An Improved Trust Based Approach For Detecting Malicious Nodes in MANET

Nachammai. M[1], Dr. N. Radha[2]

[1]Research Scholar, Department of Computer Science (PG), PSGR Krishnammal College for Women
Coimbatore - 641004, India

[2]Assistant Professor, Department of Computer Science (PG), PSGR Krishnammal College for Women
Coimbatore - 641004, India

Abstract — *Mobile ad hoc network (MANET) is an infrastructure-less network of mobile devices connected wirelessly. MANET is used widely today because of its nature as self configuring, easy to move independently in any directions. MANET acts like a router and therefore changes its links to other devices frequently. Due to its nature MANET has been used in various applications like Military applications, Wireless Sensor Network and so on. As its infrastructure-less and dynamic nature, it is highly affected by various attacks like black hole attack, gray hole attack, DoS attack and many collaborative attacks. Hence security is the main challenge in MANET. Many existing work has done on the basis of detecting attacks by using various approaches like Intrusion Detection, Bait detection, Cooperative malicious detection and so on. But this Trust based approach mainly focuses on detecting the malicious nodes on the trusted path than the shortest path as discovered by using DSR mechanism.*

Keywords — *MANET, Collaborative attacks, DSR and Trust based approach.*

I. INTRODUCTION

Mobile ad hoc network (MANET) is wireless network consists of mobile nodes, that communicates with each other node while moving without any base stations. Mobile devices present in this network moves independently and therefore often modify its link to other devices. It contains peer-to-peer, self-forming, self-healing network. In MANET each mobile device acts as both host and router. It is a kind of wireless ad hoc network where the mobile devices cooperate and forward messages from one node to another node.

A. Types of MANET

- Vehicular Ad hoc Networks (VANETs) are used for communication among vehicles and between vehicles and roadside equipment.
- Internet based mobile ad hoc networks (iMANET) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal adhoc routing algorithms don't apply directly.
- Intelligent vehicular ad hoc networks (In VANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents, drunken driving etc.

MANET becomes more popular after the growth of laptops and 802.11/Wi-Fi wireless networking. Many academic works evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Hence different protocols are then evaluated based on measures such as the packet drop rate, overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

II. LITERATURE REVIEW

Vishvas Haridas Kshirsagar et al. [1] proposed trust based solution to packet drop attacks in MANET, the main contribution of the work is to differentiate the trusted node and untrusted node for detecting malicious node by using AODV protocol. The energy and trust can also be calculated for differentiating an altruism and selfish node. The process of separating the trusted list can be done on the basis of acquiring route request and route reply.

S.Aravindh et al. [2] proposed a trust based approach for detection and isolation of malicious nodes in MANET, in which it states the overview of trust calculated in MANET. The proposed solution gives trust value for each and every node presented in routing called trust counter value. If the trust counter value falls below the range of threshold value then those node will be considered as a malicious node and also will be isolated from the whole network for increasing the performance of the network.

Kamini Singh et al. [3] proposed a trust based approach for detection and prevention of wormhole attack in MANET. The main aim of this work is to detect and to prevent the wormhole attack based on cluster based counter-measure for the wormhole attack that alleviates this kind of attacks and effectively mitigates the wormhole attack in MANET. By using this method the malicious node was detected efficiently on the basis of rate of packet dropping compared to threshold value. Then the detected malicious nodes are excluded from the routing process of data transfer.

Sangeeta Bhatti et al. [4] proposed a novel algorithm approach for detection of sybil attack in MANET, the main aim of this work is to propose an identity verification and resource based algorithm for the detection and elimination of Sybil nodes or spoofing nodes. They proposed a technique, which generates the unique identification generated by the base server during the time of registration of the node in the network to lead a secure communication network with the detection of Sybil nodes.

A. Jayanand et al. [5] proposed a trust based collaborative attack detection in MANET, in which they proposed a detection scheme to detect and to prevent collaborative attacks based on clusters formation of neighbor nodes with a monitor node at its 1 hop neighbor. The monitor node is chosen by using an ADCLU algorithm which consider the willingness and trust value of a node for isolating the detected malicious nodes.

Ji Guo et al. [6] proposed a new trust management framework for detecting malicious and selfish behavior for Mobile Ad hoc Networks, they proposed a new trust management framework (TMF) which calculates a node's trust value based on observations from neighbor nodes by using Grey theory and Fuzzy sets. The TMF has shown good performance in calculating trust values under the normal and abnormal attacking conditions. By using TMF technology they not only detects the selfish nodes but also detects the strategy of the attacker or selfish node.

Hisham Dahshan et al. [7] proposed a trust based threshold revocation scheme for MANETs in cryptographic revocation method based on using master private key. And the proposed scheme enables a group of legitimate trusted nodes to perform fast revocation of a nearby misbehaving node. Hence it just switched from central trust to distributed trust which enables the MANETs suitable for stationary and high mobility networks.

Bo YANG et al. [8] proposed a Dempster-Shafer Evidence theory based Trust management strategy against cooperative black hole attacks and gray hole attacks in MANETs. The main contribution of this work is to detect both the cooperative black hole and gray hole attack by using Dempster-Shafer (D-S) evidence based theory. In order to detect single black hole and collaborative black hole attacks, NNOM (Neighbor Nodes Observation Model) and neighbor recommendation trust model (NRTM) is used along with direct trust value and indirect trust value.

N. Bhalaji et al. [9] proposed a dynamic trust based method to mitigate gray hole attack in mobile ad hoc networks, in which a new trust based routing protocol was proposed and analyzed. For monitoring the network behavior each node calculates the trust value and association status for all its neighboring nodes. After this the trust model will be integrated into Dynamic Source Routing protocol in MANET to mitigate the identified attacker nodes from the routing process.

Priyanka Takalkar et al. [10] proposed a trust based secure data communication in MANET, the main work concentrates on creating a multi-route routing protocols which enables secure and accurate delivery of transmitted data. Thereby an efficient route to the destination is calculated as a weighted average of the trust value of the nodes in the route. Secure routing can be done by using security algorithm in the route discovery process.

Bhimsingh Bohara et al. [11] proposed an analysis and prevention of effects of gray hole attacks on Routing Protocol in MANET, in which it states Intrusion Detection Systems (IDs) is very useful to detect the misbehaving nodes in the route. The main aim of this work is to provide security, authentication and confidentiality by means of using AODV routing protocol.

III. METHODOLOGY

Mobile ad hoc networks have been used widely because of its open nature and infrastructure less property. MANET is highly used in many fields like military crisis operations, emergency preparedness and response operations. In a MANET, each node not only works as a host but can also act as a router. For instance, the presence and collaboration of malicious nodes in the network may disrupt the routing process leads to malfunctioning of the network operations. Detecting the malicious node becomes serious issues in MANET. Hence to detect the malicious nodes a trust value should be calculated for each and every node in the routing process. Then specific Threshold value should be kept, to see the range of trust values. That is, if the trust value is less than the threshold value range then those nodes involving in the routing will be ignored. If the node's trust value exists below the specific range then those node will be considered as malicious node. And the simulation parameter was tabulated along with different set of values. Thereby DSR protocol is used and trust values are calculated for each and every node which participates in routing. Based on the trust value the malicious node was detected and will be ignored in further routing strategy.

Table I Simulation parameters

Parameter	Value
Protocol	DSR
Transmission Range	250m
Packet size	512 bytes
Transmission rate	15kbps
Transferring mode	Unicast
Pause time	10 s
Maximum speed	20 m/s
Simulation time	1000 s
Number of nodes	50
Simulation Area	1000m * 1000m
Movement	Random waypoint

For each and every node the trust value should be created, based on this trust value range the node which lies below 0.5 is considered as malicious nodes and it will be ignored in the routing process. After detecting the malicious nodes in the identified path, an alternate path will be provided.

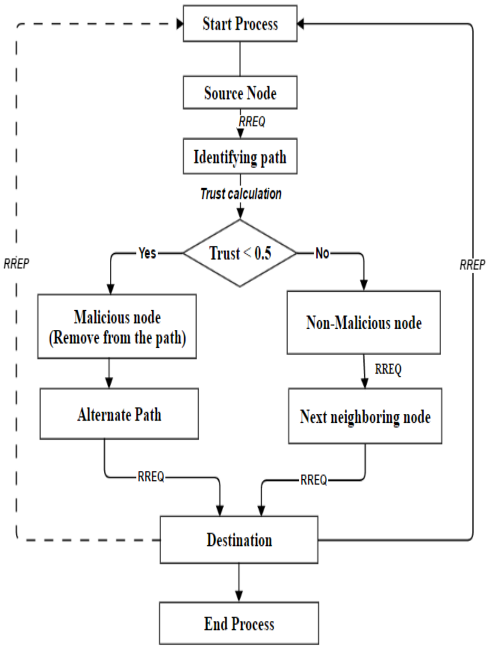


Fig. 1 Overall Framework of an improved trust based approach

A. *Trust Calculation*

Trust values can be calculated for each and every node based on the ratio of number of packets dropped by number of packets forwarded by that neighboring node. This method is evaluated by using DSR (Dynamic Source Routing) protocol.

Formula for calculating trust value:

$$T=1-D/F \qquad (1)$$

where,

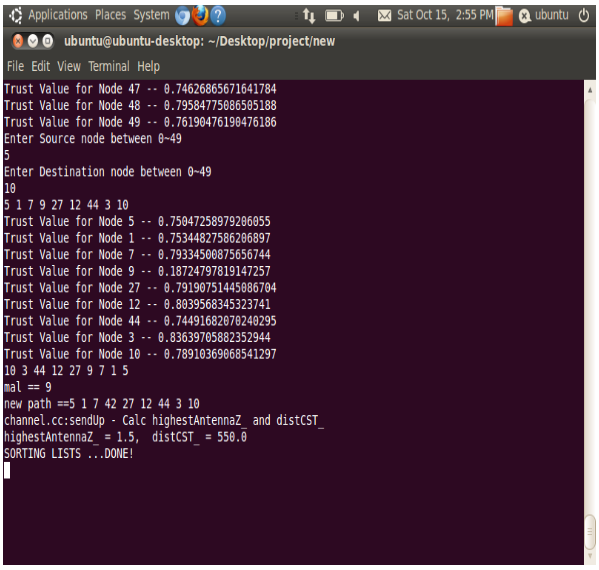
T represents Trust value

D represents Number of packets dropped by a node which should be forwarded

F represents Number of packets to be forwarded to that node which should be forwarded further to another node

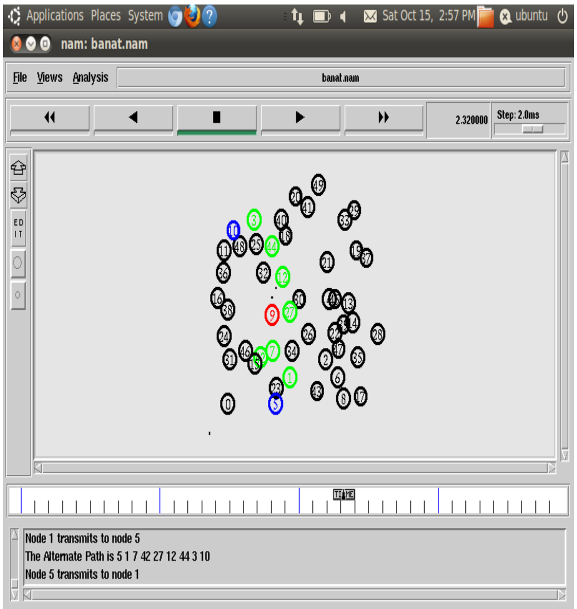
IV. EXPERIMENTAL RESULTS

The proposed system is evaluated in the Network Simulator 2.34 version. The simulation work is done in the Network Animator tool (NAM). The proposed system mainly concentrates on detecting and preventing collaborative attacks based on trust value concept. The performance of the system will be compared with some parameters called packet delivery ratio and end to end delay.


Applications Places System
Sat Oct 15, 2:55 PM
ubuntu
ubuntu@ubuntu-desktop: ~/Desktop/project/new
File Edit View Terminal Help

```
Trust Value for Node 47 -- 0.74626865671641784
Trust Value for Node 48 -- 0.79584775086505188
Trust Value for Node 49 -- 0.76190476190476186
Enter Source node between 0~49
5
Enter Destination node between 0~49
10
5 1 7 9 27 12 44 3 10
Trust Value for Node 5 -- 0.75047258979206055
Trust Value for Node 1 -- 0.75344827586206897
Trust Value for Node 7 -- 0.79334500875656744
Trust Value for Node 9 -- 0.18724797819147257
Trust Value for Node 27 -- 0.79190751445086704
Trust Value for Node 12 -- 0.80395683453237410
Trust Value for Node 44 -- 0.74491682070240295
Trust Value for Node 3 -- 0.83639705882352944
Trust Value for Node 10 -- 0.78910369068541297
10 3 44 12 27 9 7 1 5
mal == 9
new path ==5 1 7 42 27 12 44 3 10
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
```

Fig. 2 NAM window result showing the trust value calculation for the identified path



Node 1 transmits to node 5
The Alternate Path is 5 1 7 42 27 12 44 3 10
Node 5 transmits to node 1

Fig. 3 NAM window output showing the alternate path by removing detected malicious node

1) Packet delivery ratio

Packet delivery ratio is calculated as, the ratio of number of packets received by the number of packets sent.

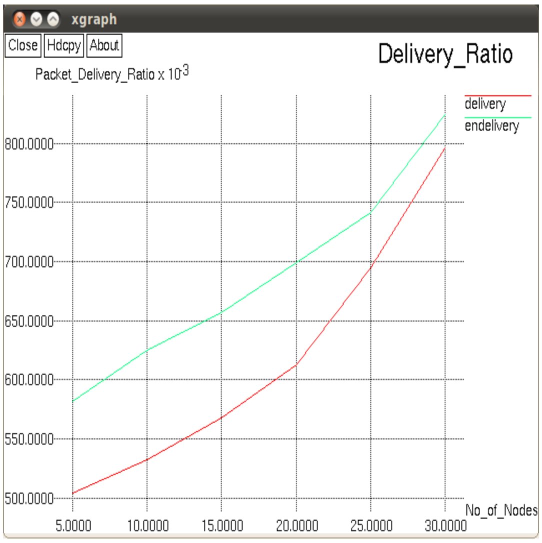


Fig. 4 Packet delivery ratio

In the Fig. 4, the green line represents the proposed trust based approach of delivery ratio and the red line represents the existing delivery ratio. If the malicious nodes detected in the identified path gets decreased then automatically the packet delivery ratio will get increased. Hence the packet delivery ratio will get increased up 94% in a successful delivery rate.

2) End to end delay

End to end delay is the time taken by a packet to travel from the source to destination, the delay depends on number of hops and congestion on the network.

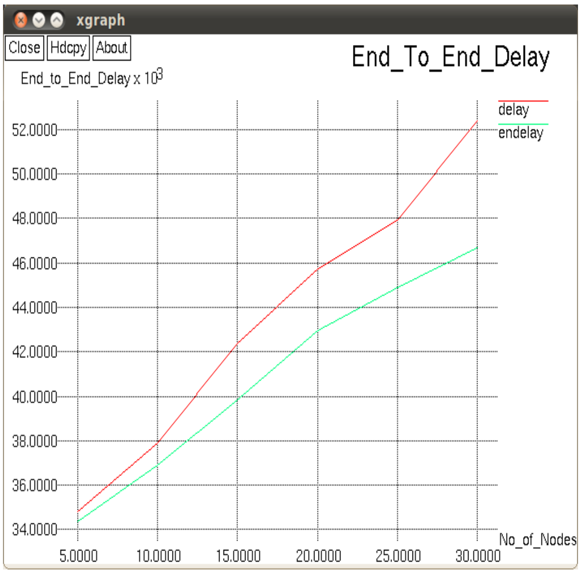


Fig. 5 End to end delay

Based on the trust value calculation the malicious node will be indentified, so that the packets can travel easily in that identified path with less delay. The green line indicates the proposed end to end delay.

V. CONCLUSION

The proposed technique aims to improve the malicious node detection scheme based on trust value. DSR protocol has been used for evaluating this technique. There by using threshold value range and the trust value the malicious node will be identified and removed completely from the routing process. The trust value can be calculated as the ratio of number of packets dropped by the number of packets to be forwarded. This will improve the proposed technique for detecting the malicious node and it is proven based on the performance of packet delivery ratio and the end to end delay. In future, the work may be extended to mitigate combined attacks in the routing path by evaluating other protocols instead of using DSR protocol.

REFERENCES

[1] Vishvas Haridas Kshirsagar and Ashok M. Kanthe, "Trust Based Solution To Packet Drop Attack in the MANET", Journal of Multidisciplinary Engineering Science and Technology (JMEST), vol. 2, no. 7, pp. 1927-1930, 2015.

[2] Aravindh S, Vinoth R S and Vijayan R, "A Trust Based Approach for Detection and Isolation of Malicious nodes in

the MANET", International Journal of Engineering and Technology (IJET), vol. 5, no. 1, pp. 193-199, 2013.

[3] Kamini Singh, Gyan Singh and Arpit Agrawal, "A Trust based Approach for Detection and Prevention of Wormhole Attack in MANET", International Journal of Computer Applications, vol. 94, no. 20, pp. 1-5, 2014.

[4] Sangeeta Bhatti and Meenakshi Sharma, "A novel Algorithmic Approach for Detection of Sybil Attack in MANET", Advanced Research in Computer Science and Software Engineering, vol. 5, no. 5, pp. 1680-1685, 2015.

[5] A. Jayanand and N. Chenthil Kumaran, "Trust Based Collaborative Attack Detection in MANET", Asian Journal of Information Technology, vol. 15, no. 4, pp. 808-816, 2016.

[6] Ji Guo and Alan Marshall, "A New Trust Management Framework for Detecting Malicious and Selfish Behavior for Mobile Ad hoc Networks", International Joint Conference of IEEE, pp. 142-149, 2011.

[7] Hisham Dahshan, Fatma Elsayed, Alaa Rohiem, Aly Elmoghazy and James Irvine, "A Trust Based Threshold", Vehicular Technology Conference (VTC Fall), IEEE, 2014.

[8] Bo YAANG, Ryo YAMAMOTO and Yoshiaki TANAKA, "Dempster-Shafer Evidence Theory Based Trust Management Strategy against Cooperative Black Hole Attacks and Gray Hole Attacks in MANETs", ICACT Transactions on the Advanced Communications Technology (TACT), vol. 2, no. 3, pp. 223-232, 2013.

[9] N. Bhalaji and A. Shanmugam, "Dynamic Trust Based Method to Mitigate Gray hole Attack in Mobile Adhoc Networks", International Conference on Communication Technology and System Design, Elsevier, vol. 30, pp. 881-888, 2012.

[10] Priyanka Takalkar and Aaradhana Deshmukh, "Trust Based Secure Data Communication in MANET", International Journal of Engineering Technology and Advanced Engineering, vol. 4, no. 12, pp. 542-546, 2014.

[11] Bhimsingh Bohara and Varun Sharma, "Analysis and Prevention of effects of gray hole attacks on Routing Protocol in Mobile Ad-hoc Networks", International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 6, pp. 2468-2472, 2013.

[12] Rajendra Aaseri, Pankaj Choudhary and Nirmal Roberts, "Trust Value Algorithm: A Secure approach against Packet drop Attack in wireless Ad-hoc Networks", International Journal of Network Security and its Application (IJNSA), vol. 5, no. 3, pp. 99-111, 2013.

[13] Renu Dalal, Manju Khari and Yudhvir Singh, "Different ways to achieve trust in MANET", International Journal on AdHoc Networking Systems (IJANS), vol. 2, no. 2, pp. 53-64, 2012.

[14] Dharmesh Patel and Yask Patel, "Intrusion Detection Systems for Trust based Routing in Ad-Hoc Networks", International Journal of Computer Science and Information Technology and Security (IJCSITS), vol. 2, no. 6, pp. 1160-1165, 2012.

[15] Priyanka Donga and Shraddha Joshi, "A Review On Trust Based Method To Detect Black Hole Attack In MANET", International Journal of Advanced Research in Computer and Communication Engineering, vol. 5, no.6, pp. 728-732, 2016.