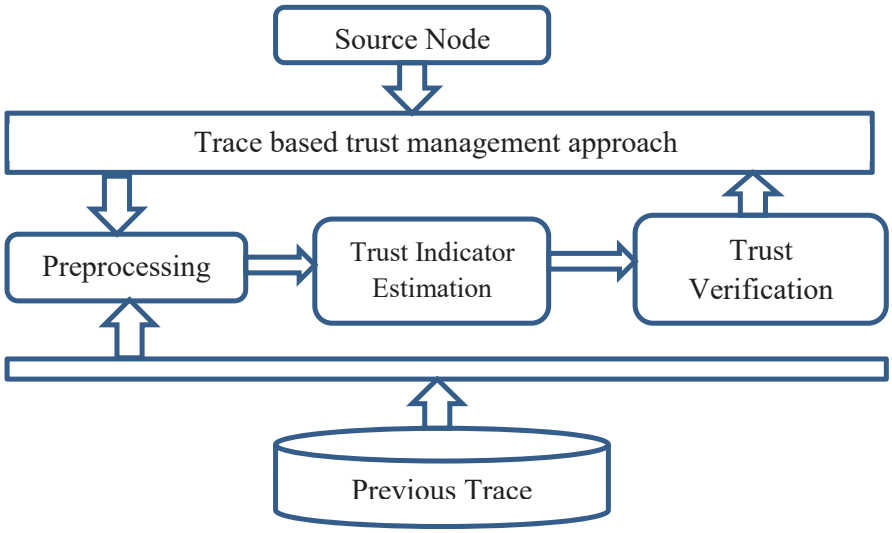


Figure 3 Block diagram of trace based trust management system

5.1.1. Preprocessing

In this stage, the method collects the trace from the previous trace maintained by different intermediate nodes. The technique separates the trace obtained from involvement by the node under consideration. To calculate the trust measure, one uses the separated trace.

5.1.2. Trust Indicator Estimation

The trust indicator shows how effective the node is at transmitting data. Based on the previously recorded traces, the trust metric is calculated. The approach determines how many data transmissions are carried out by each node. The node also makes an estimate of how many deliveries or completions were successful. These specifics are used to assess the trust factor.

5.1.3. Trust Verification

In this stage, based on the estimated trust indicator the method decides if the node or the entire route is suitable for data transmission. The trust indicator is estimated for all the nodes of the route. The route has been selected for data transmission based on the trust verification.

Each node keeps a record of the nodes involved in the data transmission as well as the preceding transmission. The prior data transfer trace is used to calculate the node's trustworthiness.

5.2. Location Based Trust Management

The location information is used to perform trust management in most cases. The node would gather the position data of the intermediate nodes after choosing the path. Based on the nodes' locations, the trust measure's node information is estimated. The general block diagram of location-based trust management is shown in Figure 4.

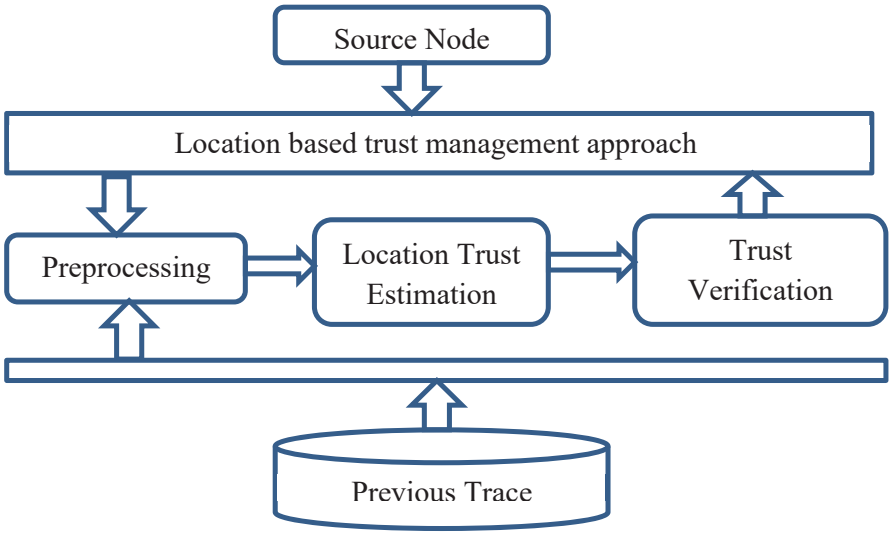


Figure 4 Block diagram for location based trust management

5.2.1. Preprocessing

The source node creates a location collection request for the chosen route at this point. The nodes in the route respond with their current location upon receiving the request. After receiving the response, the source node determines the nodes' locations.

5.2.2. Trust Indicator Estimation

The node maintains the previous trace about the location of the nodes. The location information is fetched from the received reply. Using both the location information, the location approximation is performed, a as each node is subject to move in certain direction and in different speed. It cannot be located in the same location and it also cannot be located as the neighbor for the same node. Using this information, the location approximation is performed.

5.2.3. Trust Management

Based on the outcome of the location trust measure, the approach assesses the trust of the nodes present in the chosen route. The route is not chosen if the location trust measure is insufficient for any of the intermediate nodes.

5.3. Energy Based Trust Management

When the network performs energy efficient routing, then the malicious node sends false information about its energy. Further a malicious node would recommend a false route which has low energy bound. The energy based trust management is performed to avoid this.

The general block diagram of the energy-based trust management strategy is shown in Figure 5.

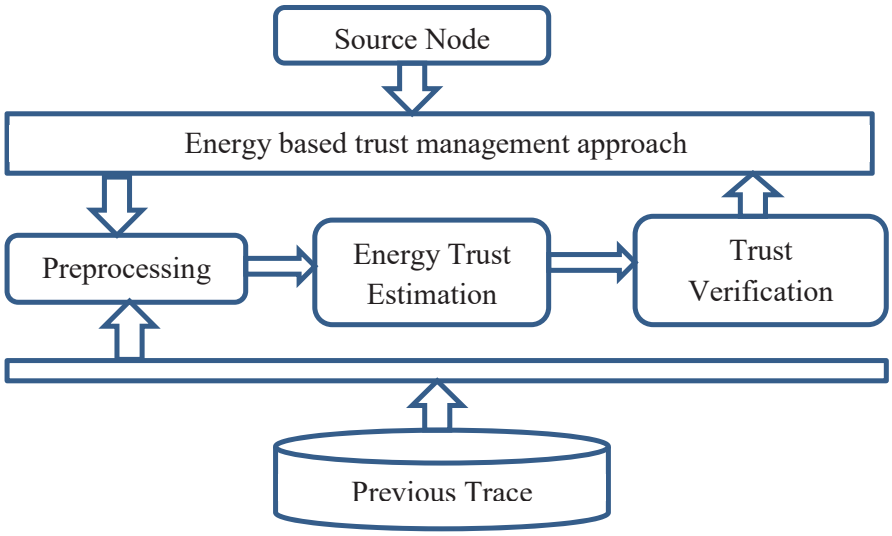


Figure 5 Block diagram of energy trust management

5.3.1. Preprocessing

In this stage, the method collects various information from the intermediate nodes. The node sends the transmission request intermediate node which in turn sends the details about the transmission involved. All of the data regarding the transmissions taking place at other nodes is gathered by the source node.

5.3.2. Energy Trust Measure

Based on the previously gathered traces, the algorithm determines the number of transmissions involved. Because a node loses energy with each data transmission, the approach estimates the trust measure using the number of transmissions involved. The trustworthiness of the route is confirmed using computed energy trust measure.

5.3.3. Trust Verification

The computed energy trust measure has been used to verify the trust of the route. The trust measure is estimated for all the nodes of the route and based on the measure estimated the route is selected or avoided for data transmission.

5.4. Trust Model Based On Recommendation

The recommendation-based methodology employs two distinct approaches. The method begins by estimating both direct and indirect trust. With the aid of the cluster manager, the trust is validated. The cluster manager keeps track of the nodes' level of trust. The recommendation is sent by the source node to the cluster manager, who then validates it and delivers the findings back to the source nodes. In order to facilitate effective trust formation, the protected DTN routing method uses the iTrust model, a probabilistic misbehavior detection scheme. Figure 6 shows the general block diagram of the recommendation based trust model and its functional components.

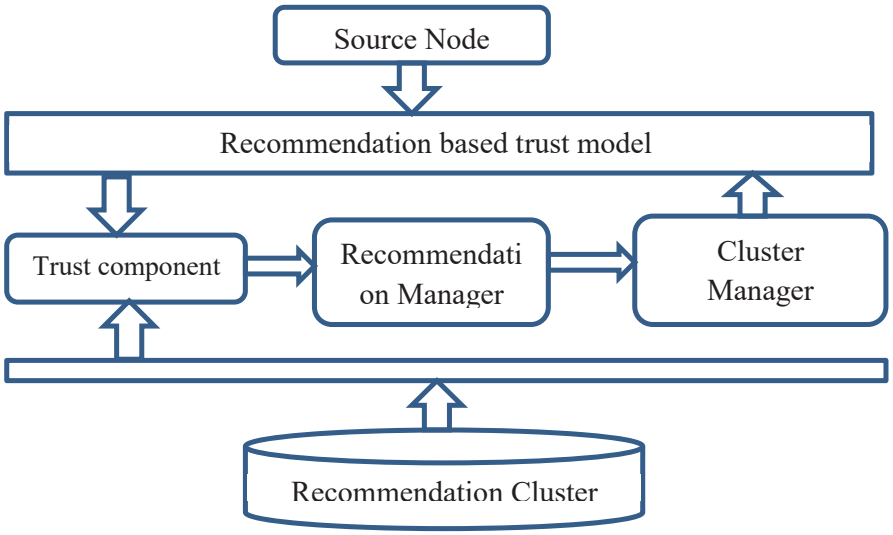


Figure 6 Block diagram of proposed trust model

The basic concept behind the iTrust-based approach is the addition of a trusted authority (TA) that is periodically accessible in order to forecast node behavior based on gathered routing data and probabilistically verifying the node.

5.4.1.Trust Component

The trust has been estimated in two ways as direct and indirect. The direct trust is measure based on the previous communication information. The method maintains the previous information about the transmission and using the previous information the method estimates the trust. The number of transmission involved and number completed in success is considered to estimate the direct trust. The direct trust measure is estimated using this information.

5.4.1.1.Direct Trust Algorithm:

Input: Previous Trace

Output: Direct Trust Measure.
Read the previous traces
Compute direct trust measure D tm = Ts / Tt
Tt - Count Number of transmission involved
Ts - Count Number of successful transmission.

5.4.1.2.Unreliable Trust

Trust may be transferred via third parties. A can trust Y to some extent, for instance, if B shares with A its trust opinion (i.e. suggestion) about Y and A and B have mutually created a relationship of recommendation trust. Trust propagation is the name of this phenomenon. Through trust propagations, indirect trust is created. Indirect trust is mainly determined by two variables. The first is the availability of recommendations and who can provide them.

5.4.2. Recommendation Manager

The proposed filtering method takes into account the evolving MANET properties. To lessen the impact of the same node's bad behavior over time, the honesty of suggesting nodes is reviewed over time. Deviated ratings can be removed from the list of suggestions using dynamic clustering over time.

5.4.3. Cluster Manager

The cluster manager groups the records and when the method receives the recommendation request, it verifies the trusts based on the cluster available.

5.4.3.1. Cluster Manager Algorithm:

1. Initialize:
    - **a.** Initialize node memory(in packet)
    - **b.** Initialize the update timer
2. Send request for allocate replica
3. If node selfish
    - **a.** Give wrong reply or no response]
4. If not
    - **a**. Send correct reply

5. If reply is received by originator
- **a**. Process the reply
- **b**. And make the route

6. If timer is triggered
- **a**. Send the query for checking

7. If node is correspond node then sends the query reply

8. Originator checks the query reply
- **a**. And forms the SCF tree
- **b**. And allocates priority and replica according to the tree

The network's selfish nodes are removed with the aid of the aforementioned method based on the node's early determined trust value.

The existing system has the following drawbacks:

1. The mobile node has a low trust value associated with packet forwarding and may face poor channel conditions at a specific location.
2. Environmental changes may cause an incompetent creature to become competent.

A concept called the iTrust model, which compares the detection techniques of two malicious nodes, is created to get over this issue. Only direct and indirect trust are utilized in the first way. Direct, indirect, and recommended trust are all applied in the second scenario. The proposed filtering method takes into account the evolving MANET properties. To lessen the impact of the same node's bad behavior over time, the honesty of suggesting nodes is reviewed over time. Deviated ratings can be removed from the list of suggestions using dynamic clustering over time.

6. Results and Discussion

The recommendation based trust model computes the direct and indirect trust for each request and recommendation is generated. A trust weight is computed to perform intrusion detection based on the values. The method has produced the following results. Figure 7 shows the snapshot of sending the message from the source to a particular destination.

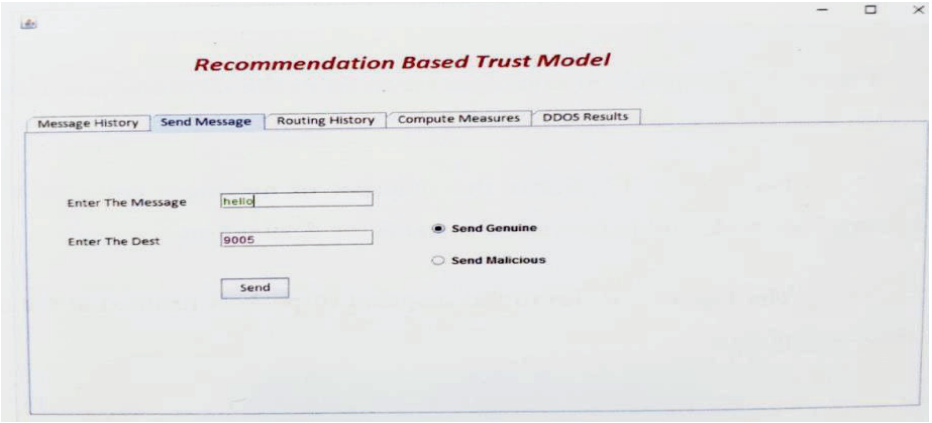
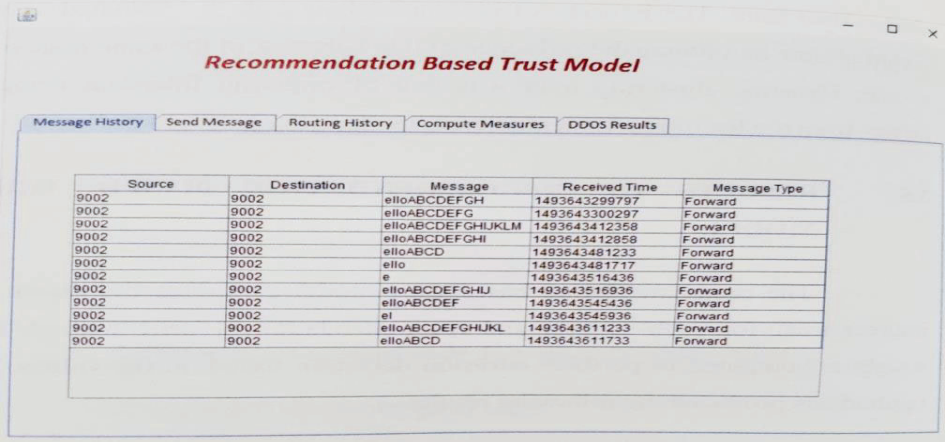


Figure 7 shows the snapshot of sending the message

Figure 8 shows the snapshot of messages collected in the intermediate node and is forwarded towards the destination.



Source	Destination	Message	Received Time	Message Type
9002	9002	elloABCDEFGH	1493643299797	Forward
9002	9002	elloABCDEFG	1493643300297	Forward
9002	9002	elloABCDEFGHIJKLM	1493643412358	Forward
9002	9002	elloABCDEFGHI	1493643412858	Forward
9002	9002	elloABCD	1493643481233	Forward
9002	9002	ello	1493643481717	Forward
9002	9002	e	1493643516436	Forward
9002	9002	elloABCDEFGHIJ	1493643516936	Forward
9002	9002	elloABCDEF	1493643545436	Forward
9002	9002	el	1493643545936	Forward
9002	9002	elloABCDEFGHIJKL	1493643611233	Forward
9002	9002	elloABCD	1493643611733	Forward

Figure 8 Snapshot of messages received in the intermediate node

Figure 9 shows the snapshot of packets handled at the route discovery phase.

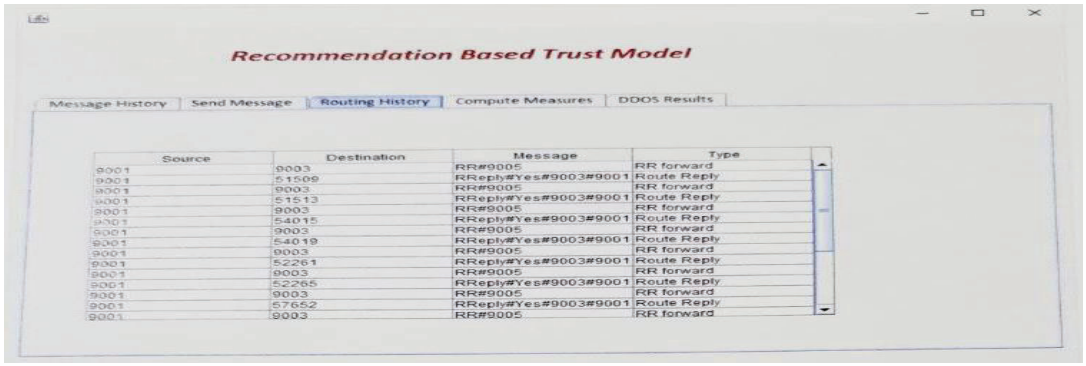


Figure 9 Snapshot of packets handling and routing history

Figure 10 shows the result of packets received in the destination and the received packet features are displayed in the interface.

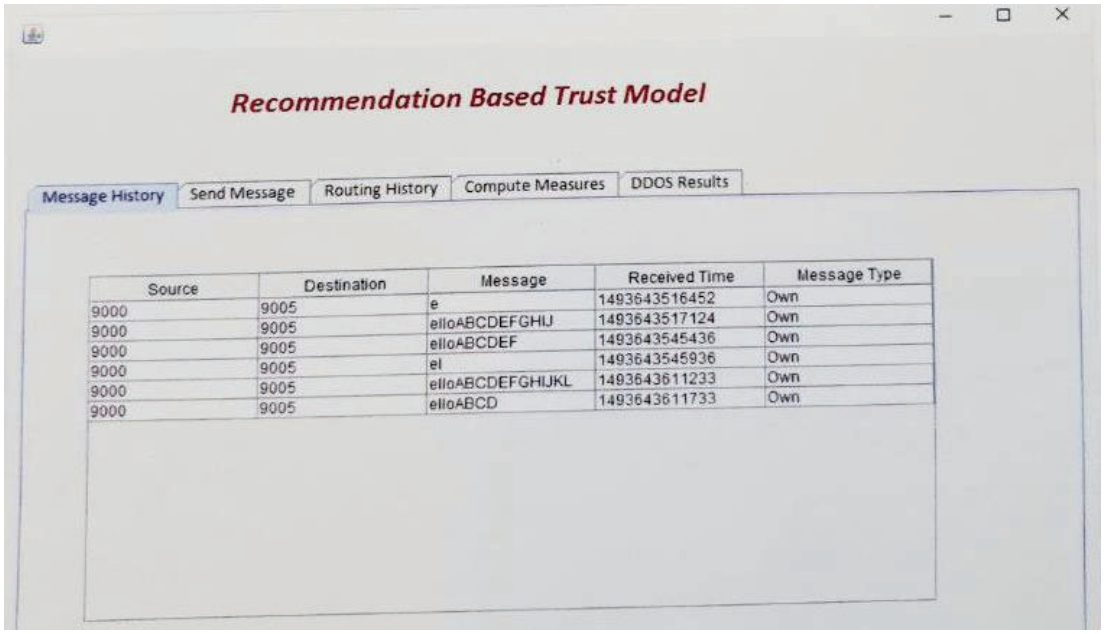


Figure 10 Result of packet reception in the destination

Figure 11 shows the result of packet features extracted in the destination and used to measure the trust.

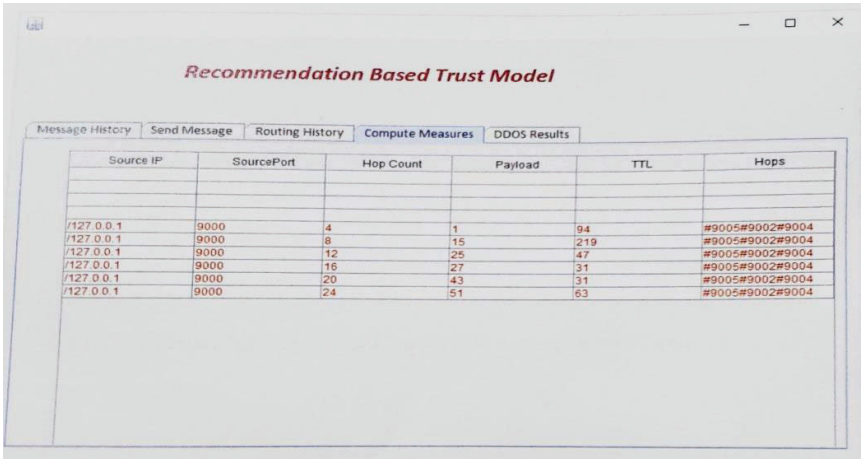


Figure 11 Result of features extracted in the destination

Figure 12 displays the outcome of intrusion detection, and the approach computes the direct and indirect trust measures for each packet received. Based on the trust measurements, the approach calculates the trust weight for the packet that was just received. Based on the derived trust weight, the approach distinguishes between malicious and genuine packets.

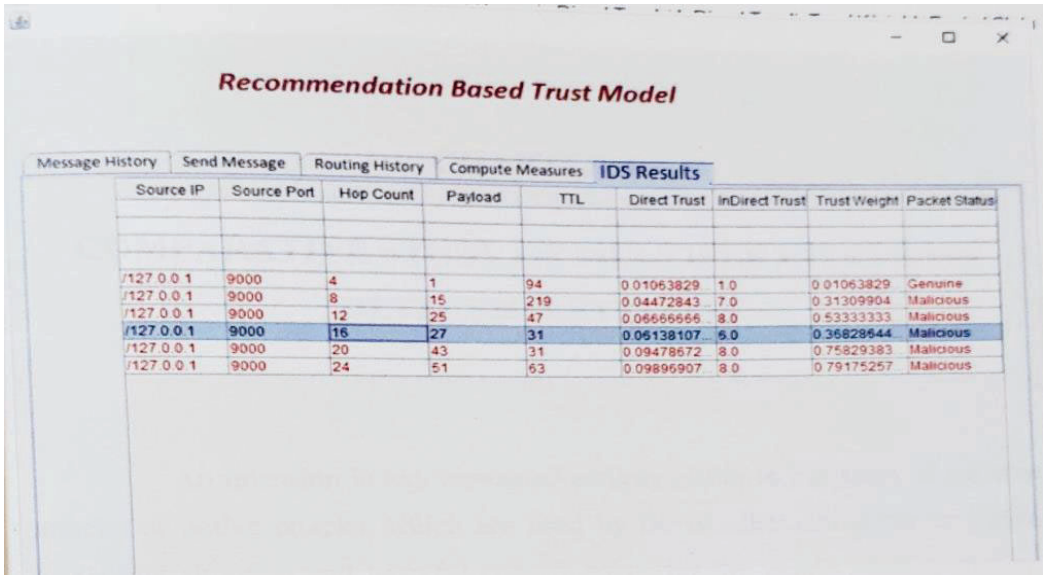


Figure 12 Result of intrusion detection

7. Conclusion and Future Scope

The modern mobile adhoc network is extremely accessible via a variety of gadgets, including mobile, PDA, and other devices. Independent of their location, mobile users use their smartphones to access numerous network services. In order to meet the needs of the users, the adhoc network must perform better across a range of criteria. However, a number of threats that are generated by some malicious nodes and present in the network have been detected. Maintaining the performance criteria depends on being able to spot such malicious activities.

The energy parameters of the mobile nodes have a significant impact on the performance of the mobile ahdoc network. The mobile nodes' energy is impacted and lost on pointless routing. These pointless routing attempts are the result of hostile nodes doing routing assaults. By providing fraudulent routing information, the authentic node expends energy transporting the data packet through an incomplete or inefficient route. Several techniques have been discussed by various researchers to recognize these routing assaults and to enhance performance. However, the majority of them struggle to deliver the necessary performance when identifying routing attacks.

As a result of the authors' presentation of a trust model that is calculated based on various parameters, the performance of intrusion detection in mobile adhoc networks is improved. The trust model calculates the level of direct trust between various agents. Similar to how direct trust between third parties is calculated, indirect trust between third parties is also computed using this method. The approach then calculates the recommended trust between various agents to carry out intrusion detection. The approach detects intrusions on the mobile adhoc network by employing all of these measures.

8. References

[1] H. Khalfaoui, A. Farchane, S. Safi, Review in authentication for mobile ad hoc network Advances on Smart and Soft Computing, Springer (2022), pp. 379-386.

[2] S. Buchegger and J.Y. Le Boudec, ‘’A Robust Reputation System for P2P and Mobile Ad hoc Networks,’’ Proc. P2PEcon’04, 2004.

[3] H. Li and M. Singhal, ‘’Trust management in distributed systems,’’Computer, 40, (2), pp. 45-53, 2007.

[4] P. Michiardi, and R. Molva, ‘‘Core: A COllaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks,’’ Communications and Multimedia Security Conference, pp. 107–121, 2002.

[5] K. Wang, M. Wu, and S. Shen, ‘‘A trust evaluation method for node cooperation in mobile ad hoc networks,’’ Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on, pp. 10001005, 2008.

[6] J. Luo, X. Liu, and M. Fan, ‘’A trust model based on fuzzy recommendation for mobile ad-hoc networks,’’ Computer Networks, 53, (14), pp. 2396-2407, 2009.

[7] S. Soltanali, S. Pirahesh, S. Niksefat, and M. Sabaei, ‘‘An efficient scheme to motivate cooperation in mobile ad hoc networks,’’ Networking and Services, 2007. ICNS. Third International Conference on, pp. 98-98, 2007.

[8] Y. Yu, K. Li, W. Zhou, and P. Li, ''Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures,'' Journal of network and computer applications, 35, (3), pp. 867-880, 2012.

[9] R. Li, J. Li, P. Liu, and J. Kato, ''A Novel Hybrid Trust Management Framework for MANETs,'' Distributed Computing Systems Workshops, 2009. ICDCS Workshops' 09. 29th IEEE International Conference on, pp. 251-256, 2009.

[10] J.-H Cho, A. Swami, and R. Chen, "A survey on trust management for mobile ad hoc networks,'' Communications Surveys & Tutorials, IEEE, 13, (4), pp. 562-583, 2011.

[11] C. Zouridaki, B.L. Mark, M. Hejmo, and R.K. Thomas, ''E-Hermes: A robust cooperative trust establishment scheme for mobile ad hoc networks,'' Ad Hoc Networks, 7, (6), pp. 1156-1168, 2009.

[12] P.B. Velloso, R.P. Laufer, D. de O Cunha, O.C.M. Duarte, and G. Pujolle, ''Trust management in mobile ad hoc networks using a scalable maturity-based model,'' Network and Service Management, IEEE Transactions on, 7, (3), pp. 172-185, 2010.

[13] H. Yu, S. Liu, A.C. Kot, C. Miao, and C. Leung, ''Dynamic witness selection for trustworthy distributed cooperative sensing in cognitive radio networks'', Communication Technology (ICCT), 2011 IEEE 13th International Conference on, pp. 1-6, 2011.

[14] MA. Azer & Saad NGED, 'Prevention of Multiple Coordinated Jellyfish Attacks in Mobile Ad Hoc Networks', International Journal of Computer Applications, vol. 120, no. 20, pp. 12-20, 2015.

[15] M. Bahekmat, MH. Yaghmaee, ASH. Yazdi & S. Sadeghi, 'A novel for detecting sinkhole attacks in WSNs', International Journal of Computer Theory and Engineering, vol. 4, no. 3, pp. 418-421, 2012.

[16] V. Balakrishnan, V. Varadharajan, UK. Tupakula & P. Lues. TEAM: Trust Enhanced Security Architecture for Mobile Ad-hoc Networks', 15th IEEE International Conference on Networks, ICON, pp. 182-187, 2007.

[17] V. Balakrishnan, V. Varadharajan, UK. Tupakula & P. Lues. TEAM, 'Trust Integrated Cooperation Architecture for Mobile Ad-hoc Networks', 4th International Symposium on Wireless Communication Systems. ISWCS, pp. 592-596, 2007.

[18] T. Bhatia & AK. Verma, Simulation and Comparative Analysis of Single Path and Multipath Routing Protocol for MANET Anveshanam - The Journal of Computer Science and Applications, vol. 2. no. 1. pp. 30-35, 2013.

[19] T. Bhatia & AK. Verma, QoS Comparison of MANET Routing Protocols, International Journal Computer Network and Information Security, vol. 9, pp. 64-73, 2015.

[20] R. Bhuvaneswari, N. Balamalathy, S. Premalatha, V. Manimozhi, S. Parvathi & A. Kumaresan. An Improve Performance, Discovery and Interruption of Sybil Attack in MANET, Middle-East Journal of Scientific Research, vol. 23, no. 7, pp. 1346-1352, 2015.