International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 1 Issue 1 March 2014

Implementation, Detection and Prevention of Black hole Attack for Mobile ADHOC Network Scenario using NS-2

Anurag Patil
Jabalpur, India
anurag.patil14@outlook.com

Abstract: *- In Manet there are several attacks, The black hole attack is one in every of the well-known security threats in mobile ad hoc networks. The attacker node utilizes the illegal action to hold out their malicious behaviors as a result of the route discovery method is critical and inevitable. Many researchers have conducted totally different detection techniques to propose different types of detection schemes. During this paper, we will suggest an answer for prevention of attacks and discuss the state-of-the-art for various routing strategies. We have a tendency to not solely classify these proposals into single black hole attack and cooperative black hole attack however additionally analyzes the classes of those solutions and provides a comparison table. We have a tendency to expect to furnish additional researchers with an in depth work in anticipation.*

Keywords*: Routing protocols, Black hole attack, Collaborative black hole attack, Mobile ad hoc networks*

1. INTRODUCTION

A Manet may be a assortment of wireless nodes that are movable naturally and even have the power to transfer knowledge with its destination node. Also there's not any mounted infrastructure additionally as no central base station. Thanks to the reason that mobile nodes don't seem to be controlled by any external entity, they need freedom in mobility and connectivity to every alternative. Network management and routing are done reciprocally by each node in network. Due to restricted reception and transmission power, associate degree design is required that is having multi hope environment for one node to communicate with another throughout the network. Generally in multi hop architecture, every node works as a number and as well as a node that forwards packets to other nodes which may not be among an immediate vary for communication. Each router participates in an exceedingly route discovery protocol that finds out multi hop routes through the mobile network between any two communicating nodes. These infrastructures-less mobile nodes dynamically produce routes among themselves to ascertain their own wireless network rapidly. Thus, mobile ad hoc networks give an extremely versatile communication technique for any place wherever geographical or terrestrial constraints are present and want network system with none fastened architecture, like battlefields, and a few disaster management situations. Recent research on Manet shows that the Manet has larger security problems than standard networks [1,2]. Any security solutions for static networks wouldn't be appropriate for MANET. Zhou et al. [1] and Lundberg [3] mentioned several varieties of attacks that may simply be performed against a Manet. Within the black hole attack, malicious nodes provide false routing data to the source node whose packets they need to intercept.

In one another attack referred to as denial of service attacks, malicious node floods the targeted node in order that the network or the node not operates properly. In route table overflow attacks, an attacker tries to create voluminous routes to non existence nodes and overflows the routing tables. In impersonation attack, malicious node could impersonate the other node while causing the request packet to make an anomaly update in routing table. During this paper, we will target the black hole and cooperative black hole attacks. The most contributions of this work are threefold. First, we have a tendency to implement the simulation of the solutions projected for the cooperative black hole attacks. Second, we have a tendency to conjointly add some changes to the algorithm to boost the accuracy in preventing black hole attacks. For instance, previously the algorithm doesn't check current intermediate node for black hole if consequent hop isn't reliable.

This pair of proposed rule doesn't offer any details concerning the implementation of the rule. During this paper we have a tendency to completely describe the implementation details that we address the many problems that aren't considered in [9]. Finally, we have a tendency to are getting to compare the performance of the changed protocol and solution with different existing answers on the idea of various performance matrices like PDR, Throghput,e2e Delay etc.

2. RELATED WORK

The routing protocols projected for MANETs are often classified into four broad classes [4]: Flat routing, Hierarchical routing, GPS routing, and Power based routing. Flat routing is that the most generally used category. These flat routing protocols are often more classified into two main sub groups [6]: table driven and on-demand routing protocols. The table driven routing protocol could be a proactive scheme within which every node maintains consistent and up thus far routing information to each alternative node within the network. Every routing modification within the network ought to be propagated through the network so as to keep up consistent routing information. Within the on-demand routing (reactive routing), any node creates route only when it must send some information to the destination. The source node initiates route discovery process once necessary.

There are three main routing protocols projected for MANETs [4]: ad hoc on demand Distance Vector (AODV) [5] routing, Dynamic source Routing [DSR] [6], and Destination Sequence Distance Vector routing (DSDV) [7]. AODV and DSR belong to on-demand routing protocols and DSDV may be a table-driven routing protocol. during this paper, we tend to target AODV. However, the projected answer is additionally applicable to other on-demand protocols, like DSR. The AODV protocol is susceptible to the well-known black hole attack. A black hole may be a node that continuously responds positively with a RREP message to each RREQ, even though it International Journal of package Engineering and Its Applications doesn’t very have a sound route to the destination node. Since a black hole node doesn't have to check its routing table, it's the primary to respond to the RREQ in most cases. Then the source routes information through the part node, which will drop all the data packets it received instead of forwarding them to the destination. During this manner the malicious node will simply misroute heap of network traffic to itself and will cause associate attack to the network with little or no effort thereon.

These black hole nodes may go as a bunch. Which means over one black hole nodes work hand and glove to mislead other nodes? This kind of attack is termed cooperative black hole attack. Researchers have proposed solutions to spot and eliminate black hole nodes. Deng et al. planned an answer for individual black holes. However they need not thought-about the cooperative black hole attacks. Consistent with their solution, information regarding succeeding hop to destination ought to be enclosed within the RREP packet once any intermediate node replies for RREQ. Then the source node sends an additional request (FREQ) to next hop of replied node and asks about the replied node and route to the destination. By mistreatment this technique we will identify trustiness of the replied node given that the next hop is trusted. However, this resolution cannot prevent cooperative black hole attacks on MANETs. For example, if succeeding hop additionally cooperates with the replied node, the reply for the FREQ are going to be merely “yes” for each queries. Then the source can trust on next hop and send information through the replied node which may be a black hole node. Ramaswamy et al. proposed an answer to defensive against the cooperative black hole attacks. no simulations or performance evaluations are done. Ramaswamy et al. studied multiple black hole attacks on mobile ad hoc networks. However, they only considered multiple black holes, within which there's no collaboration between these black hole nodes. In this paper, we tend to value the performance of the planned scheme in defensive against the collaborative black hole attack.

Yin et al. planned an answer to defending against black hole attacks in wireless sensor networks. The state of affairs that they thought of in sensor networks is kind of completely different than MANETs. They think about the static sensing element network with manually deployed cluster heads. They failed to consider the mobility of nodes. Additionally they need one sink node and every one sensors send all the info to the sink. Each node must resolve the route solely to the sink. Since this scenario isn't compatible with MANET, we tend to don't seem to be progressing to discuss it more. In this paper we tend to simulate the rule proposed with several changes to enhance the accuracy of preventing cooperative black hole attacks and to improve the efficiency of the method.

2.1. Black Hole Attack

In this attack a malicious node may advertise an honest path to a destination throughout routing method. The intention of the node is also to hinder the trail finding method or interpret the packet being sent to destination. Alternatively black-hole scenario is also outlined because the one within which the cannel properties tend to be asymmetric i.e. the signal strength in each direction might not be same. In this case a node that receives the data packet however will not forward it's termed as black hole. In either case the normal operation of the Manet is noncontiguous.

2.2 Wormhole attack

During this attack, an attacker receives packets at one location and tunnels them at another location wherever these packets are resent into the network. Within the absence of correct security mechanisms, most of the prevailing routing protocols may fail to search out the valid routes. Byzantine attack: Here compromised intermediate nodes carries out attack like loops, routing packets on non best methods and by selection dropping packets.

2.3 Information disclosure

A compromised network node could leak the necessary or confidential information like network topology, geographical information of nodes and best routes to the nodes etc.

2.4 Resource consumption attack

An attacker node acting as intermediate node could initiate extra request for routes, frequent generation of beacon packets or forwarding stale routes to nodes. This result in over consumption of nodes restricted resources and keeps the node extra occupied. In this paper we have a tendency to analyze the impact of the presence of the black-hole nodes on the painter performance. We have found that because the proportion of black hole nodes increases, the network performance degrades.

3. AD-HOC ROUTING PROTOCOLS AND BLACK HOLE ATTACK

An ad-hoc routing protocol[8] could be a convention, or standard, that controls however nodes decide that means to route packets between computing devices during a mobile unexpected network. Being one in every of the class of ad-hoc routing protocols, on-demand protocols such as AODV [4] (Ad-hoc on demand Distance Vector) and DSR (Dynamic source Routing) establish routes between nodes only they're needed to route data packets. AODV is one in every of the foremost common ad hoc routing protocols used for mobile ad-hoc networks. As its name indicates AODV is an on demand routing protocol that discovers a route solely when there's a requirement from mobile nodes within the network.

In an ad-hoc network that uses AODV[4][6] as a routing protocol, a mobile node that desires to communicate with alternative node first broadcasts an RREQ (Route Request) message to search out a recent route to a desired destination node. This method is termed route discovery each neighboring node that receives RREQ broadcast first saves the trail the RREQ was transmitted on to its routing table. It afterwards checks its routing table to envision if it's a recent enough routes to the destination node provided within the RREQ message. The freshness of a route is indicated by a destination sequence number that's connected to that. If a node finds a recent enough route, it unicast an RREP (Route Reply) message back on the saved path to the source node or it re-broadcasts the RREQ message otherwise. Route discovery could be a vulnerability of on-demand ad-hoc routing protocols, especially AODV that an adversary will exploit to perform a black hole attack on mobile ad-hoc networks. A malicious node within the network receiving an RREQ message replies to source nodes by causing a fake RREP message that contains fascinating parameters to be chosen for packet delivery to destination nodes. After promising (by causing a fake RREP to substantiate it has a path to a destination node) to supply nodes that it'll forward information, a malicious node starts to drop all the network traffic it receives from source nodes. This deliberate dropping of packets by a malicious node is what we tend to call a black hole attack.

CONCLUSION

In this paper, we studied the matter of black hole attacks under Manet scenario. Due to the unspecified design there are several limitations of routing protocol in MANETs; several researchers have conducted numerous techniques to suggest completely different types of prevention mechanisms from black hole problem under Manet scenario. The proposals are proposed in a very illogical order and divided into single black hole and cooperative black hole attack. According to this work, we observe that how the AODV routing protocol works and then implemented black hole attack on it at the same time a trust based mostly mechanism for its prevention. The trust based mostly detection methodology has the higher packet delivery ratio and correct black hole node detection probability, but suffered from the upper routing overhead due to the periodically broadcast packets. the opposite planned method that is reactive detection method eliminates the routing overhead problem from the on demand way of route generation. Our complete implementation reveals that the planned methodology of trust mechanism once applied on AODV protocol gives better results in all the cases for Manet as compared with traditional AODV just in case of black hole attack.

References

[1]. C. E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,” Computer Communications Review, pp. 234-244, October 1994.

[2]. Hongmei Deng, Wei Li, and Dharma P. Agrawal, “Routing Security in Wireless Ad Hoc Network,” IEEE Communications Magzine, vol. 40, no. 10, October 2002.

[3]. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”, 2003 International Conference on Wireless Networks (ICWN’03), Las Vegas, Nevada, USA

[4]. Jian Yin, Sanjay Madria, “A Hierarchical Secure Routing Protocol against Black Hole”, IEEE SUTC 2006 Taiwan, 5-7 June 2006.

[5]. Xiaoyan Hong, Kaixin Xu, and Mario Gerla, “Scalable Routing Protocols for Mobile Ad hoc Networks,” IEEE Network Vol. 16(4) pp11-21, July/August 2002.

[6]. Elizabeth M. Royer and Chai-Keong Toh, “A Review of Current routing Protocols for Ad Hoc Mobile Wireless Networks,” IEEE Personal Communications, pp 46-55, April 1999.

[7]. Sanjay Ramaswamy, Huirong Fu, and Kendall E. Nygard, “Simulation Study of Multiple Black Holes Attack on Mobile Ad Hoc Networks,” International Conference on Wireless Networks (ICWN’ 05), Las Vegas, Nevada, Jun. 2005.

[8]. H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, ―Security in mobile ad hoc networks: Challenges and solutions‖ (2004). IEEE Wireless Communications. 11 (1), pp. 38-47.

[9]. Hao Yang,Haiyun Luo, Fan Ye, Songwu Lu, Lixia Zhang,"Security in mobile ad hoc networks: challenges and solutions",Wireless Communications, IEEE Feb 2004.

[10]. Hongmei Deng, Wei Li, D.P.Agrawal,"Routing security in wireless ad hoc networks",Communications Magazine, IEEE Oct 2002.

[11]. B.Kannhavong, H.Nakayama, Y.Nemoto, N.Kato, A.Jamalipour,"A survey of routing attacks in mobile ad hoc networks",Wireless Communications, IEEE October 2007.