



Necessity of Trust for security in MANETs

¹Gayathri.D, ²Dr. S. Janakiraman¹ Research Scholar, Bharathiar University, Coimbatore, Tamil Nadu, India² Assitant Professor, Department of Banking Technology, Pondicherry University, Pondicherry, India

Abstract: Mobile Ad-hoc Networks are infrastructure less network of mobile nodes with wireless medium such as radio frequencies and infrared rays. Earlier routing protocols did not include security considerations. However subsequent protocols included cryptographic methods to secure the transactions. But these methods fail if the malicious nodes are included in the transaction itself. (for example: if the node drops or delays the key information). So came a concept called trust which is the reliability on a node by other nodes to include the trusted node in the transactions. In this paper of survey trust, its importance and some of the basic attacks that can be overcome by the trust value and a simple computation of trust value has been discussed.

Keywords: ROUTE ERROR

I. INTRODUCTION

MANETs are network of autonomous mobile nodes that communicate over wireless links with no central administration. Hence used in places that have no communications infrastructure or a severely damaged infrastructure such as in disaster relief, low enforcement, military operations and in emergency rescue operations. Hence the protocols designed should be able to withstand and response to dynamically changing topology. In the fore coming years effective security enforcement in these protocols is major issue. Many research has been carried out for the same.

II. TRUST

Trust is a notation of human behaviour. The definition of trust is diverse with respect to different context. Trust is the quantified belief by a trustor with respect to the competence, honesty, security and dependability of trustee within a specified context.

Trust is the degree of reliability of a node by other nodes with prior experiences in the networking concept. It is the value of a node that is measured by other nodes at the time of data transmission to decide for the packet or data transmission through the trusted node.

III. IMPORTANCE OF INTEGRATING TRUST VALUE IN ROUTING PROTOCOLS

Initial MANET routing protocols such as AODV were not designed to withstand malicious nodes. Subsequent protocols started to apply to cryptographic methods to handle security issues. But there was no guarantee if the nodes inside the network of key exchange were malicious leading denial of service.

Hence comes the trust value which tells the degree of reliability of the node for the operation. Previous research proved there is some amount of delay in calculating the trust value and forwarding the packets but this negligible time delay outweighs the security issues.

IV. TRUST COMPUTATION

When we evaluate the experience of a trust vector, an important observation that needs to be undertaken is the measurement of the number of out-coming packets the immediate neighbouring node has genuinely sent. To understand this, node participation in packet forwarding should be monitored. When node comes to know that its immediate neighbour nodes are forwarding the packet, it checks packet integrity to determine that the packet is unmodified by other malicious nodes. If it observes that the neighbour node passes the integrity test, the out coming packet counter of this neighbour node should be incremented. But if they fail to pass the integrity test or if the neighbour node does not cooperate in forwarding the packets it is supposed to, its corresponding forwarding counter will remain unchanged. After sometime, its experience value would be exceedingly low on account of malicious behaviour.

The previous research papers gave different perception in evaluating trust value. The trust value can either be got by itself known as direct trust value or from other neighbour nodes or a combination of both of these values can be taken in to consideration.

The trust value will be adjusted based on the experiences that the node has with its neighbour nodes. Here a simple trust evaluation technique has been discussed.

$$TV = \tanh (R_x + R_y + A)$$

$$R_x = N_x / T_x \quad \text{and}$$

$$R_y = N_y / T_y$$

Where TV = trust value

R_x = ratio of number of packets forwarded successfully from neighbour node(N_x) to the total number of packets to be forwarded by neighbour node(T_x)

R_y = ratio of number of packets received successfully from neighbour node but originated by other node(N_y) to the total number of packets received from that neighbour node(T_y)

A = acknowledgement bit

To make security decision with the computed trust value, we need to define trust threshold for each ongoing task. And this threshold value depends upon the security requirement level for each task. By comparing the computed trust value and the threshold trust value, it is easy to see whether the trustee node satisfies the trust requirement or not. A simple equation for making decision is defined as follows:

$$D = TV - TT,$$

Where TT = threshold trust value

If $D \geq 0$, it means the computed trust value satisfies the trust requirement of the ongoing task. If $D < 0$, it means that the trust requirement is not satisfied.

V. OPTIMAL ROUTING WITH TRUST FACTOR

All the nodes perform its trust evaluation locally. To store the trust information, each node is expected to maintain a trust information table, which may contain the fields of trustee node' ID, trust value. The table is maintained with a soft-state approach, which means, unless it is refreshed, the trust information will expire after a period of time t . During the operation of the system, the nodes may choose to exchange their trust information periodically or upon request. If the information about a trustee node is not updated with the time t , the correspondent trust values will be assigned with 0.

The Optimal Routing Algorithm Can Be Summarised As Follows:

- Whenever a node has some packets that need to be sent or forwarded, it should first scrutinize the routing table or routing cache for all probable paths which can arrive at the same destination.
- After doing this, it makes a comparative study of trust value of all the next hops in those candidate paths and selects the path that is most proper and has the highest trust value.
- If the next hop is unknown by the sender or forwarder before, the least number of hops path to the destination is selected.
- All nodes should select neighbour nodes that have a trust value greater than or equal to the predefined trust value threshold in order to increase reliability.
- A local link repair process is initiated if there is unavailability of next hop in candidate paths according to trust level which should be greater than the trust threshold. Therefore, if there had been any data packets which should be forwarded with an improper trustworthy next hop, the forwarding action is stopped and buffered for a certain interval of time in which another route discovery would be started to find an alternate route that should be trustworthy.
- The packet would be sent to an alternate route if such a route is discovered. If this is not the case, then a ROUTE ERROR message would be sent to the source node informing it of the link error. Based on the various application environments, the trust value can be set up in several ways.

VI. CONCLUSION

In this paper of survey trust factor ,its computation ,importance and the integration has been discussed .This drastically increases the security but still the packet droppings due to overcrowding makes a question of the reliability of a node which is a successful mission to be undertaken.

REFERENCES

- [1] Imrich Chlamtac ,macro Conti ,Jennifer J,N.liu "Mobile AdhocNetworking:imperatives and challenges",Ad hoc networks 1(2003) 13-64 ,www.elsevier.com/locate/adhoc
- [2] Xia li,Jill Slay,Shaiokai Yu,"Evaluating Trust in Mobile Ad hoc Networks"
- [3] Manchala, D.W., "E-Commerce Trust metrics and models",IEEE Internet computing,IEEE 2000,pp 36-44
- [4] Shilpa S G ,Mrs. N.R. Sunitha ,B.B. Amberker,"A Trust Model for secure and QOS Routing in MANETs',International Journal Of Innovative Technology and creative Engineering(ISSN:2045-8711) vol.1 NO.5 may2011
- [5] Pirzada, A.A.,McDonald,C.:Establishing Trust in pure Ad hoc networks.Proceeding of 27th Australian computer science Conference(ACSC'04),2004,26(1):47-54