INTERNATIONAL RESEARCH JOURNAL OF MATHEMATICS, ENGINEERING AND IT
VOLUME -1, ISSUE -2 www.aarf.asia ISSN No. : (2349-0322)

A SURVEY PAPER ON DETECTION AND PREVENTION OF BLACK HOLE IN MANET

Mr. Abhisek Kumar,
Student [M.Tech. CSE]
Galgotias University, Plot No-17A Greater Noida, India.

ABSTRACT

The black hole attack is one of the common security threats in wireless mobile ad hoc networks. The intruders utilize the loophole to carry out their malicious behaviors because the route discovery process is necessary and inevitable. Many researchers have conducted different detection techniques to propose different types of detection schemes. In this paper, we survey the existing solutions and discuss the state-of-the-art routing methods. We not only classify these proposals into single black hole attack and collaborative black hole attack but also analyze the categories of these solutions and provide a comparison table. We expect to furnish more researchers with a detailed work in anticipation.

Keywords

Mobile ad hoc networks, routing protocols .single black hole attack

1. Introduction

Mobile Ad Hoc Network (MANET) consist of mobile devices that are capable communicate to each other without any centralized system. MANET is self organized not fixed infrastructure, automatic self configuration, quick deployment etc. It is particularly vulnerable due to its fundamental characteristics such as open medium, dynamic topology, distributed cooperation, and constrains capabilities [1] [2]. One of popular routing protocol is Ad-hoc on demanding vector (AODV) [1]. According the discussion in [2], it is suitable for applying in high mobility devices, which the network topology is changed frequently. Due to mobility of nodes, routing path for communication may be disrupted. Mobile nodes have to discover and setup a routing path first when data communication is needed. In such a environment, malicious nodes have

INTERNATIONAL RESEARCH JOURNAL OF MATHEMATICS, ENGINEERING AND IT
VOLUME -1, ISSUE -2 www.aarf.asia ISSN No. : (2349-0322)

many opportunities to join the process of setup routing path. Therefore security problems should be paid more attention. In AODV routing protocol, source node broadcasts a Route Request (RREQ) message including a sequence number to discover a routing path to destination. The purpose of sequence number is used to identify freshness of routing paths. That is the more large sequence number, the more fresh routing path. On receiving RREQ message, intermediate nodes will check where there exists a fresh routing path destined to destination nodes in their routing table. If the sequence number of routing path in routing table is larger than or equal to the sequence number of RREQ, then a Route Reply(RREP) will be sent and propagate back to source node. Otherwise, RREQ message will be broadcasted to neighboring nodes toward destination node. Therefore malicious node can easily reply a faked RREP message with large sequence number to spoof the source node. Then malicious node can be on the path from source to it, even there is not a real path from it to destination node. Packets from source node may be dropped by the malicious node; it is a well-known black holes problem [3].

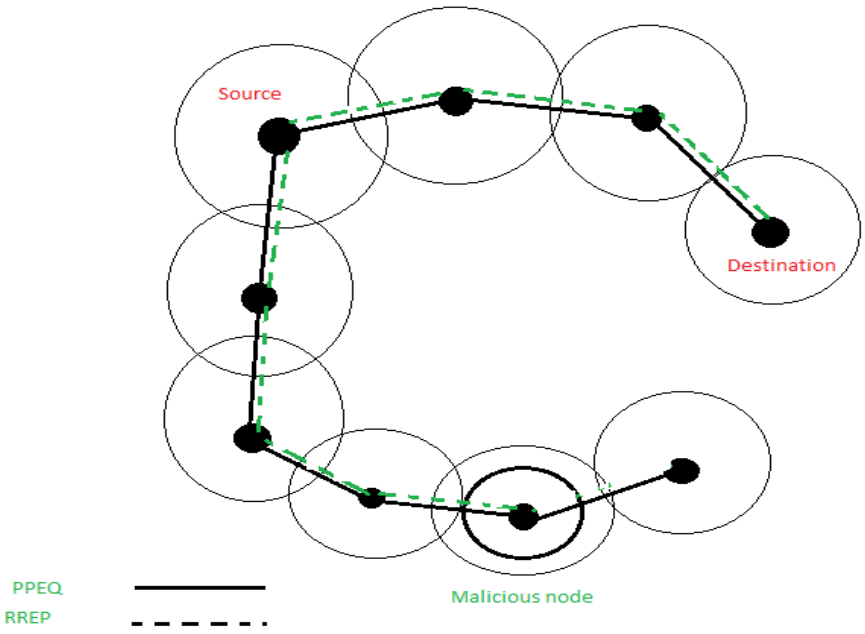

Figure 1. Malicious node behavior in a network

INTERNATIONAL RESEARCH JOURNAL OF MATHEMATICS, ENGINEERING AND IT
VOLUME -1, ISSUE -2 www.aarf.asia ISSN No. : (2349-0322)

2. Back ground

Nodes communicate with each other by sending RREQ to their neighbors. Each neighbors reply with RREP when they got route from the destination node. On the basis of characteristic of route, they are classifying in three categories.

a. Proactive (table driven) routing protocol:

In proactive protocol, mobile nodes periodically broadcast their routing information to the neighbors. Each node need to maintain the routing table which not only records the adjacent nodes and reachable nodes but also number of hopes. Ex. - destination sequence distance vector (DSDV) and optimized link state routing (OLSR) [7].

b. Reactive (on-demand) routing protocol:

Unlike the proactive routing, the reactive routing is simply started when nodes desired to transmit data packet. The strength is that the wasted bandwidth include from the cyclically broadcast can be reduced. Ex – ad hoc on demand distance vector (AODV) and dynamic source routing (DSR) [7].

c. Hybrid routing protocol:

Hybrid protocol combines the advantages of proactive and reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The choice of one or the other method requires predetermination for typical cases. Ex – Zone routing protocol (ZRP) [9].

Security issues research is very immerging field in the MANET. MANET supports to connectivity to internet so attackers can easily attack on the MANET, it not necessary to attackers are belong from the same network or just neighbor node. There are several attacks in this so we can classify it in layered manner

INTERNATIONAL RESEARCH JOURNAL OF MATHEMATICS, ENGINEERING AND IT
VOLUME -1, ISSUE -2 www.aarf.asia ISSN No. : (2349-0322)

Serial no.	Layers	Attacks
1.	MAC layer	Malicious Behavior, Selfish Behavior, Active, Passive, Internal External
2.	Physical layer attack	Jamming, interruption, eavesdropping
3.	Network layer	Black hole attack, Gray hole attack, Wormhole attack, Information discloser, Message altering, Sending data to node out, Transmission range, Routing attacks.
4.	Transport layer attacks	Session hijacking , SYN flooding
5.	Application layer attacks	Repudiation, Data corruption.
6.	Others	DOS, Impersonlasation, Device terming, reply, Man in the middle.

Table1- table contain the list of layered attach in the networks.

3. Black hole attack

INTERNATIONAL RESEARCH JOURNAL OF MATHEMATICS, ENGINEERING AND IT
VOLUME -1, ISSUE -2 www.aarf.asia ISSN No. : (2349-0322)

Black hole attack is very common attack in the MANET. An attacker use the routing protocol to advertise it as having shortest path compare to all RREP (highest sequence number and lowest hope count). In the figure-[2] see that if a source node broadcast RREQ and wait for the RREP, malicious node reply RREP to sender with highest sequence number and lowest hope count, if the RREP come from the actual node then nothing going wrong but when malicious node reply first then source node think to this is shortest path and ignore all the later RREP so send data to malicious node and attackers perform a DOS on the data [6][9].

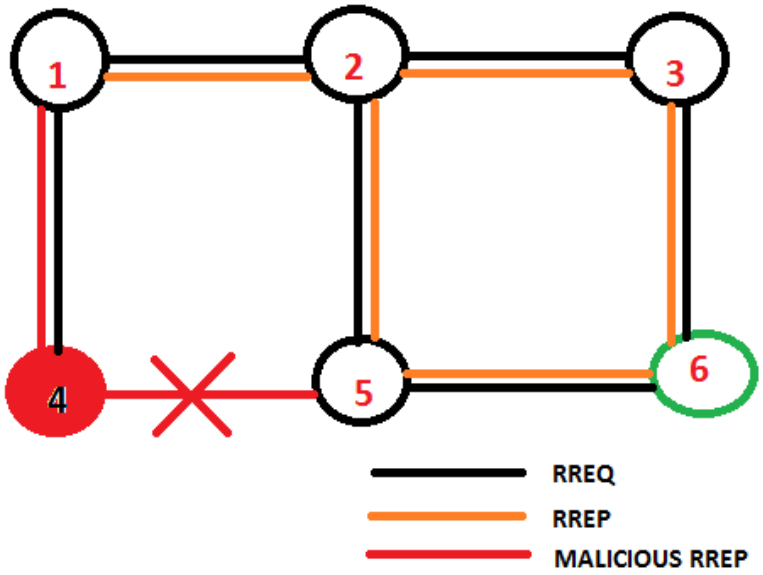

Figure 2- The black hole problem with 6 nodes where node 4 is a malicious node.

4. Related work

A novel automatic security mechanism proposed by authors [1] to detect/find out the black hole attack (malicious node) by the help of the behavior/performance of the intermediate nodes. Authors proposed method called Support Vector Machine (SVM) on using AODV routing protocol. Technique in SVM method, behavior of the node on the basis of the PDED (Pocket delivery ratio), PMOR (pocket modifying ratio) and PMSIR (pocket misroute ratio). A standard ratio defines for this above ratio on the basis of previous. So if node not follows the standard, that node is malicious node or black hole.

INTERNATIONAL RESEARCH JOURNAL OF MATHEMATICS, ENGINEERING AND IT
VOLUME -1, ISSUE -2 www.aarf.asia ISSN No. : (2349-0322)

A technique for prevention from the Black Hole attack on AODV routing protocol for MANET, created by authors [2]. Method use promiscuous mode to detect malicious node and if yes, broadcast the presence of malicious node in the network. If the intermediate node send a PPER to the source then a node providing to the node which sent RREP pocket switch on its promiscuous mode and send a *hello* message to the destination node through the intermediate node which is RREP. If it is legitimate node then message forward from it to the destination node else it's a malicious node and broadcast a message to it's a malicious node and source refresh its route table and find again new route by broadcasting RREQ .

Meenakshi et al. [3] introduced an approach to detect and prevent from the MANET flooding attack. Authors used a Pocket Delivery Ratio (PDER), Control Overhead (CO) and Pocket Misroute Ratio (PMIR) behavior of the node to define the flooding attack. If a node send RREQ without considering the RREQ_RATELIMIT within per second. Due to flooding attack nodes route table full by the bogus RREQ , so it not perform operation on the actual RREQ and misrouting the packet is consider and read the behavior and create a matrix to read it, by it author defines nodes are me litigate or malicious.

Authors [4] developed a novel approach to avoid the malicious node attack in MANET. Malicious node adversities that I have the greatest sequence number and lowest hope count. Proposed approach, each RREP have extra three properties such as node ID, PPN number and cluster head ID. Each cluster head maintain a neighbor table which is keep information about the entire node. Neighbor table maintain the node ID and cluster head ID. Each node in the network has a specific prime number which acts as node Identity and this identity must not be change.

A novel method described in research paper [5] called source routing discovery to prevent black hole attacks (SRD-AODV). Author define the Threshold, minimum and maximum number of nodes on the network. The Threshold id also defines in small, medium and large environment and have malicious node in this environment respectively 6%, 4% and 2%. Malicious node

INTERNATIONAL RESEARCH JOURNAL OF MATHEMATICS, ENGINEERING AND IT
VOLUME -1, ISSUE -2 www.aarf.asia ISSN No. : (2349-0322)

always generate the greatest sequence number because malicious do not know the destination sequence number and if the sequence number is greater than the total number of node in the network so we easily find out the malicious node or black hole attack in the network. Here authors compare the malicious sequence number with the Threshold Number. If sequence number is greater than the Threshold Number, it's a malicious node and need to broadcast that node is malicious node and rebroadcast the RREQ.

In paper [6] authors proposed a method for identification of the black hole in the network by authentication mechanism. It's a prevention mechanism. In this authentication based on the Hash function, message authentication code (MAC), and pseudo random function (PRF) on the top of the AODV routing protocol. It's a faster approach to identification of malicious node. The technology used in this paper say that when RREP generated by the destination node at the time RREP message encrypt and sends to the intermediate node with public key and private key. At each intermediate node take the packet and just forward it. When it reaches at the source node then using private key, open the packet. Before the open the packet it check the packet is same as the send packet. If the message packet (RREP) is affected then just discard it and broadcast the fresh RREQ to the neighbor node and broadcast a message to detect a malicious node in the network.

Authors Proff. Sanjeev Sharma et al [7] proposed a technique to detection of the black hole attack in manet called Secure-ZRP protocol which can used to prevent from black holes in zones and out zones. Authors divided the security in two group (a) local communication attack, inside the zones (b) when inter zone communication, outside the zones. In local communication source node broadcast the bluff probe packet. This contains the address of the destination but in actual this is the address of non existence node. This message is directly revised by the neighbor node. If the malicious node present in the zone it will give immediate response to the source node.

Authors Mr. Golak Panda et al [8], introduced a algorithm on the authentication manner to prevent the black hole in manet. Using AODV protocol authors sends a HELLO message is

INTERNATIONAL RESEARCH JOURNAL OF MATHEMATICS, ENGINEERING AND IT
VOLUME -1, ISSUE -2 www.aarf.asia ISSN No. : (2349-0322)

broadcast to its neighbor node and a routing table maintain by the all nodes for the temporary basis in active state. The total bits consume by this route discovery and route maintenance is 32 bit each. But here both RREQ and RREP packets the 9 bit is reserve sector will be there. This proposed algorithm is based on the key mechanism process. First is key generation process in this process use 12 digit left shift of binary number and AND operator for reshuffling and this will fitted in 9 bit reserve sector packet. Second is key authentication process here after comparison both the key the trust value will be decided.

Caparison of all above related papers

Scheme	Routing Protocol	Simulator	Detection Type	Publish Year	Result	Defects
Behavioral approach	AODV	NS-3.14	Single detection	2013	Increase pocket delivery ratio	Take more time in comparison
Comparison technique	AODV	Qual net	Single detection	2013	Throughput increase 40%.	Also increase end-to-end delay and network overheads.
Behavioral matrices using SVM	AODV	NS-3	Single detection	2013	Increase pocket delivery ratio and high throughput	Decrease the network overheads.

INTERNATIONAL RESEARCH JOURNAL OF MATHEMATICS, ENGINEERING AND IT
VOLUME -1, ISSUE -2 www.aarf.asia ISSN No. : (2349-0322)

Avoiding technique	AODV	MATLAB	Single detection	2013	By CRCMD&R scheme improve throughput 75% from 40% provided by AODV	More network overload and time delay.
Verification technique using SRD-AODV	AODV	NS-2	Single detection	2013	PDR increased by 88-97%	Need more comparison so time dely.
Encryption technique using hash-function	AODV	NS-2	Single detection	2008	Throughput increase	Also increase detection time so time delay.

Table 2- contain the summary of the related work summery.

5. Conclusion and Future Work

Due to the inherent design disadvantages of routing protocol in MANETs, many researchers have conducted diverse techniques to propose different types of prevention mechanisms for black hole problem. In this paper, we first summary the pros and cons with popular routing protocol in wireless mobile ad hoc networks. Then, the state-of-the-art routing methods of existing solutions are categorized and discussed. The proposals are presented in a chronological order and divided into single black hole and collaborative black hole attack. According to this

work, we observe that both of proactive routing and reactive routing have specialized skills. The proactive detection method has the better packet delivery ratio and correct detection probability, but suffered from the higher routing overhead due to the periodically broadcast packets. The reactive detection method eliminates the routing overhead problem from the event-driven way, but suffered from some packet loss in the beginning of routing procedure. Therefore, we recommend that a hybrid detection method which combined the advantages of proactive routing with reactive routing is the tendency to future research direction. However, we also discover that the attacker's misbehavior action is the key factor. The attackers are able to avoid the detection mechanism, no matter what kinds of routing detection used. Accordingly, some key encryption methods or hash-based methods are exploited to solve this problem. The black hole problem is still an active research area. This paper will benefit more researchers to realize the current status rapidly.

6. Reference

[1] Patel, M.; Sharma, S., "Detection of malicious attack in MANET a behavioral approach," *Advance Computing Conference (IACC), 2013 IEEE 3rd International* , vol., no., pp.388,393, 22-23 Feb. 2013

[2] Singh, P.K.; Sharma, G., "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET," *Trust, Security and Privacy in Computing and Communications (Trust Com), 2012 IEEE 11th International Conference on* , vol., no., pp.902,906, 25-27 June 2012

[3] Patel, M.; Sharma, S.; Sharan, D., "Detection and Prevention of Flooding Attack Using SVM," *Communication Systems and Network Technologies (CSNT), 2013 International Conference on*, vol., no., pp.533, 537, 6-8 April 2013.

[4] Gambhir, S.; Sharma, S., "PPN: Prime product number based malicious node detection scheme for MANETs," *Advance Computing Conference (IACC), 2013 IEEE 3rd International*, vol., no., pp.335, 340, 22-23 Feb. 2013.

[5] Tan, S.; Keecheon Kim, "Secure Route Discovery for preventing black hole attacks on AODV-based MANETs," *ICT Convergence (ICTC), 2013 International Conference on* , vol., no., pp.1027,1032, 14-16 Oct. 2013.

[6] Junhai Luo; Mingyu Fan; Danxia Ye, "Black hole attack prevention based on authentication mechanism," *Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on*, vol., no., pp.173, 177, 19-21 Nov. 2008.

[7] Hsun Tseng , Li-Der Chou and Han-Chieh Chao, "A survey of black hole attacks on MANET " , *international conference on black hole attack in MANET , Human-centric Computing and Information Sciences* 2011, **1**:4*Springer* 11/2011

[8] Harb, L.M.T.; Tantawy, M.; Elsoudani, M., "Performance of mobile ad hoc networks under attack," *Computer Applications Technology (ICCAT), 2013 International Conference on*, vol., no., pp.1, 8, 20-22 Jan. 2013.

[9] C.K Toh," *Ad hoc mobile wireless networks, protocols and systems*" ISBN 978-81-317-1510-9, chapter 3 sec 3.7.8 pp-37. Publisher- PEARSON, 10th impression 2012.

[10] Teerawat Issariyakul and Ekram Hossain "Introduction to Network Simulator : NS2" ISBN: 978-0-387-71759-3, Publisher- Springer, 2009