Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 9, September -2017

Improved Technique for Prevention of Black Hole Attack in Mobile Ad Hoc Network

Arti Yadav (Research Scholar)
Department of Computer Science & Engineering
Maharana Pratap College of Technology
Gwalior, India

Krishna Kumar Joshi (H.O.D)
Department of Computer Science & Engineering
Maharana Pratap College of Technology
Gwalior, India

Abstract— *Today's Mobile Ad hoc Networks known to be (MANETs) become well-liked issue intended for scientists, and different studies have been ready to raise presentation of ad hoc networks. In the MANET nodes is compromise to promote packets for every other communicate further than to their range of transmission. The mobile node are communicating through each other devoid of some type of infrastructure. One of such attack is known Wormhole Attack with the reason of 2 adversary node work mutually to transmit packets in absent of band channel. In this propose paper we create wormhole attack on DSR (dynamic source routing) protocol, and for avoidance and detection we initially calculate the distance of each node and then apply multipath for sending data for destination. Sender wait receiving acknowledge of packet on basis of distance if it not get acknowledge on calculated distance or RTT time then it send data to next path if same thing happen again it send packet to neighbor to bring up to date the distance table again with add the information of previous paths, so that every node check those paths and their neighbors also if there is any problem take place it create boundary for those non malicious nodes and make these node id as malicious.*

Keywords— *Mobile Ad Hoc Network, RREQ, Black Hole Attack, RREP, RTT, Malicious Node.*

I. INTRODUCTION

MANET is wirelessly and an independent system that means it's not recur communications. The wireless network is not used physically wired. Nodes implement dynamically or the randomly into the ad-hoc network in the MANET. The random nature of MNAET create it further exposed [1]. In MANET such a lot of class of attacks e.g. collaborative black hole and the black hole attack. Black hole attack is kind of active attacks and the use of such malicious node which accept to all the data packets in the ad-hoc network. In this way, the beneficial each packets inside the ad-hoc network are dropped. When a set of black hole nodes and no longer create utilize of a difficulty hired at the issue of routing in MANET. This kind of attack is figuring out collaborative black hole attack. Due to immoderate mobility of approach routing is large dispute in ad-hoc network. The routing protocol is identified and transmit packet from sender node to receiver node. This routing protocol is the usage of most effective sequence number. In define work, belief depend on routing protocol is being defined in which faith computation is made using tangent type of hyperbolic function that calculate trust value of their nearby nodes promiscuously [2, 3].

Fig.1 MANET architecture

II. COOPERATIVE BLACK HOLE ATTACK

In AODV protocol, dispatcher node which is S have need of to communicate by means of recipient node which is D, after that sender node S broadcasts route request which is (RREQ) packet to their adjacent active nodes and up to date their routing table with an entry for the source node S, and check if It's the receiver node or has a generally update path to receiver node. If doesn't contain, then middle node that updates the RREQ and passes RREQ to receiver node D until it discover their recipient or any further middle node that has a novel sufficient route to D, as described by example in Figure 2. The receiver node D or the middle node with enough newest route to D, initiates a route reply (RREP) in the opposite path, as described in Figure 3. The sender node S initial transmit the data packets to their adjacent node that reply first, and rejects the other replies.

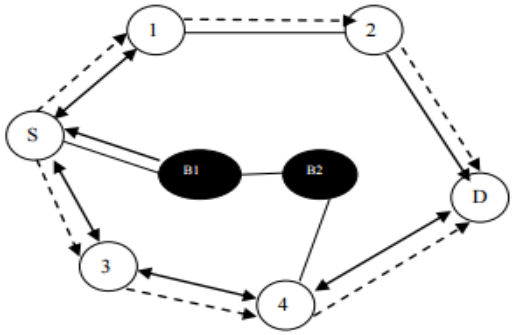

Fig.2 Flooding of RREQ

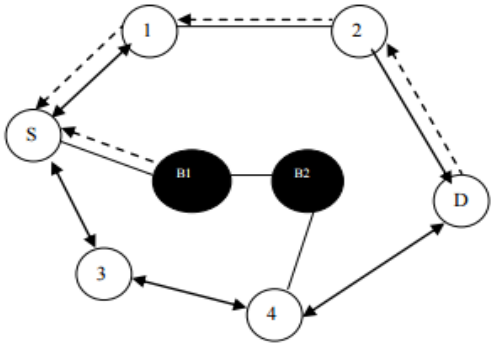

Fig.3 Propagation of RREP

Various writers have define an algorithm and techniques to distinguish and eliminate a single black hole node. Nevertheless, In case of several type of black hole nodes meantime in coordination hasn't been addressed. For instance, while black hole nodes are performing in coordination with each dissimilar, the primary black hole node B1 mentions to one of its associative black hole B2 as the further hop, as described in the figure 3. According to the sender node S transmit a "Further Request (FRq)" to B2 by a distinct path (S-3-4-B2) apart from thru B1. Node S requests the B2 if it have a path to node named B1 and a path to recipient node which is D. as B2 is cooperate with B1, its "Further Reply (FRp)" might be "OK" to each and every one enquiries. Now as according to the rationale advised, node S begins passing the records packets supposing that the direction S-B1- B2 is at ease. Nevertheless, in truth, the packets are consumed through node B1 and the security of the network is conceded [4].

III. LITERATURE SURVEY

Sathish M, et al. [2016] this paper defines a original method to reduce single and the collaborative black hole attack, through decreasing routing, the storage and computational overhead. The method incorporates false route request, receiver's sequence no. and subsequently next hop information to get better the limits of presented schemes. AODV routing is considerably conventional routing protocol for the MANET. The inadequacy of security problem within the AODV layout creates it susceptible to black hole attack. Malicious nodes type of trap data packets and the drop them as a replacement for of furthering in a black hole attack. Among prevailing black hole discovery schemes, merely a few techniques manage mutually single and joint attack and that too with a lot routing, computational overhead and storage. [5].

Emimajuliet. P et al. [2016] This paper define a approach known Modified Cooperative Bait Detection Scheme. It's more appropriate for defending against collaborative attacks. CBDS along with DSDV Protocol performs better than the DSR and 2ACK scheme. MANET is the greatest needed device that is still under research. The wired networks cannot be used

during any emergency situation like natural disasters hence the need of wirelessly device is increased. MANET make the easier communication for the duration of emergency situation. Due to features of the MANET e.g. infrastructure less and dynamic topology, it's simply to deploy whenever and wherever needed. Such features make it more suitable for many applications. However the flexibility of these characteristic creates the security threats. The nodes within the network may be without problems attacked through means of collaborative attacks comprising gray hole attack, jellyfish attack and black hole attack. These are the most hazardous attacks which drops the packet without transmitting. Hence a secure mechanism is needed [6].

P.S.Hiremath, et al. [2016] this paper, A exceptional approach that prevents and detects helpful black hole attack on the MANETs is superior. The designed way is being based on adaptive fuzzy inference kind of scheme for MANET to notice and keep away from the supportive black hole attack. The popular protocol utilized in MANET is AODV protocol, and is simulated using NS2. The imitation results of define approach are being compared with that of adaptive technique, in which sender node checks each and every nodes activity via DAT table with the aim of maintenance from-node-to-next node's information and that declares black hole node all the way through channel overhearing method. It is observed that the define method depend on adaptive fuzzy logic system shows better performance as compared to adaptive method in terms of throughput, end-to-end delay and PDR [7].

Lineo Mejaele et al. [2016] this paper define performance of DSR and the AODV when attacked all the way through black hole, through changeable the mobility nodes in network. The analysis is passed out by simulating scenarios of the AODV based MANET and the DSR based MANET by means of Network Simulator 2 (NS-2) and introducing black hole attack into each of scenarios. The dissimilar scenarios are being generated by altering mobility nodes. The performance metrics which may be applied to do the evaluation are throughput, end-to-end delay and PDR. The simulation consequences demonstrate that overall presentation of each DSR and AODV degrades within the incidence of black hole attack. Throughput and the PDR reduce while the network is attacked by means of black hole due to fact the malicious node rejects a few of packets. End-to-end delay is also reduced inside the attendance of a black hole attack because a malicious node pretends to have a legitimate route to receiver without checking the routing table, and consequently shortens the path detection procedure. The outcome also illustrate that throughput decreases to some extent when mobility of nodes is greater than before in the network. The rise in the nodes speed reductions both PDR and end-to-end delay [8].

P.Rathiga, et al. [2016] in paper, a latest hybrid black or gray hole detection technique is define for the detecting both the black and the gray hole attacks inside Dynamic Source Routing which is called as (DSR) protocol for the MANET by using the same technique. Protocol of DSR is vigorously discovers a dispatcher route across different network hops to whichever destination in MANET. In this hybrid approach, the initialized monitor nodes gather the packet flow information about the nearby nodes. Then the data distance metric is being computed using which two detection thresholds are determined. Then distance metric for all the nodes are compared among the first threshold. If the data distance metric of node is bigger than the first detection threshold, then the node is taken interested in consideration to be malicious nodes. If the information distance metric of the nodes are below the second threshold but not lesser than the first threshold, the nodes are marked as gray hole attackers while if they are greater than the second threshold, the nodes are marked as black hole attackers. The hybrid black/gray hole detection approach detects and eliminates the attacks effectively with better throughput, packet drop rate, routing overhead and PDR [9].

Neha Sharma, et al. [2016] in this method, A novel process a type of trap method is insert in AODV procedure for malicious nodes detection. When the Black-hole node is detected following that an alarming method is brought on to make other nodes conscious to malicious nodes. A various mobility network works in these days network MANET is a unique sort of network which works on variable (now not fixed) networks. Due to dynamic characteristics and addictive functionality, these are suffers from diverse varieties of attacks. Gray-hole and the Black-hole attack is 1 kind of assault which troubles and attack on MANET. In this attack the malicious (undesirable node) distract the data packets that it feels is having shortest and the novel to date path to the receiver node so source node forward every data packets to it. After receiving the data packets, it drops them to create a DoS attack or strategies to extract statistics from the packet. In this paper a method is being define for detection of the black-hole or malicious node [10].

Apurva Jain, et al. [2016] In this study, TAODV is utilized below extraordinary traffic pattern like CBR, Exponential and Pareto. As a propagation atmosphere, indoor shadowing atmosphere is utilized and have a look at exclusive Quality of Services (QoS). MANET is an agglomeration of mobility nodes that could speak without the presence of a restore infrastructure; this lack of infrastructure makes it at danger and open to several attacks. The black hole attack is a perilous security hazard that grows the network overhead and interrupts the normal functioning of the network, TAODV routing protocol is most appropriate under such situations [11].

Dhiraj Nitnaware, et al. [2016] This studies work attempts to increase a mitigation algorithm to avoid and save you authentic nodes from malicious attacks. Black hole attack be a security threat inside which traffic is being redirected to node so as to nearly doesn't be present for a longer time inside network. The black hole node is to provides itself in

kind of way to alternative nodes and the networks for which it is aware of shortest route. The whole research work is assessed into 3 classes which are without attack, with attack and preventive state of affairs. The parameter performance taken for evaluation are throughput and PDR towards the different parameters like speed, lots of nodes, pause time, region to observe the effect of black hole attack and define mechanism with exclusive situation. A Qualnet 5.2 simulator contain been used evaluate and to simulate presentation of the solution which is proposed. The whole experimental system concludes that enhancement in mobile node enhance the network presentation but also raise impact of black hole . Subsequently, development in speed of node degrades black hole contact [12].

IV. PROPOSED WORK

In our proposed work, we are calculating distance among each participating nodes but the most considering the case of transmission between those nodes. In our mechanism we 1st calculate distance of each node and then apply multipath for sending data for destination. Sender wait receiving acknowledge of packet on basis of distance if it not get acknowledge on calculated distance or RTT time then it send data to next path if same thing happen again it send packet to neighbour to update the distance table again with add the information of previous paths, so that every node check those paths and their neighbours also if there is any problem occur it create boundary for those non malicious nodes and make these node id as malicious.

Proposed Algorithm

Step1 calculate distance between nodes
Step2 on the basis of distance calculate RTT
Step3 sending the data and wait for acknowledge
Step4 if we are not getting acknowledgement in expected time.
Step5 then we will found the paths from which we are not getting any acknowledgement.
Step6 now we will find out common nodes in those paths which advertising for shortest path to destination.
Step7 now we put this node id in malicious queue.
Step8 delete all the entries of RREQ table and create boundary of secure nodes for transmitting data.
Step 9 exit

V. RESULT ANALYSIS

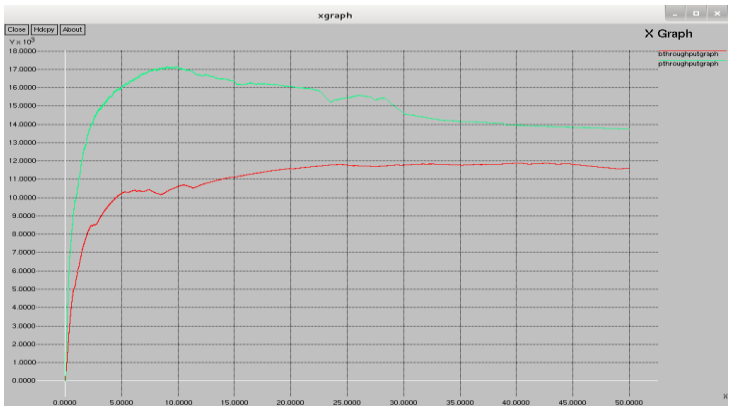

Fig. Throughput Graph

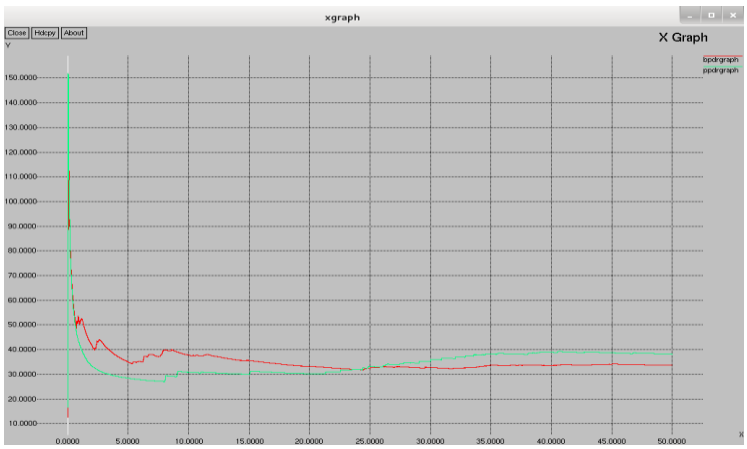

Fig. PDR Graph

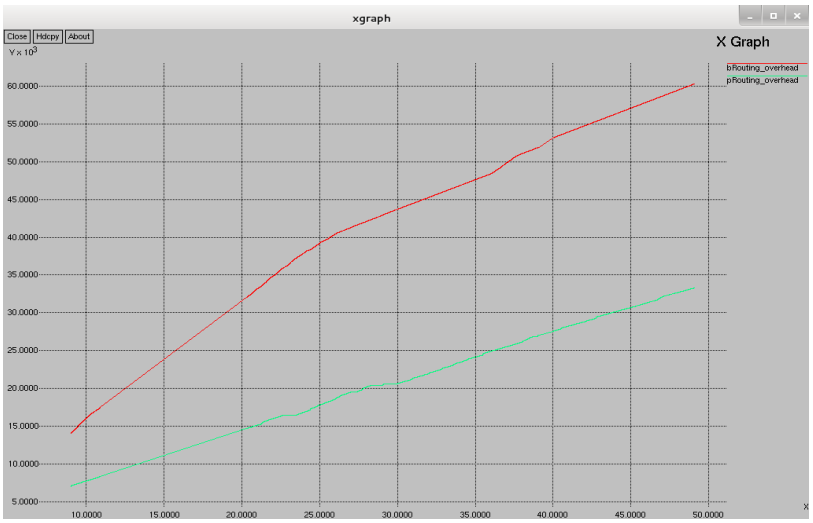

Fig. Routing Overhead Graph

Conclusion

Wireless network is dissimilar from wired network and self configured that's why it's more vulnerable for attacks, security is one of main issues of wireless network here we analyses, On-demand routing protocol DSR performance under wormhole attack and apply avoidance and detection method by which we attempt to get better presentation of this type of protocol. With the help of our proposed mechanism we protect our network against wormhole assault in MANET and we newly developed network which provide more security and give improved results in a variety of system parameters like end in the direction of end hindrance, throughput, PDR.

References

[1] Sushama Singh , Atish mishra Dinesh Bhuriya , Upendra Singh "Collaborative Black hole attack on MANET" International Journal of Computer Science and Information Technologies, Vol. 7 (3) , 2016, 1358-1361.

[2] A Sharma, D bhuriya, U singh , "Secure data transmission on MANET by hybrid cryptography technique", IEEE 2015 International Conference on Computer, Communication and Control (IC4), 10-12 Sept. 2015 Pages1 – 5 .

[3] Alka Chaudhary, V.N. Tiwari," Design an Anomaly Based Fuzzy Intrusion Detection System for Packet Dropping Attack in Mobile Ad Hoc Networks", 978-1-4799-2572-8/14/$31.00_c 2014 IEEE.

[4] Harsh Pratap Singh, Virendra Pal Singh and Rashmi Singh "Cooperative Blackhole/ Grayhole Attack Detection and Prevention in Mobile Ad hoc Network: A Review" International Journal of Computer Applications (0975 – 8887) Volume 64– No.3, February 2013

[5] Sathish M, Arumugam K, S.Neelavathy Pari Harikrishnan V S "Detection of Single and Collaborative Black Hole Attack in MANET" 978-1-4673-9338-6/16/$31.00 c 2016 IEEE.

[6] Emimajuliet.P, Thirilogasundari.V "Defending Collaborative Attacks in Manets Using Modified Cooperative Bait Detection Scheme" International Conference On Information Communication And Embedded System(ICICES 2016).

[7] P.S.Hiremath, Anuradha T and Prakash Pattan "Adaptive Fuzzy Inference System for Detection and Prevention of Cooperative Black Hole Attack in MANETs" 978-1-5090-1987-8/16/$31.00 ©2016 IEEE.

[8] Lineo Mejaele and Elisha Oketch Ochola "Effect of Varying Node Mobility in the Analysis of Black Hole Attack on MANET Reactive Routing Protocols" 978-1-5090-2473-5/16/$3l.00 ©2016 IEEE.

[9] P.Rathiga, Dr.S.Sathappan "Hybrid Detection of Black hole and Gray hole attacks in MANET" 978-1-5090-1022-6/16/$31.00 ©2016 IEEE.

[10] Neha Sharma, Anand Singh Bisen "Detection As Well As Removal Of Black hole And Gray hole Attack In MANET" International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016.

[11] Apurva Jain, Urmila Prajapati, Piyush Chouhan "Trust Based Mechanism with AODV Protocol for Prevention of Black-Hole Attack in MANET Scenario" 2016 Symposium on Colossal Data Analysis and Networking (CDAN).

[12] Dhiraj Nitnaware, Anita Thakur "Black Hole Attack Detection and Prevention Strategy in DYMO for MANET" 2016 3rd International Conference on Signal Processing and Integrated Networks.

