Trust and Shortest Path Selection based Routing Protocol for MANET

Naveen Kumar Gupta
Department of CSE
JIIT
NOIDA, INDIA

Amita Garg
Department of CSE
JIIT
NOIDA, INDIA

ABSTRACT
Mobile Ad hoc Network (MANET) comprises a Collection of wireless nodes that does not rely on any fixed infrastructure or base station. Trust based routing in MANET is challenging task due to its on demand dynamic nature which makes it susceptible to various types of attacks such as black holes, Byzantine, rushing attacks etc. The proposed trust based Management framework gives an overview about trust in MANETs. It works on the concept of trust factor in (initialization phase), for selecting the most efficient route and a routing path is evaluated using the concept of trust value that is updated during the route exchange process. The performance metric considered are throughput, number of drop packets and packet delivery ratio (PDR). The simulation results show that the proposed protocol gives better performance than existed protocol.

Keywords
Trust, security, shortest path, AODV, attacks, MANET.

1. INTRODUCTION
A MANET is a self-organized wireless network composed of autonomous nodes or terminals that communicate with each other in order to forward the packet from one hop to other hop before it reaches to the required destination by using the routing protocol. Examples of routing protocol in MANET are ad hoc on demand distance vector (AODV) [1], dynamic source routing (DSR) [2], destination sequenced distance vector (DSDV) [3] etc. The main objective of these routing protocols is to find the shortest path from source to destination and choose the best path by using the appropriate route selection mechanism. While transmitting the route packets and data packets, mobile nodes are vulnerable to various types of attacks such as eavesdropping attack in which valuable information is stolen from the targeted nodes without any disrupting the operation of the network. Therefore, detecting this type of passive attacks [4] are very difficult. Another type of attacks like message modification impersonation attacks which usually happen against route message that are modified with forged nodes to disrupt the operation of network activities. Further some attacks such as a black hole attack, wormhole attack etc. are categorized in terms of internal attacks [4] because these attacks are done by the nodes presented in the network. Therefore, it is a very important aspect to maintain the trust between the nodes to achieve security.

Security in wireless network is a major aspect due to its characteristics like infrastructure less, mobility of nodes, path loss and interference. To establish the secure way of transmission and communication, all types of threats and attacks should be prevented. Many researchers have been proposed secure and trust based algorithms to prevent routing attacks. Most of these mechanisms focused on how to protect the data transmission in the network, as they are excellent in data protection. However current ad hoc routing protocols have not fully addressed performance issues related to security by considering the shortest path. This paper proposed an enhanced trust based framework to secure the efficient routing protocol AODV by using the trust factor and trust value. Related work is described in section 2. The proposed algorithm is described in section 3. .The performance metrics and simulation results of our proposed scheme are discussed in detail in Section 4 followed by last section concluded and gives some suggestions for future work.

2. RELATED WORK
Many researchers have been proposed several routing protocols such as DSR, DSDV, AODV, ZRP etc., but they didn't consider any security issue. Improve security using a trust in MANET is an active area of research. Several secure routing protocols have been proposed to address various types of attack, still none of the protocol exists which can provide security against several types of attacks. Ad-hoc On-demand Distance Vector (AODV) routing protocol is one of the most efficient reactive routing protocol designed for MANET. It is an On-demand routing protocol meaning that it builds routes between nodes only as desired by the source node. In this protocol sequence number are used to maintain the current updating of routes. When a source node wants to send packets to destination, but it does not have a proper route entry to that particular destination then source node broadcast a RREQ (route request) packet across all its neighbours. When the neighbouring node receives this RREQ packet, firstly it checks the route entry for that particular destination .If it does not have, then it will set up a reverse path towards the source node (from which it receives). Secondly, it checks the path to that destination in its routing information, if a neighbouring node has path about the destination or if itself a destination node then current node destination sequence numbers (contained in RREQ packet) are compared to the neighbours dsn number and whichever having greater than or equal sequence number that routing path in the form of RREP packet to be unicasted to that source via reverse pointer. But In case, if neighbours node does not have path to that destination then it broadcasts the RREQ packet to their neighbours. This process continues and nodes keep information about the source IP address and Broadcast id that it can discard the RREQ packet if it already processed. When the source node receives the RREP packet then it sends the data information to that destination. But later on source node may receive the more than one RREP packets, if these packets having greater sequence number or packets having same

sequence number lesser hop, then the source node update its routing information to that destination .The route should be maintained unless route remains active.
Route maintenance process happens in following ways: firstly node may send a HELLO message to their neighbours locally for maintaining the positive information about the connectivity of the nodes. Secondly, a node can maintain information about link connectivity to their next hop through some mechanism based on link layer .If somehow link breaks and the route are active then node upstream propagates the RERR (routeerror message) towards the source node that the route is unreachable . While receiving the RERR message , if a source node still wants to send more packets than it re-initiates the route discovery method. While routing the information AODV does not consider any security concerned. As a result, it is vulnerable to various types of attacks.

Zapata and Asokan [5] proposed Secure AODV (SAODV) by considering the AODV as a base protocol. This protocol use one way hash chain and digital signature to make AODV secure. In first hash chain are used to authenticate the hop count information (mutable information) in the messages and digital signatures are used to authenticate and protect the non-mutable information of RREQ and RREP messages. Several attacks performed on AODV can be prevented with the extension of SAODV mechanism. However, SAODV uses digital signature, since processing power in computing the signature might be expensive for certain kinds of wireless networks. As SAODV provide authenticity by computing signatures on nodes but it does not provide route reliability.

Another protocol based on securing DSR is On-Demand secure routing protocol called ARIADNE [6]. It relies on compromising the nodes by using the symmetric key cryptography. It can prevent the selfish nodes which can perform attacks on the uncompromised nodes in the uncompromised Routes. Denial of Service attacks can also overcome by ARIADNE protocol. Since this protocol basically works on single layer not for multiple-layer, that's why it is not efficient to prevent every type of attacks.

Ying Dong [7] proposed TAODV (Trusted AdHoc On Demand Routing Protocol) to secure the AODV routing protocol. This protocol focus on the concept of the trust model to provide security for routing protocols in the network layer. The trust model is derived from the extension of subjective logic which defines the trust between nodes using probabilistic opinion Trust's recommendation, combination and judging are the three basic modules of TAODV. TAODV prevent external attack and DOS attack using digital signatures

3. PROPOSED ALGORITHM

In this section, a trust based management framework for securing Ad hoc On Demand Distance Vector Routing Protocol has been presented. In this mechanism, Constant trust factor is used to evaluate the trusted and shortest path for communication in the network. To prevent the attack by malicious node, the identity information like IP address and Trust factor value has been used. This identity information is

assigned to each node in initialization phase or when the node will be configured.
In the proposed scheme, a mechanism to check the next node whether it is trusted or not have been deployed where each node will be configured with the constant trust factor value,that value will be known to each and every node. The trust value is initiated in the route discovery phase. Each node keeps a constant trust value that will change in the RREP phase. Initially each node will be configured with the constant trust value 50 using node_trust function. Source node broadcasts RREQ to neighbouring nodes until a destination node or node having a route to destination determines, during this process hop count is initialized. If the current node is final destination it will check the trust value of the previous hop and if it is not the destination then it will forward the request to all its neighbouring nodes. If the current node is destination then it will evaluate the shortest path from destination to source.
AODV can select the better path (trusted and shortest) using trust value and the number of hops. When the RREQ and RREP message are generated in the network, each node append its own trust value to the trust accumulator on these route discovery phase.
Each node also updates its own routing table.
The following formula can be used to evaluate the trusted and shortest path.

$$\frac{\text{Sum of trust values} * \sqrt{\text{No of hops}}}{\text{No of hops}}$$

Where,

Sum of trust value = $\sum$ *trustvalue (i)*

4. SIMULATION RESULTS

An NS-2 simulator has been used to simulate the results. NS-2 is an object oriented simulator written in C++ and OTcl (object oriented tool command language). In this section, the performance metric and implementation details of the proposed protocol has been presented.

4.1 Performance Metrics

Three performance metric are evaluated in our simulation:
1. Packet delivery Fraction- The packet delivery fraction is the total number of data packets received by the destination over the total number of data packets transmitted by the source.
2. Throughput – The ratio of data packets received to the destination to those generated by the source.
3. Number of drop packets – It is the number of packets lost by the routers at the network layer due to the capacity of the buffer.

4.2 Implementation

The Random Way Point Mobility Model describes the movement of nodes. In this simulation, files are categorized by number of nodes such as 10,30,50 and 70. The pause time is set to 10 sec. and maximum speed set to 5 m/s. The simulation time is set to 100 sec. and nodes are equally distributed in 800x800 m area.
The TCP traffic connection has been used for our simulation because it is reliable as compare to CBR (Constant Bit Rate).Different traffic files have been generated by varying the number of nodes.
Different trace files have been generated for each scenario and for each protocol. The trace files have been parsed with the help of programs written in awk script to extract the information needed to analyse the result. After getting the values of each performance metric according to each protocol, the graph has been plotted to show the comparison between AODV and EAODV.
The simulation parameter in this work is shown in table-1.

Table 1 Simulation Parameter

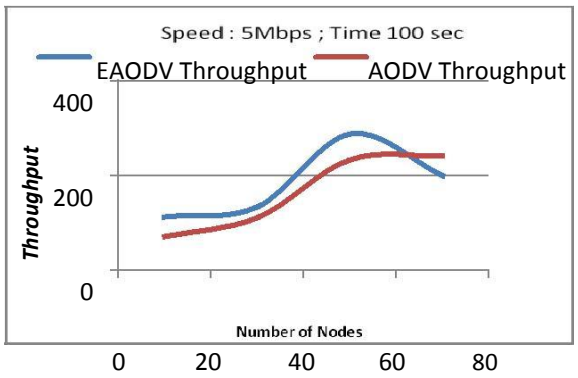
Simulator	NS-2 (v-2.34)
Area(m x m)	800 x 800 m
Nodes	10,30,50,70
Simulation Time(s)	100
Node Speed(m/s)	5

Pause Time(s)	10
Traffic Type	TCP
Packet Size	512 bytes
Protocol Used	AODV
Mobility Model	Random Way Point
MAC layer Protocol	Mac/802_11
Antenna type	Antenna/Omni Antenna

4.3 Results

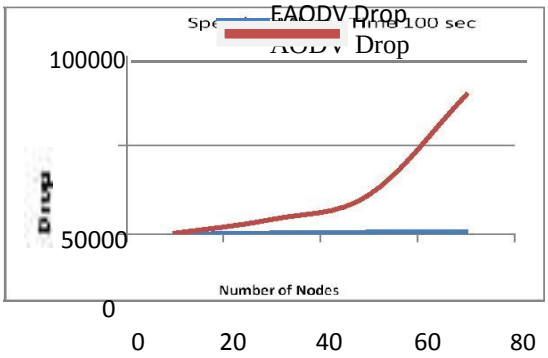
In this section, the results have been analysed using the three performances metric are Packet delivery fraction (PDR), Throughput and number of dropped packets. In all graphs x-axis represents the number of nodes and y-axis represents the value of performance parameter.

Throughput- Results show that the throughput of EAODV is better as compared to AODV. Generally, By increasing the number of nodes, throughput also increases.



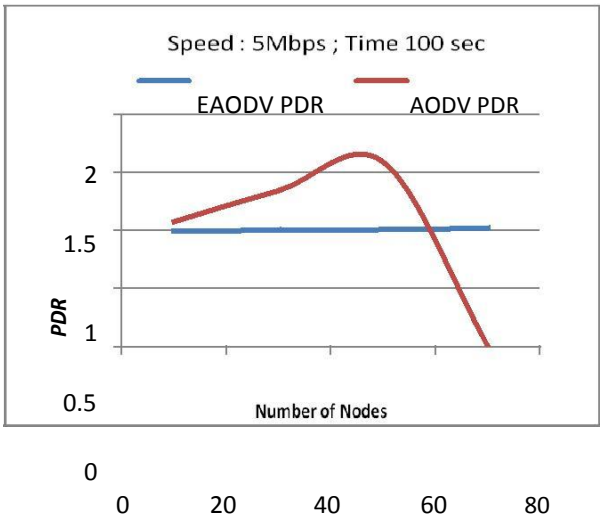
Graph 1.1– Throughput, speed 5Mbps, simulation time 100sec.

Number of drop packets – The graph shows that the number of drop packet using AODV is increasing by varying the number of nodes but using EAODV, least number of packets has been dropped.



Graph 1.2- Number of drop packet, speed 5Mbps, simulation time 100 sec

Packet delivery Ratio – The simulation result shows that the PDR of AODV is increasing and decreasing at some point by varying the number of nodes but EAODV is giving better result as compared to AODV.



Graph 1.3- PDR, speed 5Mbps, simulation time 100 sec

5. CONCLUSION

In this paper, a new MANET routing protocol EAODV has been proposed which is basically an extension of the AODV routing protocol that incorporates a trust based mechanism to enhance its security. The proposed algorithm has implemented and simulated using the NS-2 simulator. The performance of the proposed protocol has been analysed using the parameter named as throughput, number of drop packets and packet delivery fraction. The performance of the proposed protocol is better in terms of throughput, number of drop packets and PDR.

In the future works, we would like to optimize our proposed algorithm in terms of number of nodes and establishing a fast mechanism to detect and prevent the malicious nodes even when we have a large number of nodes.

6. REFERENCES

[1] C. Perkins, E. Royer and S. Das, "Ad hoc on demand distance vector routing", RFC-3651, (July 2003).

[2] David B. Johnson, David A. Maltz, Josh Broch ,"DSR:The Dynamic Source Routing Protocol for Multi-HopWireless Ad Hoc Networks", Computer Science Department, Carnegie Mellon University, 1994.

[3] Charles E. Perkins and Pravin Bhagwat, "Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers", ACM SIGCOMM '94, 1994.

[4] 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.

[5] Manel Guerrero Zapata ," Secure Ad hoc On-Demand Distance Vector Routing", Mobile Computing and Communications Review, Volume 6, Number 3, 2006.

[6] Y.C. Hu, A.Perrig and D.B.Johnson, "Ariadne: A secure on demand routing protocol for ad-hoc networks" in Proc. 8th ACM conf. Mobile Computing Network, Sep.2002, pp 12-23.

[7] Rajiv K. Nekkanti, Chung-wei Lee, "Trust Based Adaptive On Demand Ad Hoc Routing Protocol", ACMSE, Huntsville, Alabama, USA, 2004.

[8] Jin-Hee Cho, Ananthram Swami, Ing-Ray Chen ," A Survey on Trust Management for Mobile Ad Hoc Networks", IEEE Communications Surveys & Tutorials, 2011.

[9] NaghamH. Saeed, MaysamF. Abbod, and Hamed S. Al-Raweshidy ," MANET Routing Protocols Taxonomy", International Conference on Future Communication Networks 2012.

[10] Sunil Taneja and Ashwani Kush ," A Survey of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010.

[11] NS-2 Reference "http://www.isi.edu/nsnam/ns/".

[12] Watchara and Sakuna ,"CAODV: Free Blackhole Attack in Ad Hoc Networks", International Conference on Computer Networks and Communication Systems, IPCSIT vol-35, 2012.

[13] Tameem Eissa & Shukor Abdul Razak & Rashid Hafeez Khokhar & Normalia Samian ," Trust-Based Routing Mechanism in MANET: Design and Implementation" , Springer Science, 2011.