RESEARCH ARTICLE OPEN ACCESS

A Combined Approach for Worm-Hole and Black-Hole Attack Detection in MANET

Amber Jain[1], Ashish J Tiwari[2]
[1]Department of Computer Science, Vindhya Group of Technology and Science Khandwa Road, Indore, India
[2]Department of Computer Science, Vindhya Group of Technology and Science Khandwa Road, Indore, India

Abstract
Mobile ad hoc network is a kind of wireless network, in this network all nodes are connected through the wireless links and perform cooperative communication.Due to limited radio range of these devices any time can leave or join the network. Therefore the routing techniques are responsible for the network organization and communication flow. Due to this the performance of MANET is low as compared with the traditional wired communication networks. In addition of that network is suffers from the probability of attacks. Thus in this paper MANET routing strategy and their attacks are investigated and learned. In addition of that in order to secure the communication recent approaches of security in MANET also investigated. Finally a new algorithm for prevention of malicious attack in MANET is suggested. Additionally the based on the concluded facts, future extension of the proposed work is also suggested.

Keywords— MANET, Routing, routing attacks, malicious node detection and prevention

I. INTRODUCTION

Mobile ad hoc network is a new generation network technology that is self-defined by their name ad hoc network. The main advantage of such kind of network is their rapid configuration and hurdle free operation. The MANET is adoptable in those areas where the network management and maintenance is complex enough such as remote areas and battle field. Due to their advance technique there are no needs to install a stable infrastructure for organizing the network. Therefore mobile ad hoc network is a group of communication devices these nodes (network devices) are independent to move. The connectivity between these nodes is provided using the wireless links and any time can leave or join the network. In this network the main responsibility for creating and organizing the communication routing protocols are responsible. These protocols are help to obtain optimum path between sender and receiver. Using the discovered route the network can transmit data.

Mobile ad hoc network supports a number of routing protocols; these protocols can be categorized in two main domains active and passive routing technique. According to the type of routing technique the attack is also categorized as active and passive attacks. An active attack tries to modify the data being exchanged during communication, by disrupting the standard working of the network. It can be divided into two categories external attacks and internal attacks. External attacks are passed out by nodes that do not belong to the network. These attacks can be forbidden using typical security mechanisms like cryptographic approach and firewalls. Internal attacks are passed out by compromised nodes that are actually part of the network. Since the attackers are by now part of the network, internal attacks are more simple and problematic to detect as compared to external attacks. A passive attack does not disturb appropriate function of the network. The attacker sneaks the data exchanged in the network without altering it. Here, the necessity of privacy can be degraded and an attacker is also able to understand the data gathered through snooping. Detection of passive attacks is very tricky for the operation of the network. A technique of preventing such exertion is to use powerful encryption mechanisms to encrypt the data being transmitted; thereby making it impracticable for eavesdroppers to find any essential information from the data eavesdropped.

Therefore in MANET a different kind of attack deployment techniques are exist, but there are two most frequent kind of attacks are found in mobile ad hoc network according to the literature, but there is not a single combined effort is found for their detection and prevention. In this presented paper a combined approach is developed for preventing black-hole and wormhole attack. Therefore first in next section both attack techniques are explained.

II. BACKGROUND STUDIES

In this section black hole and wormhole technique is presented additionally how these attacks are deployed in network is also discussed in detail.

Worm hole

In wormhole attack, a tunnel is created between two nodes that can be used to secretly transmit

packets. In a wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network and then replays them into the network from that point. For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive sooner than other packets transmitted over a normal multi-hop route, for example through use of a single long range directional wireless link or through a direct wired link to a colluding attacker. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. If the attacker performs this tunneling honestly and reliably, no harm is done; the attacker actually provides a useful service in connecting the network more efficiently. The wormhole attack is particularly dangerous against many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of (and thus a neighbor of) that node. For example, when used against an on-demand routing protocol such as DSR or AODV, a powerful application of the wormhole attack can be mounted by tunneling each ROUTE REQUEST packet directly to the destination target node of the REQUEST. When the destination node's neighbors hear this REQUEST packet, they will follow normal routing protocol processing to rebroadcast that copy of the REQUEST and then discard without processing all other received ROUTE REQUEST packets originating from this same Route Discovery [1] [2].

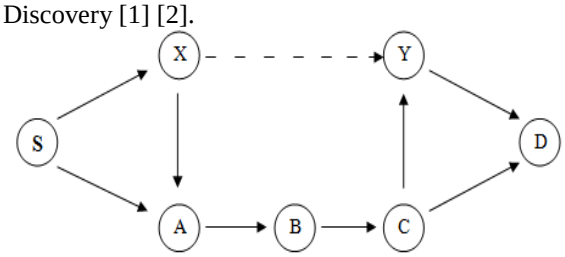

Figure 1 wormhole attack

Classification of Wormhole Attack

It is difficult to detect such dangerous attacks and no one can predict what the wormhole nodes can do and where and when. The wormhole attack is invisible at the higher layer and therefore, two end points of the wormhole are not visible in the route in which detection becomes much more complex. Wormhole can be classified into further five categories as proposed

- Wormhole using Encapsulation.
- Wormhole using out of band channel.
- Open wormhole attack.
- Closed wormhole attack.
- Half open wormhole attack.
- Wormhole with high power transmission.

Black Hole

In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

In Black hole attack, using routing protocol to an attacker advertises itself as the shortest path to the target device. An attacker watches the routes request in a flooding based routing protocol. When the attacker receives an appeal for a route to the target node, it forms a respond involving of really short route. If the mischievous respond reaches the initiating node before the reply from the genuine node, a fake route gets created. Once the malicious device joins the network itself among the communicating nodes, it is bright to do anything with the packets passing through them. It can crash the packets between them to perform a denial-of-service attack, or on the other hand use its position over the route is the first step of man-in-the-middle attack [3]. The black hole attack is a well-known security issue in MANET. The intruders develop the loophole to deploy their malicious activities because the route detection process is necessary and predictable. Many researchers have conducted different detection techniques to propose different types of detection schemes.

For example, in Fig. 2, source node S wants to send data packets to destination node D and initiates the route detection process. Suppose that device 2 is a malicious device and it claims that it has a route to the destination whenever it receives route request packets, and straight away sends the reaction to node S. If the reply from the malicious node 2 influences firstly to node S, then node S considers that route detection is finished, than S ignores all other replies and starts to send data packets to node 2. As an outcome, all packets through the malicious node is consumed or lost.

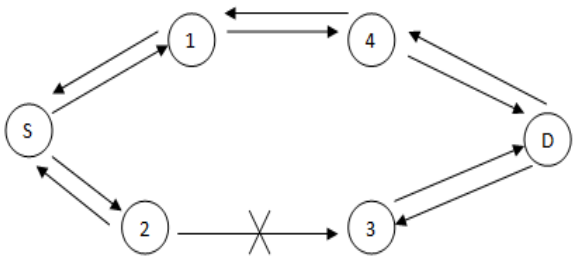

Figure 2 black hole attack

III. BLACK HOLE DETECTION TECHNIQUES

There are a large number of studies related to the Black hole attack detection and prevention techniques are available. In order to classify them an important contribution placed by [4], in their studies they provide various Black hole detection and prevention techniques and their description some of them are listed in this section.

Neighbourhood-based and Routing Recovery Scheme

Author claim that after a slightly modified the on-demand routing like DSR can also suitably applied over detection scheme uses on a neighbor-hood-based method. To recognize the black hole attack and a routing revival protocol to build the correct path. The neighbor-hood-based technique is working to identify the unsubstantiated nodes, and the source node sends a Modify Route Entry control packet to destination node to renew routing path in the recovery protocol. In this organization, not only a lower detection time and higher throughput are achieved, the precise detection is also achieved. To validate the mentioned approach, the routing control overhead does not increase. Conversely, this organization is impractical when the attackers cooperate to forge the reply packets [4].

Redundant Route Method and Unique Sequence Number Scheme

To find alternative route from the source node to target node, in other words, there exist some redundant routes inside the routing path, and authors believe that there are three routes at least in the scenario. The receiver who has a route, to the target will reply this request, and a allow investigation at source node. After that sender will store RREP packet till more than two RREP packets are received, and send the buffered packets after recognizing a secure route. It demonstrates that there are at lowest two routing paths available. Then, the source node distinguishes secure route from the number of hops, and avoid black hole attacks.

Time-based Threshold Detection Scheme

That is an improvement of AODV routing protocol. The design concept is based on a timer setting in the Timer Expired Table for gathering the request from other nodes after accepting the first request. It will accrue the packet's sequence number and the received time, counting the timeout value based on the arriving time of the first route request, inspecting the route valid or not based on the above threshold value. The simulation using GloMoSim reflects that, a higher PDR is gained with negligible delay and overhead. However the end-to-end delay may affect even when the suspicious device is away from the source device.

Next Hop Information Scheme

This technique is composed in two parts, reaction and detection, in first part field next hop is introduced in the RREP packet. Earlier source node conveys the data packets; the RREP packet is examined initially between intermediate node and target node. Each node manages BIT, and the fields in his table. That includes source, target, PRC, current node ID, PFC, PMC. Then the PMC is restructured by locating the BIT from their neighbours. If the node acts correctly, the corresponding count value multiplies. Then, a malicious node can be found out if the number of receiving packets differentiates from sending packets. The second part is separating the black hole, thus each node maintains an IT and stores the black node ID. The ID is broadcasted to every node in order to eliminate the malicious node by checking the isolation table.

IV. WORMHOLE DETECTION TECHNIQUES

Packet leashes [6] are available to detect and defend against the wormhole attack. In particular, the authors proposed two types of leashes first is temporal leashes and second is geographical leashes. For the temporal leash approach, each node computes the packet expiration time t, based on the speed of light c and includes the expiration time, t, in its packet to prevent the packet from traveling further than a specific distance, L. The receiver of the packet checks whether or not the packet expires by comparing its current time. The author also proposed TIK, which is used to authenticate the expiration time that can otherwise be modified by the malicious node. The main drawback of the temporal leash is that it requires all nodes to have tightly synchronized clocks. For the geographical leash, each node must know its own position and have loosely synchronized clocks. In this approach, a sender of a packet includes its current position and the sending time. Therefore a receiver can judge neighbor relations by computing distance between itself and the sender of the packet. The advantage of geographic leashes over temporal leashes is that the time synchronization needs not to be highly tight [5].

In [7], the authors offer protection against a wormhole attack in the OLSR protocol. This approach is based on location information and requires the deployment of a public key infrastructure and time-stamp synchronization between all nodes that is similar to the geographic leashes proposed in [6]. In this approach a sender of a HELLO message includes its current position and current time in its HELLO message. Upon receiving a HELLO message from a neighbor, a node calculates the distance

between itself and its neighbor, based on a position provided in the HELLO message. If the distance is more than the maximum transmission range, the node judges that the HELLO message is highly suspicious and might be tunneled by a wormhole attack [5].

In the authors propose a statistical analysis of multipath (SAM), which is an approach to detect the wormhole attack by using multipath routing. This approach determines the attack by calculating the relative frequency of each link that appears in all of the obtained routes from one route discovery. In this solution, alink that has the highest relative frequency is identified as the wormhole link. The advantage of this approach is that it introduces limited ov erhead when applied in multipath routing. However, it might not work in a non-multipath routing protocol, such as a pure AODV protocol.

V. PROPOSED WORK

Mobile ad hoc network is completely dependent on the routing techniques for communication. Therefore any malicious node can join the network any time. Thus a secure routing technique is required to design which consume the route parameters for finding the secure and optimum route between source and target destination.

Therefore there are two most frequent kind of attack deployments are considered. During black hole attack the malicious attacker attract most of the traffic in network and demonstrate the higher drop ratio. On the other hand during the wormhole deployment the malicious route consumes higher time as compared to legitimate route. Therefore a combine technique which utilizes the RTT (round trip time), buffer length and packet drop ratio for network routing strategy. The proposed routing algorithm can be defined as:

Let there are N number of nodes in network, a node S (source) wants to send data to a targeted node D (destination). Then first source send a control message to the target in the same time a timer is initiated as T_s and after receiving the route reply message from destination the time stoped and extract the time T_d. Thus between source and destination the path distance in terms of hop count is 2Hc. Thus for each hop the total time consumption is denoted by Rt

$$R_t = \frac{T_d - T_s}{2H_c}$$

Now, at the time of communication the malicious route can prevented using the following step.

1. Sender send a RREQ message
2. Initialize timer
3. Receive a RREP then Stop timer
4. Calculate Rt
5. For each node in routing table in source node
   a. Transmit a hello packet
   b. Get time of acknowledgment
   c. If $ack_{time} \leq R_t$
   d. If PDR< threshold
   e. If buffer_length < threshold
      i. Select as next hop
   f. End if
   g. End if
   h. Else
   i. Return from loop
   j. End if
6. End for

This section demonstrates the proposed routing algorithm for securing the communication path from the malicious attacker. The next section describes the conclusion of the presented paper.

VI. CONCLUSION

The given paper provides an analysis of the mobile ad hoc network routing techniques and their attacks. In addition of that recent development on the wormhole and black hole detection technique is also studied. Based on the previous techniques a new method for both attack detection and prevention a new routing enhancement is suggested and listed. In near future the proposed work is extended for simulation and results analysis during attacks on the mobile ad hoc network.

References

[1] T. Krishna Rao,Mayank Sharma,Dr. M. V. VijayaSaradhi, "*Securing Layer-3 Wormhole Attacks in Ad-Hoc Networks*", International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.1, Jan-Feb 2012 pp-230-234 ISSN: 2249-6645

[2] K. Sivakumar, Dr. G. Selvaraj, "*Analysis of Worm Hole Attack in MANET And Avoidance Using Robust Secure Routing Method*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January 2013 ISSN: 2277 128X

[3] SavithruLokanath, AravindThayur, "*Implementation of AODV Protocol and Detection of Malicious Nodes in MANETs*", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Volume 2 Issue 11, November 2013

[4] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "*A survey of black hole attacks in wireless mobile ad hoc networks*", licensee Springer. 2011, http://link.springer.com/article/10.1186/2192-1962-1-4/fulltext.html

[5] BOUNPADITHKANNHAVONG, HIDEHISANAKAYAMA, YOSHIAKINEMOTO,ANDNEIKATO, "*A SURVEY OF ROUTING ATTACKS IN*

MOBILE AD HOC NETWORKS",IEEE Wireless Communications • October 2007 1536-1284/07/$20.00 © 2007 IEEE

[6] Y-C. Hu, A. Perrig, and D. Johnson, "*Wormhole Attacksin Wireless Networks*," IEEE JSAC, vol. 24, no. 2, Feb.2006.

[7] D. Raffo et al., "*Securing OLSR Using Node Locations*," Proc. 2005 Euro. Wireless, Nicosia, Cyprus, Apr. 10–13,2005.

[8] L. Qian, N. Song, and X. Li, "*Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multi-path*," IEEE Wireless Communand Networking Conf. '05..