Research Paper
Impact Factor - **2.262**
Peer Reviewed Journal

IJMDRR
E- ISSN –2395-1885
ISSN -2395-1877

IMPROVED TRUST BASED MOBILE AD-HOC NETWORK ROUTING PROTOCOL FOR MANET

Shiv Kumar Dwivedi* **Mohammed Bakhtwar Ahmed****
**M.Tech (OOSD), Kalinga University, Chhattisgarh.*
***Assistant Professor of Computer Science, Kalinga University, Chhattisgarh.*

Abstract
Mobile Ad-hoc networks (MANET) is a situate of wireless nodes without any fixed infrastructure or base station, in which nodes communicate honestly to the other nodes inside its transmission range over comparatively bandwidth constrained wireless links. MANET is vulnerable to various types of attacks from malicious nodes due to its spontaneous nature of communication and the absence of centralized administrator. There are many attacks in MANET due to which the legitimacy of a network is compromised such as, Black Hole Attack, Worm Hole Attack, Byzantine attack, DoS attack. So, secure communication in MANET is essential and challenging task. In this paper, we present "Improved Trust Based Mobile Ad hoc Network Routing Protocol for MANET". Our proposed algorithm works on the concept of honest value which is calculated on the concept of hop and trust to protect the network from malicious node. The performance of the proposed protocol is analyzed using throughput, number of drop packets, packet delivery ratio and number of received packets with the variation of number of nodes, speed and simulation time. Results show that the proposed method has better performance and enhance the security in the network.

Key Words: - Trust, Honest Values, Security, Attacks, AODV, Security, Trusted AODV, MANET.

Introduction

A Mobile ad hoc network is an infrastructure fewer networks self-possessed of wireless network nodes. These nodes are self configurable and dynamically setup the paths among themselves to transmit packet. In a MANET, each node act as router and the connectivity is achieved using multihop communication between nodes where any wire- less node can join and leave the network at an instant of time. Several routing protocols have been proposed by various researchers such as DSR [13], DSDV [14] and AODV [8] etc. but they did not consider any security issues. These protocols can be categorized into two main types: proactive and reactive [4]. Proactive protocol depends on the routing tables which are maintained at each node whereas reactive protocol finds a route to a destination on demand, whenever communication is needed. Ad hoc on demand distance vector (AODV) is reactive routing protocol proposed by C. Perkins [11] which is very efficient in terms of performance and widely used protocol so far. AODV is on demand routing protocol where routes are only established when needed and it belongs to the class of distance vector. In distance vector every node knows its neighbors and costs to reach them. A node maintains its own routing table, storing all nodes in the network, the distance and the next hop to them. If a node is not reachable the distance is set to infinity. Every node sends the whole routing table to its neighbors, so they can check if there is another useful or shortest route to another node using this neighbor as next hop. When a link gets breaks, count-to-infinity problem could arise. The count- To-Infinity [11] and loop problem is solved with the sequence number concept. Security in MANET is a major aspect in terms of packet forwarding and routing. The dynamic nature of mobile ad hoc networks makes it more susceptible to various types of attacks. Attacks in mobile ad hoc networks can be classified into two main categories: passive attack and active attack [7]. In Passive attack the attacker snoops the data exchanged in the network without altering it or disrupts the operation of the network. Detection of a passive attack is very difficult for the operation of the network itself does not get affected. An active attack attempts to alter or destroy the data being exchanged in the network and it disrupts the normal operation of the network. Further active attacks can be classified into two categories: external attacks and internal attacks [7]. External attacks are carried out by the nodes that do not belong to the network and internal attacks are carried out by compromised nodes that are actually part of the network. Internal attacks are more severe and difficult to detect when compared to external attacks. Wormhole, Black hole, DOS attack etc. comes under the category of internal attacks. Routing algorithm needs mutual trust between nodes for secure communication.

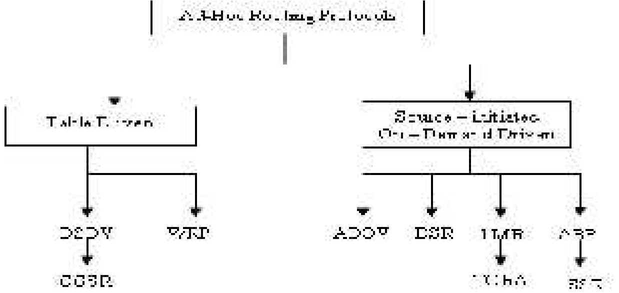


Figure: Categorization of Ad-Hoc Routing Protocols

As shown in Figure above, these routing protocols may generally be categorized as: (a) table-driven and (b) source-initiated on-demand driven.

Ad-hoc On-Demand Distance Vector Routing (AODV)
The Ad-hoc On-Demand Distance Vector (AODV) routing protocol builds on the DSDV algorithm previously described. AODV is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on an on-demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm. The authors of AODV classify it as a pure on-demand route acquisition system, as nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges. When a source node desires to send a message to some destination node and does not already have a valid route to that destination, it initiates a Path Discovery process to locate the other node. It broadcasts a route request (RREQ) packet to its neighbours, which then forward the request to their neighbours, and so on, until either the destination or an intermediate node with a “fresh enough" route to the destination is located. AODV utilizes destination sequence numbers to ensure all routes are loop-free and contain the most recent route information. Each node maintains its own sequence number, as well as a broadcast ID. The broadcast ID is incremented for every RREQ the node initiates, and together with the node's IP address, uniquely identifies a RREQ. Along with its own sequence number and the broadcast ID, the source node includes in the RREQ the most recent sequence number it has for the destination. Intermediate nodes can reply to the RREQ only if they have a route to the destination whose corresponding destination sequence number is greater than or equal to that contained in the RREQ.

During the process of forwarding the RREQ, intermediate nodes record in their route tables the address of the neighbour from which the first copy of the broadcast packet is received, thereby establishing a reverse path. If additional copies of the same RREQ are later received, these packets are discarded. Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination/intermediate node responds by unicasting a route reply (RREP) packet back to the neighbour from which it first received the RREQ. As the RREP is routed back along the reverse path, nodes along this path set up forward route entries in their route tables which point to the node from which the RREP came. These forward route entries indicate the active forward route. Associated with each route entry is a route timer which will cause the deletion of the entry if it is not used within the specified lifetime. Because the RREP is forwarded along the path established by the RREQ, AODV only supports the use of symmetric links. Routes are maintained as follows. If a source node moves, it is able to reinitiate the route discovery protocol to find a new route to the destination. If a node along the route moves, its upstream neighbour notices the move and propagates a link failure notification message (a RREP with infinite metric) to each of its active upstream neighbours to inform them of the erasure of that part of the route. These nodes in turn propagate the link failure notification to their upstream neighbours, and so on until the source node is reached. The source node may then choose to reinitiate route discovery for that destination if a route is still desired.

Dynamic Source Routing (DSR)
Dynamic source routing (DSR) is based on source routing where the source specifies the complete path to the destination in the packet header. All intermediary nodes along the path simply forwards the packet to the next node as specified in the packet header. This means that intermediate nodes only need to keep track of their neighbouring nodes to forward data packets. The source on the other hand, needs to know the complete hop sequence to the destination. This eliminates the need for maintaining latest routing information by the intermediate nodes as in DSDV. In DSR, all nodes in a network cache the latest routing information. When more than one route to the destination is found, the nodes cache all the route information so that in case of a route failure, the source node can look up their cache for other possible routes to the destination. If an alternative route is found, the source node uses that route; else the source node will initiate route discovery operations to determine possible routes to the destination. During route discovery operation, the source node floods the network with query packets. Only the destination or a node which already knows the route to destination can reply to it, hence avoiding the further propagation of query packets from it. If a broken link is detected by a node, it sends route error messages to the source node. The source node on receiving error messages will initiate route discovery operations. Unlike DSDV, there are no periodically triggered route updates.

Problem Identification
Security issues in MANET have drawn considerable attention over past few years. Using trust to improve the security is an active area of research. As per our knowledge, no solution has been proposed so far to secure the network against internal attack using such mechanism which is combination of hop value and trust value. Here, we present the related work done by various researchers on trust based scheme for mobile ad hoc network, which extended Ad Hoc On-demand Distance Vector (AODV) routing protocol. AODV is an on demand routing protocol which comes under the category of reactive routing

protocol. Route discovery and route maintenance are the two basic operation of AODV. Route discovery operation is used to discover the route by using RREQ (route request) and RREP (route reply) control message. When a source node wants to send the data to destination node, it will broadcast RREQ packet to neighbours and then to their neighbours & so on. When a destination node receives RREQ, it will send RREP to source node. In this paper existing work has been discussed about an trust based ad hoc on demand routing protocol for MANET called HAODV (honest ad hoc on demand distance vector routing protocol) where honest value will be initialized (one value will be based on the hop and other will be based on the trust) in the initialization phase. Security issues in MANET have drawn considerable attention over past few years. Using trust to improve the security is an active area of research. As per my knowledge the following problems are identified:

a) There is no solution has been proposed so far to secure the network against internal attack using such mechanism which is combination of hop value and trust value.
b) Network is depending on trust value and based on single methodology (used single routing factor).

Proposed Methodology

T.Eissa and S.Abdul [1] proposed a FrAodv for securing AODV routing protocol using friendship mechanism. In this protocol they have used two algorithms (FwEvaluate and RvEvaluate) to evaluate the forward and reverse path respectively. In this scheme each node keeps a list of friends and friendship value of these friends. The bigger the number, the more it trusts in that node. The IP and MAC address have been used to check the friend's authentication in the network. FrAodv uses two algorithm to calculate trust as a result it increases extra overhead to the network.

Rajiv K. Nekkanti & Chung-wei Lee [8], proposed a routing protocol that is based on securing the routing information from unauthorized users. Even though routing protocols of this category are already proposed, they are not efficient, in the sense that, they use the same kind of encryption algorithms (mostly high level) for every bit of routing information they pass from one intermediate node to another in the routing path.

M.G.Zapata and N.Asokan [5] have proposed Secure AODV (SAODV) based on the AODV routing protocol. In this protocol two mechanisms are used (Hash chains and Digital Signatures) to secure the AODV message. Hash chains are used to secure the hop count which is mutable information in the message and digital signatures are used to authenticate the non-mutable fields of the message. SAODV can prevent only blackhole attack and SAODV's signatures require a processing power that might be excessive for certain kinds of ad hoc scenarios.

Yogendra Kumar Jain and Pankaj Sharma [14] have proposed some assumptions and establish the network model of Trust AODV (TAODV). We also argue why we focus our security solution on routing protocol in the network layer instead of link layer. Mobile nodes in MANETs often communicate with one another through an error-prone, bandwidth-limited, and insecure wireless channel.
Here,

1. Each node in the network has the ability to recover all of its neighbours;
2. Each node in the network can broadcast some essential messages to its neighbours with high reliability;
3. Each node in the network possesses a unique ID that can be distinguished from others.

Naveen Kumar Gupta and Kavita Pandey, Trust Based Ad-hoc On Demand Routing Protocol for MANET is the base paper presented honest based general framework for trust establishment and management in the network using AODV routing protocol. We proposed a best trust-based scheme for securing AODV routing protocol in MANET using the honest mechanism. In the honest mechanism, two honest value will be initialized (one will be based on the hop and other will be based on the trust). The honest value based on the hop will be incremented and decremented during RREQ and RREP phase respectively and the honest value based on trust value will be used for trust calculation of path. In the proposed HAODV routing protocol, the nodes can evaluate the routing paths according to our trusted metrics before forwarding the data through these routes. For identity information we will use password value. This scheme is believed to provide a robust environment where MANET nodes can trust each other in a secure community.
We are including new trust based network routing factors as follows:

a) Distance- which is based on Physical Distance.
b) Degree-which is based on Connection.

For solving these routing factors the following algorithm is described as follows:

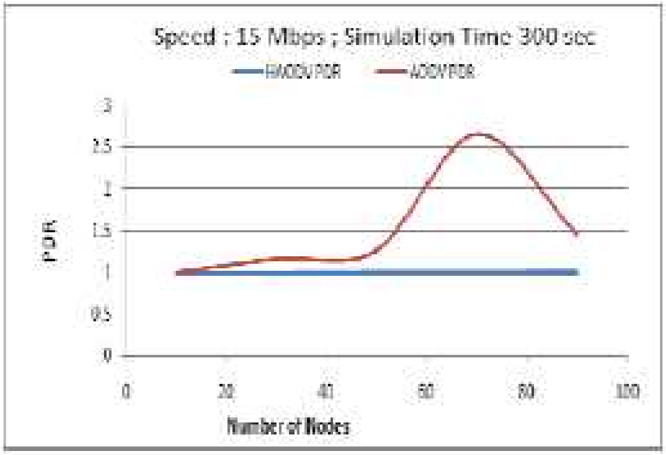
1) Node creation and authentication.
2) Honest value initialization (Based on the Hop and Based on the Trust)
3) Communication and path evaluation

Expected Outcomes

In this section, the results have been analyzed using three performance metrics. The performance metrics are Number of drop packets, Packet Delivery Ratio and throughput. The following simulation parameters have been considered for the performance comparison of different routing protocols as given below:

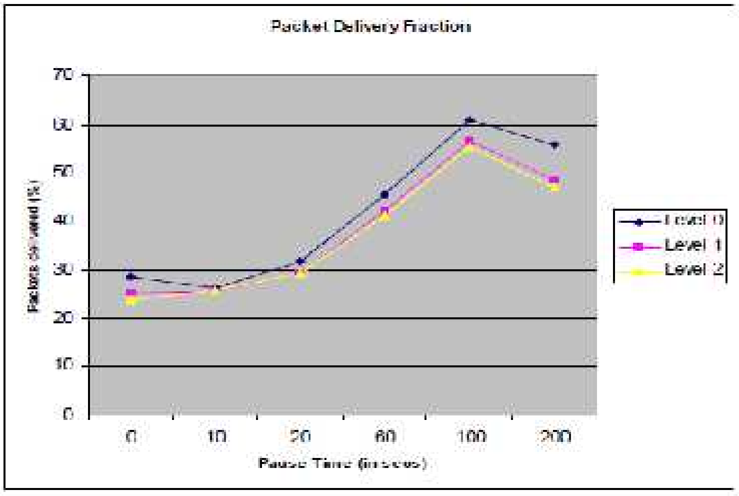
References	Parameters	Simulator	Network Size(m)	Nodes	Simulation Time	Packet Size	Traffic Type	Pause Time(s)	Speed
Based Paper	Values	NS-2	800x800	20	100 Sec	512 bytes	TCP	10	5m/sec
Paper [14]		NS-2	1000x1000	30	900 Sec	1024	UDP	10	1 m/sec
Paper [8]		NS-2	500x500	50	100 Sec	60	CBR/30	10	20
Paper [16]		NS-2	1000x1000	70	100 Sec	512	CBR	2	100 s

Table: Comparison between Simulation Parameters



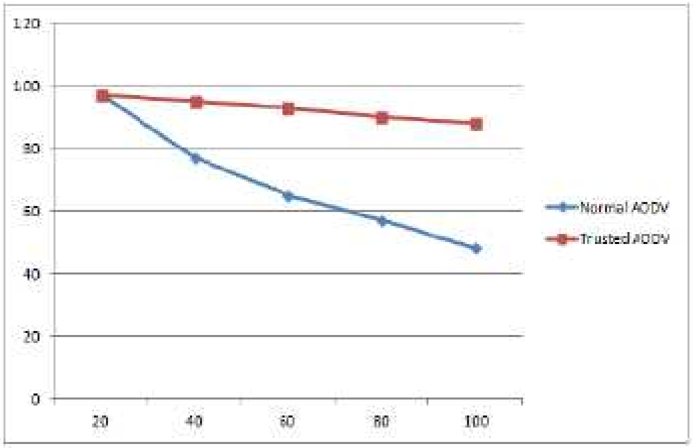
PDR Vs Number of Nodes

(Based Paper- Trust Based Mobile Ad-hoc Network Routing Protocol for MANET)

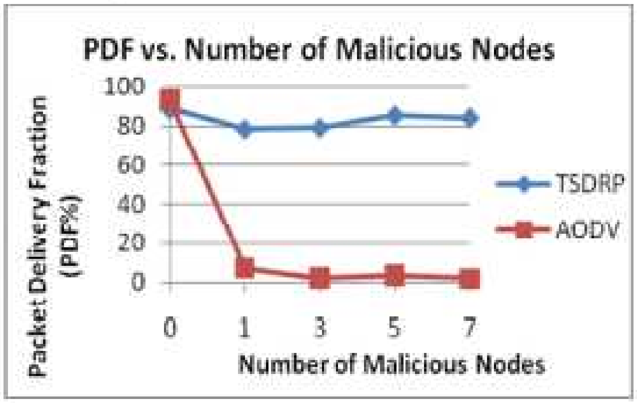


PDR Vs Number of Nodes

(“Trust based Ad hoc On-demand Distance Vector for MANET”)



PDR Vs Number of Nodes
(Trust Based Adaptive On Demand Ad Hoc Routing Protocol)



PDR Vs Number of Nodes
(Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs)
Graph: Comparison PDR Vs Number of Nodes based on different Routings.

Conclusion & Future Work

A method based on the honest method to protect the AODV routing protocol has been accessible. The performance of HAODV has been analyzed via the four parameters i.e. the number of dropped packets, Throughput and Packet delivery ratio. The based paper’s simulation results show that HAODV performs well in terms of throughput and no of dropped packets but in terms of PDR, AODV is better. The throughput of HAODV is always improved as compared to AODV even by increasing the number of nodes, by unreliable the velocity, etc. In HAODV least number of packets is dropped in comparison to AODV. Honest based routing protocol proved to be best in terms of packet loss, throughput and power consumed.

The future work of this research is to implement the proposed scheme with more numbers of parameters as like End to End Delay and Overhead Routing while evaluating the path. Our future work is to be minimizing the dropped packets with a single node, show the reason why packets are dropped and find out which nodes will drop packets. It will also choose a best path and shortest path for requesting packets to send from source to destination at a time except on single path.

References

1. Tameem Eissa & Shukor Abdul Razak & Rashid Hafeez Khokhar & Normalia Samian, “Trust-Based Routing Mechanism in MANET: Design and Implementation”, Springer Science, 2011.
2. Jin-Hee Cho, Ananthram Swami, Ing-Ray Chen, “A Survey on Trust Management for Mobile Ad Hoc Networks”, IEEE Communications Surveys & Tutorials, 2011.

3. Naghamh. Saeed, maysamf. Abbod, and Hamed S. Al- Raweshidy, “MANET Routing Protocols Taxonomy”, International Conference on Future Communication Networks 2012.
4. Manel Guerrero Zapata ,“ Secure Ad hoc On-Demand Distance Vector Routing”, Mobile Computing and Communications Review, Volume 6, Number 3, 2006.
5. S.A.Razak, S.M.Furnell,P.J.Brooke ,“Attack against Mobile Ad Hoc Networks Routing Protocols”, Network Research Group ,University of Plymouth, 2009.
6. C. E. Perkins and E. M. Royer, “Ad-Hoc on-Demand Distance Vector Routing,” Proc. 2nd IEEE Wksp. Mobile Computer Systems and Applications, 1999.
7. Poonam Gera, Kumkum Garg, Manoj Misra, “Trust Based Multi-Path Routing for End to End Secure Data Delivery in manets”, ACM 978-1-4503-0234-0/10/09, 2010.
8. Rajiv K. Nekkanti, Chung-wei Lee, “Trust Based Adaptive on Demand Ad Hoc Routing Protocol”, ACMSE, Huntsville, Alabama, USA, 2004.
9. Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, “Different Types of Attacks on Integrated MANET-Internet Communication “, International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3), 2005.
10. David B. Johnson, David A. Maltz, Josh Broch, “DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks”, Computer Science Department, Carnegie Mellon University, 1994.
11. Charles E. Perkins and Pravin Bhagwat, “Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers”, ACM SIGCOMM 94, 1994.
12. Yogendra Kumar Jain, Pankaj Sharma “Trust based Ad hoc On-demand Distance Vector for MANET” National Conference on Security Issues in Network Technologies (NCSI-2012).
13. Dr. S.S.Dhenakaram, A.Parvathavarthini , An Overview of Routing Protocols in Mobile Ad-Hoc Network,2012.
14. Ku. Vishakha V. Vyas, Nitin K.Bhil, Mobile Ad-Hoc Network (MANET) and its Security Aspects, 2015.
15. R.S.Mangrulkar, Pallavi V Chavan, S.N. Dagadkar, Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MANET, 2010.
16. Akshai Aggarwal, Savita Gandhi & Nirbhay Chaubey,Trust Based Secure on Demand Routing Protocol (TSDRP) for manets, IEEE, 2014.