Mobile Ad Hoc Network Security Vulnerabilities

Animesh K. Trivedi
Indian Institute of Information Technology, India

Rajan Arora
Indian Institute of Information Technology, India

Rishi Kapoor
Indian Institute of Information Technology, India

Sudip Sanyal
Indian Institute of Information Technology, India

Ajith Abraham
Norwegian University of Science and Technology, Norway

Sugata Sanyal
Tata Institute of Fundamental Research, India

INTRODUCTION

Mobile ad hoc networks inherently have very different properties from conventional networks. A mobile ad hoc network (MANET) is a collection of mobile nodes that are self configuring (network can be run solely by the operation of the end-users), capable of communicating with each other, establishing and maintaining connections as needed. Nodes in MANET are both routers and terminals. These networks are dynamic in the sense that each node is free to join and leave the network in a nondeterministic way. These networks do not have a clearly defined physical boundary, and therefore, have no specific entry or exit point. Although MANET is a very promising technology, challenges are slowing its development and deployment. Nodes in ad hoc networks are in general limited in battery power, CPU and capacity. Hence, the transmission ranges of these devices are also limited and nodes have to rely on the neighboring nodes in the network to route the packet to its destination node. Ad hoc networks are sometimes referred to as multi-hop networks, where a hop is a direct link between two nodes.

MANET has many important applications, including battlefield operations, emergency rescues, mobile conferencing, home and community networking, sensor dust and so forth.

Due to limited memory and computational power, nodes in MANETs have limited services and security provision. Unlike wired networks which have a higher level of security for gateways and routers, ad hoc networks have characteristics such as dynamically changing topology, weak physical protection of nodes, no established infrastructure or centralized administration and high dependence on inherent node cooperation. The routing protocols used in the current generation of mobile ad hoc networks, like Dynamic Source Routing (DSR), and Ad hoc On Demand Distance Vector Routing Protocol (AODV), are based on the principle that all nodes will cooperate, but dynamic and cooperative nature of MANETS presents substantial challenges to this assumption (Johnson, Maltz, & Broch, 2001; Perkins & Royer, 1999). Without node cooperation in a mobile ad hoc network, routes cannot be established, and packets cannot be forwarded. As a consequence, access control mechanisms, (similar to firewalls in wired networks) are not feasible. However, cooperative behavior, such as forwarding other node's messages, cannot be taken for granted because any node could misbehave. Misbehavior means deviation from regular routing and forwarding protocol assumption. It may arise for several reasons, non-intentionally when a node is faulty or intentionally when a node may want to save its resources. Cooperation in mobile ad hoc networks is a big issue of consideration. To save battery, bandwidth, and processing power, nodes should not forward packets for others. If this dominant strategy is adopted, the outcome is a nonfunctional network when multi-hop routes are needed, so all nodes are worse off. Without any counter policy, the effects of misbehavior have been shown to dramatically decrease network performance. Depending on the proportion of misbehaving nodes and their strategies, network throughput could decrease, and there could be packet losses, denial of

service or network portioning. These detrimental effects of misbehavior can endanger the entire network.

Wireless ad hoc networks are vulnerable to various attacks. These include passive eavesdropping, active interfering, impersonation, modification of packets and denial-of-service. Intrusion prevention measures, such as strong authentication and redundant transmission, can be used to tackle some of these attacks. However, these techniques can address only a subset of the threats, and moreover, are costly to implement due to the limited memory and computation power on nodes. We can identify two types of uncooperative nodes: faulty or malicious and selfish. Faulty or malicious behavior refers to the broad class of misbehavior in which nodes are either faulty and can therefore not follow a protocol, or are intentionally malicious and try to attack the system. Selfishness refers to no cooperation in certain network operations. In mobile ad hoc networks, the main threat from selfish nodes is dropping of packets (black hole), which may affect the performance of the network severely. Faulty, malicious and selfish nodes are misbehaved nodes.

ROUTING IN MANETs

Dynamic Source Routing is a popular routing protocol for ad hoc networks and was proposed for MANET by Johnson, Maltz and Broch (2001). In DSR, nodes do not store route to different nodes but they are discovered as they are needed. This type of routing is called R*eactive* routing and protocols used in this are called R*eactive* P*rotocols* (e.g., DSR, AODV, etc.). DSR works as follows: Nodes send out a ROUTE REQUEST (RREQ) message, all nodes that receive this message put themselves into the source route and forward it to their neighbors, unless they have received the same request before. If a receiving node is the destination, or has a route to the destination, it does not forward the request, but sends a REPLY (RREP) message containing the full source route. It may send that reply along the source route in reverse order or issue a ROUTE REQUEST including the route to get back to the source, if the former is not possible due to asymmetric links. After receiving one or several routes, the source selects the best (by default the shortest) route, stores it, and sends messages along that path. The better the route metrics (number of hops, delay, bandwidth, or other criteria) and the sooner the REPLY arrives at the source, the higher the preference given to the route and the longer it will stay in the cache. Because route to the destination is put into the packet, it is called source routing.

Attacks on DSR

There are a number of attacks possible on DSR protocol because there is no security measure and it assumes honest coordination of nodes among them and to protocol. A few attacks are outlined in this section and others are discussed in detail in the cited references.

- Dropping of packets by a node takes into account the following scenarios-Drop all packets not destined to it or perform only partial dropping. Partial dropping can be restricted to specific types, such as only data packets, or route control packets that contain it or packets destined to specific nodes.
- Avoid sending a ROUTE ERROR when having detected an error, to prevent other nodes from looking for alternative routes.
- By sending forged routing packets, an attacker can create a so-called black hole, a node where all packets are discarded or all packets are lost.
- Attempt to make routes that go through one appear longer by adding some virtual nodes to the route. Thus, a shorter route will be chosen, avoiding this node.
- Modify the nodes list in the header of a ROUTE REQUEST or a ROUTE REPLY to misroute packets and to add incorrect routes in the route cache of other nodes.
- Decrease the hop count (TTL) when receiving a packet, so that the packet will never be received by the destination. This attack could be detected by the previous node in route by enhanced passive acknowledgment.
- Initiate frequent ROUTE REQUEST to consume bandwidth and energy and to cause congestion.
- Send route replies with a time not proportional to the length of the route. This can give more priority to long routes, thus attracting routes to the attacker, or less priority to short routes, thus avoiding the attacker.

Listed above are some frequent attacks possible on DSR operating without any security measurements.

INTRUSION DETECTION SYSTEMS

Intrusion detection systems (IDS), especially those which are reputation-based, are a new paradigm and are being used for enhancing security in different areas. These systems are lightweight, easy to use and are capable to face a wide variety of attacks as long as they are observable. Among these mechanisms, some of the popular ones are CORE, CONFIDANT, OCEAN and SAFE.

Reputation-Based IDS

Reputation-based IDS do not rely on the conventional use of a common secret to establish confidential and secure communication between two parties. Instead, they are simply based on each other's observations (Buchegger & Le Boudec, 2005). To be more precise, every node in the network moni-