International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 7 278 - 281

Evaluation of Trust and Revocation of Malicious Nodes in MANETs

Neethu Jayan
Computer Engineering, PIIT
Navi Mumbai, India
neethu.jayan5@gmail.com

Madhumita Chatterjee
Computer Engineering, PIIT
Navi Mumbai, India
mchatterjee@mes.ac.in

K. S. Charumathi
Computer Engineering, PIIT
Navi Mumbai, India
kscharumathi@mes.ac.in

***Abstract*—** Mobile adhoc network (MANET) is formed by a set of mobile hosts which communicate via radio waves within the transmission range. Manets are wireless communication where nodes can freely move within the network. Manets operate in the absence of base station and central access point. Applications of Manets are different in various areas. Manets are famous because of its self configuring, wireless and dispersed. The main factor in Manet is its security. The features of Manets are actually nontrivial problems to the security design in Manets. Manets are vulnerable to attacks due to the absence of the centralized control, dynamic topologies. Hence it's very important to protect Manets from various types of attacks and revocate the certificate of the malicious nodes.

Index Terms—Manets, Trust, Secure, Revocation

*****

I. INTRODUCTION

Mobile Adhoc Network is an independent system of mobile nodes communicating via wireless links with no fixed infrastructure. The independent nature and dynamic topology of the Manets leads to various 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.

Mobile Adhoc Network consists of mobile nodes which can move freely in any direction. Manet has some significant features such as wireless medium, dynamic topology and autonomous operation. 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. Thus Manets are self-configuring network, fully distributed and does not need any fixed infrastructure Wireless network become popular in the past years, especially within the 1990's and Mobile Adhoc network become one of the liveliest and active fields of communication and network research. There are many critical challenges and problems to be solved in Manets. Trust is very important in Manets for forwarding packets. If the node is not trusted enough then it's very risky to forward the packets through these types of non trusted nodes. Manets are self configuring network, it does not have any fixed network and there is no base station. All this results in various types of attacks in Manets such as black hole attack, Grey hole attack, Byzantine attack, Sybil attack.

For a secure network trust in Manet is very important and there are many ways for the calculation of trust in Manets.

2. RELATED WORKS

Trust is major concern in Manets. Trust of nodes in the network can be calculated in different ways. If the trust of any node in the network is less can be considered as a malicious node and these malicious nodes are a threat to the network.

In [1], S J. Indhu Lekha, R. Kathiroli proposed a trust based certificate revocation in Manets where the nodes forms a cluster and the trust of the nodes are calculated on the basis of novel vector based trust mechanism (VBM).A credit is assigned to each bit position and trust is calculated on the basis of the energy and trust vector. Revocation is based on the concept of Warn list and black list.

In [2], author proposed a system where the trust is calculated on the basis of direct and recommendation trust, Where Indirect trust value can be collected based on Recommendation Exchange Protocol (REP).REP consists of trust recommendation request, Trust recommendation reply and trust recommendation advertisement.

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. Final trust is calculated on the basis of Energy value, Direct trust and Indirect trust.

Zeinab Movahedi, Michele Nogueria, Guy Pujolle [4] stated that each node collect information about the neighbour nodes and store the information in LTT and GTT. For trust calculation each and every node have ATM (Autonomous Knowledge Monitoring) Scheme consists of Analyzing, planning, Execution and Monitor.
Kuldeep Sharma, Neha Khandelwal, Prabhakar.M [5] describes classification of security attacks such as active and passive attack. Security attacks are further classified into different types where author describes each type in detail, also explains some advanced attacks in Manets.

3. PROPOSED SYSTEM

The aim of our proposed system is to detect malicious nodes in the network and avoid transmitting messages through them by adding those malicious nodes in Black list (BL). Our proposed system consists of four modules Cluster formation, Trust calculation including direct as well as indirect trust, Cluster head selection and Revocation. 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.

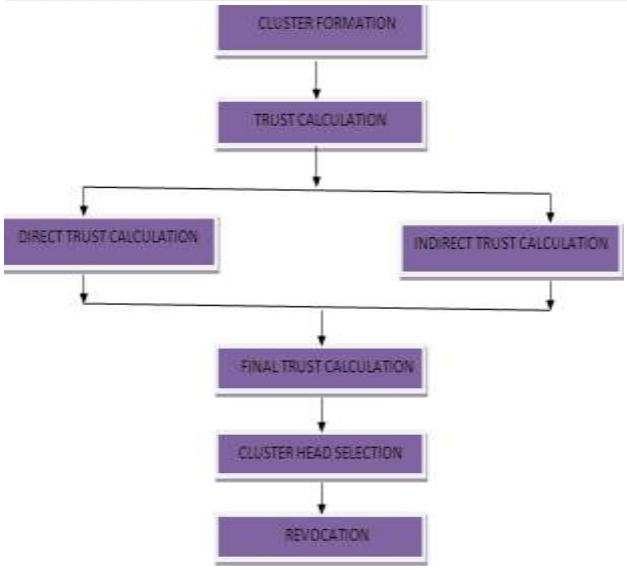

Fig. 1. Flow of proposed system

A. Cluster Formation

Grouping of nodes is termed as cluster. In our system, Cluster formation of nodes is on the basis of distance formula[1], 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 formula is derived from the Pythagorean theorem.

B. Trust Calculation

Trust calculation and its management is a strenuous task in Manets due to the unpredictable nature of nodes and computational complexity constraints in the network [1].There are many ways to calculate the trust of nodes in Manets. In our proposed system, nodes trust is calculated on the basis of direct trust and indirect trust methods. 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 DT is the direct trust, s is the number of packets sent by a node, d is the number of packets dropped, m is the number of packets misrouted.

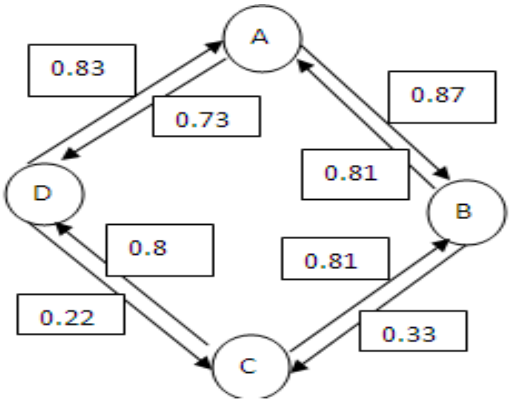

Fig. 2. Example for trust calculation

NODES	DIRECT TRUST (DT)
AB	0.87
BA	0.81
AD	0.73
DA	0.83
CD	0.8
DC	0.222
BC	0.333
CB	0.81

Table 1. Direct Trust Calculation

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

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

Where TR is the Indirect Trust calculation, TD^1 is the direct trust value that the node (Node A) has on the third node (Node B and Node D), Vi is the trust value that the third node (Node B and D) based on its own evaluation.

If there are many intermediate nodes for calculating the recommendation trust, it can be calculated as,

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

Node A can calculate the indirect trust for Node C with the recommendation values of Node B and Node D and vice versa. Node B can calculate the indirect trust value of Node D through Node A and Node C.

NODES	INDIRECT TRUST (IDT)
AC	0.222
CA	0.66005
BD	0.428
DB	0.450

Table 2. Indirect Trust Calculation

Final direct trust can be calculated as **FDT = εDT / n** where n is the number of intermediate nodes and Final Indirect trust can be calculated as **FIDT = εIDT/ n.**

Final trust can be calculated as

FT = (FDT + FIDT) / 2

NODES	(DT + IDT)/2	FINAL TRUST (FT)
FT(A)	(0.82 + 0.66005)/2	0.740025
FT(B)	(0.84+0.450)/2	0.645
FT(C)	(0.2775+0.222)/2	0.24975
FT(D)	(0.765+0.428)/2	0.5965

Table 3. Final Trust Calculation

Trust value ranges from 0 to 1 where 0 means least trust and 1 mean highest trust.

C. Cluster Head Selection

Trust of each node in the cluster is calculated and the node which has highest final trust will become cluster head. From our example Node A has highest trust value and it will become our cluster head.

CH ← Cluster Head, FT← Final Trust
S1 : Trust Calculated
S2 : i = 0;
S3 : if FT [i+1] > FT [i]
Then
CH ← FT[i+1]
Else
CH ← FT[i]
S4 : i ← i +1;
S5 : Display CH

D.Revocation

In certain cases the certificate authority (CA) revokes some digital certificates and is termed as certificate revocation list (CRL) before their scheduled expiration date and they are no longer trusted.If any node's trust value is less than the threshold value then its neighbour 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 based on the algorithm given in the below table [1]

```
AC → CH // Accuser sends AP to CH
if (FT.AC > FT.ACD)
      if(Check ACD in the WL)
        Move ACD to BL // Second Accusation
      Else
        Insert into BL // First Accusation
Else
Insert ACD and AC into WL // leads to second accusation
While(Isempty(BL))
      CH → CA // CH sends AP to CA
      Revocate(BL)
```

In our example Node C's trust value is less than the threshold value and the neighbour Node B will send an accusation packet (AC) to the cluster head(CH) Node A, regarding the trust value of its neighbour.

Case

If the final trust value of the accused node(ACD) Node C is less than the accuser node(AC) Node B then the accused node will insert into black list.

Case

If the accuser node (Node B) final trust value is less than the accused node (Node C), 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 revocate 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 CH sends AP (Accusation packet to CA(Certificate Authority) consists of packet type, sender node id, accuser node id, accused node id, destination id and data information.

4. IMPLEMENTATION

Our simulation settings and Configuration Parameters are summarized in Table 4.

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	50
Routing Protocol	AOMDV
Antenna Model	OmniAntenna
Communication Range	250
Traffic Source	UDP/CBR

Table 4. Simulation Parameters

5. CONCLUSION

Trust and its management are exciting fields of research. Trust as a concept has a wide variety of adaptations and applications, which causes divergence in trust management terminology. Our proposed system name evaluation of trust and revocation of malicious nodes in Manets aims to spot the malicious node with the trust based scheme and revocate the malicious nodes from the further communication. We Hope to improve trust calculation and revocation of malicious nodes on the basis of direct and indirect trust calculation.

REFERENCES

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

[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*",Vol 5 No 1

Feb-Mar 2013, International Journal of Engineering and Technology (IJET)

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

[5] Kuldeep Sharma, Neha Khandelwal, Prabhakar.M ,"*An Overview Of security Problems in MANET*"

[6] Adnan Nadeem, Member, IEEE, and Michael P. Howarth "*A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks*", IEEE Communications surveys & tutorials,vol.15,No.4,Fourth Quarter 2013

[7] Michele Nogueira Lima, Aldri Luiz dos Santos, and Guy Pujolle" *A Survey of Survivability in Mobile Ad Hoc Networks*", IEEE Communications Surveys & Tutorials,vol.11,No.1, first quarter 2009

[8] A. Vani ,"*Review of Basic Secure Routing Protocols for MANETs"*, International Journal on Recent and Innovation Trends in Computing and Communication