International Journal of Smart Sensor and Adhoc Network

Volume 2 | Issue 3 Article 5

April 2012

# ATTACKS IN MOBILE AD HOC NETWORKS: DETECTION AND COUNTER MEASURE

R. MADHUMATHI
*Anna University of Technology, Coimbatore.*, madhumathir14@gmail.com

J. JENNO RICHI BENAT
*Angel College of Engineering and Technology, Tirupur.*, jennorichi@gmail.com

# ATTACKS IN MOBILE AD HOC NETWORKS: DETECTION AND COUNTER MEASURE

**R.MADHUMATHI[1] & J.JENNO RICHI BENAT[2]**

[1]Anna University of Technology, Coimbatore.
[2]Angel College of Engineering and Technology, Tirupur.
Email:madhumathir14@gmail.com, jennorichi@gmail.com

**Abstract** –In Wireless Ad hoc network Stealthy packet dropping is a suite of four attacks—misrouting, power control, identity delegation, and colluding collision—that can be easily launched against multi hop wireless ad hoc network. Stealthy packet dropping disrupts the packet from reaching the destination through malicious behavior at an intermediate node. In the same way Mobile ad hoc network also having the different types of attacks in network layer such as flooding attacks, rushing attacks, black hole attacks, gray hole attacks, wormhole attacks, sinkhole attacks, and Sybil attacks. We analyses different routing protocols and its route discovery technology.

***Keywords*** *– Wireless Ad hoc network, Mobile Ad-hoc Networks, Routing Attacks, Routing Protocols, Route Discovery*

## I. INTRODUCTION

Ad hoc networks are a promising paradigm for easy communication, especially the wireless ad hoc network for mobile hosts. Ad hoc network requires no fixed infrastructure or any kind of central servers. All nodes in ad hoc manner usually have equivalent status in the services. Nodes are connected either directly if within the radio range or via the intermediary nodes, which relay messages as routers, for remote destinations. Frequent changes such as positions and available status of the nodes can be accepted without severely influence on the quality of services. The ad hoc networks can adjust its topology dynamically. The pleasing characteristics above bring good benefits, for example, fast deployment, self-organize and great flexibility, surpassing other traditional networks [4].

However, many applications run in untrusted environments and require secure communication and routing. Applications that may require secure communications include emergency response operations, military or police networks, and safety-critical business operations such as oil drilling platforms or mining operations. Ad hoc networks generally use a wireless radio communication channel. The main advantages of such networks are rapid deployment and low cost of operation, since the nodes and wireless hardware are inexpensive and readily available, and since the network is automatically self-configuring and self-maintaining. However, wireless networks are vulnerable to several attacks. In most wireless networks, an attacker can easily *inject* bogus packets, impersonating another sender. We refer to this attack as a *spoofing* attack.

In this paper we studied different types attacks, such as misrouting, power control, identity delegation, colluding collision, flooding attacks, rushing attacks, black hole attacks, gray hole attacks, wormhole attacks, sinkhole attacks, and Sybil attacks. The rest of paper is organized as follows; section 2 presents routing algorithms types such as table driven, on demand routing protocols and we describe some routing protocols. Section 3 provides details description about various different types of attacks such as misrouting, power control, identity delegation, and colluding collision, flooding attacks, rushing attacks, black hole attacks, gray hole attacks, wormhole attacks, sinkhole attacks, and Sybil attacks and section 4 gives the conclusion of the paper.

## II. PROTOCOLS

MANET routing protocols can be categorized into 2 classes as: table-driven/proactive and source-initiated (demand-driven)/reactive and some other protocols [10]. In this section we describe the routing protocols.

### *A. Table – Driven Routing Protocols*

Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and they respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view. The areas in which they differ are the number of necessary routing-related tables and the methods by which changes in network structure are broadcast. Some of the table – driven routing protocols are Destination-Sequenced Distance-Vector (DSDV), Optimized link state routing (OLSR) protocol, Wireless routing protocol (WRP) and Cluster head gateway switch routing (CGSR) protocol [4]. In this section, we discuss about DSDV and OLSR protocols.

*1) Destination-sequenced distance-vector (DSDV):* The Destination-Sequenced Distance-Vector (DSDV) routing protocol [11] is a table-driven algorithm. In DSDV every node in the network maintains a routing table in which all of the possible destinations within the network and the number of hops to each destination are recorded. Each entry is marked with a sequence number assigned by the destination node. The sequence numbers enable the mobile nodes to distinguish stale routes from new ones, thereby avoiding the formation of routing loops. Routing table updates are periodically transmitted throughout the network in order to maintain table consistency. To help alleviate the potentially large amount of network traffic that such updates can generate, route updates can employ two possible types of packets: full *dump* and *s*maller *incremental* packets. Each of these broadcasts should fit into a standard-size of network protocol data unit (NPDU), thereby decreasing the amount of traffic generated. The mobile nodes maintain an additional table where they store the data sent in the incremental routing information packets. New route broadcasts contain the address of the destination, the number of hops to reach the destination, the sequence number of the information received regarding the destination, as well as a new sequence number unique to the broadcast. The route labeled with the most recent sequence number is always used. In the event that two updates have the same sequence number, the route with the smaller metric is used in order to optimize (shorten) the path. Mobiles also keep track of the settling time of routes, or the weighted average time that routes to a destination will fluctuate before the route with the best metric is received. By delaying the broadcast of a routing update by the length of the settling time, mobiles can reduce network traffic and optimize routes by eliminating those broadcasts that would occur if a better route was discovered in the very near future.

*2) Optimized link state routing (OLSR) protocol:* Optimized link state routing (OLSR) protocol [12] is a proactive routing protocol and based on periodic exchange of topology information. The key concept of OLSR is the use of multipoint relay (MPR) to provide an efficient flooding mechanism by reducing the number of transmissions required. In OLSR, each node selects its own MPR from its neighbors. Each MPR node maintains the list of nodes that were selected as an MPR; this list is called an MPR selector list. Only nodes selected as MPR nodes are responsible for advertising, as well as forwarding an MPR selector list advertised by other MPRs. Generally, two types of routing messages are used in the OLSR protocol, namely, a HELLO message and a topology control (TC) message. A HELLO message is the message that is used for neighbor sensing and MPR selection. In OLSR, each node generates a HELLO message periodically. A node's HELLO message contains its own address and the list of its one-hop neighbors. By exchanging HELLO messages, each node can learn a complete topology up to two hops. HELLO messages are exchanged locally by neighbor nodes and are not forwarded further to other nodes. A TC message is the message that is used for route calculation. In OLSR, each MPR node advertises TC messages periodically. A TC message contains the list of the sender's MPR selector. In OLSR, only MPR nodes are responsible for forwarding TC messages. Upon receiving TC messages from all of the MPR nodes, each node can learn the partial network topology and can build a route to every node in the network. For MPR selection, each node selects a set of its MPR nodes that can forward its routing messages. In OLSR, a node selects its MPR set that can reach all its two-hop neighbors. In case there are multiple choices, the minimum set is selected as an MPR set.

*B. On demand Routing Protocols*

On demand protocols create routes only when desired by source nodes [13, 15]. When a node requires a route to destination, it initiates route discovery process within the network. This process is completed once a route is found or all possible route permutations are examined. Once a route is discovered and established, it is maintained by route maintenance procedure until either destination becomes inaccessible along every path from source or route is no longer desired. In this section we describe Ad hoc on-demand distance vector (AODV) and Dynamic Source Routing (DSR).

*1) Ad hoc on-demand distance vector (AODV):* AODV [13, 14] is an improvement of DSDV algorithm previously described. It is typically minimizes the number of required broadcasts by creating routes on a demand basis, while DSDV algorithm maintain a complete list of routes. The authors of AODV classify it as a pure on demand route acquisition system, since nodes that are not on a selected path do not maintain routing acquisition or participate in routing table exchanges. In AODV, when a source node S wants to send a data packet to a destination node D and does not have a route to D, it initiates route discovery by broadcasting a route request (RREQ) to its neighbors. The immediate neighbors who receive this RREQ rebroadcast the same RREQ to their neighbors. This process is repeated until the RREQ reaches the destination node. Upon receiving the first arrived RREQ, the destination node sends a route reply (RREP) to the source node through the reverse path where the RREQ arrived. The same RREQ that arrives later will be ignored by the destination node. In addition, AODV enables intermediate nodes that have sufficiently fresh routes to generate and send an RREP to the source node.

*2) Dynamic Source Routing (DSR):*
Dynamic source routing (DSR) protocol is an on-demand routing protocol that is based on the concept of source routing [15]. Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. Entries in the route cache are continually updated as new routes are learned. The protocol consists of two major phases: route discovery and route maintenance. When a mobile node has a packet to send to some destination, it first consults its route cache to determine whether it already has a route to the destination. If it has an unexpired route to the destination, it will use this route to send the packet. On the other hand, if the node does not have such a route, it initiates route discovery by broad-casting a *route request* packet. This route request contains the address of the destination, along with the source node's address and a unique identification number. Each node receiving the packet checks whether it knows of a route to the destination. If it does not, it adds its own address to the *route record* of the packet and then forwards the packet along its outgoing links. To limit the number of route requests propagated on the outgoing links of a node, a mobile only forwards the route request if the request has not yet been seen by the mobile and if the mobile's address does not already appear in the route record. A *route reply* is generated when the route request reaches either the destination itself, or an intermediate node which contains in its route cache an unexpired route to the destination. By the time the packet reaches either the destination or such an intermediate node, it contains a route record yielding the sequence of hops taken.

*C. Power - aware Routing Protocols:*
In a deviation from the traditional wired network routing and cellular wireless network routing, power consumption by the nodes is a serious factor to be taken into consideration by routing protocols for ad hoc wireless networks. This section discusses some of the important routing metrics that take into consideration this energy factor.

*1) Power-Aware Routing Metrics*
The limitation on the availability of power for operation is a significant bottleneck, given the requirements of portability, weight, and size of commercial hand-held devices. Hence, the use of routing metrics that consider the capabilities of the power sources of the network nodes contributes to the efficient utilization of energy and increase the lifetime of the network. The routing protocols that select paths so as to conserve power must be aware of the states of the batteries at the given node as well as at the other intermediate nodes in the path.

i) *Minimal Energy Consumption per Packet*
This metric aims at minimizing the power consumed by a packet in traversing from source node to destination node. The energy consumed by a packet when traversing through a path is the sum of the energies required at every intermediate hop in that path. This metric maintain the uniform consumption of power throughout the network.

ii) *Maximize Network Connectivity*
This metric attempts to balance the routing load among the subset of the nodes in the network

iii) *Minimum Variance in Node Power Levels*
This metric propose to distribute the load among all the nodes in the network. So the power consumption pattern remains uniform across them.

iv) *Minimum cost per Packet*
To maximize the life time of every node in the network, this routing metric is made as a function of the state of the node's battery. The cost decrease with an increase in its battery charge. With the availability of a battery discharge pattern, the cost of a node can be computed.

v) *Minimize Maximize node Cost*
This metric minimize the maximum cost per node for a packet after routing a number of packets.

## III. CLASSIFICATION OF ATTACKS

*Flooding Attacks:*
In flooding attack, the malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service. In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. Flooding attacks are classified into

- RREQ Flooding Attack
- DATA Flooding Attack

*2) RREQ Flooding Attack*
In the RREQ Flooding Attack, the attacker sends RREQ (Route –Request) packet for unknown node in network, each node will rebroadcast fake RREQ packet to entire network. It makes entire network with RREQ packets. The malicious node breaks the RREQ-RATELIMT, It makes entire network with RREQ packets. This results in the situation that the communication bandwidth is exhausted by the flooded RREQ packets. The node resource such as battery is consumed by flooding packets.

2) DATA Flooding Attack

In this attack, the attack node builds up paths to all nodes in the network. Then, the attacker sends large volumes of useless DATA packets to all nodes along these paths. The mass useless DATA packets will exhaust the communication bandwidth in the network and the destination node will be busy for receiving the excessive useless packets from the attack node and therefore cannot work normally [3].

*B. Rushing Attacks*

In rushing attack, if a node want to discover route for target node, then it will initiates a Route Discovery for the target node, the attacker could capture the RREQ and the attackers rebroadcast that RREQ. If the RREQ for this Discovery forwarded by the attacker are the first to reach each neighbor of the target then any route discovered by this Route Discovery will include a hop through the attacker. That is, when a neighbor of the target receives the rushed RREQ from the attacker, it forwards that RREQ, and will not forward any further RREQ from this Route Discovery. When non-attacking RREQs arrive later at these nodes, they will discard those legitimate RREQ [5], as a result, the initiator will be unable to discover any usable routes (i.e., routes that do not include the attacker) containing at least two hops (three nodes). In general terms, an attacker that can forward RREQ more quickly than legitimate nodes can do so, can increase the probability that routes that include the attacker will be discovered rather than other valid routes [5].

*C. Blackhole Attacks and Gray hole Attacks*

In a blackhole attack, 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 [6]. For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker.

Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic. In a gray hole attack, a malicious node refuses to forward certain packets and simply drops them. If a malicious node drops all the packets, the attack is then called a black hole which is easy to detect as opposed to a gray hole attack in which the attacker selectively drops the packets [7]. Fig. 1 shows an example of a black hole attack, where source node S sends RREQ for node D, the attacker node E sends RREP that, it has route for D with highest sequence number. So that node S starts further packet transfer with node E and S discards other RREP

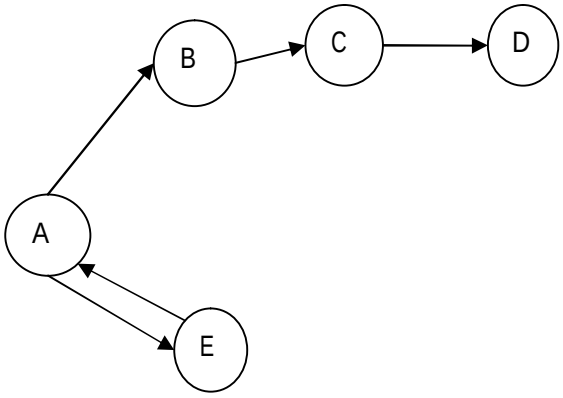


**Fig. 1 Blackhole Attack**

*D. Wormhole Attacks*

A wormhole is a tunnel which connects two remote nodes [7]. A particularly devastating security attack known as a *wormhole* has been discussed in the context of ad-hoc networks where a malicious node records packet in one location and with the help of another colluding node replays the packet in a distant part of the network. The colluding nodes can use communication techniques such as an out-of-band channel (a point-to-point link) or high power transmission (using directional antennas) to tunnel packets. This tunneling enables the tunneled packet to arrive with fewer hops or lower delay than if the packet traversed a normal path.

The arrival of packets with low delay or hop count attracts nearby traffic towards the malicious node, thus affecting routing [1]. In a *wormhole attack*, an attacker builds the tunnel between two points. An attacker receives packets at one point in the network, sends them (through tunnel) to another point in the network, and then replays them into the network from that point. This creates the false impression that the two end points of the tunnel are very close to each other [8]. This tunneling enables the tunneled packet to arrive with fewer hops or lower delay than if the packet traversed a normal path. A wormhole is a tunnel which connects two remote nodes. As shown in Fig. 2, the upper black dot called as M1 and lower black dot called as M2. The attacker tunnels the routing beacon from M1 to M2.

The nodes in the remote area build the route through the wormhole located between M1 and M2. All the traffic in the remote area will be channeled through the wormhole. Now nodes which are near to M1 are considered as one hop neighbor to nodes which are near to M2. The devices used to mount the attack do not need to hold any valid network Ids and, hence, the adversary does not need to compromise any cryptographic quantities or network nodes in order to perform the attack. However, the wormhole puts the attacker in a very powerful position relative to other nodes in the network. The attacker discards rather

than forwarding all the data packets. Thereby, it creates a permanent denial-of-service attack, where the base station cannot receive any information from the target area**.**

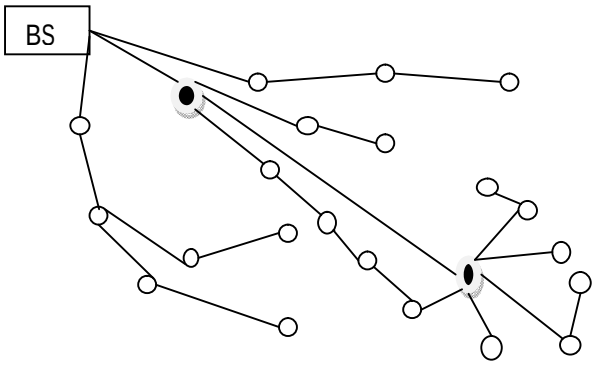


**Fig 2. Route discovery with wormhole attack**

In Sybil attack, a node illegitimately claims multiple identities. The Sybil attack was first described by Douceur in the context of peer-to-peer networks [10].

Sybil attacks are especially harmful as they are often the gateway to other attacks (such as those on resource exhaustion, voting, etc.). In [11] authors discussed various attacks which are launched by sybil attacks, these are, distributed storage, data aggregation, voting, fair resource allocation, misbehavior and routing.

Sybil attack can launch replication fragmentation. While the system may be designed to replicate or fragment data across several nodes, it could actually be storing data on Sybil identities generated by the same malicious node, so it may cause distributed storage. The Sybil attack can disturb the many routing algorithms. It may cause multi Sybil identity and route disturbance. By using the Sybil attack, one malicious node may be able to contribute to the aggregate many times. With enough Sybil nodes, an attacker may be able to completely alter the aggregate reading. Wireless networks use voting for a number of tasks. The Sybil attack could be used to "stu the ballot box" in any such vote. Depending on the number of identities the attacker owns, he may be able to determine the outcome of any vote. For example, this could be used to perform blackmail attacks, in which the attacker claims that a legitimate node is misbehaving. Conversely, if there is a vote on whether the attacker's identities are legitimate, the attacker could use his Sybil nodes to vouch for each other. Some network resources may be allocated on a per node basis. For example, nearby nodes sharing a single radio channel might each be assigned a fraction of time per interval during which they are permitted to transmit. The Sybil attack can be used to allow a malicious node to obtain an unfair share of any resource shared in this manner. This both denies service to legitimate nodes by reducing their share of the resource, and gives the attacker more resources to perform other attacks.

*F. Summary of the Stealthy Attacks*

(i) Misrouting
Relays the packet to the wrong next hop.

(ii) Power control
Control the transmission to the exclude next hop.

(iii) Colluding Collision
Simultaneous transmission to create a collision at the next hop.

(iv) Identity delegation
Delegate the relay responsibility to a colluding partner close to the sender.

## IV. CONCLUSION

In this paper we studied different routing protocols and routing attacks. We survived route discovery technology in different important routing protocol algorithms. We studied different routing attacks. In this study, we discover wormhole attack cause more harm in network as well as it is difficult identified in network and it can possible to make Denial of Service (DOS). Sybil attacks are especially harmful as they are often the gateway to other attacks. The many attacks are launch at network layer and with route request packets

## REFERENCES

[1] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless ad hoc networks ", in*Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), IEEE*, San Francisco, CA, 2003.

[2] Ibrahim, M.M.; Sadek, N.; El-Banna, M.; "Prevention of flooding attack in wireless ad-hoc AODV-based networks using Real-time Host Intrusion Detection", *in Proceedings of IFIP International Conference on Wireless and Optical Communications Networks*, 2009

[3] Bo-Cang Peng *et al.*, "Prevention Techniques for Flooding Attacks in Ad Hoc Networks," ieeexplore.ieee.org /iel5/9755/30769/01425219.pdf, 2003.

[4] Pin Nie "Security in Ad hoc Network", 28 –Mar-2007

[5] Yi-Chun Hu, Adrian Perrig, David B. Johnson ," Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols", *in Proceedings of the ACM Workshop on Wireless Security (WiSe)*, San Diego, California, USA, September 19,2003,pp. 30-40.

[6]. B. Partibane, Balasathis, Amaradeepan, R. Nakkeeran "Isolating the Black Hole Node in Mobile Ad Hoc Network using AODV Protocol" *in National conference in communication, NCC-2007*, pp. 193-196

[7] A.A. Pirzada and C. McDonald, "Establishing Trust inPure Ad-Hoc Networks," Proc. Australasian Conf.Computer Science (ACSC '04), vol. 26, no. 1, pp. 47-54, 2004.

◈◈◈