International Journal of Information Technology and Knowledge Management
July-December 2011, Volume 4, No. 2, pp. 569-571

ATTACKS ON WIRELESS MANET

Niki Devi

Security has always been a key issue with wireless networks since there are no physical boundaries. Experience has shown numerous vulnerabilities to a variety of attacks even when security measures are in place. In the combined Internet-MANET environment also security is an important issue keeping in view the Internet connectivity and attack on the MANET protocols.

Keywords: Adhoc Wireless Networks, Adhoc Threats, Blackhole Attack, Wormhole Attack, Internet-MANET.

1. INTRODUCTION

By definition, Mobile Adhoc Networks (MANETs) differ from existing networks by the fact that they rely on no fixed infrastructure. Nodes forming the network perform all functionality of the network with each node performing the functionality of both host and router. Data is relayed to establish connectivity between source and destination nodes not directly within each other's transmission range. With the increasing demand of ubiquitous computing, the interconnection of mobile ad hoc networks (MANETs) to Internet is also getting more in demand, which is so-called hybrid or connected MANET.

In the integrated MANET-Internet communication, a connection could be disrupted either by attacks on the Internet connectivity or by attacks on the ad hoc routing protocols. Because of this almost all possible attacks on the traditional ad hoc networks also exist in the integrated wired and mobile ad hoc networks [1].

2. PROTOCOLS COMMONLY USED FOR MANET'S

2.1 AODV (Ad Hoc On-Demand Distance Vector Routing)

It is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. When the valid route is not known by the source node, it initializes a route discovery process by broadcasting a Route Request (RREQ) to its neighbours. Each node discards Route Requests (RREQs) it has already seen by checking the Broadcast ID and the Sequence Number which had been included into the Route Request (RREQ).

2.2 DSR (Dynamic Source Routing)

Determining source routes requires accumulating the address of each device between the source and destination during route discovery. The accumulated path information is cached by nodes processing the route discovery packets. The learned paths are used to route packets. To accomplish source routing, the routed packets contain the address of each device the packet will traverse.

2.3 Zone Routing Protocol

Zone routing protocol combines Proactive protocol features and Reactive protocol features. All nodes within hop distance at most d from a node X are said to be in the routing zone of node X. All nodes at hop distance exactly d are said to be peripheral nodes of node X's routing zone.

In Zone Routing Protocol Intra-zone routing involves maintaining state information for links within a short distance from any given node whereas Inter-zone routing involves using a route discovery protocol for determining routes to far away nodes.

3. METRICS COMMONLY USED FOR MANET'S

3.1 Packet Delivery Ratio (PDR)

The ratio of the number of data packets received to the number of data packets transmitted.

3.2 End-to-End Delay

The time needed to deliver a packet from the data source to the data destination. Average end-to-end delay of data packets accounts for all possible delays caused by buffering of packets during route discovery, queuing at the node interfaces and retransmission delays in the MAC layer.

3.3 Routing Delay

The total amount of routing protocol traffic transmitted.

3.4 Average Route Length

Defined as the average number of hops traversed by data packets travelling from source to destination.

Research Scholar, Department of Computer Science Singhania University, Rajasthan, INDIA
E-mail: chahal_sk@rediffmail.com

3.5 Other Metrics

Other metrics such as Link Capacity, number of nodes, topological changes, Number of neighbours of the nodes can also be considered.

4. NETWORK LAYER THREATS

The Network Layer is susceptible to the following attacks:

4.1 Blackhole Attack

An attacker creates forged packets to impersonate a valid mesh node and subsequently drop packets. The attracting packets involve advertising routes as low-cost [2].

In networking, black holes refer to places in the network where incoming traffic is dropped without informing the source that the data did not reach its intended recipient.

In Blackhole Attacks a node uses the protocol and advertises itself as having the shortest path to the destination node where the packet is destined to.

As shown in Figure 1. the Blackholenode (BH) drops all the packets received by it without forwarding it to its next hop node Node 2 (N2).

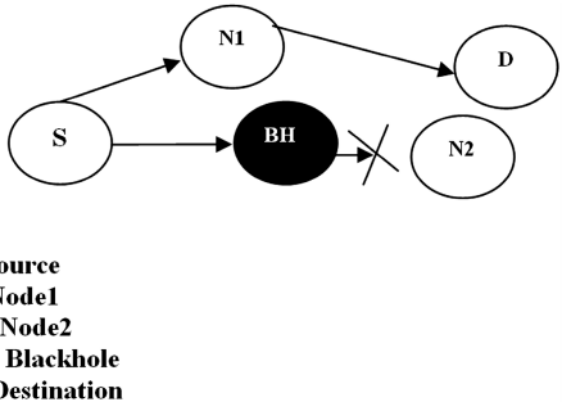

Fig. 1: Blackhole Attack

4.2 Greyhole Attack

Grey Hole is a node that can switch from behaving correctly to behaving like a black hole. This is done to avoid detection. Some researchers discussed and proposed a solution to a black hole attack by disabling the ability for intermediate nodes to reply to a Route Reply (RREP); only the destination is allowed to reply [3].

4.3 Wormhole Attack

In a wormhole attack, an attacker forwards packets through a high quality out-of-band link and replays those packets at another location in the network.

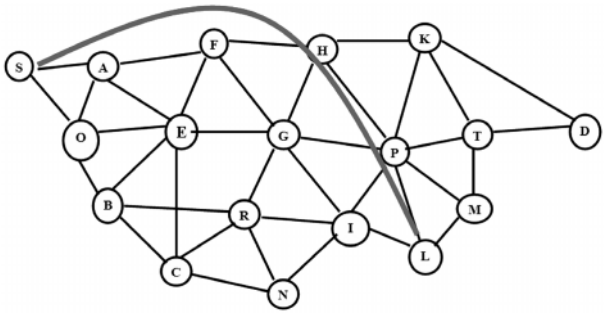

Fig. 2: Wormhole Attack

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 with better metric. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received. An attacker can create a wormhole even for packets not addressed to itself, since it can hear them in wireless transmission and tunnel them to the attacker at the opposite end of the wormhole.

5. PROPERTIES OF BLACKHOLE, GREYHOLE AND WORMHOLE ATTACKS

First, the Blackhole node exploits the 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 packets are consumed by the Blackhole node. Third, the Blackhole nodes can conduct coordinated attacks. Grey Hole is a node that can switch from behaving correctly to behaving like a black hole.

Wormhole attacks depend on a node misrepresenting its location. Hence, location based routing protocols have the potential to prevent wormhole attacks.

6. COUNTERMEASURES

6.1 Wormhole Attack Countermeasure

Wormhole attacks depend on a node misrepresenting its location. Hence, location based routing protocols have the capacity to prevent wormhole attacks. Localization may be done using globally accessible beacons that broadcast known locations [4].

A solution to wormhole attacks was proposed in which in which all nodes are equipped with directional antennas. Nodes use specific 'sectors' of their antennas to communicate with each other. Each copule of nodes examine the direction of received signals from its neighbour. If the direction of both pairs match the neighbour relation is set [4]. This method may only be used in networks using Directional antennas [6].

Another solution was proposed in which nodes estimate the distance of its neighbours using the Received Signal Strength. The value is sent to a central controller which calculates the physical topology based on individual sensor distance measurement. Wormhole can be caught as without wormhole attack the topology is usually flat [5]. The mobility and varied terrains were not studied [6].

6.2 Blackhole and Greyhole Attack Countermeasure

To detect black and gray hole nodes, one proposal is having the sender occasionally check through all available routes to determine if the destination received all of its messages intact. This must be done after some data has been sent. In order to circumvent any black hole nodes that might interfere with message traffic, the sender broadcasts a "check" request message (Fig. 3), and the destination's response would follow the same route as the request (Fig. 4). To deal with the possibility of a node altering or faking the client's response, the sender compares each response with the data that it sent to the destination. If the responses differ from what the sender sent, it may indicate a bad link or a malicious node. If any two client responses differ, that is almost a sure sign of a malicious node [3].

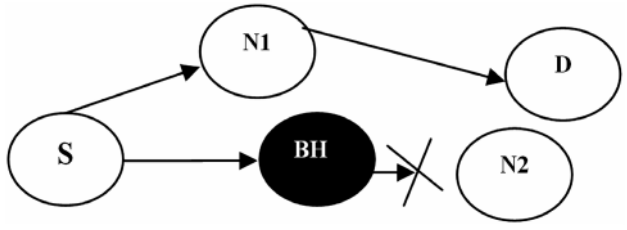

Fig.3

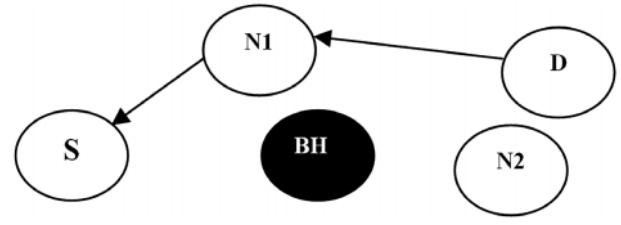

Fig. 4

Some researchers also discussed and proposed a solution to a blackhole attack by disabling the ability for intermediate nodes to reply to an RREP, and only allowing the destination to reply [7].

7. FUTURE WORK

The countermeasures of Blackhole attacks such as occasionally checking through all available routes to determine if the destination received all of its messages intact and location based routing protocols to countermeasure Wormhole attacks is being investigated so as to improve the Internet connectivity in the Internet-MANET environment.

8. ACKNOWLEDGEMENT

I would like to express my special thanks to Dr. Adel Ben Mnaouer, Senior Member, IEEE and ICT Department, University of Trinidad and Tobago for his valuable comments and his feedback.

REFERENCES

[1] A. Rai, R. Ranjan Tewari and S. Upadhyay, Department of Electronics & Communication, "University of Allahabad, India, Different Types of Attacks on Integrated MANET-Internet Communication".

[2] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon and Kendall Nygard , "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks".

[3] E. Mohammed and L. Dargin, Oakland University School of Computer Science and Engineering CSE 681 Information Security, "Routing Protocols Security in Ad Hoc Networks".

[4] L. Hu and D. Evans, Department of Computer Science, "University of Virginia Charlottesville", Using Directional Antennas to Prevent Wormhole Attacks", VA IJCSNS International Journal of Computer Science and Network Security, 8 No.7, July 2008.

[5] W. Wang and B. Bhargava., "Visualization of Wormholes in Sensor Networks", Proceedings of the 2004 ACM Workshop on Wireless Security, pp. 51-60, 2004.

[6] K. Win, Department of Engineering Physics, "Mandalay Technological University, Pathein Gyi, Mandalay", Analysis of Detecting Wormhole Attack in Wireless Networks, World Academy of Science, Engineering and Technology 48 2008.

[7] H. Deng, W. Li, and D. Agrawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Comm. Magazine, 40, no. 10, 2002, pp. 70 75.