International Journal of Research in Engineering, Science and Management
Volume-1, Issue-12, December-2018
www.ijresm.com | ISSN (Online): 2581-5792

Simulation and Analysis of Black Hole Attack

M. Anusha[1], R. Latha Manju[2]
[1]*UG Student, Dept. of Electronics and Communication Engg., Saveetha School of Engineering, Chennai, India*
[2]*Assistant Professor, Dept. of Electronics and Communication Engg., Saveetha School of Engg., Chennai, India*

***Abstract*: A MANET is a framework – less kind of ad-hoc system that comprise of number of versatile nodse to influence correspondence among hubs portable to build up unique way among one hub to another through remote system interfaces. In a MANET rating is an especially difficult undertaking when contrasted with other traditional system. Because of one of a kind qualities, for example, restricted power, dynamic system topology and constrained data transmission. In the accessibility of vindictive hubs , one of the primary issues in MANET is to plan the vigorous security to alleviating different sort of directing attacks troublesome component have been proposed utilizing different cryptographic Techniques.In this paper we are talking about the routing attacks in MANET and answers for Black hole attack.[1].In this paper we discussed about the routing attacks in Manet and also the solution for black hole attack by using some steps by using AODV protocol and Diffie-Hellman algorithm.**

***Keywords*: MANET Attacker node and malicious node**

1. Introduction

A MANET is quickly developing innovation which depends on quickly conveyed system and self-sorted out. Because of its essential highlights,

Fig. 1. Manet

MANET draws in different genuine application regions where the systems topology changes quick [2]. Hubs are interconnected through remote interface. There is no settled arrangement of foundation and concentrated organization in this sort of systems. Exchange of parcels is finished with the assistance of steering conventions. In which help in deciding the reasonable course from source to goal for starting and in addition keeping up an association between the two. System topologies are dynamic in nature, because of which there are interface breakage and interruption in distributed association.

2. Review of literature

- Chu-Hsing Lin, Tunghai University: He proposed about the wormhole attack. He discover answer for this assault i.e SEAD. But, it doesn't give an approach to keep an assailant from messing with "Next hop" columns, but it depends on doing neighbor verification.
- Sanjay Ramaswamy, proposed the answer for distinguishing the different dark gap nodes[3].The arrangement depends on the altered AODV protocol by showing the cross checking and information directing data table(DRI).This table is kept up for each and every section of the node. For exchanging the parcels we depended just the confided in hubs.
- S.Sankara Narayan et.al a safeguard system is introduced against the collaborative dark opening attacks. He proposed an anchored algorithm. This strategy utilizes MAC deliver of goal to approve every hub in its way by giving an immediate arrangement to anchor route.[4]
- Latha Tamilselvan presented an improvement in the current AODV protocol, which are skilled to hold back agreeable dark holes.[5].
- An algorithmic approach for improving the security of AODV protocol is introduced by Rajib Das et al with the ability to identify and remove the black hole nodes in MANET [6]
- Cerri D Politec di Milan, Ghioni A proposed SAODV protocol. But it requires heavyweight asymmetric cryptographic algorithm.
- Bridget, Brain NEIL, Elizabeth ROYER,
- Clay shields. Proposed ARAN technique for detecting active attacks. But cannot defend against authenticated selfish nodes.

A. Types of attacks

Active attack

- Black Hole attack
- Wormhole attack
- Spoofing attack

Passive attack

- Eavesdropping
- Traffic Analysis

1) Active attack

The data which is directing through the hubs in MANET is adjusted by an attacker node. Attacker node likewise streams some false data in the system. Attacker node additionally do the task of RREQ (re ask for) however it's anything but a confirmed

node so the other node dismissing its demand due to these RREQs the data transmission is consumed and network is strucked .

2) Black hole attack

A malicious node sends false routing data and asserting that it has a unique course and makes other good node course information through malicious one [7]. All movement will be directed through the attacker, and the aggressor can abuse or dispose of the activity.

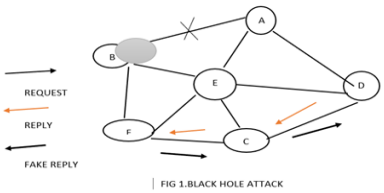

Fig. 2. Black hole attack

3) Wormhole Attack

In Wormhole attack two malicious nodes make a passage between them. This passage is called worm hole. Wormhole assault is moreover known as the tunneling attack. An attacker gets a bundle at one point and passages it to another malevolent hub in the system. Along these lines learner accept that he found the briefest way in the system. This passage between two plotting aggressors is known as the wormhole [1, 2, and 3]. The reality of this assault is that it tends to propelled against all correspondence that give privacy and verification.

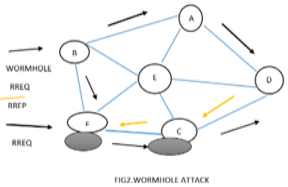

Fig. 3. Wormhole Attack

4) Spoofing

Spoofing is the making of web protocol (IP) packets with a false source IP address, for reason for concealing the character of the sender or imitating another figuring framework.

5) Passive attack

In Passive attack there isn't any adjustment inside the message that is transmitted. There is an assailant (intermediated hub) between senders and recipient that peruses the message. This halfway assailant hub is furthermore doing the undertaking of system recognition to dissect which sort of correspondence is goes on. The name of some detached assaults is Eavesdropping, movement examination, and Monitoring [8].

6) Eavesdropping

This happened inside the versatile specially appointed system. The point of listening stealthily is to locate some mystery or classified data that ought to be kept mystery amid the correspondence. [9].

7) Traffic analysis

In this kind of attack, an attacker tries to detect the correspondence way between the sender and collector. Thus attacker found the measure of information which is travel between the course of sender and receiver. There is no modification in information by the movement analysis [9].

B. Solution for black hole attack

In black hole attack, the solicitations are listened by the attackers. At the point when a course ask for message is got by the attacker to the goal node for a way foundation, it makes an answer with the littler course and goes into the way to drop the bundles got by the attacker node [10]. In MANET, communicated demands for course disclosure are tuned in by an aggressor. Dark hole issue can be clarified as the way toward misusing a steering convention by a malicious node by speaking to that it has the most brief way to the destination node, rather than sending bundles to its neighbors it drops the direct nodes. From the Fig. 2, given us a chance to expect that M is a malicious node. In the above figure node A is the source node and hub E is the destination node, in which A is attempting to reach. With the goal that it transmits the RREQ parcel to every one of its neighbors "B", "D" and "M" individually. As we realize that M is a pernicious hub, it answers with a RREP bundle when it gets the RREQ parcel, it announces that it has the most limited course to the goal without checking it steering table [11]. Along these lines, the source hub will get the primary RREP from M and after that from alternate hubs in the system. Based on the RREP arrangement gotten by An, it will trust that M has the most limited way to the coveted goal E and it can transmit bundles to by means of M to achieve the goal E. M being a malicious node will expend every one of the parcels got by it which is expected exchange to E [12]. Thus we can state that M is a Black Hole Node.

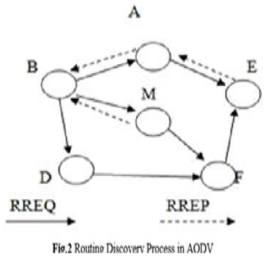

Fig. 4. Black hole Attack

C. Proposed technique

1) Diffie -hellman algorithm

It is a key understanding protocol (1976) was the foremost down to business procedure for working up a common sharing over an unbound correspondence direct continuously.

2) Steps of diffie-hellman algorithm

Among all of the attacks, black hole attack is the most widely recognized dynamic kind of attack. Black hole attack is the denial of administration attacks which is activated by the malicious node in the system. In the past times, numerous systems have been proposed to disconnect black hole attacks from the system. At the point when black hole attack is activated in the system, throughput of the system diminished

and postpone increment as steady rate. The black hole attack is far more terrible if the various black hole attack exist in the system. At the point when various black hole attack exist in the system, all the malicious nodes are in charge of setting off the black hole attack. This kind of attack is called various black hole attack. In our work, we deal with to recognize and separate various black hole attacks in versatile Ad hoc organize. Above all else, we will convey limited way will built up based on AODV. Source will send fake route request ask for bundles to the system. The node which will be malicious send course answer bundle to the system. Along these lines we will distinguish the whole malicious node which trigger balck hole attack. After this for greater security, we will again send caution nodes from source. It will again separate black hole attack after accepting alert nodes. In third step will apply Diffie-Hellman calculation to check the reliability of the particular way. Thus, we will detect the black hole attack. The entire situation will be simulated on NS2 test system.

3) Software used

NS2 Simulator

D. Flow chart for detecting black hole attack

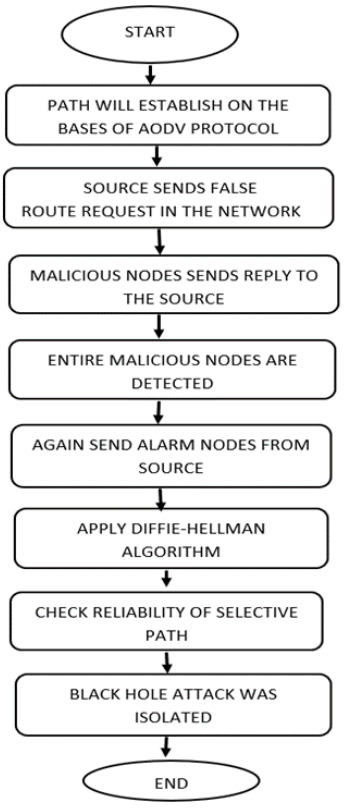

Fig. 5. T D. Flow chart for detecting black hole attack

3. Experimental results

1) Throughput graph

In the above figure red line indicates old throughput and green line demonstrate new throughput. X-pivot indicates time and y hub demonstrates bundles. It reasoned that new system has more throughput when contrasted with old strategy.

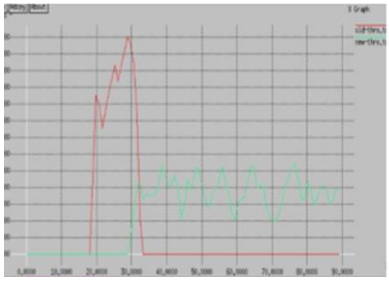

Fig. 6. Throughput graph

2) Delay graph

In the above figure, red line demonstrates old postponement and green line indicate new deferral. X-hub indicate time and y hub demonstrates bundles. It presumed that new method has less deferral as contrast with new strategy. It demonstrates that new procedure is superior to old method.

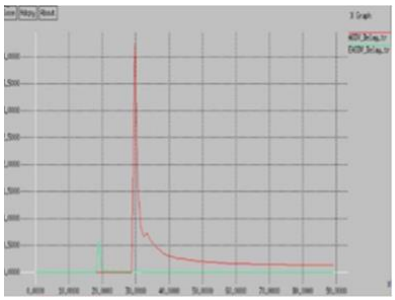

Fig. 7. Delay graph

3) Packet loss delivery

In the above figure, red line demonstrates bundle misfortune and green line indicate new parcel misfortune. X-hub demonstrate time and y pivot indicates parcels. It presumed that new strategy has less parcel misfortune as contrast with new procedure. It demonstrates that new method is superior to old procedure.

Fig. 7. Packet loss delivery

4. Conclusion

Hence, we infer that various dark gap assault is one of the overwhelming attack done on the network. Due to this attack parcel misfortune may happen by applying Deffie-Hellman calculation we can distinguish the black hole attack and furthermore we can decrease the bundle loss, delay and we can build the throughput. In this paper we acquainted another method with recognize the black hole attack.

References

[1] Karan Singh, Rama Shankar Yadav and Ranvijay, "A Review Paper on Ad-Hoc Network Security," International Journal of Computer Science and Security, Volume (1): Issue (1) 2010

[2] J. Nafeesa Begum, K. Kumar and V. Sumathy, "Multilevel Access Control in a MANET for a Defense Messaging system using Elliptic Curve Cryptography," International Journal of Computer Science and Security, Volume 4: Issue (2) 2012.

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

[4] S. Sankara Narayanan and S. Radhakrishnan, "Secure AODV to Combat Black Hole Attack in MANET", 2013 International Conference on Recent Trends in Information Technology (ICRTIT).

[5] Latha Tamilselvan and V. Sankaranarayanan "Prevention of Co-operative Black Hole Attack in MANET", Journal of Networks, vol. 3, no. 5, May 2008.

[6] Rajib Das, Bipul Syam Purkayastha and Prodipto Das "Security Measures for Black Hole Attack in MANET: An Approach".

[7] Sarita Choudhary, Kriti Sachdeva. Discovering a Secure Path in MANET by Avoiding Black/Gray Holes. International Journal of Recent Technology and Engineering (IJRTE), Volume-1, Issue-3, August 2012.

[8] Sukla Banerjee ―Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks‖ Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[9] Sun B, Guan Y, Chen J, Pooch UW, "Detecting Black-hole Attack in Mobile Ad Hoc Networks," 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.

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

[11] Songbai Lu, Longxuan Li, Kwok-Yan Lam and Lingyan Jia "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack", 2009 International Conference on Computational Intelligence and Security.

[12] Sheenu Sharma, Roopam Gupta "Simulation Study Of Black hole Attack in the Mobile Ad Hoc Networks", Journal of Engineering Science and Technology, vol. 4, no. 2 (2009), 243 – 250.