be difficult to accomplish in a MANET due to the absence of any central support infrastructure. Second, mobile nodes are roaming independently and are able to move in any direction. Therefore, any security solution with a static configuration would not be adequate for the dynamically changing topology. In most routing protocols for a MANET, nodes exchange information about the topology of the network so that routes can be established between a source and a destination. All messages are transmitted over the air; any intruder can maliciously give incorrect updating information by pretending to be a legitimate change of routing information. For instance, denial of service (DoS) can easily be launched if a malicious node floods the network with spurious routing messages. The other nodes may unknowingly propagate the messages.

Third, decentralized decision making in the MANET relies on the cooperative participation of all nodes. The malicious node could simply block or modify the traffic traversing it by refusing cooperation to break the cooperative algorithms. This property makes some centralized intrusion detection schemes fail.

Finally, some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. An attacker could create a new type of DoS attack by forcing a node to replay packets to exhaust its energy. Due to the limited network capacity and battery power of wireless nodes, frequent disconnection is common in wireless MANETs, which makes anomalies hard to distinguish from normalcy.

In general, the wireless MANET is particularly vulnerable due to its fundamental characteristics of open medium, dynamic topology, and absence of central authorities, distributed cooperation, and constrained capability. The existing security solutions for wired networks cannot be applied directly in wireless MANETs. In this Paper we study the security issues when routing is performed in a MANET, analyse in detail one type of attack -the "black hole" problem — that can easily be deployed against MANETs, and propose a feasible solution for ad hoc on-demand distance vector (AODV) routing protocol [3]. The rest of the Paper is organized as follows. We discuss the routing security issues in a MANET and give an overview of current security schemes proposed for MANETs in the literature. The different routing protocols are also introduced. We describe the black hole problem in AODV protocol in detail. To mitigate the attacks, one feasible solution to the black hole problem is presented. Finally, we provide conclusions and directions for future research.

2. Literature Review

A. Routing protocols of MANETs

Many different routing protocols [4] have been developed for MANETs. They can be classified into two categories:

Table-driven: Table driven routing protocols essentially use proactive schemes. They 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 any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view.

On demand: A different approach from table driven routing is source-initiated on-demand routing. This type of routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined.

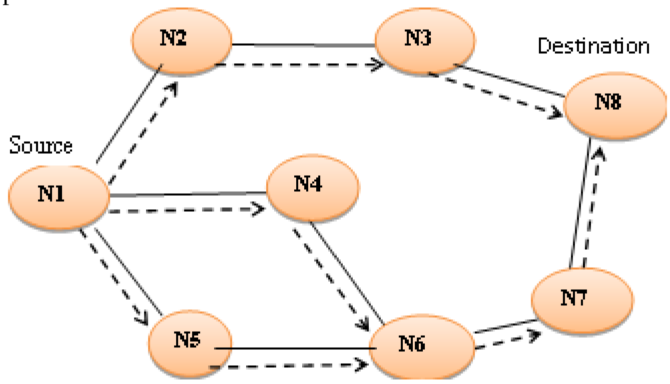

Figure 2: *Propagation of RREQ.*

Three main routing protocols for a MANET are destination-sequenced distance-vector routing protocol (DSDV), AODV, and Dynamic Source Routing protocol (DSR). DSDV is a table-driven routing protocol based on the classical Bellman-Ford routing mechanism. In this routing protocol, each mobile node in the system maintains a routing table in which all the possible destinations and the number of hops to them in the network are recorded. AODV builds on the DSDV algorithm described above and is an improvement since it typically minimizes the number of required broadcasts by creating routes on a demand basis, as opposed to maintaining a complete list of routes as in DSDV. It is an on demand route acquisition system, since nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges. DSR is different from AODV in the sense that each mobile node keeps track of the routes of which it is aware in a route cache. Upon receiving a search request for path, it consults with its route cache to see if it contains the required information. This protocol uses more memory while reducing the route discovery delay in the system.

Effective operation of a MANET is dependent on maintaining appropriate routing information in a distributed fashion. But no security is considered in currently proposed routing protocols, which makes the routing protocol an easy target for attackers.

B. Routing security in MANETs

Security always implies the identification of potential attacks, threats and vulnerabilities of a certain system. Vesa Karpijoki [1] and Janne Lundberg [5] discussed selected types of attacks that can easily be performed against a MANET. Attacks can be classified into *passive* and *active attacks*. A passive attack does not disrupt the operation of a routing protocol, but only attempts to discover valuable information by listening to routing traffic, which makes it very difficult to detect. An active attack is an attempt to improperly modify data, gain authentication, or procure authorization by inserting false packets into the data stream or modifying packets transition through the network. Active attack can be further divided into external attacks and internal attacks. An *external attack* is one caused by nodes that do not belong to the network. An *internal attack* is one from compromised or hijacked nodes that belong to the network.

Internal attacks are typically more severe, since malicious nodes already belong to the network as authorized parties. Therefore, such nodes are protected with the network security mechanisms and underlying services. Next, we describe some types of active attacks [1, 5] easily performed against a MANET in the network layer.

- **Black hole**: In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. We provide a detailed description herein.
- **Denial of service**: The DoS attack results when the network bandwidth is hijacked by a malicious node. It has many forms: the classic way is to flood any centralized resource so that the network no longer operates correctly or crashes. For instance, a route request is generated whenever anode has to send data to a particular destination. A malicious node might generate frequent unnecessary route requests to make the network resources unavailable to other nodes.
- **Routing table overflow**: The attacker attempts to create routes to non-existent nodes. The goal is to have enough routes so that creation of new routes is prevented or the implementation of routing protocol is overwhelmed.
- **Impersonation**: A malicious node may impersonate another node while sending the control packets to create an anomaly update in the routing table.
- **Energy consummation**: Energy is a critical parameter in the MANET. Battery-powered devices try to conserve energy by transmitting only when absolutely necessary. An attacker can attempt to consume batteries by requesting routes or forwarding unnecessary packets to a node.
- **Information disclosure**: The malicious node may leak confidential information to unauthorized users in the network, such as routing or location information. In the end, the attacker knows which nodes are situated on the target route.

The research in security for MANETs is still in its infancy. Several security schemes for MANETs have been proposed. In distributed key management services [2], the task of transmitting routing information is achieved in a redundant way such that if some route fails or a relatively small amount of nodes are compromised, the network is not critically affected. To frustrate attacks that attempt to find out the certificate authority's secret key within a short span, the share refreshing is also used. But it is assumed that the shared signature of private key of key management service cannot be disclosed to adversary. This assumption may not be true if the internal node is compromised. Stajano and Anderson [6] elucidate some of the security issues facing MANETs and investigate ways for low-compute-power MANETs such as sensor networks, and personal digital assistants (PDAs) where full public key cryptography may not be feasible. Sergio Marti *et al.* [7] introduced *Watchdog* and *Pathrater* techniques that improve throughput in a MANET by identifying misbehaving nodes that agree to forward the packets but never do so. *Watchdog* is used to identify misbehaving nodes, and *Pathrater* to help routing protocols avoid these nodes. Zhang and Lee [8] first presented a new intrusion detection and response mechanism for MANETs. The basic assumption is that the user and associated program activities are observable, and the underlying distributed system needs to be cooperative. In this architecture, every node participates in the intrusion detection and response mechanism. The data collection mechanism present in every node gathers streams of real-time audit data from various sources. Local detection analyses the local data traces gathered by the local data collection module for evidence of anomalies. This Paper provides a good guide for designing an intrusion detection model for MANETs. Albers [9] recently defined adapted intrusion detection architecture for the MANETs by going through the requirements of intrusion detection mechanism coupled with a mobile-agent-based intrusion detection system could ensure the security services required by users in the MANET.

An external attack prevention and internal attack detection model for AODV was proposed in [10]. The External Attack Prevention Model (EAPM) secures the network from external attacks by implementing *message authentication code* (MAC) to ensure integrity of route request packets. A scheme to eliminate excessive flooding of the authentication control message is also proposed. The Internal Attack Detection Model (IADM) is used to analyse local data traces gathered by the local data collection module and identify the misbehaving nodes in the network. Whenever the IADM determines a misbehaving node, the response model (RM) sends out alarm messages to the whole network to isolate the misbehaving node. One problem of the IADM is the high false positive rate since abnormal behaviour is sometimes very difficult to separate from normal behaviour. In this Paper we attempt to avoid the high false positive rate problem.

3. Problem Statement: The Black Hole Problem in Current AODV Protocol

AODV is an important on-demand routing protocol that creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a *route discovery* process within the network. It broadcasts a route request (RREQ) packet (Fig. 2) to its neighbours, which then forward the request to their neighbours, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located. In this process the intermediate node can reply to the RREQ packet only if it has a fresh enough route to the destination. Once the

RREQ reaches the destination or an intermediate node with a fresh enough route, the destination or intermediate node responds by unicasting a route reply (RREP) packet (Fig. 3) back to the neighbour from which it first received the RREQ.

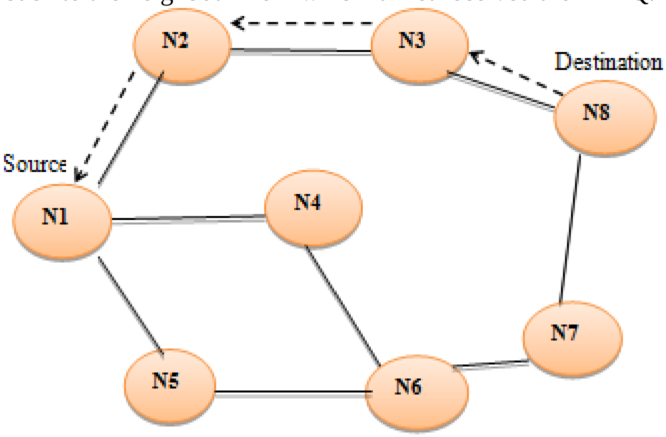

Figure 3: *The path of a routing reply.*

After selecting and establishing a route, it is maintained by a *route maintenance* procedure until either the destination becomes inaccessible along every path from the source or the route is no longer desired.

In this Paper we address one routing attack that could easily happen in wireless MANETs, the black hole problem. According to the original AODV protocol, any intermediate node may respond to the RREQ message if it has a fresh enough route, which is checked by the destination sequence number contained in the RREQ packet. This mechanism is used to decrease the routing delay, but makes the system a target of a malicious node. The malicious node easily disrupts the correct functioning of the routing protocol and makes at least part of the network crash.

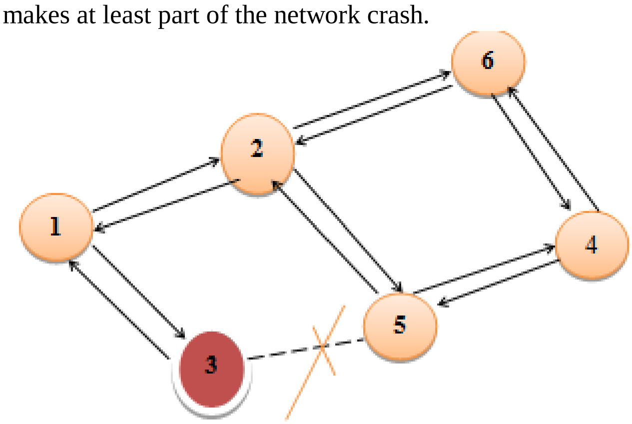

Figure 4: *The black hole problem.*

For example, node 1 wants to send data packets to node 4 in Fig. 4, and initiates the route discovery process. We assume node 3 to be a malicious node with no fresh enough route to destination node 4. However, node 3 claims that it has the route to the destination whenever it receives RREQ packets, and sends the response to source node 1. The destination node and any other normal intermediate nodes that have the fresh route to the destination may also give a reply. If the reply from a normal node reaches the source node of the RREQ first, everything works well; but the reply from malicious node 3 could reach the source node first, if the malicious node is nearer to the source node. Moreover, a malicious node does not need to check its routing table when sending a false message; its response is more likely to reach the source node first. This makes the source node think that the route discovery process is complete, ignore all other reply messages, and begin to send data packets. As a result, all the packets through the malicious node are simply consumed or lost. The malicious node could be said to form a black hole in the network, and we call this the black hole problem. In this way the malicious node can easily misroute a lot of network traffic to itself, and could cause an attack to the network with very little efforts on its part.

4. A Proposed Solution to the Black Hole Problem

One possible solution to the black hole problem is to disable the ability to reply in a message of an intermediate node, so all reply messages should be sent out only by the destination node. Using this method the intermediate node cannot reply, so in some sense we avoid the black hole problem and implement a secured AODV protocol. But there are two associated disadvantages. First, the routing delay is greatly increased, especially for a large network. Second, a malicious node can take further action such as fabricate a reply message on behalf of the destination node. The source node cannot identify if the reply message is really from the destination node or fabricated by the malicious node. In this case, the method may not be adequate.

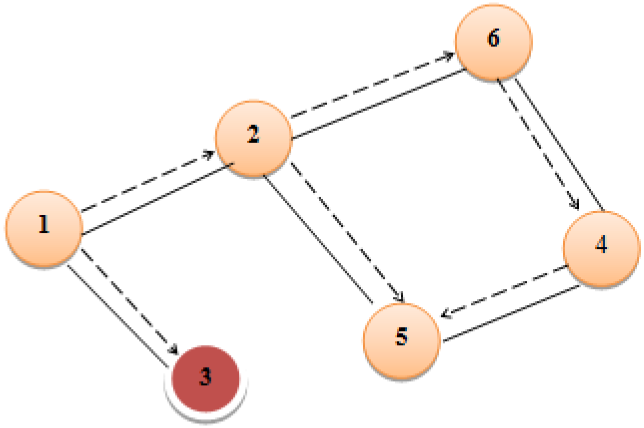

Figure 5: Propagation of Further Request.

We propose another solution using one more route to the intermediate node that replays the RREQ message to check whether the route from the intermediate node to the destination node exists or not. If it exists, we can trust the intermediate node and send out the data packets. If not, we just discard the reply message from the intermediate node and send out alarm message to the network and isolate the node from the network.

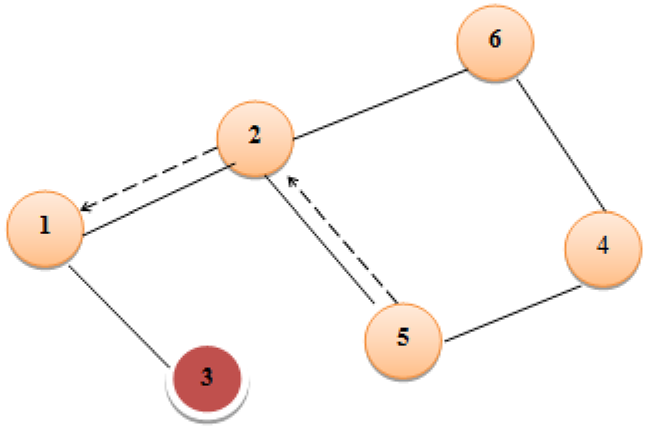

Figure 6: *The path of Further Reply.*

The following is the detailed checking process. We use the same example as in Fig. 4, and assume node 3 is a malicious node. In the proposed method, we require each intermediate node to send back the *next hop* information when it sends back an RREP message. Thus, node 3 sends back the *next hop* information when it sends the RREP packet to source node 1. Here we assume the *next hop* it sends back is node 5. When node 1 receives the reply message from node 3, it does not send the data packets right away, but extracts the *next hop* information from the reply packet and then sends a *Further- Request* to the *next hop* (node 5 in Fig. 5) to verify that it has a route to the intermediate node who sends back the reply message, and that it has a route to the destination node. To avoid the problem of reclusiveness, only the requested *next hop* can send back a *Further Reply* message, which includes the *check result*. The inquired intermediate node may also send back the *Further Reply* message when it receives the *Further- Request*. In this method we ignore the *Further Reply* message from the inquired intermediate node (node 3 in Fig. 6). Thus, we avoid the situation of the intermediate node taking further action such as fabricating the reply message on behalf of the *next hop* node. When the source node receives the *Further Reply* from the *next hop*, it extracts the *check result* from the reply packets. If the result is yes, we establish a route to the destination and begin to send out data packets. If the *next hop* has no route to the inquired intermediate node, but has a route to the destination node, we discard the reply packets from the inquired intermediate node, and use the new route through the *next hop* to the destination. At the same time, send out the alarm message to the whole network to isolate the malicious node. If the *next hop* has no route to the requested intermediate node, and it also has no route to the destination node, the source node initiates another routing discovery process, and also sends out an alarm message to isolate the malicious node.

Using this method, we avoid the black hole problem, and also prevent the network from further malicious behaviour. We don't disable the ability of a replying message from intermediate nodes, but the routing overhead is greatly increased if we do the check process to every intermediate node that sends a reply message simulation results show that we are able to secure the AODV protocol from black hole attacks and achieve increased throughput, while keeping the routing overhead minimal.

5. Conclusion and Future Work

The MANET is an emerging research area with practical applications. However, a wireless MANET presents a greater security problem than conventional wired and wireless networks due to its fundamental characteristics of open medium, dynamic topology, absence of central authorities, distributed cooperation, and constrained capability. Routing security plays an important role in the security of the entire network. In general, routing security in wireless networks appears to be a nontrivial problem that cannot easily be solved. It is impossible to find a general idea that can work efficiently against all kinds of attacks, since every attack has its own distinct characteristics. In this Paper we study the routing security issues of MANET, analyse one type of attack, the black hole, that can easily be deployed against a MANET, and propose a feasible solution for it in the AODV protocol.

6. Acknowledgment

This research is supported by MANETs Research Program through the Sinhgad Institute of Technology, Lonavala, Pune, Maharashtra, India. Development of global path relate to mobility because its current trends in MANETs.

References

[1] V. Karpijoki, "Security in Ad Hoc Networks," http://www.hut.fi/~vkarpijo/netsec00/netsec00_manet_sec.ps
[2] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," *IEEE Net.*, vol. 13, no. 6, Nov./Dec. 1999.
[3] E. Perkins, S. R. Das, and E. Royer, "Ad-Hoc on Demand Distance Vector (AODV)," Mar. 2000; http://www.ietf.org/internet-drafts/draft-ietf-manetaodv-05.txt
[4] P. Agrawal and Q.-A. Zeng, *Introduction to Wireless and Mobile Systems*, Brooks/Cole Publishing, Aug. 2002.
[5] J. Lundberg, "Routing Security in Ad Hoc Networks," Helsinki University of Technology, http://citeseer.nj.nec.com/400961.html
[6] Stajano and R. Anderson, "The Resurrecting Ducking: Security Issues for Ad-Hoc Wireless Networks," *Security Protocols, 7th Int'l. Wksp. Proc., LNCS*, 1999.
[7] S. Marti *et al.*, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *6th Int'l. Conf. Mobile Comp. Net.*, Aug. 2000, pp. 255–65.
[8] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc networks," *Proc. 6th Int'l. Conf. Mobile Comp. Net., MobiCom 2000*, Aug. 2000, pp. 275–83.
[9] L. Venkatraman and D. P. Agrawal, "Strategies for Enhancing Routing Security in Protocols for Mobile Ad Hoc Networks," *J. Parallel Distrib. Comp.*, 2002.