International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering 2015 [ICIREIE 2015]

ISBN	978-81-929866-3-0	**VOL**	01
Website	www.icireie.org	**eMail**	icireie@asdf.res.in
Received	10 - July - 2015	**Accepted**	31- July - 2015
Article ID	ICIREIE001	**eAID**	ICIREIE.2015.001

Comparative Performance analysis of Trust implemented AODV with Trust implemented OLSR under the Blackhole Attack

Gayathri.D[1], Dr.S.JanakiRaman[2]
[1]Research Scholar, Bharathiar University, Coimbatore, Tamil Nadu ,India.
[2]AssistantProfessor, Department of Banking Technology,Pondicherry University, Pondicherry, India.

Abstract: *MANETs are group of nodes that get in to communication and resolve at any place or at any point of time without a central authority or infrastructure. The nature of these network are vulnerable to many type of attacks which lead to security issues where valuable information are compromised. There are many available protocols to guide them. But lacuna in secure routing has come in to limelight and vigorous research is in progress to get a robust protocol. One such security measure called Trust, a metric has been implemented in AODV, a reactive routing protocol and OLSR, a proactive routing protocol and under a type of attack i.e. security threat to MANET called Black –hole a comparison of performance analysis is performed in this paper.*

Keywords: MANET; Black hole Attack; AODV; reactive protocol; OLSR; proactive protocol; Trust; (key words)

I. INTRODUCTION

MANETs are Mobile Ad hoc Networks where the nodes coming in to communication act both as hosts and routers. They are boon to the military operations, rescue operations, battlefield areas and where the infrastructure is not found or damaged severely. Since they are formed and deployed anywhere without a access point or base station they are gaining popularity in every aspect. But due to their limited bandwidth, poor scalability, dynamic topology, limited energy and loss of security bring in many challenges in routing. These pave way for their low performance which should be handled efficiently by routing protocols. The routing protocols do not defend MANET due to attacks of data compromise. Off late, many research have given enhancement in improving the protocols to manage and secure MANETs. The attack types are many and one such attack called black hole attack is implemented and a metric Trust is implemented in Ad hoc On Demand Distance Vector (AODV), reactive protocol and Optimized Link State Routing (OLSR), a proactive protocol and comparative study is performed in this paper.

II. ROUTING PROTOCOLS

Routing is the process of forwarding information or data packets towards its destination using the best and efficient path which is talked in terms of number of hops, traffic, security, etc. in MANETs each host node acts as a specialized router itself. Routing protocols have been designed to route in MANETs where they possess a great task of routing with no infrastructure and with no rigid

Cite this article as: Gayathri D, Dr. S JanakiRaman. "Comparative Performance analysis of Trust implemented AODV with Trust implemented OLSR under the Blackhole Attack." *International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering (2015)*: 01-06. Print.

topology. MANET routing protocols can be categorized in to the following based on their methodology. They are proactive protocols, reactive protocols and hybrid protocols.

A. Proactive protocols

In these type of protocols the nodes know the complete routing information of the network before the actual transfer of data packets start. This is done by flooding network periodically with network status information to find out possible change in topology. Examples of proactive protocols are:

- GSR : Global State Routing Protocol
- OLSR : Optimised Link State Routing Protocol
- HSR : Hierarchical State Routing protocol

B. Reactive protocols

In reactive protocols the nodes know only the active paths to the destination nodes. A route search is made for every new destination. Example of reactive protocols are :

- AODV : Ad hoc On demand Distance Vector Routing protocol
- DSR : Dynamic Source Routing Protocol
- LAR : Location Aided Routing Protocol

C. Hybrid protocols

They are the combination of proactive and reactive protocols. They remain globally reactive and locally proactive. Example of Hybrid protocol is ZRP, Zone Routing protocol.

III. OVERVIEW OF AODV PROTOCOL

Ad hoc On-demand Distance Vector Routing protocol is a type of reactive protocol. Here the routes for the destination are found only when needed. The routing table is maintained in the nodes and not in the packets reducing Memory overhead. The search for the route by the source to the destination is as follows. If the source node has the route to the destination and if the destination sequence number is the highest it means the route is a fresh one and therefore forwards the packets towards the destination. Else it generates RREQ, Route Request packets and forwards to its one hop neighbors. If the neighbors find itself to be the destination or if has route to the destination it forwards the RREP, Route Reply packet to the source node else it again forwards the RREQ, Route Request packets to its neighbor. The neighbors do the same as its previous node. On getting the RREP, Route Reply packets the source checks for the Destination Sequence Number in the RREP, Route Reply packets greater than the RREQ, Route Request Packets itself. If it finds the Destination Sequence Number to be greater it uses the route to forward the packets in that route to the destination. By the time RREP, Route Reply packets reaches the source all the intermediate nodes know the route to source as well as to the destination. AODV uses HELLO messages to indicate its presence in the network to its neighbor nodes. AODV uses RRER, Route Error Packets for the link failure.

IV. OVERVIEW OF OLSR PROTOCOL

OLSR, Optimized Link State Routing protocol is a proactive routing protocol. By sending periodic control messages it maintains the latest topology information. As its name denotes it as a optimized routing protocol as its makes use of Multipoint Relay (MPR) nodes in-order to decrease the routing overhead. Each node selects its subset of neighbors as MPRs. MPR nodes are responsible for rebroadcasting control packets of nodes which have selected this node as MPR. Other non-MPR neighbor nodes receive and process packets without relaying them. MPRs are selected based on 2 criteria, first is they are one hop neighbors of the node and second is they cover all the two hop neighbors of that node. OLSR uses two type of messages namely HELLO and TC messages. They are periodically transmitted. All the nodes contain a table that includes information of its current neighbors. HELLO messages are generated using this information. Each node propagates Link State information between itself and its neighbors by HELLO messages. Upon receiving these HELLO messages the nodes know their one hop and two hop neighbors and this makes them to choose their MPR set. In addition nodes can create and update their MPR selector list. Upon this list creation nodes start to send TC messages. Hello messages are processed but not relayed by the nodes. But TC messages contain the MPR selectors of a node and existing link from this node is represented. Other nodes update their topology table. All the nodes receive and process TC messages but the MPR relays them. Finally all the nodes extract current detectable routes with regard to information in topology table and store them in this routing table. At the time of sending data packets the nodes use this information.

V. BLACK HOLE ATTACK

Black hole attack is a type of active attack in MANETs. The malicious node advertises itself having the shortest route to the destination and directs the traffic towards itself. It receives the packets from the source by advertising itself with a spoofed destination address.

D. Black hole attack implementation in AODV and OLSR

In AODV, the black hole attacker sends fake RREP message to the source which has higest Destination Sequence Number than any other node stating that it has the fresh route to the destination there by getting the data packets towards itself and starts dropping the packets.

In OLSR, the malicious node sends false HELLO messages, where it shows to have many neighbors than it actually has. It keeps its willingness field to WILL always constantly in HELLO messages. Thus, gaining the probability of acting as MPR. Due to the fake

Cite this article as: Gayathri D, Dr. S JanakiRaman. "Comparative Performance analysis of Trust implemented AODV with Trust implemented OLSR under the Blackhole Attack." *International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering (2015)*: 01-06. Print.

HELLO messages falsified TC messages are propagated. Thus, the attacker captures route. Source node S receives HELLO messages from X node , the black hole attacker and selects X as MPR and updates its routing table accordingly. To reach the destination node D,TC and data packets should pass via X where it is dropped.

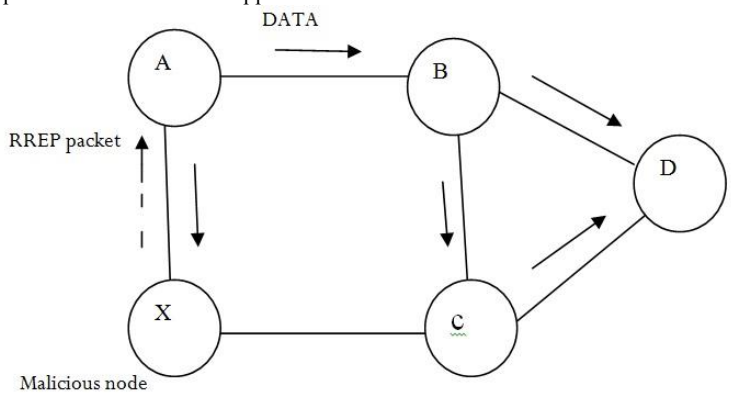

Figure.1. Black hole Attack in AODV Protocol

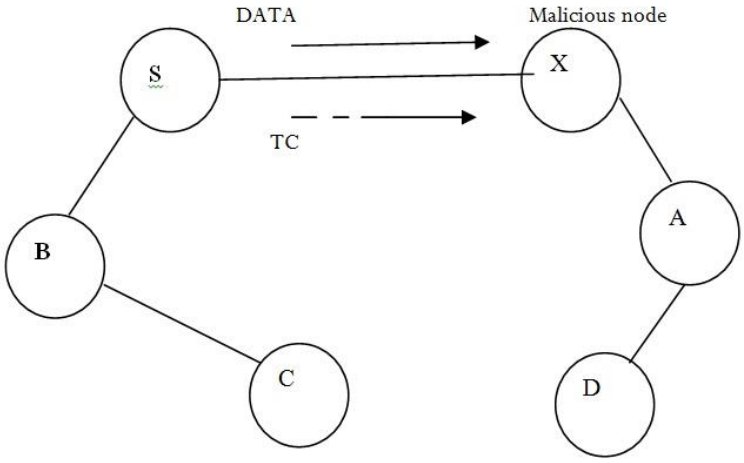

Figure.2. Black hole Attack in OLSR Protocol

VI. TRUST framework and its implementation in AODV and OLSR

Trust metric is implemented in the protocols in-order to gain reliability in routing through nodes. Trust is a measure which can be obtained out of experience. The model of Trust implemented in AODV and OLSR protocols is as follows.

The packets forwarded by the nodes are monitored promiscuously and detection is done by buffer of packets stored that have recently sent for forwarding. A cyclic buffer is used to store the packets. Here when the packets are forwarded they are deleted from the cyclic buffer and the Trust value of forwarded node increases. If the packet is not being forwarded for a long time or when the packet is being delayed for a long time the last element is removed from the cyclic buffer, thus decreasing the trust value of the node.

- Initially trust value is assigned to zero for all the nodes.
- Nodes monitor the other nodes behavior promiscuously.
- Cyclic buffer is maintained for packet storage.
- Packets forwarded, the nodes trust value increases by +1.
- Packets delayed or packets not forwarded, the nodes trust value decreases by -1.
- When the Trust value is -5, the node is blacklisted and is not included for routing.

VII. SIMULATION SET UP

NS 2.34 is used for the simulation. In this 10 -100 nodes have been used for simulation for a duration of 30 seconds, in a area of 1500 * 1000 using 802.11 MAC layer in a transmission range of 250 meters. Under the black hole attack a comparative performance analysis of Trust implanted AODV with Trust implemented OLSR have been performed and their superiority over AODV and OLSR have been witnessed under Blackhole attack. The performance metric taken for study is the Packet Delivery Ratio.

Cite this article as: Gayathri D, Dr. S JanakiRaman. "Comparative Performance analysis of Trust implemented AODV with Trust implemented OLSR under the Blackhole Attack." *International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering (2015)*: 01-06. Print.

TABLE 1.
simulation parametrs and values

parameter	value
simulator	ns 2.34
nodes	10 – 100
attack	black hole attack
simulation area	1500 * 1000
routing protocols set 1	TRUST implemented AODV and TRUST implemented OLSR
routing protocols set 2	AODV and OLSR
traffic	cbr (constant bit rate)
data rate	2 Mbps
interval	0.01 seconds
simulation time	30 seconds
antenna	omni directional
packet size	512 bytes
transmission range	250 m
number of attackers	one
propagation	two ray ground

RESULTS AND DISCUSSIONS

In this investigation Packet delivery ratio has been taken as a metric of talk to compare the efficiency of trust implemented AODV and Trust implemented OLSR and its superiority over their base protocols namely AODV and OLSR discussed in terms of Packet Delivery Ratio.

Packet Delivery ratio is the ratio of the number of packets received by the destination to the number of packets being forwarded by the source.

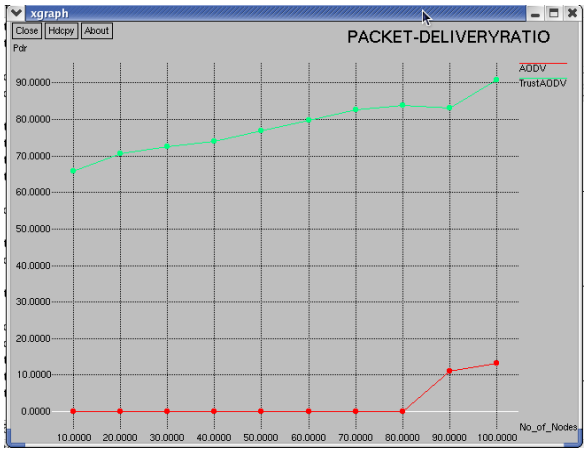

FIGURE. 3. Packet Delivery Ratio for AODV and Trust AODV.

Cite this article as: Gayathri D, Dr. S JanakiRaman. "Comparative Performance analysis of Trust implemented AODV with Trust implemented OLSR under the Blackhole Attack." *International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering (2015)*: 01-06. Print.

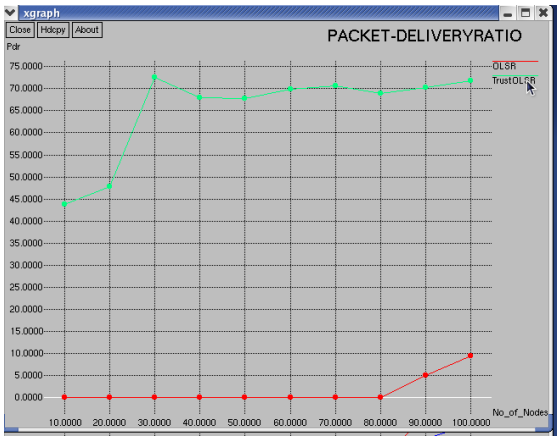

FIGURE. 4. Packet Delivery Ratio for OLSR and Trust OLSR.

From the graph we deduce that the performance of both Trust implemented AODV and Trust implemented OLSR are better in Packet delivery Ratio than their base protocols AODV and OLSR respectively. This is due the black hole attack where it does not allow the packets got by it for further routing and drops it thus adversely lowering the Packet Delivery ratio.

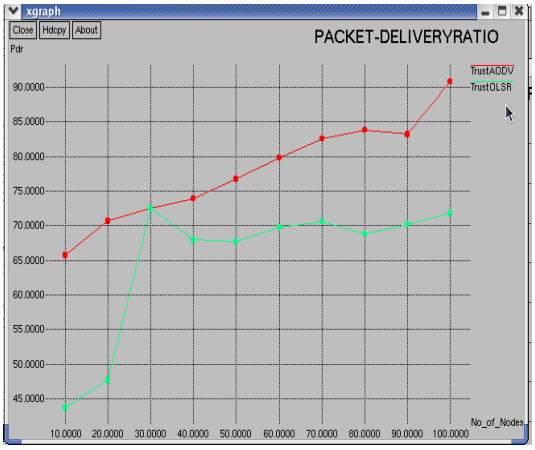

FIGURE. 5. Packet Delivery Ratio for Trust AODV and Trust OLSR.

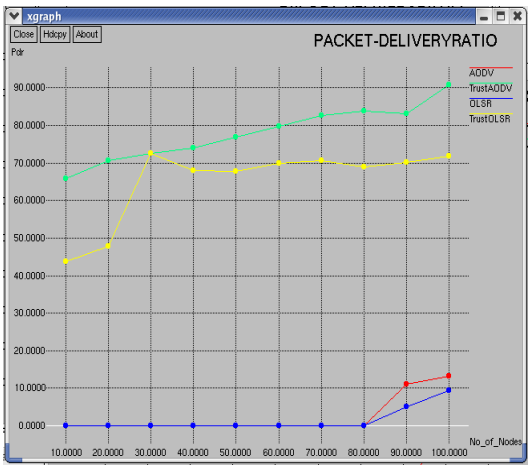

FIGURE. 6. Packet Delivery Ratio for AODV, OLSR, Trust AODV, Trust OLSR.

It is evident from the graph that under black hole attack the above discussed trust framework gives better Packet Delivery Ratio for the trust implemented AODV than the Trust implemented OLSR.

Cite this article as: Gayathri D, Dr. S JanakiRaman. "Comparative Performance analysis of Trust implemented AODV with Trust implemented OLSR under the Blackhole Attack." *International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering (2015)*: 01-06. Print.

XI. CONCLUSION AND FUTURE EXTENSION

On the whole the trust implemented AODV gives better performance than Trust implemented OLSR. This investigation shows the better performance of these trust implemented protocols than their base protocols. This trust implementation can be constructed in other MANET routing protocols as well and can be modified a little to suit Jelly fish Attack.

REFERENCES

[1] S.Corson, J.Marker,"Mobile Ad hoc Networking",RFC-3651.

[2] C.Perkins, E.Royer and S.Das,"Ad hoc On demand DistanceVector

[3] T.Clausen, P.Jacquet, "Optimised Link State Routing protocol (OLSR)", RFC : 3626.

[4] Hoang Lan Nguyen, Uyen Trang Nguyen, "A Study of Different Types of Attacks on MANETs" Elsevier – Ad hoc Networks 6(2008)32-46.

[5] Pradip M.Jawandhiya, Mangesh M.Ghonge, Dr.M.S.Ali, "A Survey of Mobile Ad hoc Network Attacks", International Journal Of Engineering and Technology vol 2(9),2010, 4063-4071.

[6] Monika Roopa K, Prof. BVR Reddy, "Blackhole implementation in AODV Routing Protocol" International Journal of scientific and Engineering Research, vol 4, Issue 5, May-2013 ISSN 2229-5518.

[7] Fan-Hsun tseng, Li-Derchou, han-chieh Chao, "a Survey of blackhole Attacks in wireless mobile ad hoc Networks" Human Centric Computing and Information Sciences, a Springer open journal.

[8] Anuj Gupta, Navjot kaur, Amandeep Kaur, "A Survey on Behaviour of AODV and OLSR routing Protocols of MANETS under Black Hole Attack", International Journal of Computer Science and Technology, vol;2, Issue $, oct.Dec.2011.

[9] Harjeet Kaur, Manju Bala, Varsha Sahni, "Study of Black hole Attack using Different Routing Protocols in MANET", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering , ISSN : 2278-8875, vol 2,Issue-7, July 2013.

[10] Bo Sun, Yong Guan, Jian Chen and Udo W.Pooch, "Detecting Black-hole Attack in Mobile Ad hoc Networks" The Institution o Electrical Engineers, 2003.

[11] XiaoQiLi, Michael R.Lyu, and JiangehuanLiu, "trust Model Based Routing Protocol for Secure Ad hoc Networks", IEEEAC paper# 115

[12] Kamal Deep mekha, Mohit Virendra, Shambhu Upadhaya, "Trust Based Routing Decisions in Mobile Ad hoc Networks"

[13] Mohmood Salehi, Hamed Samvati, "Injection and Evaluation of New Attacks on Ad hoc proactive Routing algorithms", international journal of information Security Research, vol 2, Issue 2, March-june-2012.

[14] Harmandeep Singh, Gurpreet Singh, Manpreet Singh, "Performance Evaluation of Mobile Ad Hoc Network Routing protocols under Black hole Attack", International Journal of Computer applications, 0975-8887, vol.42- No-18, March 2012.

Cite this article as: Gayathri D, Dr. S JanakiRaman. "Comparative Performance analysis of Trust implemented AODV with Trust implemented OLSR under the Blackhole Attack." *International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering (2015)*: 01-06. Print.