Implementation of Reputation Based Trust Management System Using NS-2 Simulator

Bhawna[1] Taruna[2]
[1]M. Tech Scholar[2]Assistant Professor
[1, 2]Computer Science & Engineering Department
[1, 2]KITM, Kurukshetra

Abstract—*Mobile Ad hoc Wireless Networks (MANET) is an infrastructure less, self-organized, and multi hop network. Distributed ad-hoc networks with no centralized nodeof command such as MANETs offer an interesting challenge inestablishing trust between nodes for the purposes of network security. Trust management becomes very important for the successful operation of MANET. Reputation system can be used to make decisions about which nodes to include and which nodes to exclude from the network. In Present study based on applying a reputation based trust management scheme on DSR (Dynamic Source Routing) protocol and through simulation results proves that the proposed method performs well compared to normal DSR.*

Keywords:- Mobile Ad hoc Wireless Networks (MANET), DSR (Dynamic Source Routing), TMS (Trust Management System, End Delay, Protocol, Node

I. Introduction

Mobile Ad hoc Wireless Networks (MANET) is an infrastructure less, self-organized, and multi hop network. MANET is autonomous system in which nodes have to act as host and as routers. It has dynamic topology. A MANET (shown in fig 1) is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure [1]. It's very important part of communication technology that supports truly pervasive computing, because in many contexts information exchange between mobile units cannot rely on any fixed network infrastructure, but on rapid configuration of wireless connections on the fly [3]. Wireless ad hoc networks themselves are an independent, wide area of research and applications, instead of being only just a complement of the cellular system [4].

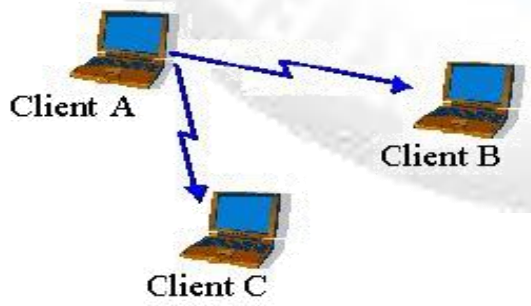

Fig. 1: Mobile Adhoc network

A. Manets Characteristics & Challenges

Manets have several characteristics & challenges they are as follows: -

1) Dynamic Topologies:-
MANET is an infrastructure less and networks are fully distributed which can work at any place without any need of infrastructure. So they are highly flexible and robust.

2) Bandwidth-Constrained, Variable Capacity Links:-
Wireless links considerably have lower capacity than their hardwired counterparts. Interference conditions, fading, noise, is frequently much less than a radio's maximum transmission rate.

3) Energy-Constrained Operation and Limited Battery Life:-
In a MANET all of the nodes may rely on batteries. Higher Packet losses due to errors in transmission such as hidden terminals that results in collisions, interference, frequent breakage in paths caused by mobility of nodes, increased collisions.

4) Limited Physical Security:
MANET does not provide a physical protection of computers due to Limited resources, generally more prone to physical security threats than fixed-cable nets. The increased risk of eavesdropping, spoofing, selfish behavior and denial-of service attacks should be suspiciously considered [2].

II. Routing Protocols In Manets

Routing protocols in Mobile Adhoc Networks are majority of two categories:
1. Proactive Protocols
2. Reactive Protocols

A. Proactive protocols: In Proactive protocols, each node maintains routing Information to every other node in the form of table. These tables are updated if network topology changes. Keeping routes to all destinations up-to-date, Even if they are not used, is a disadvantage of this protocol.

B. Reactive protocol: Reactive protocol is used to find the route when demanded or when needed by the source node in order to transmit the data to destination node. Intermediate node does not need to maintain up to date routing information. They consume bandwidth only when the node starts transmitting the data to destination node [5].

C. Dynamic Source Routing Protocol:

This protocol is reactive protocol.DSR uses source routing to deliver packet the source node add the full path to destination in terms of intermediating node in every packet. DSR operates on two mechanisms Route discovery **&** Route maintenance.

1) Route discovery:-
Route Discovery is used when a source does not know the path up to the destination. In this mechanism, the sender broadcasts a ROUTE REQUEST message which contains Source Address, Destination Address, and Identifier. Each

intermediate node adds its address in ROUTE REQUEST message and rebroadcast it, unless it reaches the destination. The destination then sends a unicast ROUTE REPLY message to source node and the source node add this new route in its cache.

2) Route Maintenance:-

Route Maintenance is used to handle route breaks. When a node encounters a fatal transmission problem at its data link layer, it removes the route from its route cache and generates a route error message. When a node receives a route error message, it removes the hop in error from its route cache [6].

III. Trust Management System

Trust management has a dynamic nature not static & it is defined as the degree of subjective belief about the behavior of a particular entity. Trust Management acts as a separate component of security services in networks and identified it as a unified approach [7]. Trust management is a special case of risk management with a particular emphasis on authentication of entities under uncertainty and decision making on cooperation with unknown entities as shown in fig 2.

Fig. 2: Trust management system [8]

Trust management includes trust establishment (i.e., collection of appropriate trust evidence, trust generation, trust distribution, trust discovery, and evaluation of trust evidence), trust update, and trust revocation. Trust establishment is defined as the process of maintaining and distributing trust among nodes. Mainly there are two schemes used to evaluate trust

1. Policy based trust management
2.Reputation bases trust management

A. Policy-based trust management: This approach usually makes a binary decision according to which the requester is trusted or not, and accordingly the access request is allowed or not. Due to the binary nature of trust evaluation, policy-based trust management has less flexibility. Furthermore, the availability of (or access to) trusted certificate authorities (CA) cannot always be guaranteed, particularly for distributed systems such as MANETs [10].

B. Reputation-based trust management: Reputation-based trust management utilizes numerical and computational mechanisms to evaluate trust [9].

IV. Present Work

Present work is to apply reputation mechanism to DSR and evaluate its performance & for that simulation tool is used to study the performance. The evaluation will be done according to the following metrics:

1. Packet Delivery Ratio
2. End to End Delay
3. Packet Drop

V. Simulation Setup And Scenario

The studied scenario consists of 7 mobile nodes. The topology is a rectangular area with 1000 m length and 1000 m width. A rectangular area was chosen in order to force the use of longer routes between nodes than would occur in a square area with equal node density. All simulations are run for 15.00 seconds of simulated time as shown in fig 3 & fig 4.

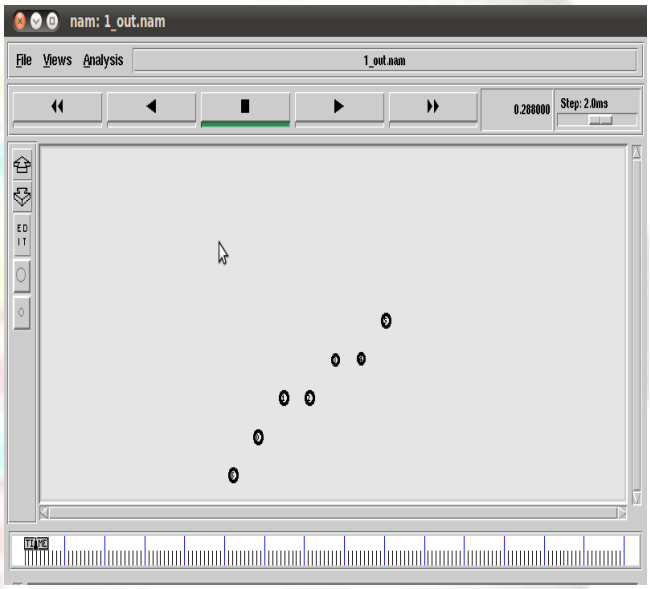

Fig. 3: Mobile nodes at initial states

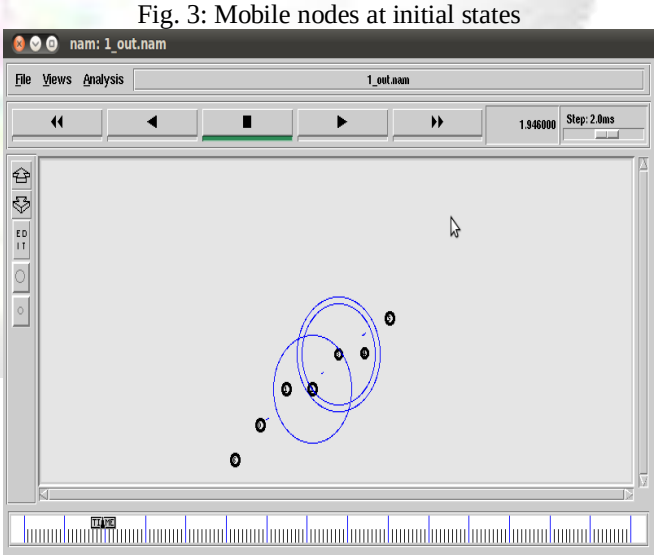

Fig. 4: Transfer of Data from node 0 to node 5 via node 2 and node 3

VI. Result & Discussions

*A. Packet Delivery Ratio:-*This parameter shows the number of packet received to the total no of packet sent during the simulation period in the network. The result shows that the reputed DSR routing protocol has higher value of data packet received as compared to the simpler DSR as shown in fig 5.

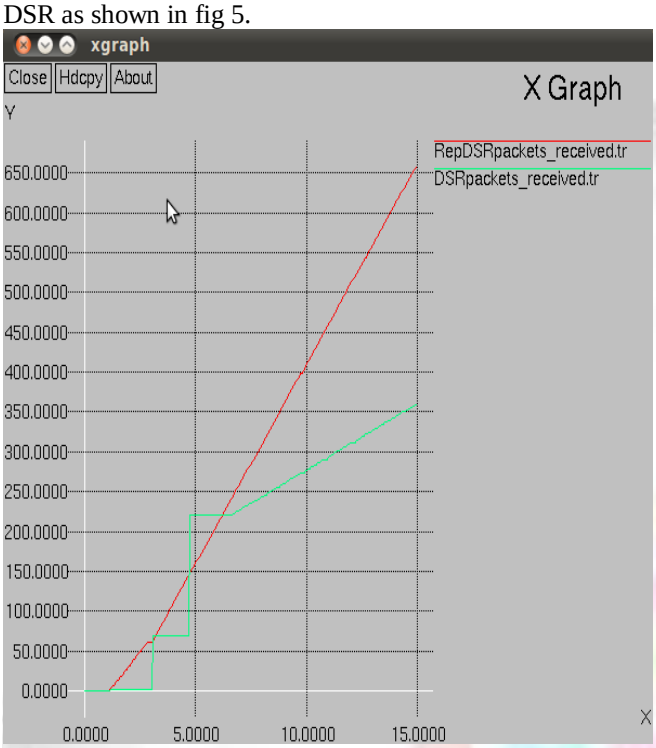

Fig. 5: X-graph of packet received in Reputed DSR & Simple DSR

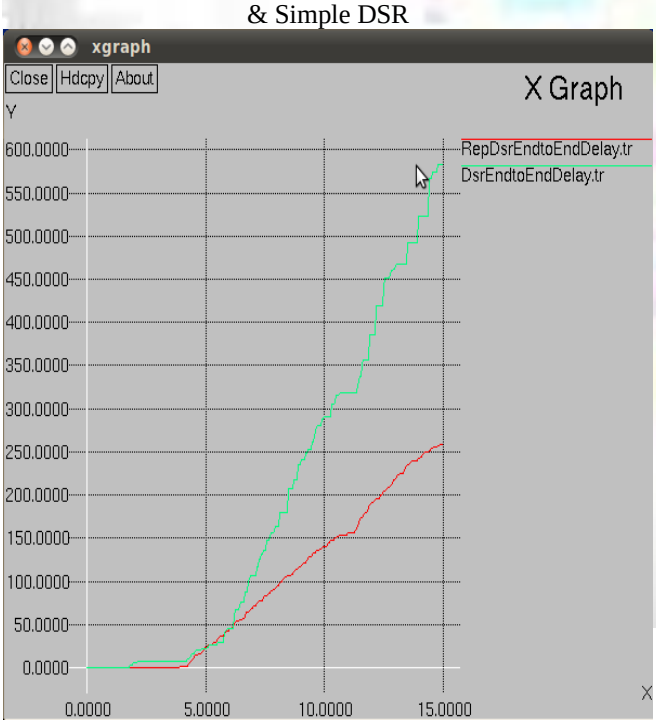

Fig. 6: X-Graph of end to end delay in Reputed DSR & simple DSR

B. End to End Delay

End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination as shown in fig 6. From the above figure we examine that the end to end delay is a lesser amount of in proposed technique as compare to the simple DSR protocol.

C. Packet Drop

Packet drop ratio is the ratio of data packets drop during the simulation period to those generated by the sources. The below figure shows that when we apply the propose scheme packet data drop ratio achieved in reputed DSR is very less as compare to simple DSR protocol as shown in fig 7.

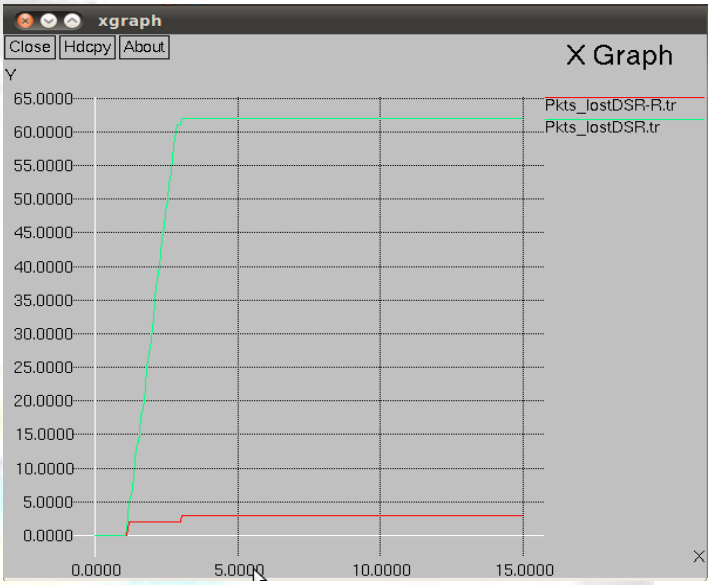

Fig. 7: Packet drops in both cases.

VII. Conclusion

Trust is not a constant value, it changes over time. Trust between nodes is important to perform functions of the network. Trust management is necessary when nodes participating with each other to perform certain actions. Trust management framework evaluates trust among nodes in the network and then form trust relations between them. In this paper, we present a scheme for ad-hoc network in order to increase the route reliability between the nodes present in network. We have shown that our scheme is robust in finding the safe and sound path for the sender and receiver. This approach has the clear advantage of simplicity, ability to get a trustworthy route etc.

References

[1] Jin-He Cho and Ingo-Ray Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks", IEEE VOL. 13, NO. 4, 2011.pp 20-25.

[2] Z. Liu, A. W. Joy, and R. A. Thompson, "A Dynamic Trust Model for Mobile Ad Hoc Networks," Proc.10th IEEE Int'l Workshop on Future Trends ofDistributed Computing Systems, Suzhou, China, 26-28 May 2004, pp. 80-85.

[3] V. Varadharajan, "A note on trust-enhanced security," Security & Privacy, IEEE, vol. 7, no. 3, 2009, pp. 57-59.

[4] J. Hu and M. Burmester, "Cooperation in mobile ad hoc networks," Guide to Wireless Ad Hoc Networks, 2009, pp. 43-57.

[5] J. Sen, "A Distributed trust management framework for detecting malicious packet dropping nodes in a mobile ad hoc network," Arxivpreprint arXiv:1010.5176, vol. 2, no. 4,2010, pp. 92-104.
[6] R. Zhou, M. Ieee, K. Hwang, F. Ieee, C. Society, and M. Cai,"Gossip Trust for Fast Reputation Aggregation in Peer-to-Peer Networks,", vol. 20, no. 9, 2008, pp. 1-14.
[7] B. Qureshi, G. Min, and D. Kouvatsos, "M-Trust: A Trust Management Scheme for Mobile P2P Networks," in 2010, IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2010, pp. 476-483.
[8] Bowman, T.H. Lacey, "Using reputation-based multilayer security to protect MANETs", Computers & security, Vol 6, 2012 pp. 122 -136.
[9] Anna Satsiou, Leandros Tassiulas, "Reputation-Based Resource Allocation in P2P Systems of Rational Users", IEEE Transactions on Parallel and distributed system, vol. 21, no. 4, 2010, pp 100-105.
[10] Jose L. Munoz, "RDSR-V. Reliable Dynamic Source Routing for video-streaming over mobile ad hoc networks", Elsevier Computer Networks, 2009, pp 50-55.