ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 4, Issue 2 (Apr. - Jun. 2016)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016)

A Black Hole Attack in MANET: A Review

[I]Manu Garg, [II]Er. Pranab Garg
[I]Student, M.Tech CSE, [II]Assistant Professor, Dept. of Computer Science
[I,II]BGIET, Sangrur, Punjab, India

Abstract
MANET has received the significant attention in every field of Information and Communication Technology industry. MANETs comprise of mobile nodes that are free to move in and out in the network. Nodes are the devices that are mobile and that participate in the networks such as mobile phone, laptop, personal digital assistance and personal computer. The nodes in Mobile Ad hoc networks continuously move leading to randomly changing topology which further leads to many problems such as malicious node present in the network and loss of packets sent by the source node to the destination. DSR is a routing protocol in Manets. This paper gives an overview of the Black hole attack and DSR protocol.

Keywords
Manets, Black hole attack, DSR Protocol

I. Introduction

In today's fast and rapidly growing world of technologies MANET can turn the dream of networking at any place and at time into reality. Mobile Ad-Hoc Networks are independent and decentralized wireless systems. Wireless network is a network in which computer devices communicates with each other without requiring any wire. The communication medium between the computer devices is wireless. When a computer device wants to communicate with any alternate device, the objective device must lie within the radio range of each other. MANETs comprise of mobile nodes that are free to move in and out in the network. Nodes are the devices that are mobile and that participate in the networks such as mobile phone, laptop, personal digital assistance, MP3 player and personal computer. These nodes can act as host/ router or both simultaneously. Numerous routing conventions have been created for MANETs i.e. AODV, OLSR, DSR etc.

A. Characteristics of MANET

MANET possesses the characteristics of wireless network in general, and extra aspects that are particular to the Ad Hoc Networking:

1. **Wireless:** Nodes communicate without requiring the wires as their mediums and share the same media (radio, infra-red, etc.).
2. **Ad-hoc-based:** A mobile ad hoc network is a temporary network structured progressively in a self-assertive way by an accumulation of nodes as need emerges.
3. **Autonomous and infrastructure-less:** MANET does not rely on any established foundation or centralized administration. Each node operates in dispersed distributed mode, acts as an independent router, and creates autonomous data.
4. **Multi-hop routing:** No devoted routers are fundamental; every node acts as a router and advances packets to empower data imparting between portable hosts.
5. **Mobility:** Each node is allowed to move about while communicating with other nodes. The topology of such an impromptu system is dynamic in nature because of steady development of the participating nodes, bringing on the intercommunication designs around nodes to change consistently

II. Black Hole Attack

A black hole problem means that a malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. Black hole is generally of two types:

1. Single Black Hole Attack: In single black hole attack only one malicious node attack on the route. The DSR protocol is vulnerable to the well-known black hole attack.

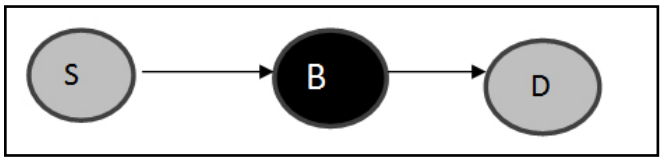

Fig.1:- Single black hole attack

2. Co-operative Black Hole Attack: Co-operative Black Hole means the malicious nodes act in a group In the A more complex form of the attack is a Co-operative Black Hole Attack where multiple malicious nodes collude together resulting in complete disruption of the routing and packet forwarding functionality of the network .

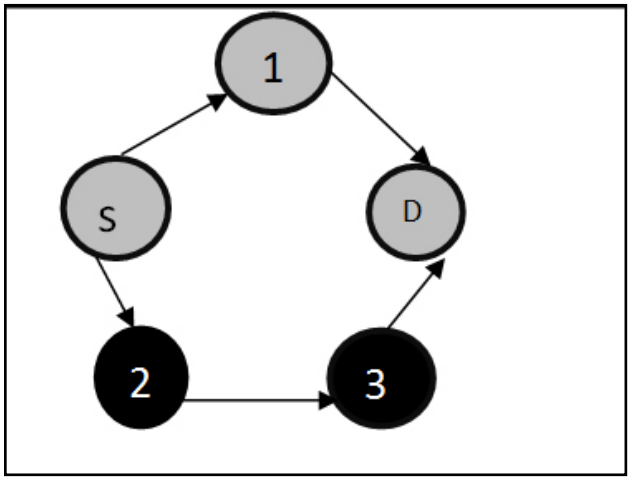

Fig. 2: Co- operative Black Hole Attack

II. Routing Protocols in Manet

A routing Protocol is a set of rules or a standard that determines in which way to route packets between computing devices in a mobile ad hoc network. There are various routing protocols in

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Manets like DSR,TORA, DSDV,ZRP,AODV,AOMDV.

A. DSR Protocol

DSR is a reactive routing protocol. It verifies the best possible route only when packet needs to be forwarded . The DSR protocol is made out of two main mechanisms that cooperate to permit discovery and maintenance of source routes in MANET.

1. Route Discovery: When a source node S wishes to send a packet to the destination node D, it obtains a route to D. This is called Route Discovery. Route Discovery is used only when Source needs to send a packet to Destination and has no information of a route to it.
2. Route Maintenance: The existing routes are no longer usable when there is a change in the network topology. In such a scenario, the source S can use an alternative route to the destination D, or invoke Route Discovery. This is called Route Maintenance.

III. Literature Survey:

1. **Jaspinder kaur** et.al. [7] in 2014 described Detect and Isolate Black hole attack in MANET using AODV Protocol. The black hole attack is the most common type of attack which is triggered by malicious node which is present in the network. In this work, new technique had been proposed which detect the malicious node and isolate it from the network which is responsible for triggering the black hole attack. The basic idea to detect and isolate malicious node from the network is using fake route request packets.
2. **M.Mohanpriya** et.al. [3] in 2013 described Modified DSR protocol for detection and removal of selective black hole attack in MANET. They had proposed a modified DSR routing protocol which defines a threshold value and compares the ratio of number of packets received at the destination to the number of packets sent by the destination. If the number of packets received at the destination is less than 80 percent of the packets sent by the source then it initiates the process to detect the malicious node.
3. **Antony devassy** et.al. [2] in 2012 described Prevention of Black Hole Attack in Mobile Ad-hoc Networks using MN-ID Black hole is a malicious node that always gives the false replay for any route request without having specified route to the destination and drops all the received packets. This can be easily employed by exploiting vulnerability of on demand routing protocol AODV. In mobile Ad hoc networks black hole attack is a severe threat which can be prevented by broadcasting the MN-ID (malicious node id) to the whole nodes in the network. The existing method identified the attacked node, retransmit the packets and again find a new route from source to destination.
4. **Nishant Sitapara** et.al. [6] in 2010 described Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks. This paper proposed an anomaly detection scheme using dynamic training method to detect and prevent black hole attack. They evaluated the performance of network with or without black hole in the network and checked the data loss. They evaluated the difference and showed more data packet loss in presence of black hole attack. More percentage of data loss will occur if more than one black hole is present in the network as a result.
5. **Amit Puri** et.al. [5] in 2012 described black hole in network: a review. In this paper they analyzed the impact of Black hole attack on Ad Hoc. We also learnt about the Types of Black Hole and to prevent the black hole attack they provided two techniques. First is unique sequence no. and second is Using more than one route to destination. The detection and removal of selective Black Hole attack becomes easy with these methodologies. These techniques are applicable for the detection of single black hole node in the network. Performance of the network had increased and less data packet loss comparison presence of with or without black hole present in the network.
6. **H. dehghan** et.al. [4] in 2012 described Evaluation of DSR protocol under a new Black hole attack . The creators had presented and assessed a novel more ruinous attack named Deep Black Hole. This attack promotes fake route reply messages more unequivocally than past ones. Assessment of system parameters was performed identified with DSR convention in NS-2. The simulation results demonstrated that this kind of attack, contrasted with common Black hole and selfish nodes, is all the more harming and prompts system dissent of administration. This assault brought about a reduction in the quantity of system directing bundles and end-to-end defer particularly contrasted with selfish nodes.
7. **Tanupreet singh** et.al.in [13] 2012 describe Survey on Prevention of Black Hole Nodes in Mobile Adhoc Networks**.** In this paper, they detect the Black hole nodes or malicious nodes present in network and after detecting it they will remove those nodes and also find the shortest path to reach the destination by using GLOMOSIM. They proposed that our protocol is increase the throughput, security and life time of the network by reducing the delay than the other AODV protocols. They proposed that our protocol is increase the performance and life time of the network by deducting the delay than the other conventional AODV protocols.

IV. Conclusion

In this paper we have disscussed about the intro of Black Hole attack in networking . Among the other protocols DSR Protocol Can be used. DSR protocol is composed of two mechanisms Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. We just discussed about the malicious node and how it can effect on network .which leads to loss of data, time delay, throughput, energyconsumption. In future we will try to remove black hole attack.

References

[1] Jaspinder Kaur, Birinder Singh, " Detect and Isolate Black hole attack in MANET using AODV Protocol," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3, Issue 2, February 2014

[2] Harmanpreet Kaur, P. S. Mann, "Prevention of Black Hole Attack in MANETs Using Clustering Based DSR Protocol," IJCST Vol. 5, Issue 4, Oct - Dec 2014.

[3] Antony Devassy , K. Jayanthi, " Prevention of Black Hole Attack in Mobile Ad-hoc Networks using MN-ID Broadcasting," International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.3, May-June 2012

[4] M. Mohanapriya, Ilango Krishnamurthi, " Modified DSR protocol for detection and removal of selective black hole attack in n MANET," Computers & Electrical Engineering Volume 40, Issue 2, February 2014, Pages 530–538

[5] *Salehi, M., Samavati, H., Dehghan, M., " Evaluation of DSR protocol under a new Black hole attack, " 20th Iranian Conference on Electrical Engineering (ICEE), May 2012, IEEE.*

[6] *Amit Puri, Anu Priya, "Black Hole In Network: A Review, "Int J Adv Engg Tech/Vol. VI/Issue II/April-June,2015.*

[7] *Nishant Sitapara, Prof. Sandeep B. Vanjale, "Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks." International Conference" ICETE-2010" 21st Feb 2010.*

[8] *\Puja vij, V. K. Banga, Tanu Preet Singh' "Survey on Prevention of Black Hole Nodes in Mobile Adhoc Networks," International Conference on Trends in Electrical, Electronics and Power Engineering (ICTEEP'2012) July 15-16, 2012.*

[9] *Harjeet Kaur , Manju Bala , Varsha Sahni, "Study of Black hole Attack Using Different Routing Protocols in MANET," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, July 2013.*

[10] *Aman Saurabh, Rakesh Yadav, Harjeet Kaur, " Identifying & Isolating Multiple Black Hole Attack on AODV protocol in MANET," International Journal of Innovative Research in Science, Engineering and Technology Vol. 4, Issue 5, May 2015.*

[11] *Shweta Jain , Jyoti Singhai, Meenu Chawla, "A Review Paper on Cooperative Black hole And Gray hole Attacks in Mobile Ad hoc Networks," International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.2, No.3, September 2011.*

[12] *Harmandeep Singh, Manpreet Singh, "Securing MANETs Routing Protocol under Black Hole Attack," International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 4, June 2013.*

[13] *Tanupreet singh et.al.in 2012 describe Survey on Prevention of Black Hole Nodes in Mobile Adhoc Networks.*

[14] *Varsha Patidar, Rakesh Verma, "Black Hole Attack and its Counter Measures in AODV Routing Protocol," international Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5 Sept. 2012.*

[15] *Aman Saurabh, Rakesh Yadav, Harjeet Kaur, " Identifying & Isolating Multiple Black Hole Attack on AODV protocol in MANET," International Journal of Innovative Research in Science, Engineering and Technology Vol. 4, Issue 5, May 2015.*

[16] *Ei Ei Khin, Thandar Phyu , "Mitigating Scheme for Black Hole Attack in AODV Routing Protocol," International Conference on Advances in Engineering and Technology (ICAET'2014) March 29-30, 2014.*