A Survey of Trust Based AODV Routing Protocols in MANETS

Vijaya Singh, Megha Jain

Abstract— Mobile Adhoc Networks are type of wireless network which are infrastructure less, self organizing, highly mobile and quickly deployable. There is no central authority, the communication occur hop by hop based on cooperation among the nodes. Thus, secure routing protocols are needed which are robust and ensure that the nodes in the network behave in trustworthy manner otherwise detect and eliminate the untrustworthy nodes which degrade the overall network performance. There are several trust based AODV routing protocols given in the past. In this paper, we have given a survey of trust based AODV, in which concept of TRUST is used to ensure secure routing and improved network performance.

Index Terms— aodv, mobile Adhoc networks, network performance, secure routing, trust, trust based AODV, wireless networks

1 INTRODUCTION

MOBILE Adhoc networks are infrastructure less and self-configuring mobile devices connected by Wireless links [1][15]. They are characterized by limited bandwidth, power, highly mobile and quickly deployable. Due to high mobility frequent disconnections occur that lead to various security threats. As nodes can join or leave the network anytime without any prior information, it leads to frequent changes in topology of the network and making MANETs vulnerable to security attacks.

Routing Protocols can be divided in to 3 types: Reactive Protocols, Proactive protocols, Hybrid protocols. Reactive protocols are those which find routes on demand whenever needed whereas Proactive protocols find the routes for transmission beforehand and Hybrid protocols is the combination of reactive and proactive routing. AODV is a reactive protocol and TRUST mechanism is implemented in it for ensuring secure routing. Different TRUST based AODV routing protocols have been analyzed and compared along with strengths and limitations. The security mechanism for MANET must 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. Security issues are of prime importance and to deal with these proposed approach is given in the end.

The rest of the paper is organized as follows: Section 2 presents the AODV routing protocol. Section 3 presents the concept of trust and its importance. Section 4 presents the TRUST based AODV routing protocols. Section 5 presents the comparative study. Section 6 presents the proposed work and Section 7 presents conclusion and future enhancement.

- *Vijaya Singh is 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*

2 AODV ROUTING PROTOCOL

Detailed Ad-hoc On demand Distance Vector (AODV) routing protocol is a reactive protocol [2][16] that establishes the route only on demand and always search for the shortest path irrespective of reliability of the path. It uses sequence number to determine the freshness of any route and as it maintains tables in the node itself there is a less memory overhead.

2.1 Working of AODV protocol

1. Whenever there is a need to establish a connection, source node looks for the route to destination in its routing table. But if it does not exist then it sends the route request packet (RREQ) to the neighboring nodes.

2. If the neighbor node is the destination then it sends the route reply message (RREP) else it searches for the route to destination and sends route reply to the source along with route to destination. Otherwise it forwards the route request packet (RREQ) to its neighbors.

3. 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. Route Error message (RERR) is sent to the transmitting node when there is a link failure and the process repeats again.

4. HELLO messages are used by AODV periodically for Route maintenance.

2.2 Advantages/Disadvantages

The advantages of AODV are, the routes are created on demand only and it uses sequence number to find freshness of route. The connection setup delay is lower.

The disadvantages of AODV are, stale entries in sequence number, high bandwidth consumption and multiple route reply packet for single route request packet thereby increasing control overhead [16].

3 CONCEPT OF TRUST & ITS IMPORTANCE

Concept of trust is *multidisciplinary* as trust has different definitions in different disciplines [3]. Trust in any node tells about the genuineness of that node. Trust is the belief that the nodes in the network will perform in accordance with the network and will not behave selfishly.

3.1 Classification of Trust

There are different classifications of trust given below:
1. **Trust as risk factor:** whenever there is uncertainty about the chosen path to be good or bad, there is a risk.
2. **Trust as belief:** trust as belief refers to individuals will to behave 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 the transitive measure that is if a node behaves as expected then others can trust it based on others trusting it.

3.2 Properties of Trust

1. Trust is **dynamic**, it never remains constant and changes with time, location etc.
2. Trust is **context dependent**; trust value of a node can be high in a specific context but can be low in other context.
3. Trust is **asymmetric**, if a node trusts other node in the network then there is no strict condition that it will also be trusted in return.
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 different trust values can be aggregated to get the accurate trust on any node.

Trust can be **direct**, **indirect** or **hybrid**, depending on the way trust is computed [4]. Direct trust is based on nodes own observation and experience about the behavior of node. Indirect trust is based on recommendations; if a trustor node trusts a node then it can recommend that to other nodes in the network. Hybrid trust is combination of direct and indirect trust, it uses experience and recommendations based approach to compute trust for any node. Mobile Adhoc networks are highly mobile and infrastructure less networks, they are more open to security threats and selfish behaviors.

Trust is of greater importance in Manets as it helps to estimate whether a node is trustworthy or untrustworthy, as mobile nodes communicate with other far nodes based on the intermediate nodes. These intermediate nodes could be good or malicious which tries to harm the network or act selfishly to save its resource. 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.

4 TRUST BASED AODV ROUTING PROTOCOLS

We have given a survey of various trusts based routing AODV 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. Mobile Adhoc networks which are highly mobile and can crash, there is a need to design such protocols which are not very expensive and complex but competent enough to deal with security issues.

4.1 Reliable Adhoc On-demand DistanceVector Routing

Khurana et al. [5] proposed RAODV protocol which uses two new control packets RRDU and RRDU_REP along with RREQ and RREP packets for route discovery and HELLO, RERR packets for route maintenance. Reliability list (RL) field is added in the routing table of RAODV protocol. RRDU packets are sent to all the nodes and the RRDU_REP packet is send only by destination node to source node. Thus, source node can discard RREP packets received earlier and select the route based on RRDU_REP packet. HELLO packets are broadcasted periodically in RAODV in the same way as in AODV for Route Maintenance. RAODV outperforms AODV when there are any malicious nodes in the network and shows improved performance. AODV fails when there is any attack.

4.2 Trust Based Secure Routing in AODV

Pushpa [6] proposed a trust based AODV protocol giving equal importance to both node trust and route trust. After route establishment based on node trust, route trust is monitored to check if any node changes its behavior and act maliciously. Each node maintains two tables: Route Table and Neighbor Table. Route table stores the route details and route trust field is added to it and the neighbor table has two fields neighbor _id and trust value. Based on route trust value in the RREP packet, the route establishment occurs.

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.

4.3 Trust Based Reliable AODV Protocol

Subramanian et al. [7] proposed TBRAODV in which trust value for each node is calculated. Based on trust value the node is either allowed to participate in routing or could be representing as misbehaving node. These misbehaving nodes detection will lead to reliable routing with trusted nodes in the route.

The protocol is simulated on NS-2 with 50 nodes and shows improvement in terms of increased packet delivery ratio and less delay, as the misbehaving nodes are identified already.

4.4 Secure Adhoc on Demand Distance Vector Routing

Wadbude et al. [8] proposed an efficient secure AODV routing protocol which aims to secure the AODV routing packets. It uses Hash chains, Digital Signature and Protocol Enforcement Mechanism to secure packets.

Hash Chain is used to secure the Hop count. The protocol is implemented using NS-2 and it shows improved performance in terms of overhead and end to end delay ensuring secure routing. But the messages in SAODV are bigger and require heavyweight cryptographic operations.

4.5 Trusted ST-AODV

Subramanian et al. [9] proposed ST-AODV protocol in which each node is assigned a trust value and based on the trust value node is allowed to participate in routing. Threshold value is the deciding factor, when the trust value is greater than threshold node is marked as trustworthy and if it less than or equal to threshold it is marked as untrustworthy and is not allowed to participate as it has more chances to drop packets.

Protocol performs trust value check before involving any node in the routing path for data transmission that is the strength of the ST-AODV. The protocol is simulated using NS2 simulator with maximum 50 nodes and it shows improvement in packet delivery ratio, less delay and maintained throughput in comparison to Traditional AODV.

4.6 Trusted Adhoc on demand Distance Vector Routing

Sharma et al. [10] proposed trust based secure AODV protocol. It has 3 modules: AODV routing protocol, Trust model and Trusted AODV Routing Protocol. Routing table is modified with 3 fields: Positive events, Negative events and opinion. Positive events are successful communication, negative events are unsuccessful communications and opinion is nodes belief about other nodes trustworthiness. It also uses two new routing messages: TRREQ and TRREP used to establish secure routes. Trust update policies are used to update trust depending on occurrence of positive event, negative event and thus change in the opinion will be calculated. It uses the concept of Requestor, Recommender and Recommendee based on who is issuing TREQ, TREP and TWARN (trust warning message) messages.

The protocol is implemented using NS-2.34 and the performance is measured in terms of packet delivery ratio, end to end delay, throughput and average latency. The graphs are used to do comparison analysis of AODV and TAODV.

4.7 Trust Based Explicit No Technique

Islam et al. [11] proposed explicit no technique in which EXPLICIT NO packet is used. Any node when not available in the network informs the source node by sending EXPLICIT NO packet. The source increments the trust value of the node sending EXPLICIT NO packet as it shows fair behavior whereas the malicious node will never send this packet. Source node selects other alternate path for routing data.

The protocol is simulated on NS-2.35 with 50 nodes and there is considerable improvement in packet delivery ratio and less delay in comparison to traditional AODV. It has simple architecture and energy conserving. It has limitations in terms of overheads and non availability of nodes as it sends EXPLICIT NO packet to inform the source node even it has high trust value.

4.8 Secure AODV Routing Protocol based on Trust Mechanism

Simaremare et al. [12] 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.

5 COMPARISON

We have described various protocols and explained their approach, strengths and limitations for better understanding. The comparison among the different research works is given below:

TABLE 1
MODIFICATION, RESULTS, STRENGTH, and WEAKNESS OF DIFFERENT PROTOCOLS

Protocol	Modification	Performance parameters	Strength	Weakness
Khurana et al. [5]	RRDU, RRDU_REP and reliability list are used	Handles attacks and secure routing	Simple implementation, secure route	Overheads as packets are modified
Pushpa [6]	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
Subramanian et al. [7]	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.

Wadbude et al. [8]	Uses hash chain, digital signature and protocol enforcement mechanism	Overheads, end to end delay	Security and authenticity	Message overhead, complex cryptographic operations
Subramanian et al. [9]	based on threshold value the node behavior is either trustworthy or not	Packet delivery ratio, delay and throughput	Packet dropping nodes are identified and not involved in routing	Overhead
Sharma et al. [10]	Modified routing table and assumes that intrusion detection system are used	Packet delivery ratio, delay, average latency and network throughput.	Simple operations based on recommendation rather any cryptographic operations	Malicious nodes can attack as there is no packet authentication
Islam et al. [11]	Used EXPLICIT NO packet to inform non availability	Packet delivery ratio and delay	Simple architecture and energy conserving	Overhead and non availability of nodes even when trustworthy
Simaremare et al. [12]	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

6 PROPOSED WORK

In this paper, we have analyzed and discussed various trust based AODV routing protocols with their strengths and limitations. We propose our trust based AODV routing protocol to overcome the limitations. In this proposed work, we will analyze the dynamic property of trust as it never remains constant. Trust dynamics [14] which refers to the evolution of trust over time. There are different phases in trust dynamics such as trust establishment, Trust propagation and Trust aggregation.

We will also incorporate load balancing in our proposed approach along with trust to make it robust to deal with congestion problem. We will simulate both the approaches, first only trust based and second trust and load based on Manet with certain movement pattern using NS-2.35 on Linux platform. It will improve the performance parameters like packet delivery ratio, throughput, less delay and overhead.

The various performance parameters will be analyzed and compared with normal AODV to estimate the results purely on the basis of trust and based on trust and load based approach using graphs and text based results.

7 CONCLUSION AND FUTURE ENHANCEMENTS

Trust based routing in MANETS is an open area of research. Mobile Adhoc networks are highly mobile, infrastructure less, self organizing in nature and needs robust protocols to ensure secure routing. The mobile nodes forward data with the cooperation among them on basis of intermediate nodes. These nodes are at free will to join or leave the network as there is no central authority. Various protocols has been described and compared to get better understanding of trust based AODV routing protocols with their strengths and limitations.

Finally, proposed work is given which we will perform based on trust dynamics and use of load balancing to overcome the limitations and compare it with standard AODV routing protocol. Further enhancement can be done in the trust based AODV routing protocols to ensure that various parameters can be fulfilled with less complexity. Also the network dynamics and its impact on dynamics of trust can be a good advancement.

ACKNOWLEDGEMENT

Thispaper is made possible through the support and institutional facilities provided by the Department of Computer Science & Engineering JSS Academy of Technical Education, Noida.We convey our sincere thanks to other M.Tech scholars for their rigorous brainstorming sessions to shape up this research paper.

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] Khurana Sandhya, Neelima Gupta and Nagender Aneja, "Reliable adhoc 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.

[6] 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.

[7] Subramanian, Sridhar, and Baskaran Ramachandran. "Trust Based Scheme for QoS Assurance in Mobile Ad-Hoc Networks." arXiv preprint arXiv: 1202.1664,(2012).

[8] 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.

[9] Subramanian, Sridhar, and Baskaran Ramachandran. "QOS Assertion in MANET Routing Based on Trusted AODV (ST-AODV) ", in International Journal of Adhoc, Sensor & Ubiquitous Computing, vol.3, no.3, June 2012.

[10] Sharma, Pankaj. "Trust based secure aodv in manet. " Journal of Global Research in Computer Science, vol.3, no.6, pp.107-114, June 2012.

[11] Islam, M. Hassan, and Misbah Zareen. "Mitigating the effect of malicious node in Mobile Ad Hoc Networks using Trust based Explicit No Technique. "International Journal of Computer Networks and Communications Security, vol.1, no.6, pp.210-215, November 2013.

[12] 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.

[13] 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.

[14] 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.

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

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