International Journal of Reviews in Computing
10th April 2012. Vol. 9
IJRIC

ISSN: 2076-3328 www.ijric.org E-ISSN: 2076-3336

ANALYZING THE DETECTION OF ACTIVE ATTACKS IN WIRELESS MOBILE NETWORKS

[1] G.M.PADMAJA, [2]CH.RAJYA LAKSHMI

[1] Senior Assistant Professor in CSE Dept. BVRIT

[2] Assistant Professor in CSE Dept, BVRIT

E-mail: [1]padmaja.gmp@gmail.com, [2]raji_822002@yahoo.co.in

ABSTRACT

In multi hop wireless systems, such as ad hoc and sensor networks, mobile ad hoc network applications are deployed, security emerges as a central requirement. A particularly devastating attack is known as the *active attack*, where two or more malicious collision nodes create a higher level virtual tunnel in the network, which is employed to transport packets between the tunnel end points. These tunnels emulate shorter links in the network. In which adversary records transmitted packets at one location in the network, tunnels them to another location, and retransmits them into the network. An Active attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. In this paper, we analyze active attack nature in mobile ad hoc and sensor networks and existing methods to detect active attacks without require any specialized hardware. This method provides an ability in establishing a way to reduce the rate of refresh time and the response time to become more faster.

Keywords: *Mobile Ad Hoc Network, Sensor Network, Active Attack.*

1. INTRODUCTION

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. A typical 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. This active attack can affect network routing, data aggregation and clustering protocols, and location-based wireless security systems. Finally, the active attack can be launched even without having access to any cryptographic keys.

2. IMPORTANCE OF ACTIVE ATTACKS

2.1 Secure Route Discovery

The existing secure routing protocols are based on Dynamic Source Routing (DSR) . They use route discovery to learn new routes and route error propagation to remove stale routes. The route discovery consists of two stages.

(1) *Route request stage* – the source node floods the network with a route request control packet (RREQ), and each intermediate node rebroadcasts the RREQ the first time it hears.

(2) *Route reply stage* – upon receiving a RREQ, the destination sends a route reply packet (RREP), which is propagated to the source in the reverse

International Journal of Reviews in Computing
31st December 2012. Vol. 9
IJRIC

ISSN: 2076-3328 www.ijric.org E-ISSN: 2076-3336

path of the RREQ.

There are two ways in which a malicious node can obtain the authentication code generated by its colluder.

Reactive Attack (Attack 1): If RREQs carry the path traversed in clear text, a malicious node , upon receiving a RREQ, can check if the path already contains another malicious node more than one hop away from it, and query that node for the authentication information it generated. This attack is effective only when RREQs carry path list in clear text.

Proactive Attack (Attack 2): Another approach is to have the node close to source send the authentication information to all other malicious nodes proactively. To facilitate this, malicious nodes may occasionally initiate RREQs to discover the routes among themselves.

An active attack is a particularly severe attack on MANET routing where two attackers connected by a high- speed off-channel link called the wormhole link. The wormhole link can be established by using a network cable and any form of "wired" link technology or a long-range wireless transmission in a different band. The end-point of this link (wormhole nodes) is equipped with radio transceivers compatible with the ad hoc or sensor network to be attacked.

Once the wormhole link is established, the adversary record the wireless data they overhear, forward it to each other, and replays the packets through the wormhole link at the other end of the network. Replaying valid network messages at improper places, wormhole attackers can make far apart nodes believe they are immediate neighbors, and force all communications between affected nodes to go though them.

In general, mobile ad hoc routing protocols fall into two categories: *proactive routing protocols* that rely on periodic transmission of routing updates, and *on-demand routing protocols* that search for routes only when necessary.

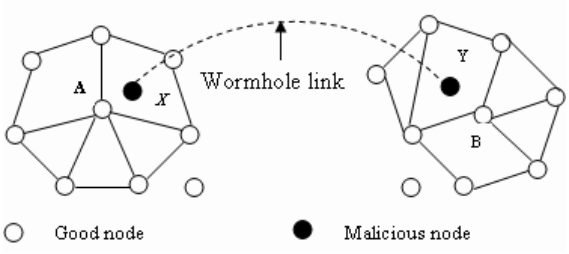

Fig.1. A network under an active attack.

A wormhole link is simply unreliable, as there is no way to protect what the attackers can do and when. Simply put the wormholes are compromising network security whether they are actively disrupting routing or not.

2.2 Types of Active Attacks

More sophisticated and subtle routing attacks have been identified recently. They are summarized in Table 1.

Name of Active attack	Description
Wormhole attack:	An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole.
Black hole attack:	The black hole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding. However, the attacker runs the risk that neighboring nodes will monitor and expose the ongoing attacks.
Byzantine attack:	A compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or

International Journal of Reviews in Computing
31st December 2012. Vol. 9
IJRIC

ISSN: 2076-3328 www.ijric.org E-ISSN: 2076-3336

	selectively dropping packets, which results in disruption or degradation of the routing services.
Rushing attack:	Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route.
Resource consumption attack:	This is also known as the sleep deprivation attack. An attacker or a compromised node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim node.
Location disclosure attack:	An attacker reveals information regarding the location of nodes or the structure of the network. It gathers the node location information, such as a route map, and then plans further attack scenarios.

Table 1: Types of Attacks

3. METHODS TO FIND ACTIVE ATTACKS

In mobile ad hoc networks, several methods have been introduced for finding active attacks specifically.

3.1. Packet leashes

Packet Leash is a mechanism to detect and defend against wormhole attacks. When temporal leashes are used, the sending node append the time of transmission to each sent packet t_S in a packet leash, and the receiving node uses its own packet reception time t_r for verification. The sending node calculates an expiration time t_e after which a packet should not be accepted, and puts that information in the leash. To prevent a packet from traveling farther than distance L, the expiration time is set to:

$$t_e = t_S + (L/c) - '$$

Where c is the speed of light and ' is the maximum clock synchronization error. All sending nodes append the time of transmission to each sent packet. The receiver compares the time to its locally maintained time and assuming that the transmission propagation speed is equal to the speed of light, computes the distance to the sender.

3.2. Time-of-flight

This is another method of finding active attack is based on the time of flight of individual packets. One possible way to avoid active attack, is to measure round-trip travel time of a message and its acknowledgement, estimate the distance between the nodes based on this travel time, and determine whether the calculated distance is within the maximum possible communication range.

The basis of all these approaches is the following. The Round Trip Travel Time (RTT) G of a message in a wireless medium can, theoretically, be related to the distance d between nodes, assuming that the wireless signal travels with a speed of light c:

$$d = G * c/2 \quad (2)$$
$$G = 2d/c \quad (3)$$

The neighbour status of nodes is verified if d is within the radio transmission range R:

$$R > d \ (d \text{ within transmission range})$$
$$R > G*c/2 \quad (4)$$
$$G < 2R/c \quad (5)$$
$$G = 2d/c = 600m/3 \times 10^{-8} \ m/s = 0.000002s = 2 \times 10^{-6} = 2\mu s \quad (6)$$

Therefore, the RTT is an order of magnitude smaller than the delay required by the protocol.

3.3 Specialized techniques

A wide variety of active attack mitigation techniques have been proposed for specific kinds of networks: sensor networks, static networks, or networks where nodes use directional antennas.

The first technique introduces an approach in which network visualization is used for discovery of active attacks in stationary sensor networks. In this approach, each sensor estimates the distance to its neighbours using the received signal strength.

International Journal of Reviews in Computing
31st December 2012. Vol. 9
IJRIC

ISSN: 2076-3328 www.ijric.org E-ISSN: 2076-3336

The second technique is a 'graph-theoretical' approach to active attack prevention based on the use of Location- Aware 'Guard' Nodes (LAGNs). It uses 'local broadcast keys' - keys valid only between one-hop neighbors - to defy active attackers: a message encrypted with a local key at one end of the network can not be decrypted at another end. This information can be exploited to detect active attacks.

Third technique proposes an active discovery mechanism based on statistical analysis of multipath routing. A link created by a wormhole is very attractive in routing sense, and will be selected and requested with unnaturally high frequency as it only uses routing data already available to a node.

4. TECHNIQUES EMPLOYED

4.1. Techniques for Active Attack Detection

There are several simple techniques to detect an Active attack in a network .

- **Link Frequency Analysis.** Analysis of the link frequency is a simple method to detect an active attack in a network.
- **Trust Based Model.** Another significant method to detect an active attack is by the use of trust information. Nodes can monitor the behaviour of their neighbour and rate them.

4.2. Monitoring Neighbours

In this security model, nodes go into promiscuous mode immediately after sending a packet to their neighbour. They monitor to check if the neighbour is transmitting it to the intended sender or dropping it. This can be found by listening to the packet header of the retransmission. If the destination is not transmitting to the intended destination or if the packet is simply dropped, then the source counts this as a drop. Hence every node in the network keeps track of the number of packets that are sent and dropped for each of its neighbours. This information is stored periodically for different intervals. For each neighbour, a node monitors the number of packets dropped *Dp* and packets sent *Sp* to it in that interval. I – 1, I – 2, I – 3, etc., are various intervals for which the observations are made.

4.3. Algorithm for Detection of An Active Attack

With the trust information available through neighbour monitoring, it is simple to detect the wormhole. The algorithm for detection of Wormhole is run during the routing phase. The procedure for wormhole detection is described by means of a flowchart given in Fig. 2.

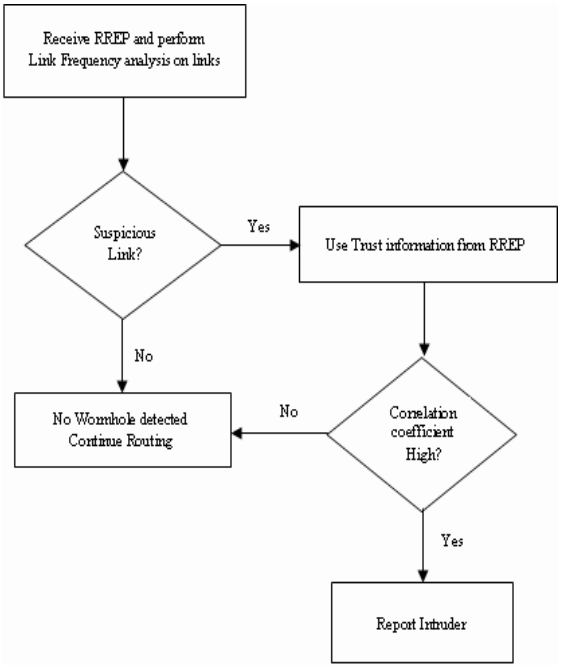

Fig. 2 Flowchart for detection of Active attack

[Broadcast RREQ]
1. Support nodes want to transmit to node d. It broadcasts the route request RREQ . It attaches its trust vector in the header.

[Append Trust Vectors]
2. Every nodes in the intermediate path also attaches it's trust vector in the RREQ message.

[Send RREP]
3. Destination node receives the RREQ and sends a route reply RREP. It copies the Trust Vectors from the RREQ into the RREP.

[Check for suspicious link]
4. Source receives various RREP coming through different routes. Check if there is a link with very high frequency using the following expression:

$$Pi = ni / N, \text{ for all } Ii$$
$$Pmax = max\ (pi)$$

International Journal of Reviews in Computing
31st December 2012. Vol. 9
IJRIC

ISSN: 2076-3328 www.ijric.org E-ISSN: 2076-3336

Where, R is the set of all obtained routes, I_i is the i^{th} link, n_i is the number of times that I_i appears in R, N is the total number of links in R, and P_i is the relative frequency that I_i appears in R.

[Confirm wormhole]

5. *If Pmax* > *Pthreshold*(0.2), check the trust information available in the RREP of that route. If the value of correlation coefficient for packets dropped to that sent is > t *threshold* (0.9),then the node is malicious, inform the operator. else continue with routing process.

5. PERFORMANCE EVALUATION

The performance of DaW was evaluated against existing method of link frequency analysis.. We have implemented both Link Frequency analysis and DaW on DSR routing protocol. Nodes monitor their neighbour by going into promiscuous mode. Each interval spans over a period of 20 seconds and at any time a maximum of 5 intervals are observed and are used for trust evaluation. The size of the interval and the number of intervals observed both are variables and can be changed based on the available resources.

5.1. Precision of Alarms

The results of the simulations in terms of the total number of alarms raised and the genuine alarms out of them are tabulated.

The precision is defined as follows:

$$\text{Precision of alarms} = \frac{\text{Number of alarms for worm holes}}{\text{Total number of alarms}} \%$$

The total number of alarms might include apart from genuine wormhole. The precision is decided by the proportion of genuine wormholes detected. Based on the simulations, the graph of Precision of Alarms versus the number of nodes is plotted in Fig.3.

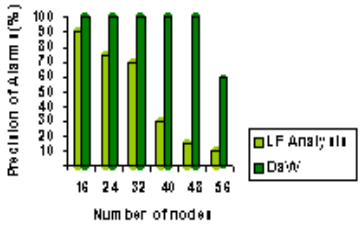

Fig 3.Precision of Alarms

From the results of the simulations, it is clear that the normal link frequency based approach could mislead into believing bottleneck links as wormholes. The precision decreases with the increase in the size of the network. This is due to the fact that the number of possible routes between two nodes increases as the network becomes bigger. There are a large number of links which have comparable high frequency. Link Frequency analysis cannot make an accurate detection and it simply gives an alarm for an active attack.

6. CONCLUSION

In this paper, we addressed various attacks that occur in routing and the various solutions available for active attack in wireless Ad hoc and sensor networks.

REFERENCES

[1] Bin Xie and Anup Kumar. "A Framework for Internet and Ad hoc Network Security". IEEE Symposium on Computers and Communications (ISCC-2004),June 2004.

[2] C. E. Perkins and E. M. Royer. "Ad Hoc On - Demand Distance Vector Routing". Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, Pages 90-100, February 1999.

[3] Y.-C. Hu, A. Perrig, D. B. Johnson, "Wormhole Attacks in Wireless Networks" Selected Areas of Communications, IEEE Journal on, vol. 24, numb. 2,pp. 370- 380, 2006.

[4] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks", in *proceedings of INFOCOM*, 2004.