



Trust Implementation in AODV Protocol: A Survey

¹Janakiraman.S., ²Gayathri.D,

¹Assistant Professor, Banking Technology, Pondicherry University, Puducherry, India

²Research Scholar, Bharathiar University, Coimbatore, Tamil Nadu, India

Abstract: A MANET is a network of mobile nodes without a fixed infrastructure. So they do not have a base station or access point to supervise them. Moreover their topology is not constant and keeps changing. These features of MANETS bring in lot of challenges in routing, energy management, QoS issues. They use wireless medium such as air to route the packets. The nodes of MANETs have limited bandwidth, limited resources, and use radio waves where they can be listened passively. These make them suffer from malicious nodes resulting in security breach and the selfish nodes to save their resources without routing. In this paper, we have given a survey of AODV, reactive protocol that has implemented TRUST metric for its enhancement in efficiency to handle the selfishness and the security issues.

Keywords: MANET, AODV, reactive protocol, Trust, selfishness, security issues.

I. INTRODUCTION

A Mobile Ad-hoc Network is an infra-structure less, self-configuring network, formed by several wireless nodes. Since they are infra-structure less networks they are used for military purposes, battle field area, rescue operations, meeting halls etc, where a infrastructure does not exist or where it is severely damaged. In recent days due to its faster network installation and mobility at lower costs, MANETS have gained importance in research areas to overcome its limited resource related issues and security related issues. They use wireless links such as radio waves or infrared rays as their carrier .Infrared rays require line of sight propagation and they need to be within short range and cannot form a big network. So MANETs use radio waves as their communication medium. The license free radio frequency bands are used for their communication. MANETS face resources constrain such as battery life limitation, bandwidth limitation and security related issues. Due to the absence of central authority any node can listen and participate to partially or fully crash the network. Due to this MANETS are vulnerable to attacks than wired networks. There are mainly 3 types of protocols for routing in MANETS. They are reactive, proactive and hybrid protocols. Our survey is on a reactive type of protocol ADOV where TRUST is implemented by having calculated with different parameters.

II. MANET routing protocols

Routing is the information passage to one node to another with the help intermediate nodes forwarding the packets. The information is passed on the route considered to be best in terms of number of hops, security, traffic, energy issues, etc. Three categories of routing protocols are

1. Flat vs hierarchical protocols
2. Pro active vs reactive protocols
3. Hybrid protocols

A. Flat versus Hierarchical protocols

Hierarchical network topology includes many network clusters and a head of the cluster on top of these layered clusters. The gateway bears the responsibility of storing its clusters topology and communicating with other gateways. The main advantage of this is other than the cluster heads the nodes are free from knowing the topology information ,thus reducing the control overhead but when there is a gateway failure the whole cluster broke ups. Example: Zone-Based Hierarchical Link State protocol (ZHLS).

On the other hand flat structured topology does not have any clusters thus the nodes store all the information. The advantage is failure of one node does not affect other. Disadvantage is the control overhead in each node.

B. Pro-active Versus Reactive protocols

Pro-active routing

In pro-active protocols every node finds the route to reach all other nodes in a given network before hand. This is done by periodically flooding information about its presence to the neighbor nodes. This paves way to find out the changes in the network topology. Examples of pro-active protocols are

- Global state Routing (GSR)
- Hierarchical State Routing (HSR)
- Destination Sequenced Distance Vector (DSDV)
- Optimized List State routing (OLSR)

Reactive routing

In reactive routing protocols the route discovery is only for the active paths to reach the destination. This reduces the network at the expense of delay. Examples of reactive protocols are

- Ad hoc On-demand Distance vector (AODV)
- Dynamic source Routing (DSR)
- Location Aided Routing (LAR)
- Temporally Ordered Routing Algorithm (TORA)

C. Hybrid protocols

Hybrid protocols initially uses pro-active routing in finding some standard paths and then reactively finding other paths on demand thus combining the advantages of both. Example; Zone routing Protocol (ZRP).

III. OVERVIEW OF ADOV PROTOCOL

AODV stands for Ad-hoc On demand Distance Vector protocol. AODV is a reactive type of protocol which finds to the destination on demand. This uses the destination sequence number to ensure the freshness of a route thus preventing routing loops. Main advantage of AODV is that it maintains the routing tables in the nodes not in the data packets preventing packet's memory overhead.

AODV Protocol

- When a node wants to communicate with other, the source node sees the route to the destination in its routing table and if it has it sends the data packet through intermediate nodes to the destination.
- Else it floods the RREQ (Route Request packets) to its neighbor nodes.
- If the neighbor nodes on receiving the RREQ packets checks if they are the destination.
- If yes they send the RREP message to the source node else sees if it has route to the destination.
- If the neighbor has the route to the destination, it sends the RREP messages to the source node with the route to the destination. This is possible because each node receiving RREQ packets caches the route back to the originator of RREQ.
- Else it forwards the RREQ packets to its neighbors, where they follow the same procedure as the previous node.
- On arrival of the RREP packet the source node checks the destination sequence number (DSN) of the destination to be greater than that of the RREQ packet
- A route is said to be fresh enough when the DSN of the sought route in the recipient node's routing table is greater than the DSN in the RREQ packet itself.
- Every node receiving the RREP packets will know the route to the destination and to the source node.
- AODV uses the HELLO messages to ensure the presence of it to its neighbors periodically.
- AODV uses RRER messages to intimate the neighbors about the link failures.

IV. TRUST AND ITS NECESSITY

Trust is the degree of reliability of a node by another node. Trust is a subjective logic and is quantified and implemented in AODV.

Features of TRUST:

- Trust is subjective
- Trust is dynamic
- Trust is asymmetric
- Trust is not necessarily reciprocal
- Trust is context dependent
- Trust is not necessarily transitive

AODV protocol behaves well and delivers remarkably under normal circumstances, but when there is a malicious node or selfish nodes present in the network, its efficiency decreases rapidly. Due to the limited resources nodes may behave selfishly to save their resource and do not co-operate for routing or they may behave maliciously in order to crash the network or to get valuable information. Earlier cryptographic techniques were built to have secure data transmissions thus avoiding external attackers to attack and to crack the network. But the existence selfish or malicious nodes in the network create a serious security breach. To overcome this TRUST concept is introduced.

V. IMPLEMENTATION OF TRUST CALCULATED WITH DIFFERENT PARAMETERS IN AODV

All the earlier work in the area of secure routing in ad hoc networks was dependent on security mechanisms such as cryptography to secure the transmissions. But are expensive and is not worth in the dynamic environment. Hence as discussed above Trust is an idle metric for constructing reliable routing. Trust calculated using different parameters are implemented in the AODV by researchers and all the proposed models

perform remarkably well in the given scenario. This survey paper points out the various researchers' work of trust implementation with different parameters.

A. TBRAODV – Trust Based Routing in Ad-hoc on demand Distance Vector Protocol

Sridhar Subramanian et al [7] proposed a trust based routing AODV protocol. In this protocol, the following parameters for trust level calculation taken in to account are success and failure rates of the transmission.

$$T = T(RREQ) * Q_r + T(RREP) * Q_p + T(DATA) * Q_d$$

This is the Trust level of the routing path.

$T(X)$ is the time factorial by the nodes.

$$Q_r = (Q_{rs} - Q_{rf}) / (Q_{rs} + Q_{rf})$$

$$Q_p = (Q_{ps} - Q_{pf}) / (Q_{ps} + Q_{pf})$$

$$Q_d = (Q_{ds} - Q_{df}) / (Q_{ds} + Q_{df})$$

Q_r , Q_p , Q_d are normalized to fall in the range of -1 to +1. if the values fall beyond the normalized range then it clearly shows that the failure rate of the node is high.

- Q_{rs} and Q_{rf} are the successful transmission and failure of route request packet
- Q_{ps} and Q_{pf} are the successful transmission and failure of route reply packet
- Q_{ds} and Q_{df} are the successful transmission and failure of data packet

$T(Trust)$ is calculated for each node during routing and is checked against the threshold value (assumed to be of 5). If lesser than threshold value then the node is marked as misbehaving node for the current transmission and cannot route the packets, but be best for some other transmission in the same network.

Simulation result

The proposed TBRAODV model is analyzed using ns-2 of 50 nodes with simulation time of 30 minutes, transmission range of 250 meters, movement speed of 100 kbps, traffic type CBR, packet size 5000, maximum speed of 100 kbps, time interval of 0.01 sec, MAC layer protocol IEEE 802.11.

The simulation result of AODV with TBRAODV shows that the TBRAODV performs well than AODV. In particular, the QoS parameters packet delivery ratio and end to end delay where remarkably favorable in TBRAODV. TBRAODV has high packet delivery ratio and decreased delay compared to AODV.

B. A Trust Model for Secure And QoS Routing in MANETs

Shilpa et al [8] proposed this model where Trust value is considered with the energy that is the life time of the network. The Trust metric is calculated with a very simple equation as follows

$$TV = \tanh(R1 + R2 + A)$$

$$R1 = Pf / TPf$$

$$R2 = Pr / TPr$$

A = acknowledgement bit

Where,

- TV is the trust value
- Pf is the number of packets forwarded successfully from neighbor node
- TPf is the total number of packets to be forwarded by neighbor node
- Pr is the number of packets received from the neighbor node that originated from the other node
- TPr is the total number of packets received from the neighbor node

In this approach the trust value with the percentage of remaining energy is taken for optimal routing.

C. A Trust based approach for detecting and isolation of malicious nodes

Aravindh s et al [9] have proposed a trust based approach for detecting and isolation of malicious nodes. The proposed work is done by implementing Trust factor in AODV by the following parameters.

- Ps packets sent from the node that needs the trust value for another node
- Pr packets received from the node that needs to be trusted.

$$FTval = Eval + DTval + IDTval$$

$$DTval = Ps / Pr$$

- FTval is the final trust value for implementation
- Eval is the Energy value of the node
- DTval is the direct trust value of a node by a trustor node
- IDTval is the indirect trust value of a node got on recommendation of other nodes on request.

Simulation result

This proposed approach used ns-2 with 60 nodes in the first scenario and 100 nodes in the second scenario. The proposed approach in both the scenario shows a high throughput ratio. After detection and isolation of malicious nodes there is a good increase in throughput and decrease in end to end delay.

D. Detecting Malicious node in MANET using Trust based Cross-Layer Security Protocol

A.Rajaram et al [10] have proposed trust based security with the addition of some authentication mechanism using encryption and CBC-X mode to enhance the overall transmission. Trust is calculated for the nodes of the every available route, and the route which has minimum number of malicious nodes is taken For Trust calculation a NTT neighbor trust counter table is maintained by every node. First a node does not have trust or distrust a node completely. It first sends RREQ packets to find the number of RREP packets. Each node keep tracks of the number of packets it has forwarded through a route using a forward counter (fc). Each time, when node n_k receives a packet from node n_i then n_k increases the forward count FCn_i .

$$FCn_i = FCn_i + 1, I = 1, 2, \dots$$

Then the NTT of node N_k is modified with FCn_i values .similarly each node does till destination D. When the destination d receives the accumulated RREQ message, it measures the number of packets in time interval. Each intermediate node checks he RREP packet to compute success ratio as

$$SR_i = FCn_i / prec$$

The destination signs the RREP packet with its Digital signature. The success ratio is added to the packets. The intermediate nodes verify the validity of digital signature of the destination and decides to forward and the source checks for the intermediate nodes and increments the Trust value count TCn_i for the node by d1. D1 is the step value used during simulation and the success ratio is measured for the nodes. If the success ratio falls below the threshold value it is decremented by d2 else incremented by d2. D2 is again a step value. For a node n_k , if $TC_k < TC_{tres}$ the node is marked as malicious node. The same procedure is repeated for the other routes R2 , R3 etc and either a route without a malicious nodes is selected as the reliable route.

Simulation result

This model used ns2 with 100 mobile nodes in a area of 1000 * 1000 sqm for 50 seconds simulation time with channel capacity of 2 mbps, IEEE 802.11 as MAC layer protocol, transmission range of 250 meters and speed varying from 10m/s to 50m/s. The simulated traffic is constant bit rate (CBR).

Here, the proposed TCLS protocol has been compared with LLSP and RSRP in presence of malicious node environment where the performance metrics control overhead, Average end to end delay, average packet delivery ratio is evaluated in 2 scenario of varying number of attackers and by varying the mobility speed of malicious nodes. In both the scenario there is high packet delivery ratio, low end to end delay and less control overhead in TCLS than the other two namely RSRP and LLSP.

E. Multiple Trust in Trust Based on Demand Routing in Mobile Ad hoc Networks

P.RamaKishore et al [12] have proposed a Trust model where trust is calculated with the control packet and data packet forwarding ratio at a time instance.

$$T_{jk}(t) = W1 * CFR_{jk}(t) + W2 * DFR_{jk}(t)$$

T_{jk} is the direct trust in node k by node j is represented as T_{jk} . CFR and DFR are control packet and data packet forwarding ratio respectively and are calculated as

$$FR(t) = \frac{Nc(t) - Nc(t-w)}{Na(t) - Na(t-w)} \quad t > w$$

$$FR(t) = Nc(t) / Na(t) \quad t < w$$

Where Nc and Na are cumulative count of correct forwarding and $Na(t)$ signifies the total count of all requesting before time t . The weights $W1$ and $W2$ are assigned to CFR and DFR. The T_{jk} lies between 0 to 1, where 0 is complete distrust and 1 is complete trust.

Simulation result

This model showed an increase in Trust value as the number of malicious nodes are isolated gradually based on time window owing to better performance than AODV.

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

Xiaoqili et al [13] have proposed a model based on Trust and have calculated the trust on a 3d metric of a node's opinion on another node which is resolved in to belief b , disbelief d , uncertainty u respectively. W_{xy} is the X's opinion about Y's trustworthiness in MANET.

$$W_{xy} = (b_{xy}, d_{xy}, u_{xy})$$

If the threshold value of these 3 are set and if

$$b_{xy} > T.V \quad \text{-----} > \text{distrusted}$$

$$d_{xy} > T.V \quad \text{-----} \rightarrow \text{trusted}$$

$$u_{xy} > T.V \quad \text{-----} \rightarrow X \text{ will verify Y's digital signature}$$

This opinion based trust calculation is applied in [14] and has got very fair result.

Simulation result

The comparative analysis is done 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. The number of malicious nodes are increased and the packet delivery ratio, throughput, packet drop ratio are compared in TAODV and AODV. The throughput and packet delivery ratio are very high in TAODV

compared to AODV for a given number of malicious nodes. The packet drop ratio is almost very minimum in TAODV but AODV cannot resist. The higher performance of TAODV is because it detects and eliminates malicious nodes as time passes.

VI. Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MANET

R.S.Mangralkar et al [15] proposed a Trust model in which Trust is calculated as:

$$RSV = (Tind / Tavg) * (RTind/RTavg) * (Havg/Hind)$$

Where RSV is the route selection value, Tind is the Trust on the individual neighbor that forwarded and generated RREP, RTind is the Trust the individual neighbor has on the route, RTavg of all the route trust obtained from the individual nodes which forwarded, generated the RREP, Hind is the number of hops in the route proposed by the individual node in its RREP and Havg is the average of all Hind's obtained from the individual neighbor which forwarded the RREP. The RSV of all the nodes in the path are taken and the path with highest RSV is taken for route selection. The trust value is initialized to be 50. Then it is incremented or decremented by its forwarding behavior of RREQ packets. It becomes 0 when it is malicious and 100 when it is trusted node.

Simulation result

This model used for simulation and result analysis of AODV and Trust based AODV. The result analysis gives the route selection values of different paths and the RSV with higher value is selected for routing and this shows Trust based AODV is far better than normal AODV.

VII. Generalization and Discussions

This survey paper definitely points out the increased performance of all the trust implemented AODV protocols with that of normal AODV protocols. Very few approaches have included energy parameter and cryptographic techniques for defining trust. In future, analysis of these approaches with the energy efficiency and cryptographic measures can be considered for optimal routing. This will result in secured, reliable efficient routing in MANETs. More over trust computation in many other forms have been implemented in other MANET protocols which can also be implemented in AODV to see the improvement.

VIII. Conclusion

In general the trust implemented AODV performance is remarkably higher than the AODV in the entire scenario. In future the comparison can be done by choosing two or more computation of the Trust values and to find out the better performance in a fixed scenario and can be extended to other protocols.

References

- [1] S.Corson, J.Macker, "Mobile Ad hoc Networking", RFC-3651.
- [2] Amit Shrivastava, Nitin Chander, "Overview of Routing Protocols in MANET's and Enhancements in Reactive Protocols".
- [3] C.Perkins, E.Royer and S.Das, "Ad hoc on-demand Distance Vector Routing", RFC-3651.
- [4] XiaLi, Jill Slay, Shaokai yu, "Evaluating Trust in Mobile Ad hoc Networks".
- [5] Dalip Kamboj and pankaj Kumar Sehgal, 'A Comparative Study of Various Secure Routing protocols based on AODV', International Journal of Advanced Computer Science and Applications, vol.2, No.7, 2011, pp 80-85.
- [6] Mousumi Sardar and Koushik Majumber, "A Comparative Study on Different Trust Based Routing Schemes in MANET", DOI:10.5121/ijumn.2013.5510.
- [7] SridharSubramanian and Baskaran Ramachandran, "Trust Based Scheme for QoS Assurance in Mobile Ad hoc Networks".
- [8] 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,may 2011.
- [9] Aravindh S, Vinoth R S and Vijayan R, "A Trust Based Approach for Detection and Isolation of Malicious Nodes in MANET", International Journal of Engineering and Technology, (ISSN: 0975-4024), vol.5 no1 feb-mar march.
- [10] A.Rajaram, Dr.S.Palaniswami, "Detecting Malicious Node in MANET using Trust Based Cross-Layer Security Protocol", International Journal of Computer Science and Information Technologies, vol.1(2), 2010, 130-137.
- [11] RenuMishra, Inderpreet Kaur, SanjeevSharma, "New Trust Based Security Method for Mobile Adhoc Networks", International Journal of Computer Science and Security (ijcs), vol.4, issue:3.
- [12] P.RamaKishore, O.SrinivasaRao and M.KrishnaPrasad, "Mul;tiple Trust in Trust Based on Demand Routing in Mobile Ad Hoc Networks", ISSN: (print):2278-5140, vol1, issue-2, 2012.
- [13] XiaoQiLi, Michael R. Lyu, and Jiangehuan Liu, "Trust Model Based Routing Protocol for Secure Ad hoc Networks", IEE EAC paper# 1150
- [14] P.Vigneshwari,R.Anusha,D.Preethi,R.Jeyashree,V.Nandini, "Comparitive Analysis of AODV and Trusted AODV in MANET", International Journal of Advanced Information Science and Technology (ISSN:2319-2682) vol.10,no.10feb 2013.
- [15] R.S.Mangrulkar, PallaviVChavan, S.N.Dagadkar, "Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MANET", International Journal of Computer Applications (0975-8887) vol7-no.10, October 2010.
- [16] KamalDeepMeka, MohitVirendra, Shambhu Upadhyaya, "Trust Based Routing decisions in Mobile Adhoc Networks".