A SURVEY BLACK HOLE ATTACK IN MANET

Arshdeep kaur[1*] Mandeep kaur[2*]

[1*]Student, Guru Kashi University Talwandi Sabo, Bathinda (PB.)

[2*]Asst Prof, Guru Kashi University Talwandi Sabo, Bathinda(PB.)

ABSTRACT

The black hole attack is single of the well known safety intimidation in wireless mobile ad hoc networks. The intruder operates the get-out to carry out their spiteful behaviors since the route finding development is compulsory and foreseeable. Many reviews have conduct unlike uncovering technique to recommend unlike types of finding scheme. In this article, we investigation the offered solution and converse the state of the drawing routing methods. We in attendance two potential solutions. The first is to discover more than one route to the purpose. The second is to develop the packet series number built-in in any packet header. Processor simulation shows that compare to the original ad hoc on-demand distance vector routing scheme, the second solution can verify 75% to 98% of the route to the purpose depending on the silence times at a least amount cost of the holdup in the networks.

KEYWORDS: MANET, routing protocols, black hole attack, mutual black hole attack, AODV Protocol.

1. INTRODUCTION

Wireless mobile ad hoc network is a self configuring network which is collected of several variable user tools. These mobile nodes converse with each other with no any communications, furthermore, all of the broadcast links are established through wireless average. According to the message mode mention before. MANET is extensively used in armed purpose, tragedy area, personal area system and so on [1]. Though, there are still many open issues about MANETs, such as security problem, finite transmission bandwidth, rude sharing messages, reliable data release, dynamic link establishment and controlled hardware caused processing ability. The safety coercion have been extensively discuss and investigate in the wired and wireless networks, the likewise perplexing circumstances has also happen in MANET due to the intrinsic aim defects. There are numerous security issues which have been calculated in recent years. For case, questioning attacks, wormhole attacks, black hole attacks, routing table overflow and

poisoning attacks, packet duplication, denial of service attacks, disseminated DoS attacks, et cetera [2]. Particularly, the misconduct routing problem is one of the popularized security intimidations such as black hole attacks. Some recommend their secure routing idea to solve this topic, but the sanctuary problem is still not capable to stop totally.

In this document, we focus on dissimilar types of black hole attacks in MANET which can be alienated into ordinary black hole attack and joint black hole attack. Furthermore, several detection schemes are discussed clearly and comparably. The assessment metrics of routing protocol include packet delivery ratio, mobility difference with total number of errors, packet routing in the clouds, end-to-end delay by varying in node density [2].

1.1 BLACK HOLE ATTACK

In current years the alarm over the security of computer networks has been extensively discuss and popularized. The conversation has, however, characteristically concerned only still and wired network while the portable or ad-hoc networking issue have not been handled lengthily. The appearance of such new networking approach sets new challenge even for the basics of routing since MANET are considerably diverse from the wired networks. In addition, the established routing protocols of the Internet have been premeditated for routing the traffic between wired hosts coupled to a inert backbone; thus, they cannot be functional to ad hoc networks because the basic idea of such networks is mobility with lively topology[3].Black hole attack is denial of service attack in which hateful node send fake in order by claim that it has a fresh or straight route to purpose node and hence source nodes select this straight path and go through this hateful node and result data mistreatment or superfluous [4]. Once the route is set up, at the instant it's up to the node whether to drop the entire packet or recognizable it to the nameless address. This special node, which disappears the data packet, is named as spiteful nodes.

Black hole problem in MANETS is a serious security problem to be solved. In this problem, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. In flooding based protocol, if the malicious reply reaches the requesting node before the reply from the actual node, a forged route has been created. This malicious node then can choose whether to drop the packets to perform a denial-of-service attack or to use its place on the route as the first step in a man-in-the-middle attack.
Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network

and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self configuration ability, they can be deployed urgently without the need of any infrastructure. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols. Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed for MANETS, i.e. AODV, OLSR, DSR etc.

Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats[5].

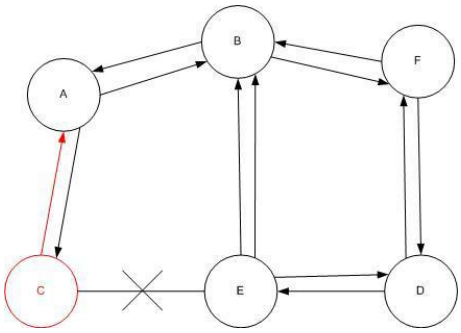

Figure 1.1: Black hole attack

1.2 PREVIOUS TECHNIQUES:

1.2.1 DSR

DSR is an on-demand, source routing protocol. It is an on-demand protocol because routes are discovered at the time a source sends a packet to the destination for which it has no cached route. DSR has two main functionalities: route discovery and route maintenance. The basic approach of this protocol during the route discovery phase is to establish a route by flooding Route Request (RREQ) packets in the network. The destination node, on receiving a RREQ packet, responds by sending a Route Reply (RREP) packet back to the source by reversing the route information stored in the RREQ Packet. On receiving the RREQ, any intermediate node can send the RREP back to the source node if it has the route to reach the destination. During the Route maintenance phase, the link breaks are handled. A link break occurs when any intermediate node which involves in the packet forwarding process moves out of the transmission range of its upstream neighbor [6]. If an upstream node detects a link

break when forwarding a packet to the next node in the route path, it sends back a route error (RERR) message to the source informing it of that link break. The source either tries an alternate path available or initiates the route discovery process again.

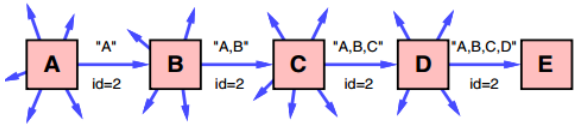

Figure no: 1.2.1 Route discovery

1.2.2 Bacterial Foraging Optimization Algorithm (BFO):

Bacteria Foraging Optimization (BFO) algorithm is a novel class of in nature certain stochastic global search method based on imitate the foraging actions of E.coli bacteria. This method is used for locate, conduct, and ingesting the food. Through foraging, a bacterium can exhibit two unlike events: dropping or swim. The topple action modify the direction of the bacterium. During swim means the chemo taxis step, the bacterium will move in its recent direction. Chemo taxis society is continuous until a bacterium goes in the way of positive-nutrient gradient. Following a sure number of complete swims, the best halve of the population undergo the simulation and eradicate the rest of the population. In order to run off local optima, an ending dispersion event is carried out where some bacteria are clear up at random with a very small opening and the new stand-in are initialized at random locations of the search space[7].

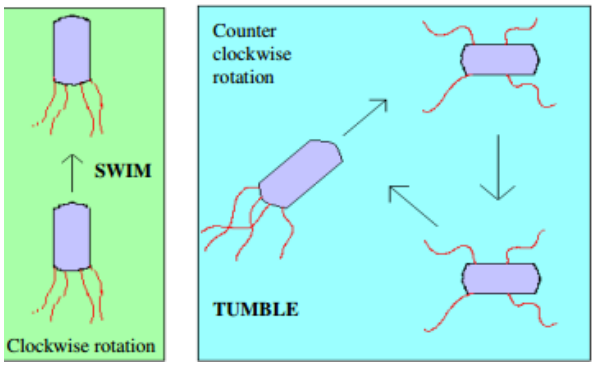

Figure no: 1.2.3 Bacterium

1.2.3 AODV

AODV orchestrates a course to a destination just when a hub needs to send a bundle to that destination. Courses are kept up the length of they are required by the source. Grouping numbers guarantee the freshness of courses and certification the circle free directing. AODV additionally gives topology data to the hub. AODV manufactures courses utilizing a course ask for/ course answer question cycle. At the point when a source hub fancies a course to a destination for which it doesn't have a course, it shows a course ask for (RREQ) bundle over the system. Hubs getting this parcel overhaul their data for the source hub and set up in reverse pointers to the source hub in the course tables. Notwithstanding the source hub's IP address, current succession number, and show ID, the RREQ likewise contains the latest grouping number for the destination of which the source hub is mindful.

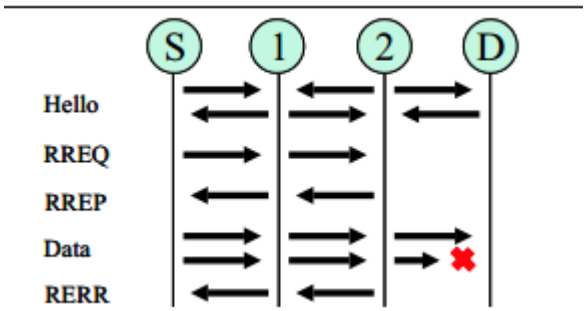

Figure no: 1.2.3 AODV protocol Message

2. TECHNIQUES USED:

TECHNIQUES AND PROTOCOL	ADVANTAGES	DISADVANTAGES	PARAMETERS
Data Routing Information Technique, AODV	It can detect misbehavior at forwarding level	It can't detect ambiguous collision, selfish nodes, partial dropping[13]	Delay =35 sec Throughput 86 % Packet delivery ratio 80%
Clustering Algorithm AODV	Detect the misbehavior node and isolate the node in network [14]	Some overhead in terms of calculation of maturity level	Route request 1.9 % Route replay verification 1.5%
RREP and RREQ based weight updation algorithm AODV	It is simple and efficient according to the obtained performance enhancement[15]	Calculation of trust is complex	Packet Delivery ratio = 87%
Acknowledgement signaling Packet sequencing AODV,DSDV,DSR	Find a secure end route based on collaborative effort of nodes in MANET	Dynamic calculation of trust is not present[16]	RREQ= 2.5 Verification= 1.5 Delay =0.1 sec

3. RELATED WORK

Swagatam Das, Arijit Biswas[6],2010 Bacterial foraging optimization algorithm has been extensively established as a global optimization algorithm of existing notice for distributed optimization and control. BFOA is encouraged by the social foraging behavior of Escherichia coli. BFOA has by now drawn the awareness of researchers because of its competence in solving real-world optimization problems arise in numerous application domains. The basic biology behind the foraging approach of E.coli is emulated in a surprising manner and used as a simple optimization algorithm. This chapter starts with a logical

sketch of the classical BFOA. It then analyses the dynamics of the replicated chemo taxis step in BFOA with the help of a simple numerical model.

Passino, Kevin M[7],2010, This Article described by the Bacterial Foraging Optimization Algorithm belongs to the field of Bacteria Optimization Algorithms and Swarm Optimization, and more generally to the fields of Computational Intelligence and Met heuristics. It is interrelated to other Bacteria Optimization Algorithms such as the Bacteria Chemo taxis Algorithm, and other Swarm Intelligence algorithms such as Ant Colony Optimization and Particle Swarm Optimization. There have been many extensions of the approach that attempt to hybridize the algorithm with other Computational Intelligence algorithms and Met heuristics such as unit Swarm Optimization, Genetic Algorithm, and Tab Search.

Harley et.al [8], 2003, showed that Because of the rapidly increasing network technology there is an increased need for security of that technology. As a result, intrusion detection has become an important technology market. According to industry estimates, the market for intrusion detection systems grew from $40 million in 1997 to $100 million in 1998. This growth was driven by reports of increasing security breaches. Graph 1 indicates a disturbing increase in the number of incidents reported from 2000 through the 2nd quarter of 2003. However, this market is low compared to the cost of malicious code, as Chart 1 describes. And as graph 2 indicates, vulnerabilities are also on the rise, with an alarming increase over the past few years, and the first and second quarters of 2003. With the costs of damages combined with the increasing possibility of intrusion, there is a great need for intrusion detection systems.

Sheenu et. al [9],2009, investigated the effects of Black hole attacks on the network performance. We simulated Black hole attacks in Qualnet Simulator and measured the packet loss in the network with and without a black hole. The simulation is done on AODV (Ad hoc On Demand Distance Vector) Routing Protocol. The network performance in the presence of a black hole is reduced up to 26%.

Ahmed Shariff et . al [10],2013 showed Mobile Ad-Hoc Networks (MANETs) are characterized by the lack of infrastructure, dynamic topology, and their use of the open wireless medium. Black-hole attack represents a major threat for such type of networks. The purpose of this paper is two folds. First, to present an extensive survey of the known black-hole detection and prevention approaches. Another objective is to present new dimensions for their classification.

Pietro et. al [11],2002, provides a simulation study that identifies security issues that are specific to MANET and that illustrate the effects of those threats on network performance when

the DSR routing protocol is used. We focused our attention on the evaluation of network performance in terms of global throughput and delay of a mobile ad hoc network where a defined percentage of nodes behaved selfishly. The simulation study brought up two important conclusions. First, it shows that security issues have to be taken into account at the early stages of a routing protocol design. Indeed, when no countermeasures are taken, the simulation results showed that network operation and maintenance can be easily jeopardized and network performance will severely degrade. Second, a cooperative security scheme seems to be a reasonable solution to the selfishness problem: a selfish behavior can be detected through the collaboration between a number of nodes assuming that a majority of nodes do not misbehave.

Dokurer et. al [12],2007, investigated the effects of Black Hole attacks on the network performance. We simulated black hole attacks in Network Simulator 2 and measured the packet loss in the network.

4. CONCLUSION

Black hole attacks in wireless can be prohibited using different protocols and optimization algorithms so that data can be securely transferred from source to destination. Black hole attack is a huge hazard to the security of mobile ad hoc networks. In this paper, we suggest a scheme to detect black hole attack in MANETs namely cluster based DSR Protocol which bring clustering in the route discovery phase of DSR protocol. The projected manners is simple and well-organized and also provide better values for packet drop ratio and discovery rate as compare to obtainable scheme in imitation results.

REFERENCES:

[1] Marti, Sergio, et al. "Mitigating routing misbehavior in mobile ad hoc networks."Proceedings of the 6th annual international conference on Mobile computing and networking. ACM, 2000.

[2] Tseng, Fan-Hsun, Li-Der Chou, and Han-Chieh Chao. "A survey of black hole attacks in wireless mobile ad hoc networks." Human-centric Computing and Information Sciences 1.1 (2011): 1-16.

[3] Al-Shurman, Mohammad, Seong-Moo Yoo, and Seungjin Park. "Black hole attack in mobile ad hoc networks." Proceedings of the 42nd annual Southeast regional conference. ACM, 2004.

[4] Kaur, Harjeet, Manju Bala, and Varsha Sahni. "Study of Blackhole Attack Using Different Routing Protocols in MANET." International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering2.7 (2013): 3031-3039.

[5] Wang. Yu , "Using Fuzzy Expert System based on Genetic Algorithm for Intrusion Detection System", April 2009.

[6] Anup Goyal and Chetan Kumar, " GA-NIDS: A Genetic Algorithm based Intrusion Detection System", 2010.

[7] Yuteng Guo, Beizeng Wang, Xingxing Zhao, Xiaobiao Xie, Lida lin and Qinda Zhou,"Feature Selection based on Rough Set and modified Genetic programming for Intrusion Detection", In 33 ICRTIT-2012 proceedings of 5th International Conference of
Computer Science and Education. August 2010.

[8] Harley Kozhushko, "Intrusion Detection: Host Based and Network-Based Intrusion Detection Systems", 2003.

works under black hole attacks".Proceedings IEEE Volume, Issue, 22-25 March 2007 Page(s):148 –153.

[13] Ankur mishra1, Ranjeet Jaiswal2, Sanjay Sharma," A Novel Approach for Detecting and Eliminating
Cooperative Black Hole Attack using Advanced DRI Table in Ad hoc Network", IEEE, , 2012978-1-4673-4529-3/12/$31.00_c.

[14]Shahid Shehzad Bajwa et.al," Grouped Black hole Attacks Security Model (GBHASM) for Wireless Ad-Hoc Networks", IEEE,2010, vol-1 , 978-1-4244-5586-7

[15] Rajesh Yerneni,et,al," Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc Networks",IEEE, ICCCNT' 12 26th _28th July 2012, Coimbatore, India.

[9] Sheenu Sharma and Roopam Gupta, "Simulation Study of Black hole Attack in Mobile Adhoc Networks", In proceedings of Engineering Science and Technology. 2009.

[10] Ahmed Sherif, Maha Elsabrouty. Amin Shoukry, "A Novel Taxonomy of Black-Hole Attack Detection Techniques in Mobile Ad-hoc Network (MANET)", IEEE, pp: 346-352, 2013.

[11] P. Michiardi, R. Molva. "Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks". European Wireless Conference, 2002.

[12] Dokurer, S.; Erten Y.M., Acar. C.E., SoutheastCon Journal, "Performance analysis of ad-hoc net

[16] Ms.Nidhi Sharma et.al," The Black-hole node attack in MANET", 2012 Second International Conference on Advanced Computing & Communication Technologies.

