Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MaNeT

R. S. Mangrulkar
Assistant Professor.
B.D.College of Engineering,
Sevagram, Wardha,
Maharashtra, India

Pallavi V Chavan
Assistant Professor.
B.D.College of Engineering,
Sevagram, Wardha,
Maharashtra, India

S. N. Dagadkar
Assistant Professor.
B.D.College of Engineering,
Sevagram,Wardha,
Maharashtra, India

ABSTRACT
An ad-hoc network comprises of mobile nodes that cooperate with each other using wireless connections to route both data and control packets within the network. They are characterized by the use of wireless links, dynamically changing topology, multi-hop connectivity and decentralized routing mechanism and decision-making. The performance of Ad-hoc On Demand Vector (AODV) protocols has been modified by including the source route accumulation feature. As low transmission power of each ad-hoc node limits its communication range, the nodes must assist and trust each other in forwarding packets from one node to another. However, this implied trust relationship can be threatened by malicious nodes that may fabricate, modify or disrupt the orderly exchange of packets. Security demands that all packets be authenticated before being used. A particularly hard problem is to provide efficient broadcast authentication, which is important mechanism for MaNet. In this paper, we propose a routing algorithm which adds a field in request packet which stores trust value indicating node trust on neighbour. Based on level of trust factor, the routing information will be transmitted depending upon highest trust value among all. This not only saves the node's power by avoiding unnecessary transmitting control information but also in terms of bandwidth (channel utilization), which is very important in case of MaNet. The malicious node can attack on the control packet and misbehave in the network .The malicious node, which may or may not be trusted node. In this paper, we use trusted path irrespective of shortest or longest path which can be used for communication in the network. We are able to calculate route trust value on the complete reply path which can be utilized by source node for next forthcoming communication in the network.

General Terms

Reactive Routing Protocol.

Keywords: Ad-hoc, AODV, Route trust, MaNet, Malicious node.

1. INTRODUCTION
Most traditional mobile ad hoc network routing protocols were designed focusing on the efficiency and performance of the network [1]. Ad hoc network are wireless network with no fixed infrastructure in which nodes depend on each other to keep the networked connected. Topology based routing protocols use the information about links for packet forwarding. Position based routing protocols use node's geographical position to make routing decisions, resulting in improved performance under extremely dynamic network condition[2].The Internet is growing at very large pace and has became one of the largest public network, allowing personal and business communications. The rate at which the use of internet is growing is increasing day by day. More and more use of internet is done by managers, workers, branch offices and business tycoons to remotely connect to their networks and to perform commercial transactions via the World Wide Web[3].Due to wide use of internet by common man for personal work and tremendous use by business persons, internet is very prone to threat attacks. Although network attacks are presumably more serious when they are inflicted upon businesses that store sensitive data, such as personal medical or financial records, the important data can be lost, privacy can be violated [4].An ad-hoc network is a collection of autonomous nodes or terminals that communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner. Each node functions as both a host and a router. More critically, the network topology is in general dynamic, because the connectivity among the nodes may vary with time due to node departures, new node arrivals, and the possibility of having mobile nodes. Ad hoc networks are particularly vulnerable as compare to traditional networks mainly due to their lack of infrastructure [10]. A malicious node can easily disrupt both the routing discovery phase and the data forwarding phase of a routing protocol if it is not secured enough. Ad hoc networks, due to their improvised nature, are frequently established in insecure environments and hence become susceptible to attacks. These attacks are launched by participating malicious nodes against different network services. Routing protocols, which act as the binding force in these networks, are a common target of these nodes.

2. LITERATURE SURVEY
With the advancement in radio technologies like Bluetooth, IEEE 802.11 or Hiper LAN, a new concept of networking has emerged. This is known as ad-hoc networking where potential mobile users arrive within the common perimeter of radio link and participate in setting up the network topology for communication. Nodes within ad-hoc are mobile and they communicate with each other within radio range through direct wireless links or multihop routing. Ad-hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. The AODV can be used in various commercial fields such as military tactical and other security-sensitive operations are still the main applications of ad-hoc networks.Ad-hoc networks are a new paradigm of wireless communication for mobile hosts (which we call nodes). For example, military units (e.g soldiers, Tanks, or planes), equipped with wireless communication devices, could form an ad-hoc network & they roam in a battlefield [8][10]. Ad-hoc networks can also be used for emergency, law enforcement, and rescue missions. Since an ad-hoc network can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial use such as sensor networks. The build-up of ad-hoc network can be envisaged where support of wireless access or wired backbone is not feasible. Ad-hoc wireless network does not have any predefined infrastructure and all network services are configured and created on the fly. Thus it is obvious that with lack of infrastructural support and susceptible wireless link attacks, security in ad hoc network becomes inherent weakness. Node mobility in an ad-hoc network causes frequent changes of the network topology.

The popular and widely used Ad-hoc On-demand Distance Vector (AODV) Routing protocol as a representative candidate

for constructing our trust framework [13]. The goal is to make minimal changes to the functioning of AODV and obtain an increased level of security and reliability. Our scheme is based on incentives & penalties depending on the behaviour of network nodes. They allow source nodes to choose more trusted paths rather than just shorter paths during route discovery in ad-hoc networks and isolate any malicious nodes from the network. Our schemes incur minimal additional overhead and preserve the lightweight nature of AODV. We illustrate the adaptability of our schemes by extending them to AODV's multi-path variants. Slight modifications will make our schemes applicable to other routing protocols like DSR and ZRP.We used ns2(network simulator version-2) for displaying the various effects of trust based framework.[14] NS (version 2) is an object-oriented, discrete event driven network simulator developed at UC Berkely written in C++ and OTcl (Tcl script language with Object-oriented extensions).Existing routing protocols for MaNet use shortest path to the destination as their route selection criterion. Ad-hoc On-demand Distance Vector Routing (AODV) is one such widely used lightweight routing protocol. However, the selected shortest paths to the destination may not always be the best. Such paths may be congested, they may include malicious or selfish nodes, or they may be adversely affected by other network or physical conditions. The source node may not be aware of any such route conditions. AODV route replies would only contain information about the number of hops, route freshness, sequence numbers, and the source and destination IDs [11]. AODV has no built-in measures to detect the above mentioned adverse route conditions. A secure variant of the AODV protocol, SAODV, uses one-way hash chains and digital signatures. But even SAODV fails to provide any information on route dependability. It only guarantees message authenticity. Security and robustness of the protocol would be improved if nodes could make informed decisions regarding route selection based on transmitted route requests and additional information contained in received route replies. Thus, additional information on the nature of routes would enable the source node to choose a route that best serves its purpose. The source node could utilize route dependability information to increase the probability of its packets reaching the destination. In this project, we provide a Trust-based framework which uses Route Trust as a metric for the source node to make such informed route selection decisions. Related literature on improving the performance of AODV includes multi-path variants of the protocol which are equally susceptible to malicious node behaviour. Schemes to make the protocol secure rely on heavy encryption techniques or on continuous promiscuous monitoring of the neighbours; both of which are restrictive in the resource constrained wireless domain and would have scalability concerns. Besides, these schemes only assure node and hop count authentication while providing no information on the route quality or ambient route conditions. Additionally, our schemes also aim at preserving the lightweight nature of AODV, while being adaptive, secure, robust and scalable.

3. PROPOSED ROUTING PROTOCOL, TBAODV

Ad-hoc network consists of mobile nodes which are randomly scattered within the network. They are characterized by the use of wireless links, dynamically changing topology, multi-hop connectivity and decentralized routing mechanism and decision making.

Figure: 1 gives the network diagram for an ad-hoc network consisting of 14 nodes numbered from 1 to 14.These nodes are connected by wireless links and randomly scattered in the network.

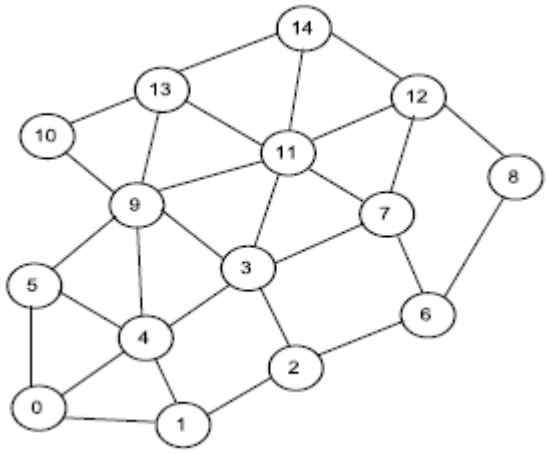

Figure 1: Network Topology

Algorithm for different functions used in packet transmission and reception routine as follows:

Step 1:-

Initially trust value 100 is assigned to all nodes in the network using assign trust ( ) function.

Step 2:-

Trust value are printed using Print_trust ( ) function.

Step 3:-

Source node broadcast request to all its neighbouring node using Send_Request( ) function.In this function hop count is initialized. Scheduler class is invoked to run the simulation.

Step 4:-

Neighbouring node receive the request then it will check whether it is destination or not. If it is Destination then it will Send_Reply( ) function otherwise forward request to its neighbouring node. This will check in Receive_Request( ) function.

Step 5:-

After confirming that it is not destination, it will further forward request to all its neighbouring node using Forward_Request( ) function. Hop count is increased at each node.

Step 6:-

6.1 If it is destination then it will send reply using Send_Reply( ) function

6.2 Trust value 200 is assigned to all nodes in the path from destination to source node.

6.3 Now, Source becomes destination for the current node.

Step 7:-

7.1 After receiving the reply then the decision will take whether the index node is destination or not using Receive_Reply( ) function.

7.2 If it is not destination then it will forward reply.

4. SIMULATION RESULT

For simulating our proposed routing protocol, we used global network simulator, NS2. We used same network topology shown in Figure: 1. The Simulation result prove that the trust based AODV is more secured as compared to Normal AODV routing Protocol.

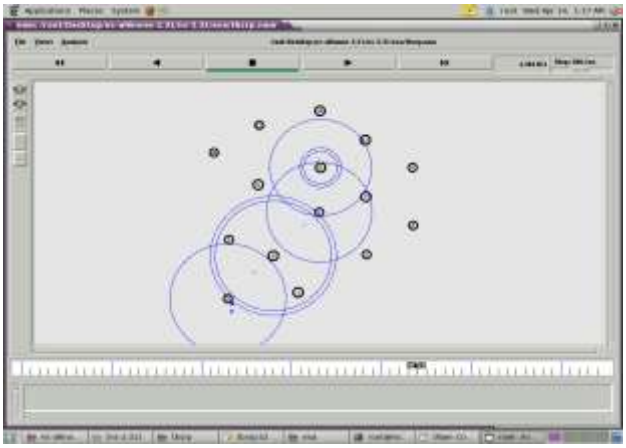

Figure 2: RREQ Transmission

Figure 3: Trust Value Calculation

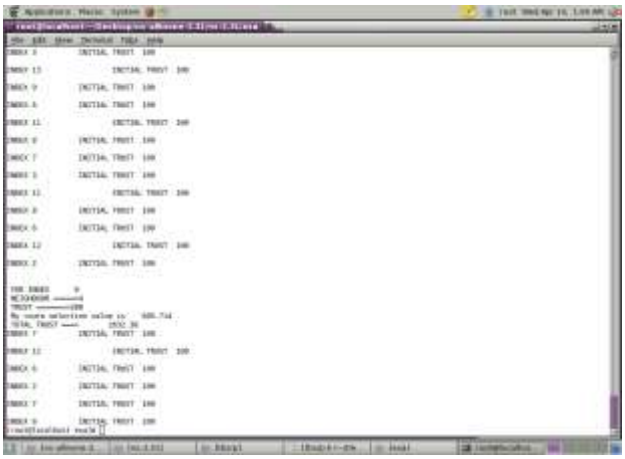

Figure 4: Trust Value Calculation

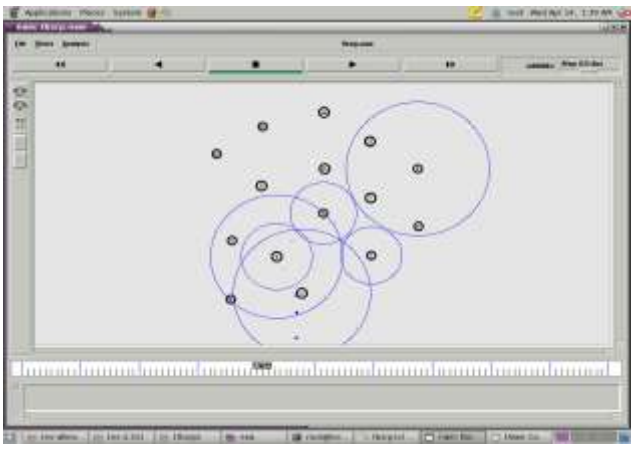

Figure 5: RREP Transmission

Figure 2 shows RREQ transmission. Figure 3 and 4 shows Calculated trust values for the nodes along the path in the network during RREQ transmission. Similarly Figure 5 shows RREP transmission.

5. RESULT ANALYSIS

For RSV Calculation we use following formula

$$RSV = \frac{Tind}{Tavg} * RTind * \frac{Havg}{Hind}$$

Tind- Trust on the individual neighbour (node trust)

Tavg-Average of all the neighbour that forwarded and generated RREP

RTavg- Trust the individual neighbour has on the route

RTavg- Average of all the route trust obtained from the individual nodes which forwarded/generated the RREP

Hind- Number of Hops in the route proposed by the individual node in its RREP

Havg- Average of all Hind s' obtained from the individual neighbour which forwarded the RREP

Consider Path 0-4-3-11-14. The Table : 1 gives the RSV value and Node Trust values.

Table 1: RSV values for Path-I

Node ID	R	Node Trust
0	**4**	**200**
4	**3**	**200**
3	**11**	**200**
11	**14**	**200**

Values of parameters are as follows

RSV_0= 685.714

RSV_4= 480

RSV_3 = 1466.66

TOTAL RSV FOR PATH-1 = **2632.38**

Consider another path 5-9-13-14. The Table :2 gives the RSV value and Node Trust values.

Table 2: RSV values for Path-II

Node ID	R	Node Trust
5	**9**	**200**
9	**13**	**200**
13	**14**	**200**

RSV_5=1440

RSV_9=1733.33

TOTAL RSV FOR PATH-2=**3173.33**

6. CONCLUSION

Trust in the network is nothing but the faith of one node on other. Trust based path is secured to use and increase the confidentiality of data being transferred. In this paper, we proposed trust based Adhoc On-Demand Routing protocol. We introduce extra field in the route request format. This field indicating trust value is updated on every successful data transmission. The forthcoming data transmission is based on the route selection value calculated for each RREQ path. This route selection value is used to select most trusted path rather than

selecting shortest or longest path. This significantly improves the trust factor of one node on the other nodes in the network. This is useful in forthcoming communication in the network. Thus we concludes that the trust based routing protocol proposed in this paper enhance the security level and also improves the faith factor of source and destination on the selected trusted path in the network. This paper suggest some modification in the working of AODV routing protocol in the direction of enhancing security level.

7. REFERENCES

[1] P Narayan, V R. Syrotiuk ,"Evaluation of the AODV and DSR Routing Protocols Using the MERIT Tool," *in the proceeding or ADHOC-NOW* in the year of 2004.

[2]B. Murthi, "AODV routing protocol" *in book on mobile communication* , 2000.

[3] Ariadne, "A Secure On-Demand Routing Protocol for Ad-Hoc Networks" *in the proceeding of MOBICOM*, 2003.

[4] G. Theodorakopoulos and J. S. Baras , "Trust evaluation in ad-hoc networks," in *Proceedings of the ACM Workshop on Wireless Security (WiSE'04)* , Oct. 2004.

[5] M. Virendra, M. Jadliwala, M. Chandrasekaran, S. Upadhyaya , "Quantifying Trust in Ad-Hoc Networks" *in the Proceedings of IEEE international Conference on Integration of Knowledge Intensive Multi- Agent systems (KIMAS)*, 2005.

[6] Y. L. Sun, Z. Han, W. Yu and K. J. R. Liu ,"A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense against Attacks" *in the proceeding of IEEE INFOCOM* , 2006.

[7] A. Perrig, J. Stankovic,D. Wagner ," Security in Wireless Sensor Networks" *in the proceeding of Communication of the ACM*, June 2005.

[8] Kamal Deep Mekaetal ," Trust Based Routing Decisions In Mobile Ad Hoc Networks," *in the proceeding of The Second Secure Knowledge Management Workshop (SKM)*,2006.

[9]Zheng Yan and Peng Zhang, "Trust Evaluation Based Security Solution in Ad-hoc Networks" 2000.

[10] "An implementation study of the AODV routing protocol" by

[11] Elizabeth. M. Royer and Charles. E. Pekins. , "Ad hoc on-demand distance vector routing" 2000.

[12] X. Li, M. R. Lyu, J. Liu ,"A Trust Model Based Routing Protocol for Secure Ad Hoc Networks" *in the Proceedings of IEEE Aerospace Conference (IEEEAC)in the year of* 2004.

[13]M. G. Zapata and N. Asokan, "Securing Ad hoc Routing Protocol" i*n the proceeding of 3rd ACM workshop on Wireless Security in the year of* 2002.

[14] Most of the NS2 source code is in c++, www.isi.edu.

[15] A. Pirzada, C. McDonald ,"*Establishing Trust In Pure Ad-hoc Networks", in the Proceedings of the 27th conference on Australasian computer science*, 2004.