ISSN 2250-3153

Study to Eliminate Threat of Black Hole of Network Worms in MANET

Sumit Agrawal, Shilpa Jaiswal

Mtech Student,, AITR, Indore

Abstract- The need of wireless network is to enforce participating nodes to forward packets to other nodes to foster secure and reliable communication. Although there are presence of vulnerable nodes that can be associated with malicious nodes and can harm networks. The varieties of these malicious nodes are vulnerable to nodes which are either compromised or falsely guided by vulnerable nodes. Malicious nodes can easily tamper the participating nodes in the networks. In mobile ad hoc network these attacks shown their significance in the terms of network worms which can attack, alter or modify the root definitions of network across all administrative and participating domains. This paper reviews the full study to eliminate thread of black hole attacks in MANET". We also address to the solution against the threat of black hole attack in MANET. In Black Hole Attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. So to rectify the possibility of occurrence of black hole attack we are proposing a technique to identify attack and a solution to discover a safe route for secure transmission. We are proposing here a Secure Ad-hoc On-Demand Distance Vector routing protocol (SAODV) to endeavor our all efforts into a common place. So the emphasis is to develop a scheme for the measure of these network worms and blackhole attacks to eliminate occurrences of communication hazards from intermediate and surrounding threads.

Index Terms- Aodv blackhole, legacy, security, network worms, saodv

I. INTRODUCTION

The promise of mobile ad hoc networks to solve challenging real-world problems continues to attract attention from industrial, academic and research needs. In a Mobile Ad Hoc Network (MANET)**,** each node serves as a router for other nodes which allows data to travel by utilizing multi hop network paths without relying on wired infrastructure. Unlike wired networks where the physical wires prevent an attacker from compromising the security challenges especially for military applications, emergency rescue operations, and short-lived conference or classroom activities. Security of such network is a major concern. The open nature of the wireless medium makes it easy for outsiders to listen to network traffic or interfere with it. These factors make sensor networks potentially vulnerable to several different types of malicious attacks. These malicious nodes can carry out both Passive and Active attacks against the network. In passive attacks a malicious node only eavesdrop upon packet contents, while in active attacks it may imitate, drop or modify legitimate packets[1]. A typical of particularly devastating security active attack is known as a black hole attack. In which Black-hole attack [2] attracts all the packets towards it by altering the routing information and then drops those packets. Gray-hole attack is a specialized version of a black-hole attack, where the malicious node selectively drops packets.

Another example of particularly devastating security active attack is known as a wormhole attack. In which, a malicious node captures packets from one location in the network, and tunnels them to another malicious node at a distant point, which replays them locally. The wormhole attack can affect network routing, data aggregation and clustering protocols, and location-based wireless security systems. Finally, the wormhole attack can be launched even without having access to any cryptographic keys or compromising any legitimate node in the network in [3].

A. Network Worm:

Currently, it seems unfashionable to strictly define worm or virus or any other perfectly good term. It's simpler and more profitable to threaten non-technical people with a worm than it is to address the real problems of a software and hardware monoculture. A worm consists of a process or set of processes that replicates without human intervention by creating an executing copy of itself on another computer via some form of network communication.

B. Types of Attacks of Network Worm in Manet:

Different types of attacks are present in network worms to eliminate of communication hazard of manet. They are,

1). Black hole Attack
2). Wormhole Attack
3). Spoofing Attack
4). Denial of service attack
5). Non repudiation Attack
6). Ignorance Attack

1). Black hole Attack:

In Black Hole Attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. A black hole attack is used by a malicious node which makes all the traffictravel through it by claiming to have the shortest route to all other nodes in the network. Then, instead of forwarding the packets, the malicious node simply drops it. In a black hole attack, a malicious node impersonates a destination node by sending a spoofed root reply packet to a source node that initiates a route discovery. The source node traffic can be deprived by malicious node [4].

*2). Wormhole Attack***:**

In this case, an attacker node receives packet at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two malicious nodes is called wormhole. [5]

3). Spoofing Attack:

In spoofing attack, the attacker assumes the identity of another node in the network; hence it receives the messages that are meant for that node. Usually, this type of attack is launched in order to gain access to the network so that further attacks can be launched, which could seriously cripple the network. This type of attack can be launched by any malicious node that has enough information of the network to forge a false ID of one its member nodes and utilizing that ID and a lucrative incentive, the node can misguide other nodes to establish routes towards itself rather than towards the original node.

4). Denial of service attack:

Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network. When an authorized entity cannot access to should be network resources or emergency operations be denied, the attack of denial of service occurs. In the MANET, it is easy to achieve service interruption, so wireless communication can be used to shield the communications spectrum.

5). Non repudiation Attack:

Non repudiation ensures that sender and receiver of a message cannot disavow that they have ever sent or received such a message .This is helpful when we need to discriminate if a node with some undesired function is compromised or not.

6). Ignorance Attack:

When trusted node send data to next node but this node is not response to trusted node or this node is not provide path for transmitting data. The behavior of this node is ignores all thing so we can say, node is corrupted by ignorance attack.

In this paper, we considered black attack for the network worm to eliminate communication hazards in Mobile ad hoc network. Black hole attack is described above in this chapter.

II. ROUTING PROTOCAL

Routing in ad-hoc network involves determining a path from the source to the destination data can be communicated and the delivery of the packets to the destination nodes while nodes in the network are moving freely. Due to this node mobility, a path established by a source may not exist after a short interval of time. To cope with node mobility, nodes need to maintain routes in the network [6]. Routing protocols for ad-hoc networks broadly fall into pro-active, reactive, hybrid and location-based categories depending upon how nodes can establish and maintain paths.

Pro-active routing protocols are table-driven protocols that maintain up-to-date routing table using the routing information learnt from the neighbors on a continuous basis. Routing in such protocols involves selecting a path form the source to the destination, where the source node and each intermediate node selects a next hop, by routing table look up, and forwarding the packet to next hop until destination receives the packet [7]. A drawback of such protocols is the proactive overhead due to route maintenance and frequent route updates to cope with node mobility. Examples of this class include DSDV, WRP.

Reactive routing protocols are demand-driven protocols that find path when necessary. In such protocols, establishing a new route involves a route discovery phase consisting of route request (flooding) and a route reply (by the destination node). Nodes maintain only the active routes until a desired period or until destination becomes inaccessible along every path from the source node. A drawback of such protocols is the delay due to route discovery. Examples of this class include AODV and DSR protocols [7] [8].

Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes TORA, ZRP. Thus mechanism for ensuring packet delivery in Pro Active and Reactive can be apply together in this category [8] [9].

A. Ad hoc On-Demand Distance Vector Protocol:

In Ad-hoc On-demand Distance Vector Routing (AODV), a node discovers and maintains a route to the destination as and when necessary [10]. Every node in an Ad-hoc network maintains a routing table, which contains information about the route to a particular destination that are actively communicating with each other. Each entry in the routing table consists of the destination ID, the next hop ID, a hop count, and a sequence number for that destination. The sequence number helps nodes maintain a fresh route to the destination(s) and avoid routing loops. Thus, each node maintains a sequence number for itself and the respective source(s) and destination(s). A node increments its sequence number if it initiates a new route request or if it detects a link-break with one of its neighbors.

Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. To establish a path to the destination, a source node broadcasts a route request (RREQ) packet [10] [11]. The RREQ packet contains the source ID, the destination ID, sequence number of the source, and the latest sequence number of the destination node that is known to the source node. When a node receives a RREQ packet, it makes an entry for the route request in the route-request cache, and stores the address of the node from which it received the request as the next hop towards the source in its routing table. If receiving node is the destination or it has a fresh route to that destination1, then it responds with a route reply (RREP). Otherwise, it rebroadcasts the RREQ to its neighbors. When a node receives a RREP, it stores the address of the node from which it received RREP as the next hop towards the destination in its routing table and unicast the RREP to the next hop towards the source node. Once the source receives the RREP packet, it starts transmitting data packets along the path traced by the RREP packet. Due to the node mobility, path(s) established by a source node may break. When a node detects a path-break, it drops the packet for the destination and generates a route error (RERR) packet for the destination and sends the RERR to the source. Upon receiving a RERR, the source node buffers data packets for the destination and tries to re-establish a path to the destination. This is illustrated in figure 1.

ISSN 2250-3153

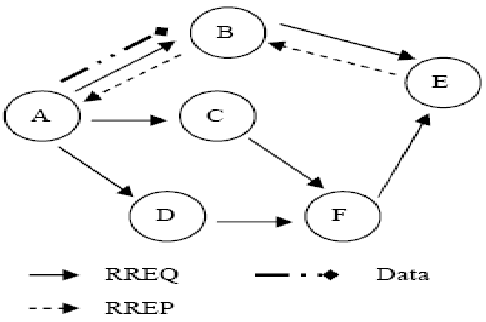

Figure 1. Propagation of RREQ & RREP from A to E

B. Threat of Black Hole Attack:

The attacker injects falsified routing packets to attract traffic. The attacker intercepts or drops control as well as data packets to deny services to authentic nodes. This attack can be prevented by establishing routes free of such nodes or by removing them from existing routes [2]. In the following illustrated figure 2, imagine a malicious node 'M'. When node 'A' broadcasts a RREQ packet; nodes 'B' 'D' and 'M' receive it. Node 'M', being a malicious node, does not check up with its routing table for the requested route to node 'E'. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node 'A' receives the RREP from 'M' ahead of the RREP from 'B' and 'D'.

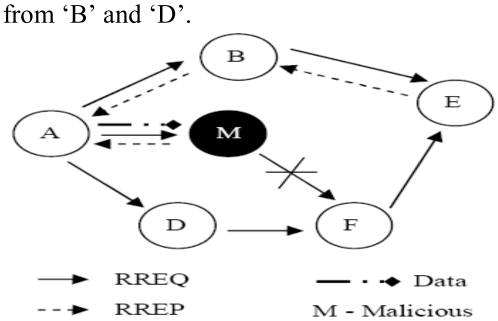

Figure 2. Black hole Attack in AODV

Node 'A' assumes that the route through 'M' is the shortest route and sends any packet to the destination through it. When the node 'A' sends data to 'M', it absorbs all the data and thus behaves like a 'Black hole'. Researchers have proposed solutions to identify a single black hole node. However in that solution next-hop also behaves as a malicious node they cannot identify it.

III. LITERATURE SURVEY

A. Neighborhood-based and Routing Recovery Scheme [12]

Sun B et al. use AODV as their routing protocol and simulation is done in ns2 simulator. The detection scheme used neighborhood-based method to detect the black hole attack and then present a routing recovery protocol to build the true path to the destination. Based on the neighbor set information, a method is designed to deal with the black hole attack, which consists of two parts: detection and response. In detection procedure, two major steps are: Step 1- Collect neighbor set information. Step 2- Determine whether there exists a black hole attack. In Response procedure, Source node sends a modify- Route-Entry (MRE) control packet to the Destination node to form a correct path by modifying the routing entries of the intermediate nodes (IM) from source to destination. This scheme effectively and efficiently detects black hole attack without introducing much routing control overhead to the network. Simulation data shows that the packet throughput can be improved by at least 15% and the false positive probability is usually less than 1.7%. The demerit of this scheme is that it becomes useless when the attacker agrees to forge the fake reply packets. This technique published in year 2003 and the simulation is done in NS-2 simulator.

B. Redundant Route Method and Unique Sequence Number Scheme [13]

A. Shurman et al. propose two techniques to prevent the black hole attack in MANETs. The first technique is to find at least two routes from the source to the destination node. The working is as follow. Firstlythe source node sends a ping packet (a RREQ packet) to the destination. The receiver node with the route tothe destination will reply to this RREQ packet and then the acknowledge examination is started at sourcenode. Then the sender node will buffer the RREP packet sent by different nodes until there are at leastthree received RREP packets and after identifying a safe route it transmit the buffered packets. Itrepresents that there are at least two routing paths existing at the same time. After that, the source nodeidentifies the safe route by counting the number of hops or nodes and thus prevents black hole attacks. Inthe second technique, unique sequence number is used. The sequence value is aggregated; hence it's ever higher than the current sequence number. In this technique, two values are recorded in two additional tables. These two values are last-packet-sequence numbers which is used identify the last packet sent to every node and the second one is for the last packet received. Whenever a packet are transmitted or received, these two table values are updated automatically. Using these two table values, the sender can analyze whether there is malicious nodes in network or not. Simulation result shows that these techniques have less numbers of RREQ and RREP when compared to existing AODV. Second technique is considered to be good compared to first technique because of the sequence number which is included to every packet contained in the original routing protocol. These both techniques fail to detect cooperative black hole attacks. As a simulator tool NS-2 used.

C. Time-based Threshold Detection Scheme [14]

Tamilselvan L. et al. proposed a solution based on an enhancement of the original AODV routing protocol. The major concept is setting timer for collecting the other request from other nodes after receiving the first request. It stores the packet's sequence number and the received time in a table named Collect Route Reply Table (CRRT). The route validity is checked based on the arrival time of the first request and the threshold value. The simulation shows that a higher packet delivery ratio is obtained with only minimal delay and overhead. But end-to-end delay might be raised visibly when the malicious node is away from the source node. Simulation is done in GloMoSim.

D. Random Two-hop ACK and Bayesian Detection Scheme [15]

Djenouri D et al. proposed a solution in to monitor, detect and remove the black hole attack in MANETs. In the monitor phase, an efficient technique of random two-hop ACK is used.Regarding the judgment issue, a Bayesian approachfor node accusation is used that enables noderedemption before judgment. The aim of thisapproach is to consider and avoid false accusationattacks vulnerability, as well as decreasing falsepositives that might be caused by channel conditionsand nodes mobility. This solution deals with all kindsof packet droppers, including as well selfish asmalicious nodes launching a black hole attack. It alsodeals with any Byzantine attack involving packetdropping in any of its steps. This solution detects theattacker when it drops packets. The simulationresults show that the random two-hop ACK is asefficient as the ordinary two-hop ACK in high true and low false detection, while hugely reducing the overhead. The solution utilizes cooperatively witness-based verification nevertheless, it's does not to avoid collaborate black hole attack for the judgment phase is only running on local side. It might be failed if there are multiple malicious nodes. Simulation is done with GloMoSim simulator.

E. DRI Table and Cross Checking Scheme [16,17]

HesiriWeerasinghe et al. proposed an algorithm to identify Collaborative Black Hole Attack. In this the AODV routing protocol is slightly modified by adding an additional table i.e. Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP). If the source node (SN) does not have the route entry to the destination, it will broadcast a RREQ (Route Request) message to discover a secure route to the destination node same as in the AODV. Any node received this RREQ either replies for the request or again broadcasts it to the network depending on the availability of fresh route to the destination. If the destination replies, all intermediate nodes update or insert routing entry for that destination since we always trust destination. Source node also trusts on destination node and will start to send data along the path that reply comes back. Also source node will update the DRI table with all intermediate nodes between source and the destination. The Simulation is done in QualNet simulator. The algorithm is compared with the original AODV in terms of throughput, packet loss rate, end-to-end delay and control packet overhead. Simulation results show that the original AODV is affected by cooperative black holes and it presents good performance in terms of throughput and minimum packet loss percentage compared to other solutions.

IV. PROPOSED WORK

We proposed a solution that is an enhancement of the basic AODV routing protocol, which will be able to avoid threads of black holes. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. According to this proposed solution the requesting node without sending the DATA packets to the reply node at once, it has to wait till other replies with next hop details from the other neighboring nodes. After receiving the first request it sets timer in the 'TimerExpiredTable', for collecting the further requests from different nodes. It will store the 'sequence number', and the time at which the packet arrives, in a 'Collect Route Reply Table' (CRRT). The time for which every node will wait is proportional to its distance from the source. It calculates the 'timeout' value based on arriving time of the first route request. According to SAODV wait and check the replies from all the neighboring nodes to find a safe route to reduce the probability of Black Hole Attack [18] [19].

After the timeout value, it first checks in CRRT whether there is any repeated next hop node. If any repeated next hop node is present in the reply paths it assumes the paths are correct or the chance of malicious paths is limited.

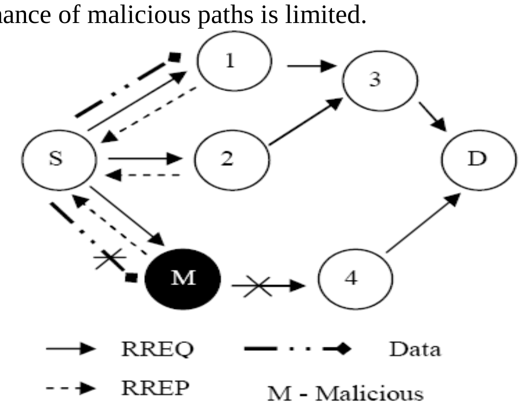

Figure 3. Solution to Black hole

In the above figure 3, S wants to transmit to D. So it first transmits the route request to all the neighboring nodes. Here node 1, node M and node 2 receive this request. The malicious node M has no intention to transmit the DATA packets to the destination node D but it wants to intercept/collect the DATA from the source node S. So it immediately replies to the request as (M – 4). Instead of transmitting the DATA packets immediately through M, S has to wait for the reply from the other nodes. After some time it will receive the reply from node 1 as (1 – 3), and node 2 as (2 – 3). According to this proposed solution it first check the path that contains repeated next hop node to the destination. If there is no repeated node select random path and transmits the data through that path. The routing table from S to D is given in table 1.

Source	Intermediate node	Destination
S	M – 4	D
S	1 – 3 2 – 3	D

Table 1. Routing Details

V. SCOPE OF THIS WORK

The scope of this study may be useful to understand the attack culture in MANET in terms of black hole attack and its countermeasures. Our solution to the problem of occurrence of attacks in any MANET scenario can be differ respect to the type of packet routing and breach in security. To develop trust across inter domain nodes is also a big challenge to overcome the possibility and effects of attacks. So the scope of this review can be a milestone in front of researchers and beginners to understand the challenge. However the simulation can describe actuality of attack culture in deep. NS-2, GloMoSim (Global

Mobile Simulator), and Qualnet simulator can be use to simulate the scenario quite clear.

VI. CONCLUSION AND FUTURE WORK

The efforts are continuous in terms of routing security, through network worm mitigation. We endeavor our work towards determination of network worms while considering black hole attack. We included the best known secure protocols for mobile ad hoc networks. In this work the challenges in routing security and related issues are discussed. However there is no such standard exist to procure the MANET hierarchy properly. The resources are poor and infrastructure less network is taken into consideration to understand all possibility of attacks feasible solution against the black hole attack in MANET is proposed. This work schematized the elimination of occurrence of black hole attack and its relevance in breach of security.

REFERENCES

[1] R.E.Kassi, A.Chehab, and Z. Dway, "DAWWSEN: A Defense Mechanism against Wormhole Attacks in Wireless Sensor Networks", in proceeding of the second International conference on innovations in information Technology (ITT' 05), UAE, September 2005.

[2] Y.-C. Hu and A. Perrig, A Survey of Secure Wireless Ad Hoc Routing, IEEE Security and Privacy, 2(3), 2004, 28 - 39.

[3] T. Park and K. Shin, "LISP: A Lightweight Security Protocol for Wireless Sensor Networks", in proceedings of ACM transaction on Embedded Computing systems, August 2004.

[4] N Sitapara& Prof. S B. VanjaleInternational Conference" ICETE-201O" on Emerging trends in engineering on 21st Feb 2010organized by J.J.Magdum College OfEngineering,Jasingpur. "Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks".

[5] S Jain &Dr.Satbir Jain International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010 (1793-8201) Manuscript received September 20, 2009."Detection and prevention of wormhole attack in mobile adhoc networks".

[6] Constantine Manikopoulosand Li Ling "Architecture of the Mobile Ad-hoc Network Security (MANS) System" CONEX Laboratory, NJWINS Center.

[7] Sanjay Ramaswamy, Huirong Fu, ManoharSreekantaradhya, John Dixon and Kendall Nygard"Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks" Department of Computer Science, IACC 258.

[8] Hongmei Deng, Wei Li, and Dharma P. Agarwal, "Routing Security in Wireless Ad Hoc Networks", University of Cincinnati, IEEE Communications magazine, October 2002..

[9] V. Karpijoki, "Security in Ad Hoc Networks", Seminar on Net Work Security, HUT TML 2000.

[10] C.E. Perkins, S.R. Das, and E. Royer, "Ad-Hoc on Demand Distance Vector (AODV)", March 2000, http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv- 05.txt

[11] Lidongzhou, Zygmunt J. Haas, "Securing Ad Hoc Networks", IEEE network, special issue, November/December 1999.

[12] Sun B, Guan Y, Chen J, Pooch UW , " Detecting Black-hole Attack in Mobile Ad Hoc Networks". 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.

[13] Al-Shurman M, Yoo S-M, Park S , " Black Hole Attack in Mobile Ad Hoc Networks". 42nd Annual ACM Southeast Regional Conference (ACMSE'42), Huntsville, Alabama, 2-3 April 2004.

[14] Tamilselvan L, Sankaranarayanan V, "Prevention of Blackhole Attack in MANET", 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27- 30 August 2007.

[15] Djenouri D, Badache N, "Struggling Against Selfishness and Black Hole Attacks in MANETs", Wireless Communications & Mobile Computing Vol. 8, Issue 6, pp 689-704, August 2008.

[16] HesiriWeerasinghe and Huirong Fu, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", Intenation Journal of Software Engineering and its Application, Vol.2, Issue3, July 2008.

[17] Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K, " Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23- 26 June 2003.

[18] Yih-Chun, Adrian Perrig, David B. Johnson, "Ariadne: A secure On-Demand Routing Protocol for Ad Hoc Networks", 2002

[19] Charles E. Perkins, Elizabeth M. Belding-Royer, Samir R. Das, Mobile Ad Hoc Networking Working Group, Internet Draft, 17 February 2003.

AUTHORS

First Author – Sumet Agrawal ,Mtech student, Electronics& communication, Acropolis Institute Of Technology & Research Indore(MP), Email: sumeetagrawal84@gmail.com
Second Author – Shilpa Jaiswal, Mtech student ,Computer Science & Engineering, Acropolis Institute Of Technology & Research, Indore (MP), Email: shilpa.jaiswal12@gmail.com