Research Paper

Volume : 2 | Issue : 3 | Mar 2013 • ISSN No 2277 - 8179

Classification of Attacks Against the Mobile AD Hoc Networks

Computer Science

KEYWORDS: AODV, Denial of Service (DoS), route request, route reply, route error

V. Karamchand Gandhi — Coordinator, Center for Distance Education, Bharathidasan University, Assistant Professor, Department of Computer Science, Bharath College of Science and Management, Thanjavur – 613 005, Tamil Nadu

D.P.Jeyabalan — Head, Department of Information Technology and, Associate Professor of Computer Science, St.Joseph's College (Autonomous), Tiruchirappalli - 620 002, Tamil Nadu.

ABSTRACT

Mobile ad hoc networks (MANETs) are one of the fastest growing areas of research. They are an attractive technology for many applications, such as rescue and tactical operations, due to the flexibility provided by their dynamic infrastructure. However, this flexibility comes at a price and introduces new security threats. Furthermore, many conventional security solutions used for wired networks are ineffective and inefficient for the highly dynamic and resource-constrained environments where MANET use might be expected. To develop suitable security solutions for such new environments, we must first understand how MANETs can be attacked. This paper provides the comprehensive survey of attacks against a specific type of target, namely the routing protocols used by MANETs. We introduce the security issues specific to MANETs and present a detailed classification of the attacks/attackers against these complex distributed systems.

1. INTRODUCTION

Smaller and more powerful mobile devices, mobile ad hoc networks (MANETs) have become one of the fastest growing areas of research. This new type of self-organizing network combines wireless communication with a high degree node mobility. Unlike conventional wired networks, they have no fixed infrastructure (base stations, centralized management points and the like). The union of nodes forms an arbitrary topology. This flexibility makes them attractive for many applications such as military applications, where the network topology may change rapidly to reflect a force's operational movements, and disaster recovery operations, where the existing/fixed infrastructure may be non-operational. The ad hoc self-organisation also makes them suitable for virtual conferences, where setting up a traditional network infrastructure is a time consuming high-cost task.

Conventional networks use dedicated nodes to carry out basic functions like packet forwarding, routing, and network management. In ad hoc networks these are carried out collaboratively by all available nodes. Nodes on MANETs use multi-hop communication. Nodes that are within each other's radio range can communicate directly via wireless links, while those that are far apart must rely on intermediate nodes to act as routers to relay messages. Mobile nodes can move, leave and join the network and routes need to be updated frequently due to the dynamic network topology.

2. VULNERABILITIES OF MANETS

Wireless Links: First of all, the use of wireless links makes the network susceptible to attacks such as eavesdropping and active interference. Unlike wired networks, attackers do not need physical access to the network to carry out these attacks. Furthermore, wireless networks typically have lower bandwidths than wired networks. Attackers can exploit this feature, consuming network bandwidth with ease to prevent normal communication among nodes.

Dynamic Topology: MANET nodes can leave and join the network, and move independently. As a result the network topology can change frequently. It is hard to differentiate normal behaviour of the network from anomaly/malicious behaviour in this dynamic environment. For example, a node sending disruptive routing information can be a malicious node, or else simply be using outdated information in good faith. Moreover, mobility of nodes means that we cannot assume nodes, especially critical ones (servers, etc.), are secured in locked cabinets as in wired networks. Nodes with inadequate physical protection may often be at risk of being captured and compromised.

Cooperativeness: Routing algorithms for MANETs usually assume that nodes are cooperative and non-malicious. As a result, a malicious attacker can easily become an important routing agent and disrupt network operations by disobeying the protocol specifications. For example, a node can pose as a neighbour to other nodes and participate in collective decision-making mechanisms, possibly affecting networking significantly.

Lack of a Clear Line of Defence: MANETs do not have a clear line of defence; attacks can come from all directions [2]. The boundary that separates the inside network from the outside world is not very clear on MANETs. For example, there is no well defined place where we can deploy our traffic monitoring, and access control mechanisms. Whereas, all traffic goes through switches, routers, or gateways in wired networks, network information in MANETs is distributed across nodes that can only see the packets sent and received in their transmission range.

Limited Resources: Resource constraints are a further vulnerability. There can be a variety of devices on MANETs, ranging from laptops to handheld devices such as PDAs and mobile phones. These will generally have different computing and storage capacities that can be the focus of new attacks. For example, mobile nodes generally run on battery power. This has led to emergence of innovative attacks targeting this aspect, e.g. "Sleep Deprivation Torture [3]".

3. AODV ROUTING PROTOCOL

There have been many routing protocols proposed to suit the different needs of MANETs. Unfortunately most of these routing protocols do not consider security. One of the most popular of them is the Ad hoc On-Demand Vector (AODV) routing protocol.

AODV is a reactive routing protocol, discovering routes only when they are needed. "It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within ad hoc network" [5]. It is claimed that AODV can handle low, moderate, and relatively high mobile rates, together with a variety of data traffic loadings [5]. However, it makes no provisions for security. There are three main types of messages in AODV: route request (RREQ), route reply (RREP), and route error (RERR) messages. When a node wants to communicate with another node in the network and does not have a fresh route to this destination, it starts the route discovery process by broadcasting a RREQ message for the destination node into the network. Intermediate nodes that receive this request either send a RREP to the source node if they have a fresh route to the destination node and the "destination only" flag is not set, or forward the RREQ message to other nodes. A fresh route is a valid route entry whose sequence number is equal to or greater than that contained in the RREQ message. If the request packet has

been forwarded by this intermediate node before, it is silently dropped. When the destination node receives a RREQ for itself, it sends back a RREP message on the reverse route.

The requesting node and the nodes receiving RREP messages on the route update their routing tables with the new route. Wireless mobile networks can have frequent link breakages due to the mobility of nodes in the network or simply due to transmission errors. AODV allows mobile nodes to respond to link breakages and changes in a timely manner [5]. The methods for a node to control its connectivity to its active next hops on AODV are:

- o link layer notification using control packets such as link layer acknowledgement messages (e.g. ACK or RTS-CTS);
- o passive acknowledgement: notification by listening on the channel to determine if the next node forwards the packet or not; and
- o Receiving any packet from the next node or sending some request packets to the next node, such as RREQ or ICMP Echo Request, or Hello messages which are periodic control messages sent only to one hop neighbours.

Let's assume that a link breakage to the next hop is detected by the absence of hello messages in the allowed time interval (or with any of the methods above). The routes affected by the link breakage in the routing table are invalidated and the nodes affected by the link breakage are notified using RERR messages. If the link breakage occurs on an active route, a local repair mechanism can be initiated. In this mechanism new RREQ messages are broadcast to the destination by nodes on the existing route who detect the link breakage.

4. ATTACKS ON MANET

At the highest level, the security goals of MANETs are not that different from other networks: most typically authentication, confidentiality, integrity, availability, and non-repudiation. Authentication is the verification of claims about the identity of a source of information. Confidentiality means that only authorized people or systems can read or execute protected data or programs. It should be noted that the sensitivity of information in MANETs may decay much more rapidly than in other information. For example, yesterday's troop location will typically be less sensitive than today's. Integrity means that the information is not modified or corrupted by unauthorized users or by the environment. Availability refers to the ability of the network to provide services as required. Denials of Service (DoS) attacks have become one of the most worrying problems for network managers. In a military environment, a successful DoS attack is extremely dangerous, and the engineering of such attacks is a valid modern war-goal. Lastly, non-repudiation ensures that committed actions cannot be denied. In MANETs security goals of a system can change in different modes (e.g. peace time, transition to war, and war time of a military network).

The characteristics of MANETs make them susceptible to many new attacks. At the top level attacks can be classified according to network protocol stacks.

Layers	Attacks
Application Layer	Data Corruption, Viruses and Worms
Transport Layer	TCP/UDP SYN flood
Network Layer	hello flood, black hole
Data Link Layer	Monitoring, Traffic Analysis
Physical Layer	Eavesdropping, Active Interference

Table 1

Table 1 gives a few examples of attacks at each layer. Some attacks could occur in any layer of the network protocol stack, e.g. jamming at physical layer, hello flood at network layer, and SYN flood at transport layer are all DoS attacks.

5. ADVERSARY MODEL

Attackers against a network can be classified into two groups: insider and outsider attackers. Whereas an outsider attacker is not a legitimate user of the network, an insider attacker is an authorized node and a part of the routing mechanism on MANETs. Routing algorithms are typically distributed and cooperative in nature and affect the whole system. While an insider MANET node can disrupt the network communications intentionally, there might be other reasons for its apparent misbehaviours. A node can be failed, unable to perform its function for some reason, such as running out of battery, or collusions in the network. The threat of failed nodes is particularly serious if they are needed as part of an emergency/secure route [6]. Their failure can even result in partitioning of the network, preventing some nodes from communicating with other nodes in the network. A selfish node can also misbehave to preserve its resources. Selfish nodes avail themselves of the services of the other nodes, but do not reciprocate.

We should also consider the misuse goals of attackers. In routing attacks attackers do not follow the specifications of routing protocols and aim to disrupt the network communication in the following ways:

- o Route Disruption: modifying existing routes, creating routing loops, and causing the packets to be forwarded along a route that is not optimal, non-existent, or otherwise erroneous.
- o Node Isolation: isolating a node or some nodes(s) from communicating with other nodes in the network, partitioning the network, etc.
- o Resource Consumption: decreasing network performance, consuming network bandwidth or node resources, etc.

Ning et al. consider each of these goals in their research which analyses insider attacks against AODV [7]. Achieving these goals depends on the capabilities of the adversary. The main factors affecting the performance of an attack are identified below.

Computational power:

This clearly affects the ability of an attacker to compromise a network. Such power need not be localised to the attached network – eavesdropped traffic can be relayed back to high performance super-computing networks for analysis.

Deployment capability:

Adversary distribution may range form a single node to a pervasive carpet of smart counter-dust, with a consequent variation in attack capabilities [8].

Location control:

The location of adversary nodes has may have a clear impact on what the adversary can do. An adversary may be restricted to placing attack nodes at the geographical boundary of an enemy network (but may otherwise choose the precise locations), may plant specific nodes (e.g. nodes left behind in territory about to be vacated), or may have the ability post facto to create a pervasive carpet of smart dust (where arbitrary degrees of pervasiveness may be achieved).

Mobility:

Mobility generally brings an increase in power. (A mobile node can always remain stationary.) On the other hand, mobility may prevent an attacker from continually targeting one specific victim. For example, a node on the move might not receive all falsified routing packets initiated by the attacker. In [9] Sun et al defined this phenomenon as being a "partial victim".

6. ATTACKS

We can classify attacks as passive or active.

6. 1.Passive attacks

In a passive attack, an unauthorized node monitors and aims to find out information about the network. The attackers do not otherwise need to communicate with the network. Hence they do not disrupt communications or cause any direct damage to the network. However, they can be used to get information for future harmful attacks. Examples of passive attacks are eavesdropping and traffic analysis.

Eavesdropping Attacks, also known as disclosure attacks, are passive attacks by external or internal nodes. The attacker can

analyse broadcast messages to reveal some useful information about the network. Solutions protecting the radio interface from attacks such as eavesdropping (and jamming) attacks have been proposed in the literature, e.g. spread spectrum communication and frequency hopping [10].

Traffic Analysis is not necessarily an entirely passive activity. It is perfectly feasible to engage in protocols, or seek to provoke communication between nodes. Attackers may employ techniques such as RF direction finding, traffic rate analysis, and time-correlation monitoring. For example, by timing analysis it can be revealed that two packets in and out of an explicit forwarding node at time t and t+€ are likely to be from the same packet flow [11]. Traffic analysis in ad hoc networks may reveal:

- The existence and location of nodes;
- The communications network topology;
- The roles played by nodes;
- The current sources and destination of communications; and
- The current location of specific individuals or functions (e.g. If the commander issues a daily briefing at 10am, traffic analysis may reveal a source geographic location).

6. 2. Active Attacks:
These attacks cause unauthorised state changes in the network such as denial of service, modification of packets, and the like. These attacks are generally launched by users or nodes with authorisation to operate within the network. We classify active attacks into four groups: dropping, modification, fabrication, and timing attacks. It should be noted that an attack can be classified into more than one group.

Dropping Attacks: Malicious or selfish nodes deliberately drop all packets that are not destined for them. While malicious nodes aim to disrupt the network connection, selfish nodes aim to preserve their resources. Dropping attacks can prevent end-to-end communications between nodes, if the dropping node is at a critical point.

Modification Attacks: Insider attackers modify packets to disrupt the network. For example, in the sinkhole attack the attacker tries to attract nearly all traffic from a particular area through a compromised node by making the compromised node attractive to other nodes. A sinkhole attack can be used as a basis for further attacks like dropping and selective forwarding attacks. A black hole attack is like a sinkhole attack that attracts traffic through itself and uses it as the basis for further attacks. The goal is to prevent packets being forwarded to the destination. If the black hole is a virtual node or a node outside the network, it is hard to detect [12].

Fabrication Attacks: Here the attacker forges network packets. In [13], fabrication attacks are classified into "active forge" in which attackers send faked messages without receiving any related message and "forge reply" in which the attacker sends fake route reply messages in response to related legitimate route request messages. In the forge reply attack, the attacker forges a Route Reply message after receiving a Route Request message. The reply message contains falsified routing information showing that the node has a fresh route to the destination node on AODV in order to suppress real routes to the destination.

Another interesting fabrication attack on MANETs is the routing cache poisoning attack [14]. A node can update its table with the routing information in the packets that it hears, even if it is not on the route of the packets. The attacker can make use of this property to poison the routes to a victim node by sending spoofed routing information packets, causing neighbouring nodes to update their tables erroneously.

Timing Attacks: An attacker attracts other nodes by causing itself to appear closer to those nodes than it really is. DoS attacks, rushing attacks, and hello flood attacks use this technique. Rushing attacks [15] occur during the Route Discovery phase. In all existing on-demand protocols, a node needing a route broadcasts Route Request messages and each node forwards only the first arriving Route Request in order to limit the overhead of message flooding. Rushing attacks can be carried out in many ways: by ignoring delays at MAC or routing layers, by wormhole attacks, by keeping other nodes' transmission queues full, or by transmitting packets at a higher wireless transmission power [15]. The hello flood attack [16] is another attack that makes the adversary attractive for many routes.

CONCLUSION
In this paper we have examined the main security issues in MANETs. They have most of the problems of wired networks and many more besides due to their specific features: dynamic topology, limited resources (e.g. bandwidth, power), lack of central management points. In this paper, we mainly concentrate on attacks carried out by malicious nodes who intentionally aim to disrupt the network communication. Firstly we have presented specific vulnerabilities of this new environment. Then we have surveyed the attacks exploit these vulnerabilities in the literature. Attacks are classified into passive and active attacks at the top level. Since proposed routing protocols on MANETs are insecure, we have mainly focused on active routing attacks which are classified into dropping, modification, fabrication, and timing attacks. Attackers have also been discussed and examined under insider and outsider attackers. Insider attacks are examined on our exemplar routing protocol AODV. Conventional security techniques are not directly applicable to MANETs due to their very nature. Researchers currently focus on developing new prevention, detection and response mechanism for MANETs.

REFERENCE

[1] Parker J., Undercoffer J., Pinkston J., Joshi A., "On Intrusion Detection and Response for Mobile Ad Hoc Networks", In Proc. of 23rd IEEE Int. Performance Computing and Communications Conference, 2004 [2] Zhang Y., Lee W., "Intrusion Detection Techniques for Mobile Wireless Networks", Wireless Networks, pp. 545-556, Springer, 2003 [3] Ning P., Sun K., "How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols", In Proc. of the IEEE Workshop on Information Assurance, pp. 60-67, 2003 [4] Yang H., Luo H., Ye F., Lu S., Zhang L., "Security in Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, 11(1), pp. 38-47, 2004. [5] Perkins C., Belding-Royer E., Das S., "RFC 3561: Ad hoc On-Demand Distance Vector (AODV) Routing", http://www.ietf.org/rfc/rfc3561.txt, 2003 [6] Yau P.-W., Mitchell C.J., "Security Vulnerabilities in Ad Hoc Networks", In Proc. of the 7th Int. Symp. on Communications Theory and Applications, pp. 99-104, 2003 [7] Ning P., Sun K., "How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols", In Proc. of the IEEE Workshop on Information Assurance, pp. 60-67, 2003 [8] Chivers H., Clark J. A., "Smart dust, friend or foe?--Replacing identity with configuration trust", Computer Networks 46(5), pp. 723-740, 2004 [9] Sun B., Wu K., Pooch U.W., "Zone-Based Intrusion Detection for Mobile Ad Hoc Networks", Int. Journal of Ad Hoc and Sensor Wireless Networks, vol.2 , no. 3, 2003 [10] Hubaux J.-P., Buttyan L., Capkun S., "The Quest for Security in Mobile Ad Hoc Networks", In Proc. of the 2nd ACM Int. Symp. on Mobile Ad hoc Networking & Computing, pp. 146-155, 2001 [11] Kong J., Hong X., Gerla M., "A New Set of Passive Routing Attacks in Mobile Ad Hoc Networks", In IEEE MILCOM, 2003 [12] Buchegger S., Tissieres C., Le Boudec J.-Y.,"A Test-Bed for Misbehaviour Detection in Mobile Ad-Hoc Networks –How Much Can Watchdogs Really Do?", Mobile Computing Systems and Applications (WMCSA '04), pp. 102-111, 2004 [13] Ning P., Sun K., "How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols", In Proc. of the IEEE Workshop on Information Assurance, pp. 60-67, 2003 [14] Wu B., Chen J., Wu J., Cardei M., "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Chapter 12, Springer, 2006 [15] Hu Y.-C., Perrig A., Johnson D.B., "Rushing Attacks and Defence in Wireless Ad Hoc Network Routing Protocols", In Proc. of the ACM Workshop on Wireless Security, 2003 [16] Karlof C., Wagner D., "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Ad Hoc Networks, pp. 293-315, 2003.