The Different Black Hole Detection Mechanism In MANET

Sahil Sharma [#1], Rupinder Kaur Gurm [#2]
[#]*CSE Dept, RIMT Mandi Gobindgarh*
[1]sssahil529@gmail.com
[2]rupindergurm@gmail.com

Abstract— A mobile Ad-Hoc network provide a survey of various security mechanism that has been proposed in Dynamic Source Routing(DSR) protocol against black hole attack which contain malicious nodes which replies the route request in the form of fresh route to the destination and then it drops all the receiving packets. In this paper, the proposed solution provide a secure route between the source and destination by identifying both single and cooperative black hole. The paper focus on network layer packet dropping attack like black hole/grey hole attack in DSR based manet.

Keywords —Mobile Ad Hoc Network, , Black Hole Attack, DSR.

I. INTRODUCTION

A network is a collection of nodes which follow different protocols. A wireless AD-HOC network is type pre existing network framework which has no router or access point but a collection of mobile nodes wich act as both host and router, equipped with wireless communication and networking capability to communicate with one another.
There is a problem of routing the data packet from source to destination node, so MANET goal is to provide communication to the area where limited communication organisation exist. Examples of ad-hoc network are laptops, mobiles, computers etc.

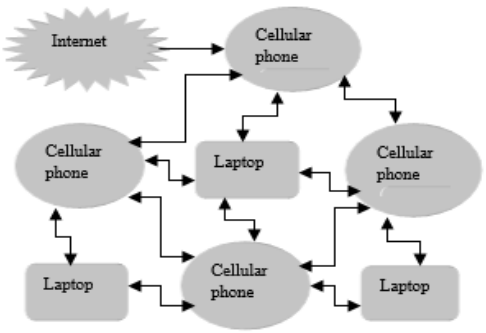

Fig 1. Mobile adhoc networks

Figure 1: A Mobile Ad-hoc Network

CHARACTERISTIC OF AD-HOC NETWORK

MOBILE AD-HOC NETWORK is a type of flexible and reliable network. It has no fix infrastructure and links and limited bandwidth which continue to have low capacity then other network which provide minimum throughput with consequences of noise and interference. It is energy compulsion operations which rely on batteries and other source of energy. Ad-Hoc network experience security attacks due to changing network topology, decentralized monitoring and there is no certification authority. It has limited physical security and responsible for discovering other nodes dynamically, and it is a self configuring server.

II. Routing in MANET

An Ad-Hoc is a type of protocol that controls how nodes decide the path to route the packet between computing device in mobile Ad-Hoc network. It is divided into two parts.

A. Topology based
B. Position based

A. *Topology Based*: Topology based protocol is of three types.

Proactive Routing Protocol: - It is maintained by nodes to use to store packet. It is table-driven which contain routing entries. It is prone to various type of attack like message dropping, delay of service. It maintains constant up to date information between nodes. Its node experience least delay where route is immediately needed to get rid of short coming reactive protocol. Example of proactive routing protocol are DSDV (Destination sequenced distance vector), OLSR (optimized link state routing).

Reactive Routing Protocol:- it consume less bandwidth then proactive protocol. It is also called On-Demand routing protocol. It creates route On-Demand to destination node initiated by source node through discovery process. It typically experience long delay communication. The main disadvantages of such type of routing, it takes high latency time in route finding and excess flooding can lead to network clogging. Example of reactive protocol are AODV(Ad-Hoc On Demand Distance Vector) DSR(Dynamic Source Routing).
Dynamic Routing Protocol:- It is an on demand routing protocol which design specially for multi hop wireless Ad-Hoc network. In DSR, node uses RREQ, RREP, and RERR packet. In this, routes are discovered when source send a packet to destination for which it do not has cache route. It

help in making the network topology which and rapidly changing. It is based on the concept of source routing.
It has two phases:-

1) Routing Discovery:- It is discovered by a source node which broadcast a RREQ packet to all its neighbors'. It is to establish a route by flooding route request packet in network. The destination node when receive RREQ packet response to route reply packet by reversing route information stored in RREQ packet

2) Route maintence:- During this phase, break of links are handled. Link break occurs when intermediate nodes involve in packet forwarding process. Source either tries an alternate path or initiates the route discovery process again.

Hybrid Routing Protocol:- It is the combination of proactive and reactive protocol. In this the routing protocol is initially establish when some proactively prospected routes and then it serves the demand from additionally activated nodes through reactive flooding. The main disadvantage of this type of network is it depends on number of other activated nodes in the network. It is suited for a network where call-to-mobility ratio is high. Example of hybrid routing protocol are ZRP (Zone Routing Protocol) TORA(Temporally Ordered Routing Algorithm).

B. *Position Based*:- This algorithm requires information about physical positioning which eliminates the disadvantages of topology based routing. In this, the sender of a packet use location service to find the position of destination.

III. SECURITY IN MANETS

A. Security Goals in MANET

1) INTEGRITY: In this assets can be edited by an authorized party. It ensures that message to be transferred from source to the destination nodes is never corrupted.

2) ACCESSIBILITY:- It provide an availability to authorized party when ensure survival of networks despite of delay of service attack.

3) PRIVACY:- It ensure computer based confidentiality to authorized party. we need to keep confidential information secretly.

4) AUNTHENTICATION:- It provides access to legal senders to ensure identity of node to which it is communicated.

5) NON-ACCEPTABLE:- It ensure the sender and receiver if a message, not to reject when they ever send or receive.

B. Vulnerabilities In MANET

MANET is prone to an unauthorized data organization because it does not identify uses the identity. It is more prone to risks then wired network.

1) DECENTRALIZED MANAGEMENT:- It does not have centralized monitor because it is enable to detect traffic in highly dynamic Ad-Hoc network.

2) SHARING:- It is assume that nodes are cooperative and non malicious as a sequence spiteful attacker, not able to disrupt network operation.

3) RESTRICTED POWER SUPPLY:- In Ad-hoc network, nodes need to consider limited power supply. Nodes show greedy nature when there finds limited power supply. These nodes are called selfish nodes.

4) RESOURCE REQUIREMENT:-It is a major conflict in MANET to provide secure communication in such modifying environment where there is a security issue.

IV. ATTACKS IN MANET

It is a challenging issue, decentralization and cooperative medium makes MANET more vulnerable to cyber attacks. These attacks are classified into following types:-

1) Passive Attack

These attacks provide proper operation of network. There is a requirement where confidentiality can be violated through snooping. Detection of these attack are difficult.

2) Active Attack

These attacks are performed by malicious nodes which can tolerate some energy cost. It involves editing of data stream or creation of pseudo stream.

3*) External Attack*

These attacks are physically stayed outside the network and create congestion in network by disrupting the entire network. External attack can become a kind of internal attack when it takes power on the internal malicious node and control it to attack the other nodes in manet. This type of attack decreases the speed of transmission of data and also makes the data packet insecure by lowering down the performance of the nodes in the network. It can be protected by using authentication and non repudiate, privacy and confidentiality methods.

4) Internal Attack

In this type of internal attack there is an internal malicious node which gets fit in between the routes of source and destination in the network. When the malicious nodes gets the chance then it makes itself an active data route element. When the data is going to start, at this stage it get capable of conducting attack during data transmission. Internal attack are more vulnerable to protect against this misbehaving because it is very difficult to detect them. Examples of internal attack are Black hole/ Grey hole.

V. *BLACK HOLE ATTACK*

Black hole attacks have been much known and as the most important concern of security in manet. The main aim of this paper is the black hole attack based DSR routing protocol, are the most vulnerable against black hole attack because DSR having a network centric property where all the nodes have to share their routing for each other. BLACK HOLE ATTACK refers to an attack by a malicious node as it acquires the route from source to destination by pseudo shortest hop count and maximum sequence number. It is an internal attack which has the attacker property like consume packets without any forwarding, to advertise itself as valid route to destination node as it can choose to drop of packet form the delay of service attack. In this attack, malicious nodes wait for the adjacent node to provide RREQ packet. The source node avoid RREP received from other node. This attack is called as black hole attack as it swallows all data packets. The diagram shows the black hole attack.

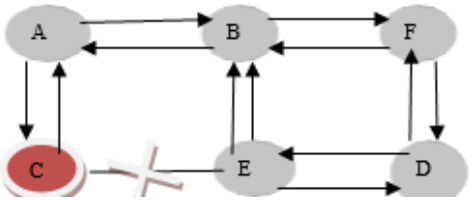

Fig. 2 Black Hole Attack

In this above example, the source A wants to communicate with the destination D. It sends RREQ (Route Request) packet to its neighbor. An attacker C, give a fake reply packet by advising a hop count for provide a shortest route to D. This leads to the existence of a fake route by the selfish nodes which help in dropping the packet. Selfish nodes are also known as black hole as they spoil the data packet and never send them

A.TYPES OF BLACK HOLE ATTACK

1). Single black hole attack:- This attack is due to individual black hole node. In this, sender sends the data to receiver through malicious nodes which drop all data somewhere.

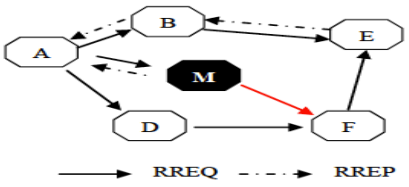

Fig. 3 Single Black Hole Attack

In this above fig. the source node A transmit RREQ packet to its neighbor nodes B and D to discover fresh route to the destination F. The black hole M quickly respond to the source node A by sending a fake RREP then the source node consider the route discovery has completed and then it reject the RREP message from other nodes. Then the attacker will drop the receive packet without sending to destination F.

2). *Collaborative black hole attack*:- This attack is due to two or more than two malicious nodes present in the network. It is very hard to detect and prevent this attack.

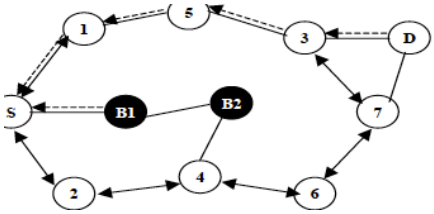

Fig. 4 Collaborative Black Hole Attack

In this above fig. the black hole node B1 is cooperating with Black hole node B2 which is its member as the next hop. The level of detecting attack is low because they work in grouped form.

VI. LITERATURE SURVEY

In this paper we will study about different black hole detection and prevention techniques.

M. Mohanapriya, Ilango Krishnamurthi proposed a routing security scheme which is considered on reputation evaluation in Ad-Hoc network as it is routed on the action of the nodes. It has a purpose of building up the participated grouping nodes for leading the data packets or to develop the activity channel of grouped nodes in the network. The authors also proposed the scheme in which the path of the intermediate nodes preferred randomly with the forwarding path as check points nodes which engages I developing community for every receive packet. An alarm packet gets up when the suspicious behavior is detected and then delivers it to the source node. They used IDS (Intrusion Detection System) for detecting Black hole/ Grey hole attack. They also approached trust based proposal which is used to improve the performance of the searching route and enhance the durability of the manet.

N. Balaji, Dr. A. Shanmuyam et al provide information about enhancement of routing security to be applied to DSR protocol of association based route selection. He proposes to apply the base route selection to fortify the existing attack through best and secure route. He provided information about the trust value which will be stored to represent the value of trusty for each node in network.

Issac Woungang et al proposed a paper in which there is a novel scheme for detecting black hole attack in manet called BDA DSR. These protocols detect and ignore the black hole problem by using fake RREQ packet to hold malicious node. Pruchee, M. Patil, Ashish T. Bhole gives the source routing and caching property of DSR which prevent the black hole attack in the network. When the black hole node and the mis-behaving node is detected, the black hole node is then go through add to route and add all remaining path for the source

to reach to the particular destination .This method of normal cache reduce the time processing and packet drop ratio.

Sanjay kumar Dhuradher, Mohammad S. obaidat et at in this paper authors proposed DBA-DSR based manet scheme in which fake RREQ packet are used which identify all the malicious nodes present in the network before the actual routing starts. In this scheme acknowledgement mechanism is also used by source and intermediate nodes, if the fake RREQ-RREP fails to identify the nodes in black hole. There are two drawback of this type of scheme used. The first one is the acknowledgements packets which are exchanged to check the intermediate node is fake are not; the overhead of routing is also increase with this scheme. The second drawback is that it takes larger time to find the path if the distance between the source and intermediate node is long.

Yogendra KumarJain, Nikesh Kumar Sharma et al in this paper, the authors provided a method which is used to find a save and secure path based on human trust analogy. In this path's trust value is used for finding a route from source to the destination to gain more secure path. Trust value is defined as equal to the minimal one of the node value in the route. In this method, nodes acquire there trust factors from experience, knowledge and advice from other nodes. Linear aggression method is used for the estimation of overall trust in a node and a minimal value is used to complete path's trust.

Po Chun TSOU, Jian- Ming Chang et al proposed a BDSR scheme to avoid black hole attack based on proactive and reactive protocol. In this paper, the author has presented an algorithm which contains two functions. The first function is initiate based. In this the black hole nodes are identify by sending bait RREQ by using non existence destination address to bait the malicious node to reply or RREP. If any node responds to that request, then is will be identified as the malicious nodes and added in the black hole list. The second function follows the normal DSR route discovery. If the packet delivery ratio is gets lower than the threshold value during its starting function, then its function calls to identify the malicious nodes and the route discovery will be successful and finally the transmission of data packets takes place.

Marti S, Giuli, T.J, Lai k. and Baker, M. et al proposed a watch dog and path rater against black hole attack which is used top of the source routing protocol such as DSR. CONFIDANT (Cooperative of Nodes, Fairness in Dynamic Ad-HOC networks) is an updated version of watch dog and path rater in which a method is used which is similar to pretty good secure for showing various certification, trust and validification. It is also implemented on unicast routing protocol like DSR.

VII. *CONCLUSION*

With developing in computing environment, the different types of services which are based on Ad-Hoc network have been increased. So, in this paper we have studied about the manet, types of routing protocols like proactive and reactive. Security and different attack in manets. Wireless Ad-Hoc network are vulnerable to various types of attack due to the physical characteristics of both the environment and the presence of nodes. In this paper authors proposed various methods to mitigate or overcome from the issue of the black hole attack on the DSR based routing protocol in manet. In our study the DSR is susceptible to black hole attack and therefore it is vital to have an efficient security function in the protocol in avoiding such type of attack in the manet.

References

1. M. Mohanapriya, Ilango krishnamurthi ,"Modified DSR protocol for the detection and removal of selective black hole attack in MANET. Comput Electr Eng (2013), http: //dx.doi.org/10.1016/j.compeleceng.2013.06.001

2. Raja Karpaga Brinda, Chandrasekar, " defence strategy for the detection of black hole attack in DSR," SriShakthi institute of engg. And technology, Coimbatore, india, 2011

3. Shashi gurung and Krishan Kumar Saluja " miting impact of black hole attack in manet," DOI:02ITC.2014.5.560, Associationof computer Electronic and electrical engineers, 2014.

4. JD. B Johnson and D.A. Maltz," The Dynamic Source Routing Protocol For Mobile Ad-Hoc network (DSR)," IETF Internetdraft, http://www.ietf.org/rfc/rfc4728.txt,jul

5. N Balaji, Dr. A. shanmugam," Association between nodes to combat black hole attack in DSR based manet," 978-1-4244-3474-9/09,IEEE 2009

6. Po Chun TSOU, Jian- Ming CHANG, Yi- hsuan Lin, han-Chich CHAO, Jiann –Liang chen," Developing a BDSR Scheme to avoid black hole attack based on proactive and reative architecture in manets", ICACT, February 2011

7. Isaac Woungang, Sanjay Kumar Dhunrandher, Rajinder Dheeraj Peddi, Mohammad S. Obaidat, "Detecting black hole attack on DSR based Mobile Ad-Hoc Network",978-1-4673-1550-0/12,IEEE 2012

8. Chandra Diwaker, Sunita Choudhary," detecting of black hole attack in DSR based MANET", International journal of software and web science, 2013

9. Prachee N. Patil, Ashish T.Bhole, black hole attack prevention in mobile ad-hoc network using route caching", 978-4673-5999-3/13, IEEE 2013

10. Yogundra kumar Jain, Nlkesh Kumar Sharma," Secure trust based dynamic source routing in manets", International

Journal of Scentific and Engineering and Research Volume 3, Issue 8, August 2012
11. Ashish T. Bhole, Prachee N. Patil, " study of black hole attack in MANET.", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 4, October 2012

12. Jieying Zhou, Junwei Chen, Huiping Hu, SRSN: Secure routing based on sequence number for MANETS,1-4244-1312-5/7/2007 IEEE

13. Swati Jain1, Naveen Hemrajani2," Study of black hole attack in MANET", International Journal of Engineering and Innovative Technology(IJEIT) Volume2, Issue 4,october 2012

14 J. Hongmei Deng, WeiLi, and Dharma P.Agrawal," Routing Security in wireless Ad-Hoc Network", IEEE communication magazine, october 2002

15. Himandri Nath Saha, Dr. Debika Bhattachryya, Dr. P.K Banerjee, Aniruddha Bhattacharyya, Amab Banerjee, Dipayan Bose," Study of Different Attack in MANET with its detection and mitigation Scheme", International journal of Advanced Engineering technology, E-ISSW 976-3945 IJAET/Vol.111/Issue/January-March, 2012/383-388

