Trust Based Security of MANETS

Taran Singh Bharati

Abstract: ***Mobile AdhocNetworks (MANETs) are non-fixed infrastructure networks and there are so many issues with them because of their dynamic topology, mobile nodes, security, bandwidth constraints, limited battery backup etc. Trust is an association, trustworthiness, reliability, and faithfulness of the nodes in the network. This paper discusses about the trust and trust computations. This paper proposes trust computation protocols and a TSD algorithm which determines the secure shortest routes. Trust is one of the ways to enhance the security of MANETs so this paperin turn contributes towards the enhancement of the security of MANETs by fusing the trust in TSD algorithm.***

Index Terms: Trust, Security, MANETs, Routing

I. INTRODUCTION

Mobile adhoc networks (MANETs) are the temporary networks formed for time being in the situations where ordinary networks cannot be formed. MANETs have many limitations i.e. lack of infrastructure, mobility of nodes, dynamic topology, bandwidth, security etc. MANETs can be secured by using cryptographic tools, key management, trust, and by securing the routing. Trust [1] refers to the faithfulness of the node which other nodes can rely on and use the data received from them. Trust is useful in network functions like routing, data aggregation, malicious node detection, time synchronization, reliability, trustworthiness, competence of nodes for some monitoring technique etc.

A. Role of Trust in MANETs

Trust of any node lets us feel how reliable, faithful, and honest is the node to its neighboring nodes. A trusted node always works honestly and sends correct information to its neighbors to do the tasks without becoming a selfish node. Trust can be quantified and it is adjustable or modifiable depending on the assessment made by its neighboring nodes.

B. Types of Trust

A trusted network can be modelled as a network with connected nodes as shown in figure (1) and every node has its own trust table which keeps the trust records of all its neighbouring nodes' trusts. The trust table may use parameters like, reliability of the node, intimacy with the node, honesty of the node, energy available to the node, and priority of the work. This trust table is varied at the time when some new observations regarding the neighbouring nodes' trust are made. Trust can be classified in various categories on the basis of its computation or its ways of usage in working. The trust can be transferred or recommended to other nodes [5], [6], [7], [8], [9], [10], [11]. A network is depicted as below (figure 1):

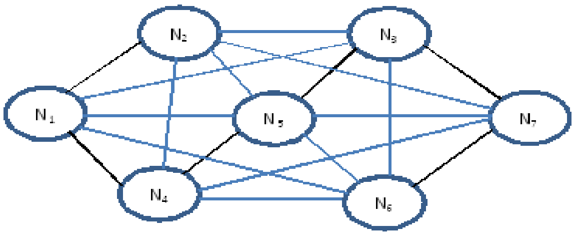

Figure 1: A Network

II. RELATED PREVIOUS WORK

Trust computations [6], [24] and trust based security for networks is proposed [11], [21], [2], [3], [4]. MANETs' issues and security concerns i.e. data transmission security, key management, etc. exist.[18], [19], [20], [21], [22], [23]. Trust and trust based security service discovery modelling, evaluation and assessment [4] are proposed. Models 'are classified in policy based, reputation based, and trusted third party [5].

Trust are computed by centralized, decentralized, distributed, trusted third party (TTP), and hierarchical [13] ways. MANETs use distributed trust management [2], [6], [8], [11].

The Trust Record: Stores the trust values and relationships. Relationship between parties shows that they trust each other and perform task. Here first party is called subject and second party is called the agent. The relationship is represented by the following notation:

{Subject: agent, action}

Hierarchical trust includes trust composition- the components of the trusted system; trust aggregation:-the way to gather the information for computing trust; trust formation- from the trust components how trust is established. Trust evaluation process uses the intimacy, honesty, energy, and usefulness of the node. A trust from node i to node j, is computed as below:

Trust = w_1*intimacy+w_2*honesty+w_3*energy+w_4* usefulness+w_5* response time+w_6 residency time in other community

where any weight (w) can take any value between 0 and 1 and the summation of all weights must be equal to one and weights are adjusted to maximize the trust. A trust matrix can be formed as:

Revised Manuscript Received on June 05, 2019

Taran Singh Bharati, Department of Computer Science JamiaMilliaIslamia, New Delhi, India

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

$$\begin{bmatrix} a_{11} & a_{12} \cdots & a_{1p} \\ a_{21} & a_{22} \cdots & a_{2p} \\ \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & a_{np} \end{bmatrix}$$

There are many numerical values, called trust values, for each relationship. Two ways to establish the trust exist. First is called **direct trust** in which subject observes the behavior of agent from the past experience and second subject receives the recommendation for the agents from other entities, is called **indirect trust**. The recommended relationship is written as {subject: agent, making correct recommendations}. Indirect trust can propagate from one node to another via third parties.

III. PROPOSED WORK

Our proposed work has three components. Firstly trust computation is done by the trust computation formula. Secondly trust value is checked for its maximum value in the group of nodes to be considered for next node. Thirdly shortest distance is calculated from source to concerned nodes. The method is pictorially depicted in figure 3.

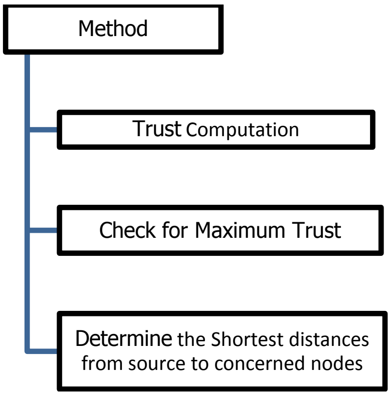
Method
Trust Computation
Check for Maximum Trust
Determine the Shortest distances from source to concerned nodes

Figure 3: Process Model

A. *Trust Computation Methods*

There is a single coordinator in MANETs and any node can become the coordinator by leader election algorithm so trust computation in distributed fashion is done as shown in figure (2).

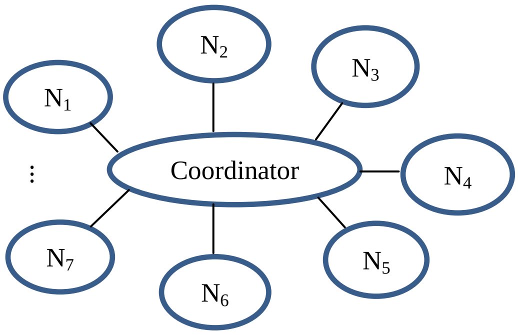

Figure 2: Trust Calculating Coordinator

Trust computation is proposed in two ways:

i) **Two Phase Computation:**Computation is decided in two phases only.

- **Phase-1:** In this phase coordinator makes a request asking its neighbours regarding their trust computations for a node. All neighbouring nodes prepare their trust values and send them to the coordinator via network. Coordinator then finally computes cumulative trust by applying some evaluation methods.
- **Phase-2:** Coordinator then updates its own trust table and sends its recommendation to other nodes.

ii)**Three Phase Computation:**It is computed in three phase.

- **Phase-1:**Coordinator prepares and send trust request to other neighbouring nodes. Nodes calculate the trust and sent them to the coordinator. Coordinator then finally evaluates overall trust of the node.
- **Phase-2:**Coordinator then stores the result in a table for a time being. Sends its final value to all neighbour. All neighbours see this value and they send yes if they agree on the computed trust.
- **Phase-3:**If coordinator receives yes from all neighbours, then coordinator permanently saves the trust values in table.

B. *TSD Secure Algorithm*

This algorithm defines the route from source to destination through trusted intermediate nodes. Multipoint relays (MPR) are employed to forward the broadcast messages during flooding. The generation and reporting is done by MPRs. Two messages HELLO and TC (topological control) are used to obtain and declare information about network topology [3]. To find the route an algorithm is developed which is inspired by Dijkstra's shortest path algorithm. This greedy algorithm always finds better route through better trusted nodes. Our algorithm uses the following parameters and data structures [16], [17].

The n represents number of nodes in network and v is the source node, dis [j], $1\leq j \leq n$ which provides us the shortest path length from source say v to nodes j. Cost [] is an n by n adjacency matrix. T [] is n by n trust matrix of nodes. S [i] is shortest secure route.

Algorithm TSD (v, cost, T, dist, n)

```
{
for i=1 to n do
{          // initialize S and T
S[i]= false; dist[i]= cost[v,i]; T[i]=$t_i$;          //trust table updation by MPR
}
S[v]=true; dist [v]=0          // put v in S
forj=2 to n   do
{  // find n-1 routes from v choose u from among   those not in S suchthat dist [u] is minimum and T[u] is maximum
S[u]=true          // put u in S
for (each w adjacent to u with S[w]=false and T[u] is maximum)   do
{// update distances and trust
if( dist[w]>dist[u]+cost[u, w] and $t_u$>$t_w$))       do
dist[w] = dst[u]+cost[u, w]
T[w] is maximum
            }
      }
}
```

IV. RESULT ANALYSIS AND DISCUSSION

A. Performance Analysis of Trust Computation Methods

Since there is a single coordinator so there would be problem of single point failure, congestion near the coordinator, overheads. The problems can be overcome by crash recovery of the coordinator and nodes by including the alternate coordinators and node failure can be overcome via logs of the nodes.

B. Correctness and Complexity of the TSD Algorithm

This algorithm first selects the source and finds the minimum distance from source to particular node on the basis of its trust. The distance and trust do update during the course of action and decisions are made on the basis of both minimum distance and trust. Therefore algorithm gives the correct and secure routes from source to all other nodes. The algorithm assigns weights and trust values to all nodes and it takes O (n) time. Then so is to find n-1 routes. To choose node u from the rest of nodes with minimum distance and maximum trust takes (log n) time. Overall complexity to update distance is O (E). Therefore the total complexity of the algorithm will be O ((n+|E|) log n) where E is the number of edges in the network.

C. Comparison with exiting algorithms

Other algorithms do not consider the trust of nodes as well in route calculations while the TSD algorithms proposed here computes the trust at time when decision about inclusion of nodes in route is made and considers this trust also as a main parameter in route finding decision.

V. SOME OTHER ISSUES

Some of the issues related to trust and their applications exist as below:

A. Trust Establishment Issue

For establishing the trust in other network it predicts the future behaviour and the diagnosis of security properties [7]. The prediction resolves the problems of assistance for decision making, adaptation to risk, and misbehaviour detection.

B. Attacks on Trust Management System

In network, nodes participate in various activities (routing etc.) with their trusted neighbours [12]. Some of the several attacks on the system are:

i) Bad Mouthing Attacks: Some nodes may not be honest it may recommend the bad node to its neighbours.

ii) On-off Attacks: Some nodes sometimes behave well and sometimes bad.

iii) Sybil Attack and new Comer Attack: Some nodes can impersonate the other nodes and can manipulate the network operations.

iv) Selective Behaviour Attacks: Some nodes may be biased also they may accept the recommendation from a certain group of nodes.

C. Trust as Parameter

The trust is utilized as one the main parameters to perform tasks in the networks such as routing security based on trust and key management.

i) **Risk Management:** Risks are managed by identifying, analysis, and monitoring and planning for malicious nodes [14], [15]. There could be various risks levels depending on their chances to occur.

ii) **Reliability and Availability:** They give the feeling of error free environment and are measured by mean-time-between-failure (MTBF):

$$\text{MTBF}=\text{MTTB} + \text{MTTR}$$

where MMR= mean-time-to repair and, MMTF: mean-time-to-failure. Availability is the chance that information will be available at particular time, can be written as:

$$\text{Availability} = \frac{\text{MTTF}}{\text{MTTF+MTTR}} \times 100\ \%$$

VI. CONCLUSIONS

In MANETs, a security is one of the main burning issues because of its nature and the way of its working. Its security has many forms for enhancing i.e. trust, key management, IDS etc. This paper proposes a secure TSD routing algorithm which finds shortest distance routing based on nodes of maximum trust. The algorithm is described and its performance is measured, compared, and validated. The algorithm is superior because it considers both shortest distances as well as computed trust values of nodes in route findings. The algorithm determines route in O ((n+|E|) log n) complexity where n is the number of nodes in network and E represents the number of connections.

REFERENCES

1. G. O. Young, “Synthetic structure of industrial plastics (Book style with Sun Y, Han Z, Liu KR. Defense of trust management vulnerabilities in distributed networks. IEEE Communications Magazine. 2008 Feb; 46 (2):112-9.
2. Boukerche A, Ren Y. A trust-based security system for ubiquitous and pervasive computing environments. Computer Communications. 2008 Dec 18; 31(18):4343-51.
3. Adnane A, Bidan C, de Sousa Júnior RT. Trust-based security for the OLSR routing protocol. Computer Communications. 2013 Jun 1; 36 (10-11):1159-71.
4. Ahamed SI, Sharmin M. A trust-based secure service discovery (TSSD) model for pervasive computing. Computer Communications. 2008 Dec 18; 31 (18):4281-93.
5. Galizia, S.; Gugliotta, A. and Domingue, J. (2007). A trust based methodology for web service selection. In: International Conference on Semantic Computing (ICSC 2007), 17-19 Sep 2007, Irvine, CA, pp. 193–200.
6. Govindan K, Mohapatra P. Trust computations and trust dynamics in mobile adhoc networks: A survey. IEEE Communications Surveys & Tutorials. 2012 May; 14(2):279-98.
7. Pirzada AA, McDonald C. Establishing trust in pure ad-hoc networks. InProceedings of the 27th Australasian conference on Computer science-Volume 26 2004 Jan 1 (pp. 47-54). Australian Computer Society, Inc.
8. Cho JH, Swami A, Chen R. A survey on trust management for mobile ad hoc networks. IEEE Communications Surveys & Tutorials. 2011 Nov; 13 (4):562-83.
9. Liu Z, Joy AW, Thompson RA. A dynamic trust model for mobile ad hoc networks. InDistributed Computing Systems, 2004. FTDCS 2004. Proceedings. 10th IEEE International Workshop on Future Trends of 2004 May 26 (pp. 80-85). IEEE.
10. Li X, Lyu MR, Liu J. A trust model based routing protocol for secure ad hoc networks. InAerospace Conference, 2004. Proceedings. 2004 IEEE 2004 Mar 6 (Vol. 2, pp. 1286-1295). IEEE.

11. Boukerch A, Xu L, El-Khatib K. Trust-based security for wireless ad hoc and sensor networks. Computer Communications. 2007 Sep 10; 30 (11-12):2413-27.
12. Lopez J, Roman R, Agudo I, Fernandez-Gago C. Trust management systems for wireless sensor networks: Best practices. Computer Communications. 2010 Jun 1;33(9):1086-93.
13. Bao F, Chen R, Chang M, Cho JH. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE transactions on network and service management. 2012 Jun;9(2):169-83.
14. Roger S. Pressman. Software Engineering: A Practitioner‘s Approach. 7th ed. Vol. US: McGraw-Hill Higher Education. 2010:666-81.
15. SOMMERVILLE I. Software Engineering. Harlow: Pearson Education Limited, 2007. 824 s. ISBN 978-0-321-31379-9.
16. Horowitz IE. sartajsahni· Fundamentals of Computer Algorithms.2nded, 2007, ISBN 978 81 7371 6126.
17. Yan Z, Zhang P, Virtanen T. Trust evaluation based security solution in ad hoc networks. InProceedings of the Seventh Nordic Workshop on Secure IT Systems 2003 Oct 15 (Vol. 14).
18. Bharati, T. S. (2015). Enhanced Intrusion Detection System for Mobile Adhoc Networks using Mobile Agents with no Manager. *International Journal of Computer Applications*, *111*(10).
19. Bharati, T. S., & Kumar, R. (2015, March). Secure intrusion detection system for mobile adhoc networks. In *Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on* (pp. 1257-1261). IEEE.
20. Bharati, T. S., & Kumar, R. (2015). Intrusion Detection System for MANET using Machine Learning and State Transition Analysis. *International Journal of Computer Engineering & Technology (IJCET)*, *6*(12), 1-8.
21. Bharati, T. S., & Kumar, R. (2016). Enhanced Key Distribution for Mobile Adhoc Networks. *International Journal of Engineering Science*, 6(4), 4184-4187.
22. Bharati T. S. (2017). Agents to Secure MANETS. *International Journal of Advanced Engineering and Research Development,* 4(11), 1267-1273.
23. Bharati T.S. (2018). MANETs and Its' Security. *International Journal of Computer Networks and Wireless Communication,* 8(4), 166-171.

AUTHOR'S PROFILE

Author is B.Tech, Master of Engineering, and Ph.D. in Computer Science stream and he has more than 18 years of experience at the time of writing this paper. He is currently working as Assistant Professor in the Department of Computer Science, JamiaMilliaIslamia (A Central University), New Delhi and before this university he has served in various Engineering Institutions at different n capacities i.e. like Associate Professor in Computer Science department.His area of interests includes Security, Theoretical Computer Science, Data Science etc.

.