Journal of Innovative Engineering and Research (JIER)
Vol.- 5, Issue -2, October 2022, pp. 30-33 (4 pages)

Machine Modified Approach of Trust Evaluation Process for Data Transmission in MANET

PROLAY GHOSH[1], DR. NISARG GANDHEWAR[2]
[1,2]*Department of Computer Science & Engineering, Dr. A. P. J. Abdul Kalam University, Indore 452016*
Correspond Author Email: prolayghosh.jis @gmail.com

Abstract— MANETs are a kind of wireless network in which a range of migratory nodes are wirelessly connected without the need of fixed networks. Numerous attacks or intrusions may occur in MANETs as a consequence of the presence of hungry or malicious nodes transferring data from one mobile node to another. Vulnerability occurs in MANETs' mobile nodes where an attacker node rapidly captures the network's traffic flow. As a result, an Intrusion Detection System (IDS) is needed to protect MANET from assaults. IDS implementation in MANET enables the monitoring of all network activity and the production of alerts for the control station to take appropriate action in the case of an attack. Additionally, MANETs employ important cryptographic methods to block attacker nodes, thereby improving the network's security and enabling efficient data transmission. This research paper gives comparative evaluation of several trust evaluation process for Intrusion Detection system in MANET. This research paper also focus on modified approach for multidimensional trust evaluation model for MANET.

Index Terms— MANET, Malicious Node, Intrusion Detection, Trust, Reputation.

I. INTRODUCTION

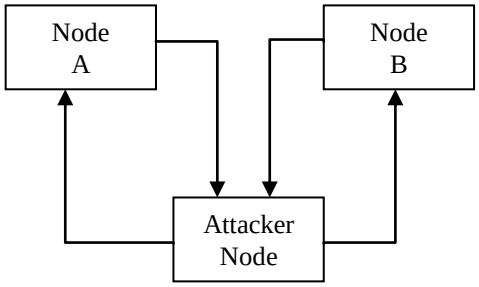
An autonomous wireless network called mobile ad-hoc network are made up of wireless nodes that can connect with one another without the assistance of access points equipment. Secure communication is a difficult problem with MANET because of the lack of permanent infrastructure, changeable topology and others. Data Protection is a mandatory need in mobile ad hoc network compared to wired networks. Because there is no reliable centralized authority and there are few resources available, MANETs are more susceptible to security assaults. In a MANET, nodes can connect directly with one another when they are within each other's wireless communication ranges, but nodes that are outside of each other's reach must rely on other nodes to forward information.

To keep an environment for ad-hoc networks stable and secure, five fundamental security goals must be addressed. They are:

Confidentiality: Preventing the disclosure of any information to undesired parties. This is particularly challenging in ad hoc networks as intermediate nodes receive
data packets for other destinations and can readily eavesdrop on the info being relayed.

Availability: Services ought to be provided whenever needed. There should be a guarantee of resilience in the face of a DoS attack. Attackers can deploy jamming strategies on the physical and media network access layers to impede communication on the physical channel. The attacker can interrupt the routing protocol at the network layer. Authentication: Assurance that a source of communication is who or where it says it is. Without which a hacker might pretend to be a node and acquire access to resources and sensitive data without authorization while interfering with the functionality of other units.

Integrity: Never is a message in transit changed. Non-repudiation: This guarantees that neither the sender nor the recipient may ever claim not to have sent or received the message.



A hacker tries to change or manipulate the data being transmitted over the network. It might prevent networks from operating normally. In an active attack, the attackers can manipulate the packets, inject them, drop them, or exploit a variety of network features to initiate the attack.

1)Wormhole Attack: In this approach, a hacker tunnels packets from one site in the network to another while recording them at the first location. Wormhole refers to this tunnel created by two attackers that are working together.

2) Black hole attack: A black hole is a suspicious node that uses the routing protocol to promote itself as having the shortest and fastest route to a destination while actually responding fraudulently to route discovery without having an active route there. By showcasing the shortest route, source station initiates sending data through the malicious node an it become the effective element in the route.

Routing based on trust management is used to limit a variety of attacks, including wormhole, black-hole,
denial_of_service, and selfish assaults.

II. RELATED WORK

To choose the shorter path as the data transmitting path that accurately assured the propagation of data packets while

analyzing method based on forecast rules and on terminals historical understanding, the trust predication model (TSR), also known as source forwarding protocol based on trust, was developed by Hui Xia et al [1]. By measuring its trust with the black-trust list's threshold, the watching node adds neighbors it believes to be malicious nodes to its black list. In this scenario, numerous loop-free routes are launched from a source in a single routing path, and each route receives a computed value made up of a counting based on hop and a path trust factor. A destined node responded with the most reliable paths to the sender that met the necessary conditions for trust.

Ahmed M. El-Haleem et al [2] established a approach based on trust, in which the score taking into account the trust component, which consists of direct as well as indirect trust and collaboration score based on the probability density function, is used to determine the link between various nodes. The algorithm used the know how to control end-to-end protocol affirmation and data link layer affirmation as tools to observe how nodes changed the value of neighbor trust from definite to indefinite depending on how they transmitted data to their neighbors and how they handled data packet losses. In order to define precisely trustworthy and untrusted nodes to route via the misbehaving node, cooperation score is employed to determine the selfishness conduct of a suspected node and confine the allowed degree of node harmful activity. To increase the security of MANETs, a modelled trust management method using uncertain reasoning is used by Zhexiong Wei et al [3]. By combining the methodology used for direct and indirect observation and evaluating trust value, security is obtained. With the use of Bayesian inference and the entire probability model that will be shown via direct approach, the trust value of an unit is produced using the direct analysis technique. Utilising Dumpster to facilitate indirect observation while taking into account the observed node's neighbours. To confim the presence of a malicious node in a data transmission path, a mechanism has been suggested by Abdalla et al. [4] for which Route validation information (PVM) and Route validation message Acknowledgement (PVMMB) are delivered. Attacker Finder information (AFM) and Attacker Finder information Acknowledgement (AFMB) are applied to determine the address of a malicious node if one is found. Attacker Isolation Message (AIM) alerts the matching node associated with that address, isolating it from the rest of the network. Boukerch et al. proposed a scheme called novel agent-based trust and reputation management (ATRM) [5]. It's important to consider the bandwidth and latency overhead while using this method. This plan's main goal is to maintain trust and reputation regionally with the least amount of administrative burden. Jia et al. [6], suggested a trust mechanism, which is multiple route reactive routing protocol, known as ad hoc on-demand trusted multi-path (AOTMDV) routing protocol in [8]. It offers a flexible method for selecting shortest path that satisfies packet transmission security criteria. On the basis of numerous in-the-moment studies, the impact of the suggested mechanism in identifying the vulnerable nodes is assessed. Xia et al. [7], introduced a trust assumption model to determine a node's trustworthiness based on the node's past behaviour as well as its anticipated future behaviour utilising extended fuzzy logic principles. Adnane et al. [8], developed reputation specification languages and demonstrated how each node can assess the behaviour of other nodes using trust-based reasoning. After identifying the malfunctioning nodes, the proposed method takes required action to eliminate the inconsistency and encounter the suspicious nodes. For key exchange in MANET, an effective broadcast encryption algorithm is adopted Cipher text attack (CCA). Here information exchange is not needed to establish a group key [8]. Novel trust-based technique for AODV is proposed in [12]. a trust model that takes mobility and frequency of cooperation into account when evaluating a neighbor's direct trust. A new technique called trust-based logic in the nodes is provided to reduce the vulnerabilities of the OLSR protocol. [10, 12]. Fuzzy reasoning and dynamic adaptive FPNs are used in a knowledge-based training and representation approach described in [14, 15]. Security models which combat different security facts have been proposed in [16]. The system's ability to survive is critically poor due to so few fish nodes. A trust-based strategy is suggested in [17].

III. PROPOSED TRUST EVALUATION PROCESS

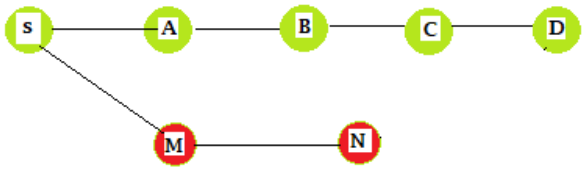


Figure 1.

Figure1 explains the need of Trust value in data transmission. S is the Source and D is the Destination. To start the route discovery, the source node will transmit a request (RREQ) message to the network. A middle node will respond to the source node with an RREP if it has routing information for the end node in its route cache. When an RREQ packet is transmitted to a node, the device adds its address details to the route log. The addresses of each intermediary node along the route might be known when the destinations is provided with the RREQ. Despite the fact that there is no live path to D, Node M sends an early fake RREP to S asking for routing. Here, we suggest a trust management method to help the source node choose a reliable node for forwarding and
The Trust value is categorized in two part-

Face to face Trust value (T_f):

Every will monitor the behavior of neighboring nodes. Every node will broad cast Hello message to its neighboring nodes, upon receiving the message neighbor nodes will rebroadcast the message. The source node will receive the message back from the active neighbor nodes.

T_f = (No of Packet Received) / (No of Packet Sent)

Face to face trust value will be within the range of 0-1. All nodes in the cluster will be assigned with a face to face trust value and all nodes will maintain a table containing trust values of its neighbor nodes.

Journal of Innovative Engineering and Research (JIER)
Vol.- 5, Issue -2, October 2022, pp. 30-33 (4 pages)

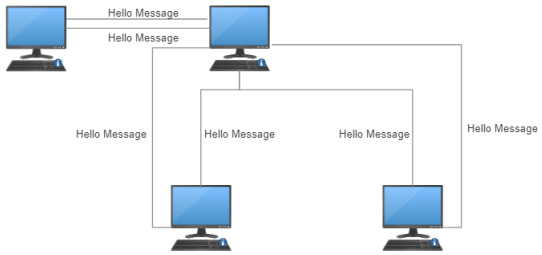


Figure 2:

Table 1:

Trust Table	
Current Id: 11	
Neighborid	**T_f**
3	0.8
25	0.7
31	0.7

Social Trust value:

Apart from face to face trust value Social trust value is also considered. In this proposal we have considered following components for Social Trust value.

1. Packet forwarding ability
2. Node Battery
3. Participation in Networks Activity
4. Packet Forwarding Queue Length

Parameters	Trust Factor
Packet forwarding ability	• Increase P_a after every successful packet forwarding up to a maximum value • Decrease P after every packet drop up to a threshold value
Node Battery	P_b=BatteryPercentage /10
Participation in Networks Activity	• P_c will increase after each control packet is initiated. • P_c will decrease if control packet is droped.
Packet Forwarding Queue Length	P_d will increase if queue empty>30% P_d will increase if queue empty<30%

Social Trust value is calculated depending on the parameter wise trust factor.

$$T_s=(P_a+P_b+P_c+P_d)/4$$

Table 2:

	P_a	P_b	P_c	P_d	T_s
Current Id: 3	1	0.7	0.8	0.6	0.7
Current Id: 25	0.5	0.3	0.5	0.4	0.4
Current Id: 31	0.6	0.8	0.7	0.5	0.6

Average Trust Value (T_{av}) = (T_f +T_s)/2

Table 3:

	T_f	T_s	T_{av}
Current Id: 3	0.8	0.7	0.75
Current Id: 25	0.7	0.4	0.55
Current Id: 31	0.7	0.6	0.65

Trust Manger will maintain the table of Average Trust value

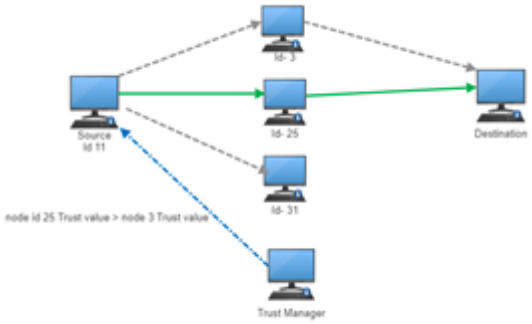


Figure 3:

Source node to Destination route travel through node 3 and node 25. Now the Trust Manager will guide the source node about the suitable and reliable path by analyzing the Table of Average trust Value. The node with higher trust value will be selected and node with less trust which can be a malicious node value will be eliminated. After the packet forwarding Trust values will be recalculated depending on the parameters.

IV. RESULTS & ANALYSIS

This proposed method has been compared with existing trust-based method mainly focusing on three parameters i.e. Execution time, Packet Loss rate and Intrusion detection rate.

Table 4:

	Execution Time (in ms)	
Number of nodes	**Existing Approach**	**Proposed Approach**
50	15.9	14.2
100	18.2	15.8
150	21.2	18.3
200	24.3	19.6

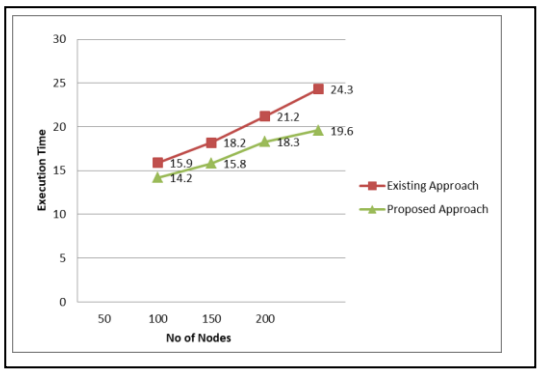


Figure 4:

Table 5:

	Packet loss rate (%)	
Number of packets	**Existing Approach**	**Proposed Approach**
10	26	16
20	29	19
30	33	23
40	34	27

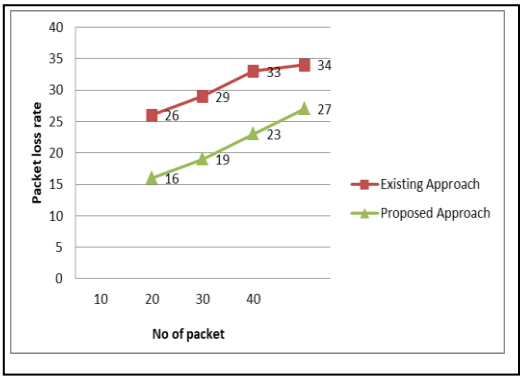


Figure 5:

Table 6:

	Rate of Intrusion Detection (%)	
Number of nodes	**Existing Approach**	**Proposed Approach**
50	62	72
100	64	78
150	65	81
200	68	85

V. CONCLUSION

The results of this investigation show that trust value directly affects packet transmission. In this research, a method for determining trust value has been developed in which social characteristics as well as face-to-face trust value have been given weight. Because trusted nodes are included in the path, this method has a lower packet loss rate. This method enhances the rate of intrusion detection by giving less weight to nodes with lower trust levels when choosing them for the route. However, it has also been noted that the trust values frequently vary as a result of the nodes' mobility. The nodes' mobility may also be taken into account when determining the trust value.

REFERENCES

1. Xia, Hui, ZhipingJia, Xin Li, Lei Ju, and Edwin H-M. Sha. "Trust prediction and trust-based source routing in mobile ad hoc networks,Ad Hoc Networks 11, no. 7, pp. 2096-2114, 2013.
2. El-Haleem, Ahmed M. Abd, Ihab A. Ali, Ibrahim I. Ibrahim, and Abdel Rahman H. El-Sawy. "Trust model for TRIDNT trust based routing Protocol", 2nd International Conference on Computer Technology and Development (ICCTD), pp. 538-544, IEEE, 2010.
3. Wei, Zhexiong, Helen Tang, F. Richard Yu, Maoyu Wang, and Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning", 2014.
4. Abdalla, A.M., Saroit, I.A., et al.: Misbehavior nodes detection and isolation for MANETs OLSR protocol. Procedia Comput. Sci. 3, 115–121 (2011) [5] Boukerch, A., Xu, L., El-Khatib, K.: Trust-based security for wireless adhocand sensor networks. Comput. Commun. 11, 2413–2427, 2007.
5. Xia, H., Jia, Z., et al.: Impact of trust model on on-demand multi-path routing in mobile ad hoc networks. Comput. Commun. 36, 1078–1093 (2013) [7] Xia, H., Jia, Z., et al.: Trust prediction and trust-based source routing in mobile ad hoc networks. Ad Hoc Netw. 11, 2096–2114, 2013.
6. Adnane, A., Bidan, C., de Sousa, R.T.: Trust based security for the OLSR routing protocol. Comput. Commun. 36, 1159–1171, 2013.
7. Clausen, T., Dearlove, C., Jacquet, P., Jia, Z.: The Optimized Link State Routing Protocol Version 2, IETF RFC7181, pp. 1–115, 2014.
8. Yang, Y.: Broadcast encryption based non-interactive key distribution in MANETs. J. Comput. Syst. Sci. 80, 533–545 2014.
9. Obaidat, M.S., Woungang, I., Abdalla et al.: A cryptography based protocol against packet dropping and message tampering attacks on mobile ad hoc networks. Secur. Commun. Netw. 7, 376–384, 2014.
10. Feng, R., Che, S.: A credible routing based on a novel trust mechanism in ad hoc networks. Int. J. Distrib. Sens. Netw. 2013.
11. Adnane, A., et al.: Autonomic trust reasoning enables misbehavior detection in OLSR. In: Proceedings of the 2008 ACM Symposium on Applied Computing, pp. 2006–2013, 2008.
12. Huang, M., Lin, X., Hou, Z.W.: Modeling method of fuzzy fault Petri nets and its application. J. Central South Univ. (Sci. Technol.) 44, 208–215, 2013.
13. Liu, H.C., Liu, L.: Knowledge acquisition and representation using fuzzy evidential reasoning and dynamic adaptive fuzzy Petri nets. IEEE Trans. Cybern. 43, 1059–1072, 2013.
14. Abdelaziz, A.K., Nafaa, M., Salim, G.: Survey of routing attacks and countermeasures in mobile ad hoc networks. In: 15th International Conference on Computer Modelling and Simulation (UKSim), pp. 693–698, 2013.
15. Cho, J.H., Chen, I.R.: On the tradeoff between altruism and selfishness in MANET trust management. Ad Hoc Netw. 11, 2217–2234, 2013.
16. Verma, S., Gujral, M.: Formal specification of trusted neighbor information base of OLSR routing protocol of adhoc network using Z language. In: Krishna, P.V., Babu, M.R., Ariwa, E. (eds.) Global Trends in Computing and Communication Systems, pp. 560–570. Springer, Heidelberg 2012.