Secure AODV Routing Protocols Based on Concept of Trust in MANET's

Vijaya Singh, Megha Jain

Abstract—**Mobile Adhoc Networks or MANET is temporary infrastructure less network which is comprised of mobile devices that dynamically form their network quickly without any central administration. The mobile nodes in the network co operate among themselves for proper functioning of network on hop by hop basis. Thus, Manets face challenges in terms of security issues, frequent topology changes, nodes limitations such as energy resource and communication limitations such as channel bandwidth, reliability. Robust protocols are required to ensure security, proper functioning, reliability of network and maintained quality of service. There are studies focused on security in Manets based on trust concepts in AODV routing protocols given in the past. In this paper, we discuss the different trust based AODV protocols proposed by researchers to ensure secure routing and improved network performance.**

Index Terms— **mobile devices, mobile Adhoc network, network performance, trust, Trust based AODV.**

I. INTRODUCTION

Mobile Adhoc networks is a collection of mobile devices or terminals which communicate with each other by Wireless links, without any central administration [1][14]. Nodes in the network act as both host and router that is it can act as destination or it can forward the data to the destination. These nodes are characterized by limited bandwidth, power, highly mobile and quickly deployable. Due to high mobility frequent disconnections occur that change the network topology and lead to various security threats. Nodes communicate on hop by hop basis for the functioning of the network in same way as happens in fixed infrastructure network but as there is no central administration, nodes are the active participants in the network.

Routing in Manets is on hop by hop basis. It depends on several factors like topology, selection of routes, initiation of request etc. Protocols can be classified in to 3 types: Reactive Protocols, Proactive protocols and Hybrid protocols. Reactive protocols or on demand protocols are those which find routes on demand whenever needed. It decreases the overheads in terms of less control messages but there is an increased latency in discovering the routes. Proactive protocols or table driven protocols find routes for transmission beforehand and every node maintains a table in which routes are updated when ever any change occur. There is no delay in route discovery but considerable overheads. Hybrid protocols are the combination of reactive and proactive routing protocols that is to take advantage of both by reducing the control message overheads and decrease the delay in route discovery. AODV is a reactive protocol; it establishes routes only on demand. Several trust implemented AODV protocols have been discussed, along with their strengths and limitations. The security mechanism for MANET should be robust enough to deal with security threats and should have low computational complexity, less overheads, and efficient to detect malicious nodes. Also there should not be any centralized authority or trusted third parties to issue trust values and observe the behavior of nodes in the network.

The rest of the paper is organized as follows: Section II presents trust and its importance. Section III presents the AODV routing protocol. Section IV presents the TRUST based AODV routing protocols. Section V presents the comparative study and Section VI presents conclusion and future enhancement.

II. TRUST & ITS IMPORTANCE

Trust has received different definitions in different disciplines thus we can say that trust is multidisciplinary [3]. Trust plays a very prominent role in mobile Adhoc networks as the routing decision in it are based on cooperation among the nodes. Thus it is necessary that nodes in the network participating in the transmission of data are trustworthy and perform as desired. Trust in any node tells about the genuineness of that node. Trust is also referred to as the belief that nodes in the network will perform in accordance with the network and will not behave selfishly. Trust is genuineness of any node in the network. Various classification and properties of trust are given below [3][4][13]:

A. Trust Classifications:

1. **Trust as risk factor:** risk is involved when there is no previous notion about the behavior of any node in the network.
2. **Trust as belief:** It is nodes belief in other node trust qualities that it will perform as expected.
3. **Trust as subjective probability:** it refers to trust as expected behavior of peers with reference to specific context and time.
4. **Trust as transitive relationship:** it refers trust as transitive in nature. If node A trust B and B trusts node C then it can be concluded that A trusts C.

B. Trust Properties:

1. Trust is **dynamic**, it is not static and changes with time, location etc. As Manet in itself is highly mobile and change

Manuscript received Dec, 2014

Vijaya Singh *ise currently pursuing masters degree program in computer science engineering, in JSS Academy of Technical Education, Noida, India. E-mail: vijayargec@gmail.com*
Megha Jain *is professor in Deptt. Of CSE JSS Academy of Technical Education, Noida, India. E-mail: meghajain12@gmail.com*

topology frequently, the trust value should be based on temporary and local information.

2. Trust is **context dependent**, trust value of a node depends on the given task may be high for one but same node may have lower trust value for other task.

3. Trust is **asymmetric**, it means that if a node trusts a particular node then there is no condition as such that the node will be trusted in return by that node to that extent.

4. Trust is **subjective**; the node may have different trust values for the same node in different situations due to changing network topology.

5. Trust is **composite**, the trust values obtained from different sources can be combined to get the accurate value thus trust is composite.

C. Trust computation:

It can be direct, indirect and hybrid combination of both direct and indirect [4]. Trust is evaluated based on ‘observation’, ‘experience’ and ‘knowledge’.

1. **Direct trust** is based on nodes own observation and experience about the behavior of node. Direct trust is computed solely on the basis of nodes own view about the behavior of a particular node.

2. Recommendations is used to compute **Indirect trust**, when any particular node does not have a direct trust on any node then the other nodes can recommend the trust value based on their own observation and experiences.

3. **Hybrid trust** is combination of direct and indirect trust, it uses experience and recommendations based approach to compute trust for any node.

D. Importance of Trust in MANETS

Mobile Adhoc networks are infrastructure less, highly dynamic and self organizing networks. As the nodes are the devices maintaining activities in the network and no centralized administration Manets are vulnerable to security threats. Trust is an important parameter to decide whether a node is trustworthy or not. As routing in Manet is hop by hop there is a dependency on intermediate nodes to forward the packets. Intermediate nodes could be good or bad nodes which try to harm the network by acting maliciously or can behave selfishly to save its own resources. Thus, the concept of trust is very important in mobile Adhoc networks to improve the performance and ensure secure routing of data through trusted peers.

III. AODV ROUTING PROTOCOL

Ad-hoc On demand Distance Vector (AODV) routing protocol is a reactive protocol or on-demand protocol [2][15] that establishes the route only on demand and always search for the shortest path irrespective of reliability of the path. There is a decrease in the control message overheads but the average latency in route discovery is increased. AODV also makes use of sequence numbers which ensure that routes do not have loops and determines the freshness of any route. AODV maintains tables in the node itself there is a less memory overhead. The working of AODV routing protocol that is route discovery and maintenance along with its advantages and disadvantages are explained in the following subsections:

A. Routing process in AODV

1. When source node wants send any message to any destination node, source node looks for the route to destination in its routing table. It sends the route request RREQ message to all of its neighbors.

2. This RREQ message forwarding continues until the destination or neighboring nodes find the route to destination.

3. The destination node sends the route reply message RREP, it travels the reverse route. When the source node receives the RREP packet it checks the destination sequence number which should be greater than destination sequence number of RREQ packet.

4. If there is any problem on the route, Route Error message (RERR) is sent to the transmitting node to inform about it and start the process of transmission again. HELLO messages are used by AODV periodically for Route maintenance.

B. Advantages/Disadvantages:

1. The advantages of AODV are, the routes are created on demand only and it uses sequence number to determine whether a route is stale or fresh.

2. The connection setup delay is lower.

3. AODV is loop free protocol and hence avoids the counting to infinity problem.

4. The disadvantages of AODV are, high latency time in route discovery as it finds route on demand.

5. Stale entries in sequence number and high bandwidth consumption.

6. Excessive flooding of route request packet leads to multiple route reply packet for single route request packet thereby increasing control overhead [15].

IV. TRUST BASED AODV ROUTING PROTOCOLS

There have been significant works earlier based on trusted third parties or key management system but they have own limitations like very expensive and complex computations. We have described here various trusts based routing AODV protocols. Mobile Adhoc networks which due to absence of any infrastructure are prone to several security threats. Existing approaches find the shortest path which may not always be the best and reliable path. The intermediate node could be malicious, thus we need such protocols which find not only shortest but reliable path and detect malicious nodes. Also there should be less overheads and can handle congestion in the network.

A. Trust Model Based Routing Protocol for Secure Ad hoc Networks

Xiaoqi Li *et al* [5] have proposed a model based on Trust and routing table has three additional fields’ positive events, negative events and opinion. The trust is computed based on opinion about the trustworthiness of any node. The three components of opinion are belief, disbelief and uncertainty. The sum of the three components is 1. In this approach node maintains record of positive and negative evidences about other node to determine the opinion about that node. Node collects all its neighbors opinion and combine them using combination operations such as Discounting Combination and Consensus Combination. Discounting combination is used when there is a recommendation approach, A has opinion about B, B has about C then A can combine the two opinions to get the opinion about C using discontinuous combination. Consensus combination is used when all nodes have contrary opinions then it will be used to get relative evaluation. It detects and eliminates malicious nodes as time passes.

The protocol is implemented using ns 2.34 with traffic type UDP, transmission range 100 m, packet size 1024 bytes, data rate 100 kb/s, pause time 10s, minimum speed 1 m/s and simulation time 900s. Packet drop is also very less in TAODV. Throughput and packet delivery ratio is improved over standard AODV.

B. Reliable Ad-hoc On-demand Distance Vector Routing

Sandhya khurana *et al.* [6] proposed the extended AODV called RAODV by adding route discovery unit (RRDU) and reliable route reply unit (RRDU_REP) as two new control messages. RRDU messages are sent by source node to the destination at regular intervals along with the RRDUID. RRDU_REP is the response message which is sent by destination to source node. The routing table is modified using Reliability List field. RL field consists of source address, forward data packet (FDPC) and RRDU-ID. HELLO messages for route maintenance. RAODV performs better than AODV when there are malicious nodes as AODV fails in presence of malicious nodes.

C. Trust Based Secure Routing in AODV

A.Menaka Pushpa [7] proposed a trust based AODV protocol based on route trust and node trust both. Route Table and Neighbor Table are maintained at every node. Route Table has an entry as route trust field which stores detail of routes. Neighbor Table has two fields' neighbor_id and trust value which stores details of node trust. Route establishment is based on node trust and route trust is computed. Any change in the behavior of nodes in the route trust is monitored regularly. Route trust value stored in the route reply packet is used to establish route.

The protocol is simulated using NS-2 with maximum of 50 nodes and shows improved results in comparison to AODV protocol. It is robust as it considers both route trust and node trust to select a route. Route congestion can occur and overheads appear to be certain limitations.

D. Trust based AODV protocol (TBAODV)

Mangrulkar *et al.* [8] proposed TBAODV to improve the route selection mechanism using trust parameter. This trust parameter is introduced in the route request format which is updated on every successful data transmission. Based on this value a route is selected which is more trusted and reliable. The NS-2 simulator is used to simulate the above protocol and it shows improvement over normal AODV. It is more secure and robust.

E. Trust Based Reliable AODV Protocol

Sridhar Subramanian *et al.* [9] proposed trust based reliable AODV abbreviated as TBRAODV. It is able to detect the misbehaving nodes and mark them untrustworthy. Trust value is computed for every node in the network. Based on the trust value the behavior of node is determined as trustworthy or not. Only reliable nodes are allowed to participate in routing for reliable routing of data and unreliable nodes are not allowed to participate. The advantage of this approach is it identifies the bad nodes already. It was simulated on NS-2 simulator and the network performance parameters like packet delivery ratio and less delay shows improvement as compared to normal AODV.

F. Secure Ad-hoc On Demand Distance Vector Routing

Durgesh Wadbude *et al.* [10] proposed an efficient secure AODV routing protocol which allows authentication of AODV routing data. Hash chains, Digital Signature and Protocol Enforcement Mechanism to secure packets in AODV. Hash Chain is used to secure the Hop count. SAODV includes another feature which allows intermediate nodes to reply to RREQ message. For a single message the signature needs to be generated and verified when it receives RREQ and similar for RREP. Intermediate nodes can store this second signature in their routing table along with other routing information. If one of the nodes receives a RREQ message it can reply with RREP message similar to AODV. To achieve that intermediate node generates the RREP message which includes the signature of source node and signs the message with its own private key. This is called double signature.

In comparison to AODV, secure AODV messages are bigger in size because there are no additional messages. The other limitation is it requires heavy weight asymmetric cryptographic operations. SAODV allows authenticating AODV routing data. The protocol is implemented using NS-2 and it shows improved performance in terms of overhead and end to end delay ensuring secure routing.

G. Secure AODV Routing Protocol based on Trust Mechanism

Harris Simaremare *et al.* [11] proposed AODV routing protocol based on trust mechanism using the concept of local trust and global trust. Local trust is based on total received packet and total forwarded packet with reference to specific nodes whereas Global trust is based on total number of packets received and total number of packets forwarded in network. Trust calculation is done before communication starts. It is able to handle Blackhole attack and Dos attack in the network. The limitation is that nodes work in promiscuous mode which is not active in AODV.

The protocol is simulated on NS-2 and the performance analysis is done in terms of packet delivery ratio, end to end delay and routing overhead.

V. COMPARISON

The comparison among the different research works is given to clearly understand the different modifications, strengths, weaknesses and performance parameters measured in every approach. It is shown below in Table 1:

TABLE 1: MODIFICATIONS, RESULTS, STRENGTH, WEAKNESS OF OF DIFFERENT PROTOCOLS

Protocol	Modification	Performance parameters	Strength	Weakness
Xiaoqi Li *et al.*[5]	Positive, negative events and opinion field in the routing table	Throughput , packet delivery ratio	Detects and eliminates malicious nodes	Complex in architecture
Sandhya khurana *et al.* [6]	RRDU, RRDU_REP and reliability list are used	Handles attacks and secure routing	Simple implementation, secure route	Overheads as packets are modified
A.Menaka Pushpa [7]	Based on node trust and route trust, modified the RREP and RREQ packet and Neighbor table	Throughput , packet drop	Ensure trusted route between source and destination	Complex architecture , overhead
Mangrulkar *et al.* [8]	Modified route request packet format	More secure and improved performance	Selection of trusted and reliable routes based on trust	Overheads in periodic updations
Sridhar Subramanian *et al.* [9]	Based on calculating trust value for every node	Packet delivery ratio, delay, throughput	detects misbehaving nodes and isolate them	Overheads and lack of authentication of nodes and packets.
Durgesh Wadbude *et al.* [10]	Uses hash chain, digital signature and protocol enforcement mechanism	Overheads, end to end delay	Security and authenticity	Message overhead, complex cryptographic operations
H. Simaremare *et al.* [11]	Used local trust and global trust concept to find the trust level	Packet delivery ratio, delay and routing overhead	Remove the attacker node before communication starts	Nodes work in promiscuous listening mode

VI. CONCLUSION AND FUTURE ENHANCEMENTS

Mobile Adhoc networks are infrastructureless, highly mobile and self organizing networks formed of mobile devices connected by wireless links. Nodes act as both router and host in the network. Manets face challenges in terms of security issues, frequent topology changes, nodes limitations such as energy resource and communication limitations such as channel bandwidth, reliability. Robust protocols are required to ensure security, proper functioning, reliability of network and maintained quality of service. We have discussed various protocols using trust factor to enhance security and performance of the network. More robust protocols with less complexity and less expensive are needed.

Other enhancement is to study the impact of network dynamics on trust, considering energy parameters in the network.

ACKNOWLEDGMENT

This paper is made possible through the support and institutional facilities provided by the Department of Computer Science & Engineering JSS Academy of Technical Education, Noida. We would also like to thank our family and friends for their suggestions and support.

REFRENCES

[1] Kukreja, Deepika, Umang Singh, and B. V. R. Reddy. "A Survey of Trust Based Routing Protocols in MANETs." *Journal of Advances in Computer Networks*, vol.1, no.4, November 2013.

[2] Janakiraman.S and Gayathri.D.” Trust Implementation in AODV Protocol: A Survey.” in *International Journal of Software and Web Sciences(IJSWS),* 2014.

[3] Jin-Hee Cho, Ananthram Swami and Ing-Ray Chen, “A Survey on Trust Management for Mobile Ad-Hoc Networks”, in: *IEEE communications surveys and tutorials*, vol.13, no.4, pp. 562-583, fourth quarter 2011.

[4] Philip England, Dr Qi Shi, Dr Bob Askwith and Dr Faycal Bouhafs, “A Survey of Trust Management in Mobile Ad-Hoc Networks”, in *Proceedings of the 13th annual post graduate symposium on the convergence of telecommunications, networking, and broadcasting*, PGNET. 2012

[5] Xiaoqi Li, Michael R. Lyu, and Jiangchuan Liu, “A Trust Model Based Routing Protocol for Secure Ad Hoc Networks”, in *Aerospace Conference, 2004. Proceedings, v*ol.2, pp. 1286-1295, 2004.

[6] Khurana Sandhya, Neelima Gupta and Nagender Aneja, “Reliable ad-hoc on-demand distance vector routing protocol”, in *Networking, International Conference on Mobile Communications and Learning Technologies*,2006. International Conference on IEEE, pp.98-98, 2006.

[7] A.Menaka Pushpa, “Trust Based Secure Routing in AODV Routing Protocol”, in *Internet Multimedia Services Architecture and Applications (IMSAA),* IEEE conference, pp.1-6 , 2009.

[8] Mangrulkar, R. S., Pallavi V. Chavan, and S. N. Dagadkar, "Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MaNeT." in *International Journal of Computer Applications (0975–8887) Volume*. 36-39, 2010

[9] Subramanian, Sridhar, and Baskaran Ramachandran. “Trust Based Scheme for QoS Assurance in Mobile Ad-Hoc Networks.” arXiv preprint arXiv:1202.1664,2012.

[10] Wadbude, Durgesh, and Vineet Richariya.”An Efficient Secure AODV Routing Protocol in MANET.” *International Journal of Engineering and Innovative Technology(IJEIT),* vol.1, pp.274-279, April 2012.

[11] Simaremare, H., Abouaissa, A., Sari, R. F., & Lorenz, P. “Secure AODV Routing Protocol Based on Trust Mechanism.” In *Wireless Networks and Security* ,Springer Berlin Heidelberg, pp. 81-105, 2013.

[12] Ankit Aggarwal and Bhumika Garg, “Survey on Secure AODV For Ad Hoc Networks Routing Mechanism”, in *International Journal of Advanced Research in Computer Science and Software Engineering,* vol.2, March 2012.

[13]Kannan Govindan and Prasant Mohapatra,” Trust computations and Trust dynamics in Mobile Ad-hoc Networks: A Survey”, in: IEEE *communication surveys and tutorials*, vol. 14, no. 2, pp.279-298, second quarter 2012.

[14] http://en.wikipedia.org/wiki/Mobile_ad_hoc_network

[15]http://en.wikipedia.org/wiki/Ad_hoc_OnDemand_Distance_Vector_Routing