ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

Prevention of BLACK HOLE attack in MANET Using Indexing Algorithm

Monika Shivhare[1], Prof. Praveen Kumar Gautam[2]
M.Tech Student[1], Assistant Professor[2]
Department of Computer Science and Engineering
Sagar Institute of Research & Technology, Indore, India

Abstract:
MANET (Mobile Ad Hoc Network) could be a collection of self configurable mobile nodes wherever every node acts as a router for different nodes, which permits knowledge to travel, utilizing multi-hop network paths. MANETs are vulnerable to various attacks in the least layers, because the design of most MANET routing protocols assumes as if there is no malicious intruder node within the network. The main aim of this work is to develop index based on-demand routing protocols for knowledge transmission below black hole attack in MANET. The proposed protocols should be efficient in terms of Packet Delivery ratio, Residual Energy and Throughput. Based on the motivations to produce new security measures to be incorporated in popular routing protocols AODV, the aim has been implement modified on-demand routing (MAODV) protocols for data transmission in MANET. Detect black hole node in MANET scenario using MAODV protocol. Prevent the network from black hole attack and improve the packet delivery fraction, throughput and Residual Energy even with the presence of black hole attacks. The results of both AODV and MAODV compare to analyze that of those 2 types of protocols provides higher performance.

Keywords: Mobile ad hoc network, NS-2.35, black hole attack, AODV and MAODV routing protocol

I. INTRODUCTION

A wireless ad-hoc network consists of a collection of mobile nodes in which nodes are communicating with each other without help from a fixed infrastructure. Routers and hosts are used to form wireless networks. A wireless ad hoc network is a decentralized type of wireless network. A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. Mobile hosts are used to form mobile ad hoc network. There is no fixed infrastructure or base station for communication in MANET. Two nodes can communicate with each other when they are within the transmission range but need cooperation of intermediate nodes by forwarding packets when they are multi hop away from each other [1]. In MANET each mobile node acts as a host when requesting/providing information from/to other nodes in the network, and acts as router when discovering and maintaining routes for other nodes in the network [2]. Routing protocols in ad hoc wireless networks can be classified into three broad categories. This classification is based on the routing information update mechanism. They are Proactive (or table-driven) protocols, Reactive (or on-demand) protocols, and Hybrid routing protocols [3]. These are further divided into sub categories. Routing protocols are vulnerable to routing attacks [3]. There are various routing attacks in ad hoc wireless networks like Attacks using Impersonation, Modification, Fabrication, Replay, and Denial of Service (DoS). In this paper, we focus on black hole attack that belongs to category of fabrication attacks. There are three main routing protocols proposed for MANET [4]: Ad hoc Ondemand Distance Vector (AODV) routing, Dynamic Source Routing (DSR), and Destination Sequence Distance Vector (DSDV) routing protocols. AODV and DSR belong to ondemand routing protocols and DSDV is a table-driven routing protocol. These protocols are vulnerable to different security attacks. In this paper, we use AODV routing protocol because the AODV protocol is vulnerable to the black hole attack. So we have simulated the behaviour of black hole attack on AODV in MANET.

II. AODV ROUTING PROTOCOL

Ad-Hoc On-Demand Distance Vector [5] (AODV) is a reactive routing protocol in which the network generates routes at the start of communication. As in [7] The Ad Hoc On-Demand Distance Vector (AODV) routing protocol described in builds on the DSDV algorithm. AODV is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on a 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, since nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges [7]. AODV builds routes using a route request / route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware.

A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it. As the RREP propagates back to the source, nodes set up forward

pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing Information for that destination and begin using the better route. As long as the route remains active, it will continue to be maintained. If a link break occurs while the route is Active, the node upstream of the break propagates a route the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery.

As a result, all the packets through the malicious node are simply consumed or lost. The malicious node can be said to form a black hole within the network, and that we call this the black hole problem. During this way the malicious node will simply misroute lots of network traffic to itself, and will cause an attack to the network with very little efforts on its part.

III. PROPOSED ALGORITHM

The proposed algorithm is based on the index values of individual nodes. All the nodes of wireless ad-hoc network have zero index value. The algorithm encompasses the following steps:

[A] Initialization:

1. Index values of all the participating nodes are initializing with zero.
2. Initialize the threshold value of the index value with 100.
3. Assumption: 1 index value = 10 packets dropped.

[B] Updating of index values:

1. If the packets are correctly transmitted from one node to another node:

(a) If the correctly transmitted no of packets is between 1 to 10, then index values of the respective nodes will be incremented by one time.

Updated index value = old index value + 0.528779;

(b) If the correctly transmitted number of packets is greater than 10, then the updated index value will be:

Updated index value = old index value + (correctly transmitted packets / 10);

2. If the packets are dropped/delayed :

(a) The number of dropped or delayed packets is between 1 to 10, and then index value of that particular node is decremented by one.

Updated index value = old index value – 0.528779;

(b) The number of dropped or delayed packets are greater than 10, then index value of that particular node will be,

Updated index value = old index value – (Packet dropped or delayed / 10);

3. If the index value of particular node is negative, then print "Invalid node".

[C] Isolating the Packet drop node from the network:

1. If (Updated index value <<< Threshold index value) Then the particular node is treated as malicious node (Black hole node)
2. If (Updated index value > Threshold index value) Then the particular node is treated as legitimate node.
3. Stop comparing the index values of nodes with threshold value.

IV. IMPLEMENTATION AND RESULT ANALYSIS

1. SIMULATION RESULTS FOR 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. Figure and table shows the Packet delivery ratio under Black hole attack detection and its prevention through Indexing Value Algorithm i.e. Attack, pre (prevent) and without attack for the various node density.

$$\text{Packet Delivery Fraction} = \frac{\text{Total No. of Packet Receive}}{\text{Total No.Packet Send}}$$

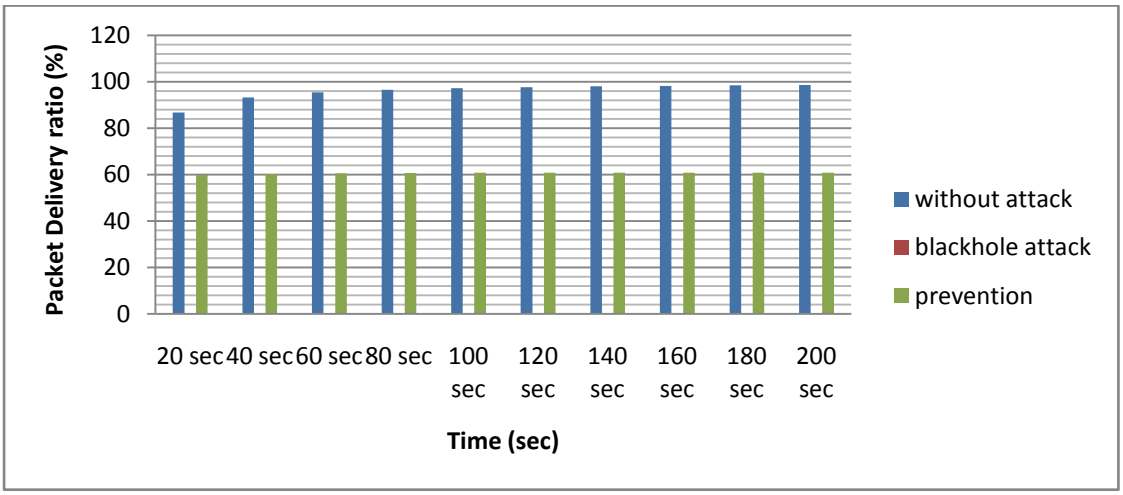

Figure: 1 Packet Delivery Ratios comparisons

2. SIMULATION RESULTS FOR THROUGHPUT

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. Figure and table shows the Throughput under black hole attack detection and its prevention through Trust based mechanism i.e. Attack, pre and without attack for the various node density.

$$\text{Throughput} = \frac{\text{Total No. of Successfully Received Packet}}{\text{Total Simulation Time}}$$

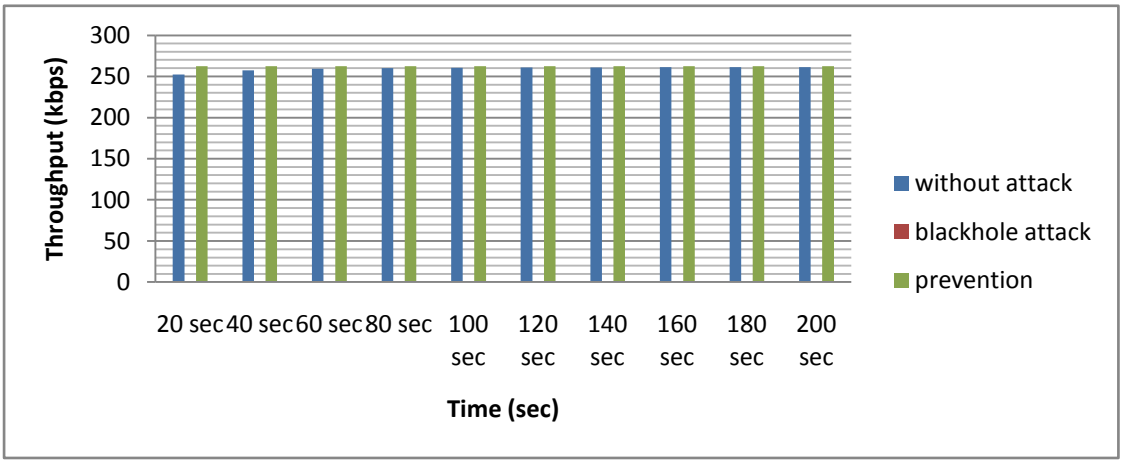

Figure: 2 Throughputs comparisons

3 SIMULATION RESULTS FOR RESIDUAL ENERGY

It is the total amount of remaining energy by the nodes after the completion of Communication or simulation. If a node is having 100% energy initially and having 70% energy after the simulation than the energy consumption by that node is 30%.The unit of it will be in Joules. Figure and table shows the Residual Energy under Black hole attack detection and its prevention through Trust based mechanism i.e. Attack, pre and without attack for the various node density.

$$\text{Residual Energy} = \text{Total Energy} - \text{Consume Energy}$$

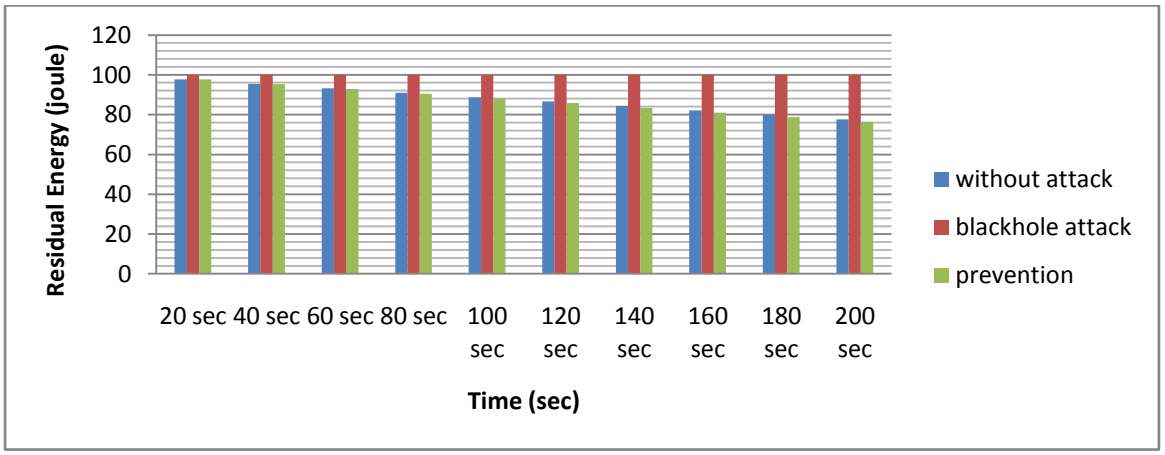

Figure: 4 Residual Energy comparisons

V. CONCLUSION AND FUTURE WORK

MANET has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. Security of MANET is one of the important features for its deployment, the detection and prevention of black hole attack in the network exists as a challenging task. In this work analyzed the effect of black hole attack in the performance of AODV protocol and prevent the network from black hole attack using MAODV protocol. The simulation has been done using the network simulator (NS-2.35). The performance metrics like packet delivery ratio, energy and throughput has been measured and analyzed with the variable time of simulation. From the simulation results it is clear that when the black hole node exists in the network, it can be affected and decreased the performance of AODV routing protocol.

As future work, research work intend to develop simulations to analyze the performance of the proposed solution based on the various security parameters like mean delay time, packet overhead ,memory, mobility, increasing number of malicious node, increasing number of nodes and also focusing on resolving the problem of multiple attacks against AODV.

REFERENCES

[1] Prachi Lodhi**,** Prof. Kamlesh Chopra "Implementation Paper on Detection and Prevention for Black Hole attack in Adhoc Network"Cognitive Technical Research Journal.

[2]Hizbullah Khattak and Nizamuddin, Fahad Khurshid," Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash" 2013 IEEE.

[3]Seryvuth Tan, Keecheon Kim," Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs" in 7/2013 IEEE.

[4]Ms Monika Y. Dangore and Mr Santosh S. Sambare," Detecting And Overcoming Blackhole Attack In manet" 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies

[5]Ketan S. Chavda and Ashish V.Nimava," REMOVAL OF BLACK HOLE ATTACK IN AODV ROUTING PROTOCOL OF MANET" 4th ICCCNT – 2013 July 4 -6, 2013, Tiruchengode, India

[6]jalpa khamar and avani Dadhania "An Performance Enhancement of AODV Routing Protocol in Manets"in IJAERD volume 1,Issue 6,june e-ISSN: 2348

[7] Madhusudhananagakumar KS , and G. Aghila, "A Survey on Black Hole Attacks on AODV Protocol in MANET" , International Journal of Computer Applications (0975 – 8887) Volume 34– No.7, November 2011

[8]Jayraj Singh, Arunesh Singh, and Raj Shree, "An Assessment of Frequently Adopted Unsecure Patterns in Mobile Ad hoc Network: Requirement and Security Management Perspective", International Journal of Computer Applications (0975 – 8887) Volume 24– No.9, June 2011

[9] S. Kannan, T. Kalaikumaran, S. Karthik and V. P. Arunachalam, "A Review on Attack Prevention Methods in MANET", Journal of Modern Mathematics and Statistics 5(1) : 37-42, 2011

[10] Vishnu K, and Amos J .Paul," Detection & Removal of cooperative Black/Gray hole attack in Mobile ADHOC Networks", International Journal of Computer Applications 2010, Volume 1-No.22, pp.38-42.

[11] Nital Mistry, Devesh C Jinwala, Member, IAENG, and Mukesh Zaveri, "Improving AODV Protocol against Black hole Attacks", IMECS2010

[12] Payal N. Raj and Prashant B. Swadas,"DPRAODV: A dynamic learning system against black hole attack in AODV based Manet", International

[13] Journal of Computer Science Issues (IJCSI), Vol. 2, Issue 3, pp: 54-59, 2009 D.M. Shila, and T. Anjali, "Defending selective forwarding attacks in WMNs", IEEE International Conference on Electro/Information Technology, 2008, 96-101.

[14] Tamilselvan L, and Sankaranarayanan V, "Prevention of Black hole Attack in MANET", Paper presented at the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August 2007.

[15] X.P. Gao; and W. Chen, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks[C]", IFIP International Conference on Network and Parallel Computing Workshops, 2007, 209-214.

[16] Jung-Shian Li and Cheng-Ta Lee "Improve routing trust with promiscuous listening routing security algorithm in mobile ad hoc networks", Elsevier Computer Communications 29 (2006) 1121–1132. Available at science direct.

[17] A J. P. Vilela and J. Barros,"A Cooperative Security Scheme for Optimized Link State Routing in Mobile Ad-hoc Networks", Proc. Of the 15th IST Mobile and Wireless Communications Summit, Mykonos, Greece, June 2006.

[18] Bo-Cang Peng and Chiu-Kuo Liang"Prevention techniques for flooding attack in Ad Hoc Networks", IEEE , 2006

[19] M. UmaparvathiDharmishtan K. Varughese "Two Tier Secure AODV against Black Hole Attack in MANETs" European Journal of Scientific Research.

[20] Sanjay Ramaswamy, Huirong Fu, ManoharSreekantaradhya, John Dixon and Kendall Nygard "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks".

[21] Fan-Hsun Tseng1, Li-Der Chou1and Han-Chieh Chao2,3,4" A survey of black hole attacks in wireless mobilead hoc networks".

[22] NishantSitapara ,Prof. Sandeep B. Vanjale"Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks".

[23] Prachi Lodhi, Prof. Kamlesh Chopra "Implementation Paper on Detection and Prevention for Black Hole attack in Adhoc Network"