COMPARISON OF THE PERFORMANCE OF TRSAODV WITH AODV UNDER BLACKHOLE ATTACK IN MANETS

Gayathri. D[1], S. JanakiRaman[2]

[1]Research Scholar, Bharathiar University, Coimbatore, Tamil Nadu, India.
gayathridhananjayan@gmail.com
[2]Assistant Professor, Department of Banking Technology, Pondicherry University, Pondicherry, India.
jana3376@yahoo.co.in

Abstract

A MANET is a self configuring, decentralized network of mobile nodes with limited energy and bandwidth. They have dynamic topology which means their topology keeps changing. These bring lot of challenges in routing. Since there is no central authority the mobile nodes act both as hosts as well as routers. They provide great comfort due to their portability and ease of installation with no infrastructure but their nature brings in security issues which could not be compromised which paves way for extensive research. They are vulnerable to many attacks and one such attack, Black hole Attack is implanted and a Trust based AODV, TRSAODV has been proposed to overcome the attack and a comparative analysis of proposed TRSAODV with AODV is done in this paper.

KeyWords: *MANET; Blackhole Attack; AODV; Trust; TRSAODV;*

---***---

I. INTRODUCTION

MANETs are Mobile Ad-hoc Networks where the mobile nodes come in to communication without a fixed infrastructure. This indicates they can be formed and resolved at any point of time or at anyplace. This nature makes them ideal for military operations, rescue operations, battle-field area and where ever infrastructure is severely damaged are not present. This decentralized nature paves way for various attacks in MANETs, where valuable information is compromised. The attacks are by malicious nodes or by active nodes which can be categorized in to active attacks or passive attacks. While passive attacks just listen to the channel, active attacks usually take place inside the network. Some common and prevailing active attacks are Rushing attack, Wormhole Attack, Jellyfish Attack, Black hole Attack and Neighbor attack. Black hole attack has been implemented in this simulated MANET and a comparison analysis of proposed Trust based AODV, TRSAODV with AODV is analyzed. This paper gives a overview of AODV protocol and that of a Black hole attack. It then gives the framework of trust implemented in the TRSAODV protocol. Following is the simulation model details and discussion of the result and the future extension of the work.

II. OVERVIEW OF AODV PROTOCOL

AODV is a protocol, finding the route to the destination only on demand. This protocol maintains the routing table in the nodes and not in the packets in order to reduce the memory overhead. AODV makes use of the destination sequence number for the route’s freshness which prevents looping. It goes as follows. If the source node has the route to the destination node then it forwards the packet via that route to the destination. Destination sequence number of the sought route in the recipient node’s routing table greater than the destination sequence number in RREQ packet itself, indicates the route is fresh route. Else the source starts flooding the RREQ packets to its neighbor nodes. The neighbor nodes checks if they are the destination. If they are the destination they forward the RREP packets to the source node else they forward the RREQ packets to their neighbor nodes follow the same procedure. The neighbor nodes on receiving the RREQ packets check if they have route to the destination. If they have they send the RREP message with the route to destination. This is possible because on receiving the RREQ packets they cache route back to the originator of RREQ. The RREP packet is checked for the destination sequence number to be greater than that of the RREQ packet by the sender. If it is, the sender establishes the route to the destination.

Every node on receiving RREP packet also creates a route to the destination in the routing table. Hence, at the time when RREP packet reaches the source node, all the intermediate nodes in the shortest route path will have routes to source as well as destination. AODV uses HELLO messages to ensure its presence to its neighbors periodically. It uses the RRER packets about the link failure.

III. BLACKHOLE ATTACK

Black hole attack is a kind of Active attacks in MANET. In this a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way the attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it.

In AODV Black hole attack the malicious node “X” first finds the route which is active between the source node and the destination node. Then it sends the RREP packet which contains the spoofed destination address including small hop count and large destination sequence number than normal to the node “B” which is the actual destination. Node “Y” forwards this RREP packet from the node “X” to the source node “A”. Now the sender or the source node uses this route to forward the data packet which is caught by the malicious node and dropped. Hence there is no communication of the sender and receiver in the black hole attack.

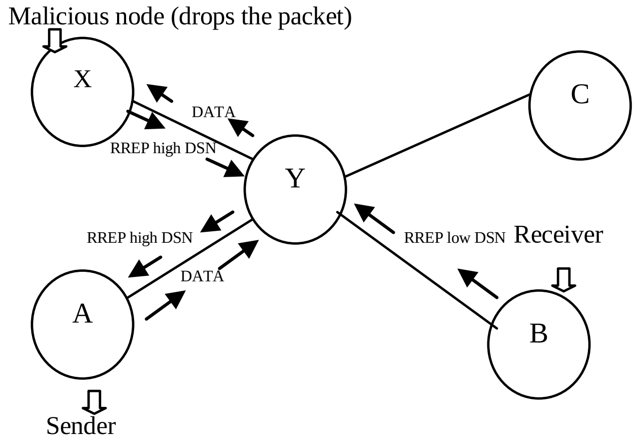

Fig-1: Black Hole Attack

IV. TRSAODV-TRUST IMPLEMENTED AODV

Trust is a metric implemented in AODV in order to enhance the security issues in MANETs. Many research work are being carried out in order to have better performance of MANETs. Here Trust has been quantized and implemented to have better outcome. Trust is the reliability of one node on another. Trust is dynamic, subjective, asymmetric, context dependent, not necessarily transitive. Normal AODV performs well in the absence of any attacks in the network but in presence of Black hole attack its performance decreases drastically and to overcome this Trust is being introduced.

Framework TRSAODV

Trust is a metric implemented in AODV in very simple yet effective way in order to overcome black hole attack. It is done by monitoring the packets forwarded in promiscuous mode. The detection is done by buffer of packets stored that have been recently sent for forwarding. A cyclic buffer is used for the packets storage. Two circular buffers have been used one to store the general packets forwarded and another to store the packets that are promiscuous watched. When the packets delayed for forwarding or if they have not been forwarded for a very long time the last element is erased thus decreasing the trust value of that node which is expected to actually forward the packet. If the packet has been successfully forwarded that packet is removed from the buffer, increasing the trust value of the node.

The promiscuous monitoring is implemented using tap function as follows:
Void TRSAODV : : tap (const packet *p)
The value is initialized to be zero. Then it is incremented that are detected to forward packets and are decremented for nodes that do not forward packets. Hence the route with node’s trust value which is higher is taken for routing and the malicious node whose trust value falls down is blacklisted and avoiding them in packet forwarding.

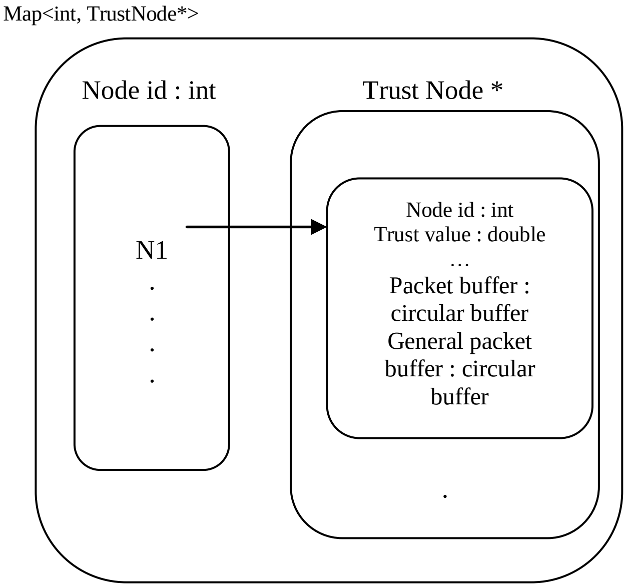

Fig-2: Trust Map

V. SIMULATION RESULT AND ANALYSIS

Under the Linux system in a virtual machine, NS2 has been used to simulate the network environment carried on a analysis of TRSAODV protocol and AODV. The examined protocols are TRSAODV and AODV with black hole implemented. The number nodes were from ten to hundred and the number of black hole attackers were varied from one to five. The traffic type is constant bit rate (CBR) ,transmission range of 250 meters with the MAC layer 802_11 implemented. The simulation time has been set to 100 seconds with area of 1500 * 1000. Here the packet delivery ratio and throughput are the metrics considered for the performance analysis of TRSAODV and AODV.

Table-1: Simulation Parameter Values

PARAMETER	VALUES
EXAMINED PROTOCOLS	AODV, TRSAODV
TRAFFICTYPE	CONSTANT BIT RATE (UDP)
PACKET SIZE	1000 BYTES
SPEED	5M/S
SIMULATION TIME	100S
AREA	1500 * 1000
PROPAGATION	TWO RAY GROUND
MAC LAYER	802_11
ANTENNA	OMNI ANTENNA

The investigation had been carried out considering throughput and packet delivery ratio with varying number of nodes where the number of attackers is kept constant and with varying number of attackers where number of nodes is kept constant.

A. Packet Delivery Ratio

Packet Delivery Ratio is the ratio of data packets delivered to the destination to those generated by the source. In the first scenario of varying number of attackers the Packet Delivery Ratio of both AODV and TRSAODV tend to decrease gradually. However, the TRSAODV's Packet Delivery Ratio remains considerably higher than that of the AODV where it becomes negligible for higher number of attackers.

In the case of varying number of nodes the Packet Delivery Ratio of TRSAODV increases gradually and remarkably but for the AODV the increase is negligible and for more dense network there is a raise in the Packet Delivery Ratio which speaks about the fairness of TRSAODV.

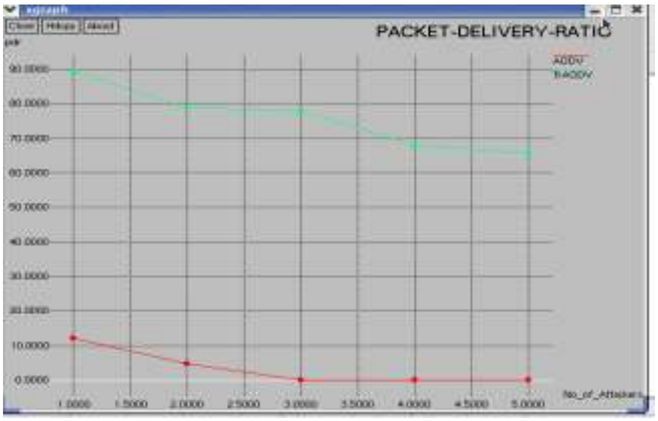

Fig-3: Packet Delivery Ratio versus Number of Attackers

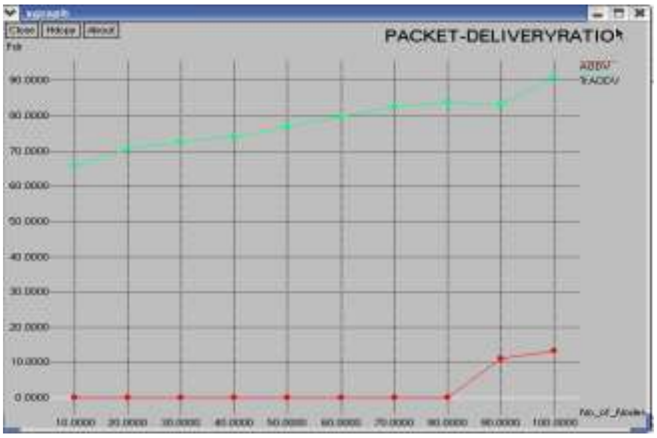

Fig-4: Packet Delivery Ratio versus Number of Nodes

B. Throughput

Throughput is the number of bytes received successfully. In case of varying number of attackers the dip is very drastic for AODV and becomes negligible for higher number of attackers but stands remarkably high for TRSAODV and manages even with higher number of attackers.

In case of varying number of nodes the TRSAODV keeps its efficiency increasing with higher number of nodes where as the AODV is able to deliver a small amount only when the node density is high.

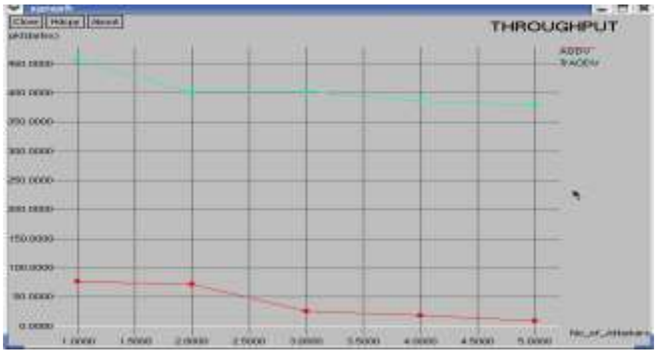

Fig- 5: Throughput versus Number of Attackers

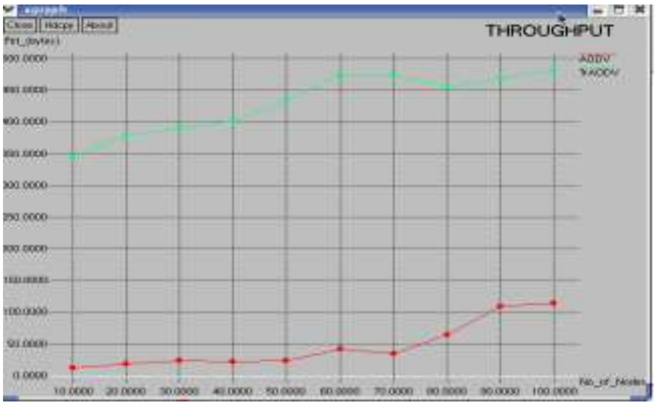

Fig- 6: Throughput versus Number of Nodes

The above investigation clearly states the remarkable fairness of TRSAODV for MANETs over AODV.

V. CONCLUSION AND FUTURE EXTENSION

Securing MANETs from vulnerable attacks is one of the most challenging area of research. This research paper has given a fair solution TRSAODV to overcome Black Hole attack in AODV. In addition to the Trust factor cryptographic measures, energy efficient strategy can be combined to give a more robust protocol. Moreover the type of attack implemented is Black hole where this can substituted with other active attacks for investigation.

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 Routing",RFC-3651.

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

[4] Mohammed AL-shurman and Seong_Moo yoo, "Blachhole Attack in Mobile Ad Hoc Networks" ACMSE'04, April2-3,2004.

[5] 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.

[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] P.Manikam, T.GuruBaskar, M.Girija, Dr.D.Manimegalai, “Performance Comparisons of Routing Protocols in MANETs” International Journal of wireless and Mobile networks (IJWMN) vol.3, No.1, February 2011.

[8] Xing, F., wang, w., “Understanding Dynamic Denial of Service Attacks in Mobile Ad hoc networks” in IEEE MilitaryCommunication Conference,MICCOM (2006).

[9] Dr.Aditya Goel, Ajaii Sharma, “Performance Analysis of MANET using AODV protocol” international Journal of Computer Science and Security (IJCSS), volume 3: Issue 5.

[10] Kamarularifin abd.Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan, “Mitigation of Blackhole Attacks for AODV Routing Protocol” International Journal of New Computer Architecture and their Applications. (IJNCAA)ISSN :2220-9085.

[11] Mangesh Ghonge, Prof.S.u.Nimbhorkar, “Simulation of AODV under Blackholen Attack in MANETs” International Journal of Advanced Computer science and Engineering ,ISSN : 2277-1287.

[12] XiaoQiLi, Michael R.Lyu, and JiangehuanLiu, “trust Model Based Routing Protocol for Secure Ad hoc Networks”, IEEEAC paper# 1150.

[13] R.S.Mangrulkar, Pallavi V Chavan, S.N.Dagalkar, “Improving Routing Selection Mechanism Using Trust Factor in AODV Routing Protocol for MANET” International Journal opf Computer Applications (0975-8887) Vol:7-No.10, October 2010.

[14] Dalip Kamboj and Pankaj Kumar Sehgal, “A Comparative Study of various Secure Routing protocol based on AODV” International journal of Advanced Computer Science and Applications, vol.2, no.7, 2011, pp 80-85.