ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Detection and Prevention of Black Hole Attack Using Trust Mechanism with various Node Density

Hitesh Nagdev[1], Mayur Rathi[2]

Research Scholar, Department of CSE, LNCTS (RIT), Indore, MP, India[1]

Assistant Professor, Department of CSE, LNCTS (RIT), Indore, MP, India[2]

ABSTRACT: Mobile Ad Hoc Networks (MANETs) are a popular form of network for data transfer due to the fact that they are dynamic, require no fixed infrastructure, and are scalable. However, MANETs are particularly susceptible to several different types of widely perpetrated cyber attack. One of the most prevailing hacks aimed at MANETs is the Black Hole attack, in which particular node within the network displays itself as having the shortest path for the node whose packets it wants to intercept. Once the packets are drawn to the Black Hole, they are dropped rather than relayed, and the communication of the MANET is thereby disrupted, without knowledge of the other nodes in the network. Due to the sophistication of the Black Hole attack, there has been a lot of research conducted on how to detect it and prevent it. In this paper format title provide their research results on providing an effective solution to Black Hole attacks, including introduction of new MANET routing protocols that can be implemented in order to improve detection accuracy and network parameters such as packet delivery ratio, end-to-end delay and throughput.

KEYWORDS:- MANET, Black hole, Routing Protocol and Secure Routing.

I. INTRODUCTION

A MANET [1], [2] is a multi-hop temporary communication network of mobile nodes equipped with wireless transmitters and receivers without the aid of any current network infrastructure. A MANET is an emerging research area with practical applications. However, A MANET is particularly vulnerable due to its fundamental characteristics [3], [4], such as open medium, dynamic topology, distributed cooperation, and constrained capability. Routing plays an important role in the security of the entire network. Thus operations in MANETs introduce some new security problems in addition to the ones already present in fixed networks. The nodes communicate by sending packets to other nodes in its radio range. The ad hoc network is characterized by a number of attributes like self organization, self-configuration, dynamic topology, restricted power, temporary network, lack of infrastructure, etc. These attributes make the ad hoc network applied in various areas, such as disaster recovery operations, smart building, military operations etc. Application fields like military operations are sensitive and prone to security attacks.

II. AODV ROUTING PROTOCOL

In proactive and reactive routing protocol, there must be good co-operation among the nodes so that the data can be routed successfully from source to destination. If nodes have good co-operation between them then there will be no packets dropping or modification in the content. If there is no co-operation between the nodes, then there are high possibilities that an attacker take the advantage of situation and perform the malicious function. AODV routing protocol provides such situation when source node want to send the message to destination node which is not directly in contact with the source node then a route discovery process is initiated by broadcasting the RREQ message in the network. Now malicious node will take the advantage of this RREQ message and immediately send the RREP message to source node of having the route to the destination node without checking its routing table. This RREP message has

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

the large sequence number and minimal hop count. When source node starts transmitting the data, the malicious nose will drop the packet rather than forwarding it to the destination node.

III. BLACK HOLE ATTACK

In a Black hole attack, a node which is called malicious node will absorb all the network traffic towards them and discard all the packet. If we want to catch the black hole attack, when malicious node checking its routing table it directly send a fake RREP with largest sequence number and smallest hop count to prove that it has the minimum path to reach the destination. By this way we can catch the black hole node in the network. Source node gets the more than one RREP from the different node but it is choose the RREP from the malicious node because that has a largest sequence number. The source node ignores the RREP which are not coming from the malicious node and then malicious node drops all the packets rather better to forward further to the destination node. [4]

The malicious node takes all the route towards them and attack all the RREQ packet. Malicious node generates the fake RREP and that will be delivered to the source node that it does know the path for destination. By this way source node assumes that it is the next node to reach the destination so it will send the packet to the malicious node and malicious node will be remove all the packets which are comes from the source node. [11]

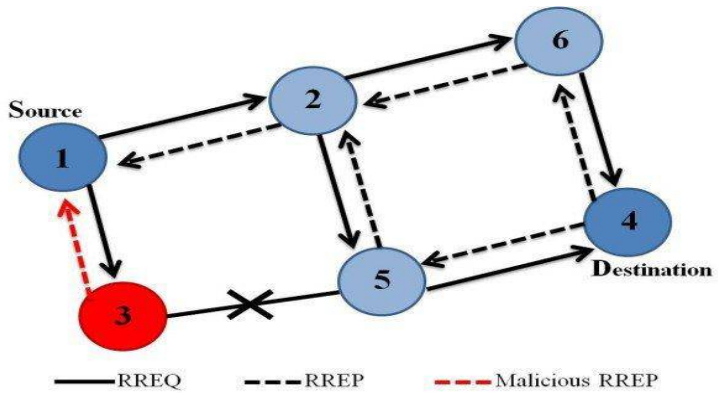

Figure:-1 Black Hole attack

Single black hole attack and Collaborative black hole attack are two types for the black hole attack. [8] In the network if all the network traffic is switched to single node, it is called single black hole attack which is malicious node and it will drops all the packets. In collaborative black hole attack, there are many malicious nodes which are work together to switch normal routing information towards the malicious node and assemble that route according to them. Some researchers had work on black hole attack and provide methods to detect malicious nodes but that is not sufficient to solve the black hole problem and the more detection method should be initiated to solve the black hole attack. [5]

IV. PROBLEM DOMAIN

In black hole attack, a node uses its routing protocol in order to broadcast 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 attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

V. IMPLEMENTATION

This work implemented i.e. Creation of MANET Scenario in NS-2 and then to analyze AODV routing protocols with malicious node and detect using trust based algorithm on the basis of various performance matrices Like Packet Delivery Ratio, End to End delay and Overall Throughput. In this work firstly created scenario file for IEEE 802.11 standard which has to be used along with TCL Script than created a TCL script consist of various routing protocols in our case these are AODV, Black Hole AODV & Secure AODV than a particular MANET scenario which consist of various node density based scenarios for static nodes work with two ray ground model. Implementation consists of typical installation process of ns-2 complexity of topography creation 2000*2000 meter area.

Table1:- Simulation scenario

Simulation TOOL	Network Simulator-2.35
IEEE Scenario	MANET(802.11)
Mobility Model	Two Ray Ground
No. Of Nodes	25, 50, 70, 90, 120, 170, 200
Node Movement speed	static
Traffic Type	CBR
Antenna	Omni Directional Antenna
MAC Layer	IEEE 802.11
Routing Protocols	AODV, BAODV, SAODV
Queue Limit	50 packets
Simulation Area(in meter)	2000*2000
Queue type	Droptail
Channel	Wireless Channel
Simulation Time	100 sec.

VI. PERFORMANCE METRICS

The following metrics are used in this work for the detection and prevention of the node replication attack with AODV routing protocol.

a. Packet Delivery Ratio

This is the fraction of the data packets received by the destination to those sent by the source. This classifies the ability of the protocol to discover routes.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

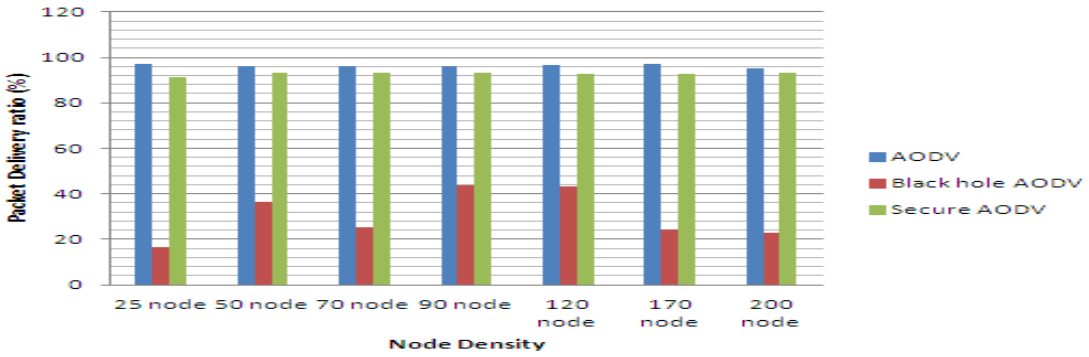

Figure:-2 Packet Delivery Ratio under AODV, RAODV and SAODV

b. End to End Delay

This is the average delay between the sending of the data packet by the source and its receipt at the corresponding receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes.

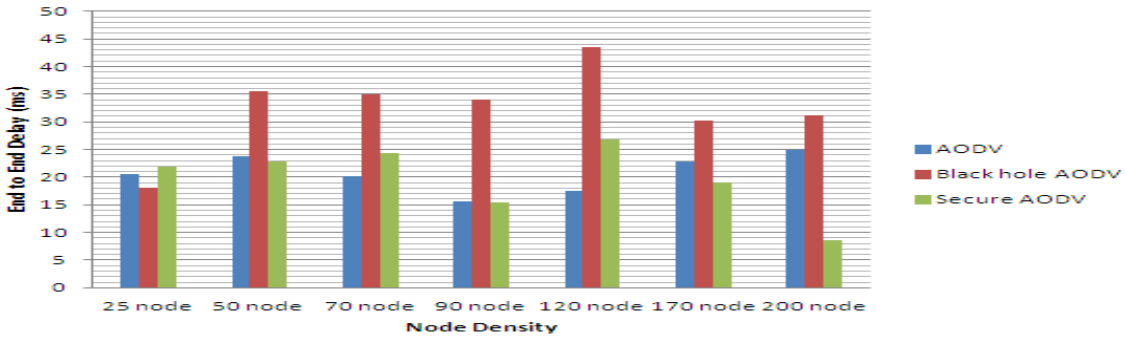

Figure:-3 End to End Delay under AODV, RAODV and SAODV

c. Throughput

It is the rate at which the packet delivered successfully, measured in Kbps.

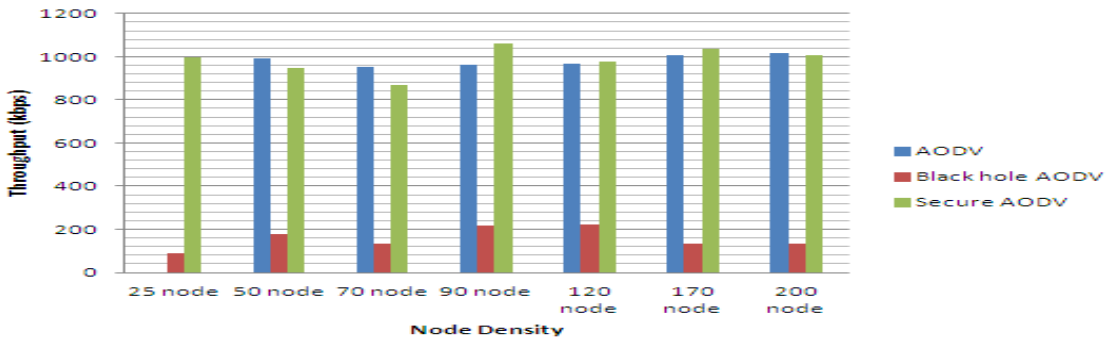

Figure:-4 Throughput under AODV, RAODV and SAODV

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

VII. CONCLUSION

This work carried out the detailed analysis of Black Hole attack prevention and its detection through the trust mechanism with AODV routing protocol which is simulated by NS-2 for MANET on the basis of different performance metrics viz. packet delivery ratio, end to end delay and average throughput. These performance metrics are analyzed for the AODV, Black Hole AODV and Secure AODV routing protocols by varying the node density for fixed network. Simulation of routing protocols provides the facility to select a good environment for routing and gives the knowledge how to use routing schemes in attack network. Simulation results show that, as the density of nodes increases in the network, the performance of the routing protocols decreases. Attacker nodes affect the performance of routing protocols most as path break increases. According to simulation results as the Black Hole AODV prevent through the Secure AODV, the packet delivery ratio, Throughput and End to End delay of routing protocol increases as compare to the detection of Black Hole AODV through the Secure AODV.

REFRENCES

[1] D.B.Roy, R.Chaki and N.Chaki, "A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Neworks," International Journal of Network Security and Its Application (IJNSA), Vol. 1, No.1, April, 2009.
[2] N.Shanti, Lganesan and K.Ramar, "Study of Different Attacks On Multicast Mobile Ad-Hoc Network".
[3] C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks," Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.
[4] S.Marti, T.J.Giuli, K.Lai, M.Baker, "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks".
[5] Zhu, C. Lee, M.J.Saadawi, T., "RTT-Based Optimal Waiting time for Best Route Selection in Ad-Hoc Routing Protocols," IEEE Military Communications Conference, Vol. 2, pp. 1054-1059, Oct, 2003.
[6] M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, "A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks," Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.
[7] V.Mahajan, M.Natue and A.Sethi, " Analysis of Wormhole Intrusion attacks in MANETs," IEEE Military Communications Conference, pp. 1-7, Nov, 2008.
[8] F.Stanjano, R.Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing," Vol. 35, pp. 22-26, Apr, 2002.
[9] H.L.Nguyen,U.T.Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad-Hoc Networks," International Conference on Networking, Systems, Mobile Communications and Learning Technologies, Apr,2006.
[10] H.Deng, W.Li and D.P.Agrawal, "Routing Security in Wireless Ad-Hoc Networks," University of Cincinnati, IEEE Communication Magzine, Oct, 2002.
[11] Hongmei Deng, Wei Li, and Dharma P.Agarwal. Routing Security in Wireless Ad Hoc network. IEEE Communication Magzine, vol 40, no.10, October 2002.
[12] Marti S, Giuli TJ,Lai K, Baker M. Mitigating routing misbehavior in mobile ad hoc networks. International conference on mobile computing and networking, August 2000. Pp 255-265
[13] Semih Dokurer, Y.M. Erten, Can Erkin. Performance analysis of ad hoc networks under black hole attacks. IEEE Conference,pp 148-153 March 2007.
[14] Buchegger S,Boudec Le J. Performance analysis of the CONFIDANT protocol, in dynamic ad-hoc networks. ACM International symposium on mobile ad hoc networking and computing (MobiHoc'02); June 2002.pp.202 236.
[15] Ming- Yang Su, Kun- Lin Chiang, Wei Cheng Liao. Mitigation of Black Hole Nodes in Mobile Ad Hoc network. Parallel and Distributed Processing with Applications (ISPA) pp.162-167, September 2010.
[16] Venkat Balakrishnan, Vijay Varadharajan, Phillip Lues, Udaya Kiran Tupakula. Trust Enhanced Secure Mobile Ad-hoc Network Routing. 21st IEEE International Conference on AINA W 2007, Niagara Falls, Canada, pp. 27 33, May 2007.
[17] Alem, Y.F.; Zhao Cheng Xuan.Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection. Future Computer and Communication (ICFCC), 2010 2nd International Conference on , vol.3, no., pp.V3-672-V3-676,
21-24 May 2010.
[18] Medadian, M., Mebadi, A., Shahri, E. Combat with Black Hole attack in AODV routing protocol. Communications (MICC), 2009 IEEE 9th Malaysia International Conference on, vol., no., pp.530-535, 15-17, Dec.2009.
[19] Lalit Himral, Vishal Vig, Nagesh Chand. Preventing AODV Routing Protocol from Black Hole Attack. International Journal of Engineering Science and Technology (IJEST) Vol. 3 No. 5 May 2011.
[20] Michiardi, P. and Molva, R. Core. A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc Networks. In Proceeding of IFIP TC6/TC I I Sixth Joint Working Conference on Communication and Multimedia Security, 2002, 107-121.