Generalized Black Hole Attack and Comparative Solution For MANET

Shanu Singh, Amit Kumar Pandey, Minu Rani

Abstract*— *MANET is widely used by defense and civilians for wide range of application. There are various applications in wide range of communication. It's various routing technique makes it more flexible for various operations. Mobile Ad-Hoc network which leads to an autonomous system, where station or nodes are connected with each other through air medium links. There is no boundary conditions on the nodes to join or leave the network, therefore the overall operation is being freely. MANET topology is dynamic that can change rapidly because the nodes move freely and it can organize themselves randomly. Such a property of the nodes makes the mobile Ad-Hoc networks unpredictable from the point of view of topology and scalability . In this paper we fetch the various attacks on MANET and compare the technique to various solutions of MANET infrastructure which does not posses attacks. This paper also contains the protocol which leads to protect the MANET by attacks.

Index Terms*— *MANET, DSDV, DRI, Cross Checking, AODV

I. INTRODUCTION

Ad hoc networks have a large number of potential and dynamic applications. Military uses such as connecting terminals or creating sensory arrays with thousands of sensors or other military units to each other on the battlefield are two typical examples. Each mobile node acts as a host when information from/to other nodes in the network, and works as router when discovering and maintaining routes for other nodes in the network. There are currently three routing protocols for ad hoc networks [1]. Ad hoc networks provide a opportunity to creating a network in situations where creating the network would be impossible prohibitively expensive or impossible. With fixed infrastructure, mobile nodes in ad hoc networks do not communicate via access points (fixed structures) just unlike a fixed network. Destination-Sequenced Distance Vector routing (DSDV) [12], Dynamic Source Routing (DSR) [9], and AODV [2]. DSDV is a table driven routing protocol. The routing table is periodically updated for every change in the network to maintain consistency. In DSDV, each mobile node in the network maintains a routing table with entries for every possibility to destination node, and total number of hops to reach the destination before it goes down. This involves frequent route update broadcasts. It is inefficient DSDV because as the network grows the overhead grows as O(n2) [1].

Dynamic System Routing is an on-demand routing protocol which maintains a route cache, and it leads to memory overhead. It has a higher overhead as each packet carries the complete route, and dynamic system routing don't support multicast. AODV is a source initiated secondary type on-demand routing protocol. Every mobile node crates table for routing that maintains the next hop node information for a route to the destination node. On other hand when a source node tries to route a packet to a destination node, it give preference to the specified route if and only if a newly established path to the destination node is available in its routing table. If not, there is no availability of route it starts a route discovery process by broadcasting the Route Request (RREQ) message to its closest cell, this leads to propagated until the destination node or itself it reaches an intermediate node with a fresh enough route to the destination node specified in the route request . Each node which is intermediate receiving the RREQ, creates an updating in its routing table for the node that is motivated by source node and RREQ message. The intermediate node or the destination node with a fresh enough route to the destination node, which unicasts the Route Response (RREP) message to the closest node also called as neighbouring node from which it received the RREQ. An intermediate node update an entry for the neighboring node by which it received the RREP, then increased and focused this to the RREP in the reverse direction. After receiving the RREP, the source node updates its routing table with an entry for the destination node. The source node starts searching the data packet for the destination node through the neighboring node that first responded with an RREP. Some researchers [3-8], [10-11] illustrated the vulnerabilities in Ad hoc routing protocols and the attacks that can be mounted. So it can be state that a black hole does not have to check its routing table, it is the primary to respond to the RREQ in most cases. The AODV protocol is vulnerable to the most dealing black hole attack. Under this A black hole is a node which always provides information without error positively with a RREP message to every RREQ, only if it does not even have though have a valid route to the destination node. assume the black hole nodes do not work as a group and propose a solution to identify a single black hole. However, the analysed method cannot be applied to identifying a cooperative black hole attack involving multiple nodes. We analysed and compare a methodology to recognise various blackhole nodes cooperating as a group. The leads to modified AODV protocol and basically based on makes use of current routing tables and the Data Routing Information (DRI) table in addition to the cached.

II. COOPERATIVE BLACK HOLE ATTACK PROBLEM

A. *Black Hole*

A black hole has two properties. Primary , the node which exploits the ad hoc routing protocol, such as AODV, to expose itself as having a valid route to a final node, on other case even if even though the route is spurious, with the intention of braking packets.

Manuscript received June, 2013.

Ms Shanu Singh, Department Of Computer Science & Technology, Gurgaon Institute of Technology & Management, Gurgaon, India.

Mr. Amit Kumar Pandey, Department of Electronics and Communication Engineering, Skyline Institute Of Engineering and Technology, Greater Noida, India.

Ms. Minu Rani, Department Of Computer Science & Engineering, SPGITM, Rewari, India.

Secondary, the node absorbs the intercepted packets. We can illustrate the following conventions for protocol representation.

B. Cooperative Black Hole Attack Issue

It is basically based according to the original AODV protocol, when communication link is to be established in between source link S and destination link D , the source node S broadcasts the route request (RREQ) packet. The neighboring active nodes increase their routing table with an entry for the source node S, and check if it is the destination node or has a fresh enough route to the destination link. If not, the mediator node also called intermediate node updates the RREQ (increasing the hop count) routing request and floods the network with the RREQ to any other intermediate node which has a fresh enough route to D, as depicted by example in Figure 1 or the destination node D until it reaches node D. The destination node D or the intermediate node with a fresh enough route to D, initiates a route response (RREP) in the reverse direction, as illustrated in Figure. Node S which is a source node starts sending data packets to the neighboring node which reply first, and cancel the other responses. This provides better result when network has no malicious nodes.

C. Security Issues In MANET

Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the general functionality of network. Availability of confidentiality and integrity of the data network services can be achieved by assuring that security issues have been met. Mobile ad-hoc network often suffer from security attacks because of its features like changing its topology dynamically, less central monitoring and management, open medium, cooperative algorithms and no clear defence characteristics of operation . These components have changed the battle field situation for the MANET against the security issues. In the last few decades, security of computer networks has been of serious concern which has widely been discussed and implemented. Generally all the research includes static and networking based on wired systems. mobile MANET is still in need of further discussions and development in terms of security issues [21]. With the current trends of ongoing and new approaches for networking, new issues arises for the basics of routing. MANET is much different technology if it is compared by wired technology. The routing protocols creates majorly for internet is different from the mobile Ad-Hoc networks (MANET). All the previous pattern of routing table was basically made for the hosts which are connected wired to a non dynamic backbone [22]. Because of this it is not possible to favour Ad-Hoc networks mainly due to topology of network and the movement. Because of various factors including lack of infrastructure, proper communication not being progressed by the mobile network due tio topology and mobile dynamic operations, the routing protocols are vulnerable to various attacks [23]. The Mail vulnerabilities which have been so far researched are mostly these types which include selfishness, dynamic nature, open network medium severe resource restriction. On other hand the above said protocols in MANET, which are attacks which can be categorized in Active and passive , Internal, External and network-layer attacks and Packet forwarding attacks routing attackers. MANET work without a centralized administration where node communicates with each other on the base of mutual trust. This characteristic makes mobile ad-hoc network more vulnerable to be exploited by an attacker from inside the network. In case of Wireless links as compared by wired network also creates MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication [9, 21]. Mobile nodes the main few issue are also known as problem of scalability, No central management and Non secure Boundaries.

III. CLASSIFICATION OF ATTACK

A)External and Internal Attack

These issues of attack can be stooped by implementing security measures such as firewall, by which access of unauthorised person can be minimized . External attackers are mainly outside the networks who want to get access to the network and once they get access to the network they start sending bogus packets, cancellation of service in order to disrupt the performance of the complete system. This is a similar attach which usually happened in wired network technology. This attack is same, like the attacks that are made against wired network. While in internal attack the attacker wants to have normal access to the network as well as participate in the normal activities of the network. The attacker achieve access in the network as new node either by compromising a current node in the network or by malicious impersonation and start its malicious behaviour. Internal attack is more severe attacks then external attacks.

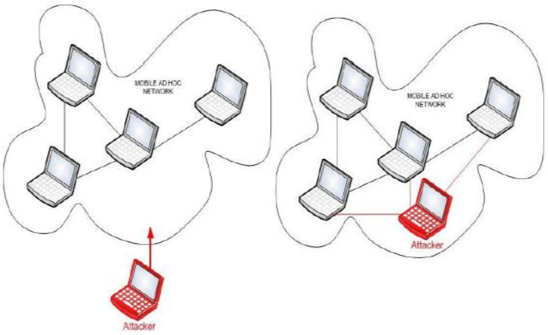

Figure1– Internal and external attack [1]

B)Active And Passive Attack

In active attack the attacker disrupts the performance of the network, destroyed the communication and try to destroy the data during the exchange in the network [13]. It can be an internal or an external attack. Such active attacks are meant to destroy the performance of network in such case the active attack act as internal node in the network. It is an active part of the network it is easy for the node to exploit and hijack any internal node to use it to introduce bogus packets injection or cancelation of service communicating in MANET. This attack brings the attacker in strong position where attacker can fabricate and replays and modify the massages. Similarly attackers in passive attacks do not disrupt the normal operations of the network [13]. In Passive attack, the attacker as compare to active network less dispute to network in order to get information, main focus of passive network what is going on in the network. It listens to the network in order to fetch and understand how the nodes are communicating with each other, how they are located in the network. The attacker contain more than enough information of the nodes where it is going to attach before attaching a node over this.

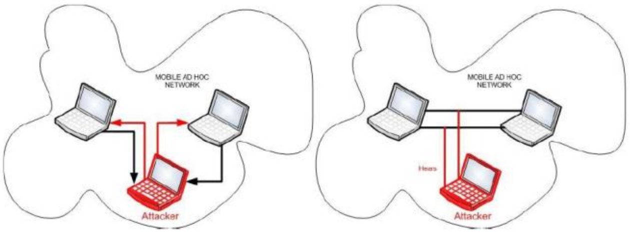

Figure2 – Active and Passive attack in MANET [1]

C)Gray Hole Attack

In this kind of attack the attacker misguide the network by agreeing to forward the packets in the network. As fast as it receive the packets from the closest node, the attacker breaks the communicational the packets. This is a type of active attack.. When it receives the packets it starts dropping the packets and launch Denial of Service (DoS) attack. The malicious behaviour of gray hole attack is different in different ways. Firstly the attacker nodes behaves normally and reply true RREP messages to the nodes that started RREQ messages It drops packets while forwarding them in the network. On other hand in other cases gray hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior [14]. Due this behavior it's very difficult for the network to figure out such kind of attack. Gray hole attack is also called as node misbehaving attack [15].

D) Flooding Attack

The flooding attack is easy to implement but cause the most loss. This kind of attack can be achieved either by using RREQ or Data flooding [16]. In RREQ flooding the attacker floods the RREQ in the whole network which takes a lot of the network resources. which can be achieved by the attacker node by selecting such I.P addresses that do not exist in the network. Doing so no node is able to answer RREP packets to these flooded RREQ. These prevent unwanted data packets in the network congest the network. The links that serves as destination node will be busy all the time by receiving useless and unwanted data all the time. In data flooding the attacker get into the network and set up paths between all the nodes in the network. Once the route are established the attacker provides insertion an immense amount of useless data packets into the network whose direction is towards outward for all the system.

E)Selfish node

The selfish node is known for dropping it's packet. When the selfish node see that the packets need lot of resources, it just simply drop the packets and do not forward it in the network the selfish node is no longer interested in the packets. In mobile ad-hoc networks the nodes perform collaboratively in order to forward packets from all individual nodes. When a node refuse to work in collaboration to forward packets in order to save its limited resources are termed as selfish node, this cause mainly network and traffic [22]. disruption [16]. The concern of the node is only to preserves and save, resources while the network and traffic disruption is the side effect of this characteristics. Selfish nodes can refuse by advertising non existing routes among its neighbor nodes or less optimal routes. Node can use the network when it needs to use it and after using the network it turn back to its silent mode. It is invisible in the network.

IV. COMPARISON TO VARIOUS TECHNIQUES FOR SOLUTION OF ATTACK

The Communication in an Ad Hoc network is a multihop communication wherein a source node communicates with a distant node using intermediate nodes in order to save the power. Thus the major activity in an ad hoc network environment is to find a suitable route such that the delivery of the message is ensured beyond doubt. The route should be so chosen that all the nodes in the path are trustworthy, non malicious , unselfish and the hop count is minimum. The first receiver of the message to a distant node is some immediate neighbor of the source node.

V. HYBRID PROTOCOL

Hybrid protocol exploit the power of both reactive and proactive protocols, and for the better result combine them together. Such network is divided into zones, and use different protocols in two separate zones i.e. one and other protocol is used within zone. The main example of hybrid protocol is Zone Routing Protocol (ZRP) . ZRP uses proactive mechanism for route establishment within the nodes neighbourhood, and to communicate among the neighbourhood it takes the advantage of reactive protocols. Such local neighbourhoods are known as zones, and the protocol is named for the same reason as ZRP. Every zone can have different size and each node may be within multiple overlapping zones. Size of zone is given by radius of length P, where P is number of hops to the perimeter of the zone [8].

VI. DATA ROUTING INFORMATION

The main solution to identify multiple black hole nodes acting in cooperation black hole involves two bits of additional information from the nodes responding to the RREQ(routing request) of source node S. Every node maintains an additional Data Routing Information (DRI) table. In the Data Routing Information table, 1 stands for 'true' and 0 for 'false'. The first bit "From" express the meaning on routing data packet *from* the node (in the Node field) on other hand the second bit "Through" stands for information on routing data packet *through* the node (in the Node field).

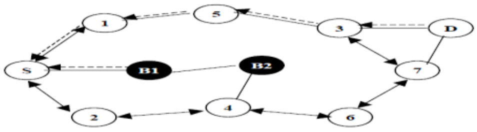

Figure3 – solution to avoid cooperative black hole attack [1]

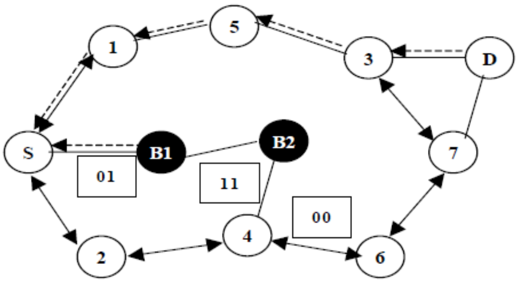

Figure4 – solution to identify multiple black hole nodes in one time check [1]

we analysis a method proposed by an researcher recently for identifying multiple black hole nodes cooperating as a group with slightly modified AODV protocol by introducing cross checking and Data Routing Information (DRI) Table.

VII. CROSS CHECKING

we depend on reliable nodes (nodes through which the source node has routed data) to transfer data packets. The analysed achieved modified AODV protocol, for our analysed methodology are illustrated in Figure 5. The source node (SN) broadcasts a RREQ message to identify a secure route to the destination node (DN). The Intermediate Node (IN) generating the RREP has to provide its Next Hop Node (NHN), and its DRI entry for the NHN. After receiving RREP message from IN, the source node(SN) will check its own DRI table to see whether IN is a reliable node. If source node has used Intermediate Node before to link data, then Intermediate Node is a reliable node and source node starts routing data through Intermediate Node . IN is unreliable and the source node sends FRq message to NHN to verify the identity of the IN, and query to NHN:
1) who is the current NHN's next hop to destination, and
2) has the current NHN routed data through its own next hop node . The NHN in starts responds with FRp message including
a) DRI entry for IN,
b) the next hop node of current NHN,
c) the DRI entry for the current NHN's next hop.
3) if IN has routed data packets through NHN,
Basically based on the FRp message from Next Hop Node(NHN), source node checks whether NHN is a reliable node or not. from the source node has routed data through NHN before, NHN is reliable; or unreliable. NHN is reliable, source node will check whether IN is a black hole or not. If the second bit (ie. IN has routed data *through* NHN) of the DRI entry from the IN is equal to 1, and the first bit (ie. NHN has routed data *from* IN) of the DRI entry from the next hop node(NHN) is equal to 0, Intermediate Node is a black hole. If it is not a black-hole and NHN is a reliable node, the route is safe for the transmission of the packets, and source node will update its DRI entry for IN with 01, and starts routing data via IN. If Intermediate Nodes is a black-hole, the source node informs all the nodes along the reverse path from IN to the node that generated the RREP as black hole nodes. Source node ignores any other RREP from the black holes and broadcasts the list of cooperative black holes. If Next Hop Node is an unreliable node, source node treats current Next Hop Node as Intermediate Node and sends FRq to the updated IN's next hop node and goes on in a loop.

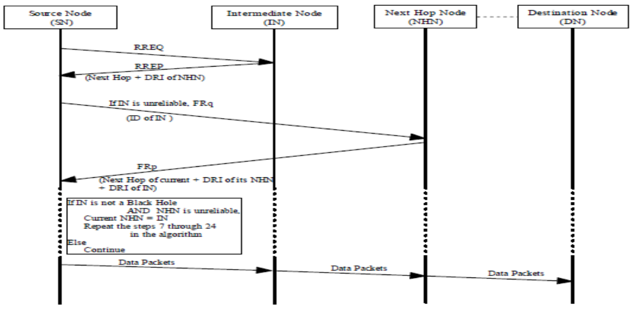

Figure 5- Modified AOVD protocol to prevent cooperative black hole attack.

VIII. CONCLUSION

The goal is achieved after presenting various techniques to avoid Black Hole Attack . the comparative study of the Cross checking and Data Routing Information keeps for the more meaning full object . In the first phase of the paper we achieve the introduction of MANET focusing on DSR (dynamic source routing) , DSDV & AODV focused approach id given for focusing the attacks. Inwards and outwards black hole attackers is also mentioned which includes the arrangement of active and passive attackers. Gray hole , flooding and Selfish node attack is mentioned to enhance the future work. Overall this papers comes to end with the all MANET attackers and few comparative approaches to achieve attack less. The various attack listed will pointing for future work.

REFERENCES

1. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks" Department of Computer Science, IACC 258 North Dakota State University, Fargo, ND 58105.
2. Charles E. Perkins, and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector (AODV) Routing," Internet Draft, November 2002.
3. Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magzine, vol. 40, no. 10, October 2002.
4. S. Marti et al,"Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," 6th Int'l. Conference Mobile Comp. Net., pp. 255-265, August 2000.
5. Vesa Kärpijoki,"Security in Ad hoc Networks," http://www.tcm.hut.fi/Opinnot/Tik-110.501/2000/papers/karpijoki.pdf.
6. Srdjan Capkuny, Levente Butty´an, and Jean-Pierre Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," Technical Report at EPFL, http://ic2.epfl.ch/publications/documents/IC_TECH_REPORT_200234.pdf.
7. Lidong Zhou, and Zygmunt J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no.6, November/December 1999.
8. Janne Lundberg, "Routing Security in Ad Hoc Networks," http://citeseer.nj.nec.com/cache/papers/cs/19440/http:zSzzSzwww.tml.hut.fizSz~jluzSznetseczSz netsec-lundberg.pdf/routing-security-in-ad.pdf
9. P.V.Jani, "Security within Ad-Hoc Networks," Position Paper, PAMPAS Workshop, Sept. 16/17 2002.
10. M.Parsons and P.Ebinger, "Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc networks"
11. D.B.Roy, R.Chaki and N.Chaki, "A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Neworks," International Journal of Network Security and Its Application (IJNSA), Vol. 1, No.1, April, 2009.
12. N.Shanti, Lganesan and K.Ramar, "Study of Different Attacks On Multicast Mobile Ad-Hoc Network".
13. C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks," Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.
14. S.Marti, T.J.Giuli, K.Lai, M.Baker, "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks".
15. Zhu, C. Lee, M.J.Saadawi, T., "RTT-Based Optimal Waiting time for Best Route Selection in Ad-Hoc Routing Protocols," IEEE Military Communications Conference, Vol. 2, pp. 1054-1059, Oct, 2003.
16. M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, "A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks," Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.
17. V.Mahajan, M.Natue and A.Sethi, " Analysis of Wormhole Intrusion attacks in MANETs," IEEE Military Communications Conference, pp. 1-7, Nov, 2008.
18. F.Stanjano, R.Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing," Vol. 35, pp. 22-26, Apr, 2002.

19. H.L.Nguyen,U.T.Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad-Hoc Networks," International Conference on Networking, Systems, Mobile Communications and Learning Technologies, Apr,2006.
20. H.Deng, W.Li and D.P.Agrawal, "Routing Security in Wireless Ad-Hoc Networks," University of Cincinnati, IEEE Communication Magzine, Oct, 2002.
21. K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007
22. G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006
23. S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," International Conference on Computational Intelligence and Security, 2009.

AUTHORS PROFILE

Ms. Shanu singh, is a student of Master of Technology from Gurgaon Institute Of Technology and Management Gurgaon . She is presenting her work over cooperative black hole attack issue as similar her thesis work. Her area of interest is Agile development, mobile technology and s/w project management.

Mr. Amit Kumar Pandey, had done his bachelor of Technology in Electronics And Communication Engineering from Skyline institute of engineering and Technology. He is working as a lecturer under ECE department in BMCTM from past two years. His area of Publications are Wireless communication .

Ms. Minu Rani, a student of Master Of technology under Computer Science and engineering Department final year from Somany Institute Of Technology & Management Rewari . She is Presenting her Second journal over Manet .

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication