Revocation of Malicious Nodes Using Trust Based Scheme

Neethu Jayan
Computer Engineering, PCE, Navi Mumbai, India.

Madhumita Chatterjee
Computer Engineering, PCE, Navi Mumbai, India.

KS Charumathi
Computer Engineering, PCE, Navi Mumbai, India.

Abstract – Mobile Adhoc networks (Manets) are one of the fastest growing areas of research. Recent years has led to the growth of Ad hoc networking standards and provision of the mobile nodes to set up self-organizing, adaptive, and short-lived networks because of heavy use of mobile computing devices. A concern in such networks is security since every node participates in the operation of the network equally; malicious nodes are hard to detect. It is clear that Manets have no centralized mechanism for resistance against threats, such as a firewall, an intrusion detection system, or a proxy. Securing the network is a challenging issue in Manet due to its dynamically changing topology. There are different methods for securing the Manets; trust management is one of the methods. A key concept of this project is to propose a trust and revocation based mechanism to secure the network from malicious attacks. We designed a cluster-based approach for discovering the malicious nodes based on direct and indirect trust of the nodes. If the node is found to be malicious it will be revoked from the network thus securing the Manet environment.

Index Terms – MANET, Network, Proxy, Security.

1. INTRODUCTION

Wireless networks are defined as computer networks connected through wireless links, such as radio frequencies and infrared rays. Mobile Ad hoc Network (MANET) do not have any permanent infrastructure and consists of wireless nodes that move dynamically without any boundary control. [3, 9, 10, 11].The autonomous nature and dynamic topology of the Manets leads to different attacks. Nodes within the transmission range can communicate directly with each other. The nodes which are not in the transmission range can communicate through intermediate nodes for forwarding the packets.

As Manets do not rely on any centralized architecture, such as access points or base stations, all the necessary network functionalities are performed by the nodes forming the network. Each node within a transmission range can directly communicate with each other whereas nodes which are not in transmission range rely on intermediate nodes to route their packets. Thus there can be several intermediate nodes between source and destination.

For a secure network, trust and revocation of malicious nodes is very important. There are different ways for securing the Manets such as Trust based system, Cryptographic method, intrusion detection method and so on. In our system, we used trust based and revocation of malicious node mechanism. For this, the final trust of entire set of nodes in the network can be calculated by applying direct and indirect trust calculation method on each and every node in the network. Nodes which have final trust value less than the threshold value can be considered as an attacker node. Cluster head within the network will verify the final trust and add the malicious nodes to warn list or black list based on the final trust value for securing the network.

Attacks in MANETs

Due to the dynamic nature of the Manets, there are different types of Attacks that may occur. Basically there are two types of attacks such as passive attacks and active attacks. These attacks try to reduce the performance of the network.

Passive Attacks

Passive attacks are silent attacks which are created by the attacker. It won’t alter the data transmitted in the network. But it “Listens” in the network or accumulates data from the network. It does not disrupt the operation of the network but it tries to sniff the important information.

Active attacks

An active attack disrupts the normal functioning of the network by modifying or destroying the data being exchanged in the network, Active attacks can be internal or external. [1].

2. RELATED WORK

S J. Indhu Lekha, R. Kathiroli [1] proposed a system where Trust is calculated on the basis of novel Vector based Trust

Mechanism (VBM). A credit (Ni) is held by each bit position in the trust vector. The credit gradually increases when it moves from LSB to MSB. MSB hold the recent transaction with highest credit. Enhanced certificate revocation algorithm is used for Revocation of malicious nodes based on the concept of warn list and Black List.

Pedro B. Velloso [2] addresses the problem of trust evaluation and management in ad hoc networks. It presented that the Trust is calculated on the basis of maturity model, where how long two nodes know each other. Recommendation Exchange Protocol (REP) is used to collect Indirect trust value and it consists of trust recommendation request, trust recommendation reply and trust advertisement. This system implies lower resource consumption and a lower vulnerability to false recommendations attack.

Aravindh S, Vinoth R S and Vijayan R [3] stated that the Trust calculation is based on the concept of Direct trust and Recommendation trust, where Direct Trust is calculated as the ratio of successful packet sent from a node x and successful packet receive from the node Y. While calculating recommendation trust they considered direct trust value for avoid the security attacks like bad mouthing. Final trust of a node is calculated on the basis of Energy value, direct trust and Indirect trust.

Zeinab Movahedi, Michele Nogueira, Guy Pujolle [4] stated that each node Collect information about the neighbor nodes and store the information in LTT and GTT. Local Trust Table contains one entry by neighbor for which it stores the data amount generated and forwarded by that neighbor as well as the local trustworthiness estimated for that neighbor. Global Trust Table is created by every node of the network which is gradually completed by trust values of all network nodes. For trust calculation each and every node have ATM (Autonomic Knowledge Monitoring) Scheme consists of Analyzing, planning, Execution and Monitor.

Mrs. Priti Rathi, Mr. Parikshit Mahalle [5] describes that each node in the network consists of a profile table and status table. Profile table information is about the number of nodes in the network, node count, accusation information where status table consists of behaviour index, weight of node's accusation and revocation quotient. If the revocation quotient result is less than the revocation threshold then the node will be revoked from the network.

3. PROPOSED MODELLING

The aim of our proposed system is to detect malicious nodes and revoke them for securing the network. Our proposed system consists of four modules Cluster formation, Trust calculation including direct as well as indirect trust, Cluster head selection and Revocation. When a node wants to estimate a neighboring node's trust, it will send some packets to its neighboring node. If a node's final trust value is less than threshold value, then the neighbor node will send an accusation packet to the cluster head. So that if there is any malicious node in the path, then the sender can choose an alternative path to the destination. Following diagram shows the architecture of proposed system.

Initially all the nodes form a cluster. The node's trust is calculated with direct trust, indirect trust and node with the highest trust value is selected as cluster head.

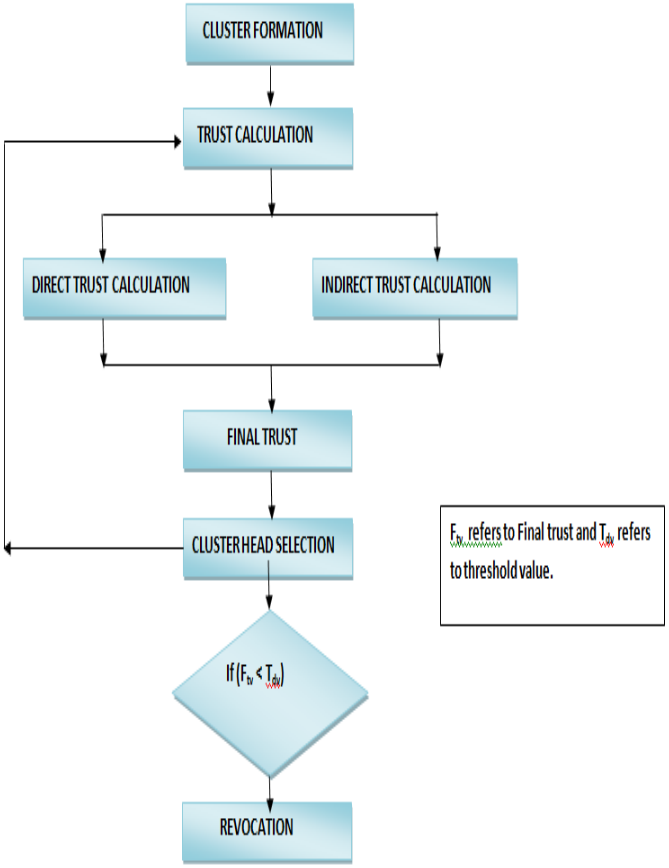


Fig. 1. Flow of proposed system

A. Cluster Formation

Grouping of nodes is termed as cluster. In the system, Cluster formation is on the basis of distance formula. D is the Distance calculation of nodes where the distance between two nodes in the plane with coordinates (x, y).

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} .$$

The distance between two points is the length of the path between them. In the plane, the distance among points (nodes) and is given by the Pythagorean Theorem. The basic idea is that the network area is divided into numerous virtual grids in equal size.

B. Trust Calculation

Trust calculation is the method used for to find out the malicious nodes in a network. Trust of nodes is calculated on the basis of direct trust and indirect trust. Direct trust value is evaluated on the basis of direct experience that a node may have on another node.

$$DT = (s - d + m)/s$$

Where s is the number of packets sent by a node, d is the number of packets dropped by a node, m is the number of packets misrouted by a node.

When a node (let node A) doesn't have enough direct experience on any other node (node D), the node may request a third node (B, C) for recommendation, and this is known as Indirect Trust.

$$TR = (TD^1 * V_i)$$

Where TR is the Indirect Trust calculation, TD' is the direct trust value that the node has on the third node, Vi is the trust value that the third based on its own evaluation. If there are many third nodes

$$TR = \frac{1}{n}\sum_{i=1}^{n}(TD^1 * V_i)$$

Final direct trust is calculated as **FDT = ε DT / n** where n is the number of nodes and we can calculate

Final Indirect trust as **FIDT = ε IDT / n**

Final trust value of a node can be calculated on the basis of final direct trust and the final indirect trust.

F_{TV} = (FDT + FIDT) / 2

Trust value of a node ranges from 0 to 1 where trust value 0 is considered as least trusted node and final trust value 1 is considered as highest trusted node. The nodes threshold value is set as 0.6. If any node's final trust value is less than the threshold value 0.6, that particular node can be considered as a malicious node.

A. Cluster Head Selection

Trust of each node in the cluster is calculated and the node which has highest final trust will become cluster head (CR_{hd}). Final trust value of all nodes are broadcasted in the network and the role of cluster head is to verify the final trust of the node which sends the accusation packet, and the final trust of the node of the accused node or victim node. Algorithm for the cluster head selection is given below

```
$CR_{hd}$ ← Cluster Head, $F_{TV}$ ← Final Trust
S1 :    Trust Calculated
S2 :    i = 0;
S3 :    if $F_{TV}$ [i+1] > $F_{TV}$ [i]
        Then
        $CR_{hd}$ ← $F_{TV}$ [i+1]
        Else
        $CR_{hd}$ ← $F_{TV}$ [i]
S4 :    i ← i +1;
S5 :    Display $CR_{hd}$
```

D.Revocation

If any node's trust value is less than the threshold value then its neighbour node (accuser node) will send an accusation packet to the cluster head. Then Cluster head will check the final trust value of the accuser node and accused node. If the final trust value of the accused node is less than the accuser node, then the accused node will insert into black list. If the accused node's final trust value is greater than the accuser node, then the accuser node and accused node will insert into warn list. If already the accused node is existed in the warn list then the accusation is the second accusation against that node and the node will insert into black list.

```
$A_R$ → $CR_{hd}$ // Accuser sends $A_{CP}$ to $CR_{hd}$
if ($F_{TV}$.$A_R$>$F_{TV}$.$A_{SD}$)
    if(Check $A_{SD}$ in the $W_N$L)
      Move $A_{SD}$ to $B_K$L // Second claim (Accusation)
    Else
      Insert into $B_K$L // First claim (Accusation)
Else
Insert $A_{SD}$ and $A_R$ into $W_N$L // leads to next (second) accusation
    Revoke ($B_K$L)
```

Where A_R refers to Accuser node, CR_{hd} refers to cluster head, F_{TV} refers to final trust, A_{SD} is accused node, A_{CP} means Accusation Packet, W_NL means warn list and B_KL means Black list.

Case

If the final trust value of the accused node (A_{SD}) is less than the accuser node (A_R) then the accused node will insert into black list.

Case

If the accuser node's (A_R) final trust value is less than the accused node (A_{SD}), then the accuser node and accused node will insert into warn list.

Case

If already the accused node is existed in the warn list then the accusation is the second accusation against that node and the node will insert into black list.

Finally the cluster head sends a certificate revocation packet to the certificate authority and the malicious node will be revoked from the network.

A certificate revocation list (CRL) is a listing of certificates (or more particularly, a list of serial numbers for certificates) that have been revoked, and consequently entities presenting those (revoked) certificates should no longer be trusted. In our proposed system cluster head ($CR_{hd)}$) sends Accusation packet ($A_{CP)}$) to CA (Certificate Authority) consists of packet type, sender node id, accuser node id, accused node id, destination id and data information.

4. RESULTS AND DISCUSSIONS

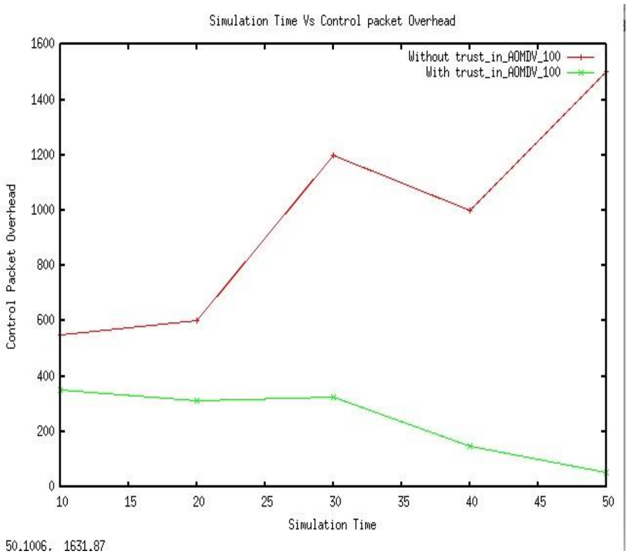
Our simulation settings and Configuration Parameters are summarized in the table 3.

Simulator	NS2
Network Area	500 * 500
Channel Type	Channel/WirelessChannel
Propagation Model	TwoRayGround
MAC Layer	802_11
Max packet in ifq	550
Number of Nodes	100
Routing Protocol	AOMDV
Antenna Model	OmniAntenna
Communication Range	250
Traffic Source	UDP/CBR

Table 3:- Configuration Parameters

Ns2 simulator was used to evaluate the performance of the on-demand routing protocol. The distributed coordination function (DCF) of IEEE 802.11 for wireless LANs is used as the MAC Layer protocol. Nodes are randomly dispersed in a field and the cluster creation is based on the distance formula. We used overhead, throughput and Packet Delivery Ratio to evaluate the performance of the proposed system.

The number of malicious nodes in the set of 100 nodes is 25; the overhead of the system with malicious nodes revocation (trust in AOMDV) is less than the overhead of the system without malicious nodes revocation (without trust in AOMDV).

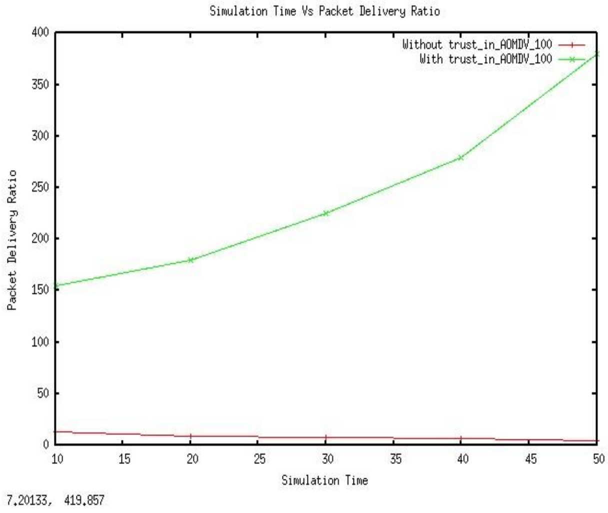


Overhead of 100 nodes

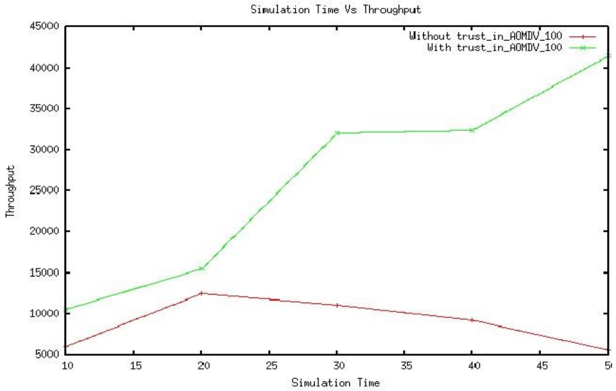
Packet delivery ratio is the ratio of packets that are successfully delivered to a destination compared to the actual number of packets transmitted by the sender; PDR can be calculated as given below,

PDR = (number of packets received) / (number of packets sent) *100

The system with malicious nodes revocation (trust in AOMDV) has more packet delivery ratio than the system without having malicious nodes revocation method (without trust in AOMDV). When the number of malicious nodes increases, the packet delivery ratio decreases.



Packet delivery ratio of 100 nodes



Throughput of 100 nodes

Throughput is a measure of how many units of information a system can process in a given amount of time. A Trusted node will forward the packets to the corresponding destination within the given amount of time itself. Hence trusted nodes have more throughput. But the malicious nodes will either drop the packet or misroute the packet to some other destination resulting in lesser throughput. Throughput of the system increases with malicious node revocation method (trust in AOMDV).

5. CONCLUSION

We propose a model for securing Manets which is based on a Trust Model. We have modified the AOMDV protocol by adding direct and indirect trust calculation mechanisms, integrated with revocation of malicious nodes by a cluster head. This minimizes monitoring overhead and results in high packet delivery ratio. This proposed scheme achieved efficient detection of misbehaving nodes. Overall trust value of the nodes increases and overhead decreases when malicious nodes in the network revoked. Results show that the modified AOMDV protocol with trust management gives higher packet delivery ratio and throughput and low overhead as compared to the original AOMDV protocol. Currently only a single trusted path is selected. As future work, this can be extended to find multiple trusted paths.

REFERENCES

[1] S J. Indhu Lekha, R. Kathiroli, “Trust Based Certificate Revocation of Malicious Nodes in MANET”, IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT) 10 May 2014

[2] Pedro B. Velloso, Rafael P. Laufer, Daniel de O. Cunha, Otto Carlos M. B. Duarte, and Guy Pujolle, “Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model”, IEEE Transactions on network and service management,vol.7 ,no.3,September 2010

[3] Aravindh S, Vinoth R S and Vijayan R “A trust based approach for detection for detection and isolation of malicious nodes in MANET”, International Journal of Engineering and Technology (IJET), Vol 5 No 1 Feb-Mar 2013

[4] Zeinab Movahedi, Michele Nogueira, Guy Pujolle , “An Autonomic Knowledge Monitoring Scheme for Trust Management on Mobile AdHoc Networks”, IEEE Wireless Communications and Networking Conference: Mobile and Wireless Networks, 4 April 2012

[5] Mrs. Priti Rathi1, Mr. Parikshit Mahalle, “Certificate Revocation in Mobile Adhoc Networks” , International Journal of Application or Innovation in Engineering & Management (IJAIEM) , Volume 2, Issue 1, January 2013

[6] Ranjana B Jadekar, Shivanand M Patil2, “Elimination of the Certified Malicious node in the MANETs with the Vindication Capability”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 6, June 2015

[7] S. R. Biradar, Koushik Majumder, Subir Kumar Sarkar, Puttamadappa C, “Performance Evaluation and Comparison of AODV and AOMDV”, International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010.

[8] Rashid Sheikh,Mahakal Singh Chandel,Durgesh Kumar Mishra , “ Security issues in MANET:A Review”, IEEE Wireless And Optical Communications Networks (WOCN), 2010 Seventh International Conference On 8 Sept. 2010

[9] Priyaganga Guruswamy, Madhumita Chatterjee. “A Novel Efficient Rebroadcast Protocol for Minimizing Routing Overhead in Mobile AdHoc Networks”, International Journal of Computer Networks and Applications (IJCNA), 3 (2), PP: 38-43.

[10] Ravneet Kaur, Neeraj Sharma. “Dynamic Node Recovery in MANET for High Recovery Probability”, International Journal of Computer Networks and Applications (IJCNA), 2(4), PP: 158-164.

[11] S.Zafar, H.Tariq,K.Manzoor, “Throughput and Delay Analysis of AODV, DSDV and DSR Routing Protocols in Mobile Ad Hoc Networks”, International Journal of Computer Networks and Applications (IJCNA) Volume 3, Issue 2, March – April (2016)