Security Threats in Mobile Ad Hoc Networks

Sevil Şen, John A. Clark, Juan E. Tapiador

Department of Computer Science,

University of York, YO10 5DD, UK

ssen@cs.york.ac.uk, jac@cs.york.ac.uk, jet@cs.york.ac.uk

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 chapter provides a 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. Then we discuss various proactive and reactive solutions proposed for MANETs. We outline secure routing solutions to avoid some attacks against the routing protocols based on cooperation between nodes. We also give an overview of intrusion detection in MANETs and indicate the nature of IDSs that have been proposed for MANETs in the past decade.

1. Introduction

With the proliferation of cheaper, 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. For example, node S can communicate with node D by using the shortest path S-A-B-D as shown in Figure 1 (the dashed lines show the direct links between the nodes). If node A moves out of node S' range, he has to

find an alternative route to node D (S-C-E-B-D). A variety of new protocols have been developed for finding/updating routes and generally providing communication between end points (but no proposed protocol has been accepted as standard yet). However these new routing protocols, based on cooperation between nodes, are vulnerable to new forms of attacks. Unfortunately, many proposed routing protocols for MANETs do not consider security. Moreover their specific features -the lack of central points, the dynamic topology, the existence of highly-constrained nodes, presents a particular challenge for security.

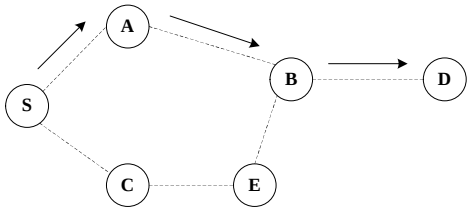

Figure 1. *Communication Between Nodes on MANETs*

Much research has been done to counter and detect attacks against existing MANET routing protocols, including work on secure routing protocols and intrusion detection systems. However, for practical reasons the proposed solutions typically focus on a few particular security vulnerabilities since providing a comprehensive solution is non-trivial. If we are to develop more general solutions we must first have a comprehensive understanding of possible vulnerabilities and security risks against MANETs. This is the main goal of this chapter. Section 2 presents the specific vulnerabilities of MANETs and the fundamentals of an exemplar routing protocol (AODV) to help understanding of the attacks given in Section 3. An overview of security solutions proposed to prevent and detect attacks on MANETs is presented in Section 4. Finally, ideas for future research are given.

2. Background

The specific features of MANETs present a challenge for security solutions. Many existing security solutions for conventional networks are ineffective and inefficient for many envisaged MANET deployment environments. Consequently, researchers have been working for the last decade on developing new security solutions or changing current ones to be applicable to MANETs. Since many routing protocols do not consider security, some research focuses on developing secure routing protocols or introducing security extensions to the existing routing protocols. Routing protocols have been proposed to counter selfish activities by forcing the selfish nodes to cooperate. Existing key management mechanisms are usually based on central points where services such as certification authorities or key servers can be placed. Since MANETs do not have such points, new key management mechanisms have had to be developed to fulfil requirements. Finally, since prevention techniques are invariably limited in effectiveness, intrusion detection systems are generally used to complement other security mechanisms. This applies to MANETs too and researchers have proposed new IDSs to detect malicious activities on these networks.

If we are to develop more general solutions we must first have a comprehensive understanding of possible vulnerabilities and security risks against MANETs. They share the vulnerabilities of wired networks, such as eavesdropping, denial of service, spoofing and the like, which are accentuated by the ad hoc context [12]. They also have further vulnerabilities such as those that take advantage of the cooperative nature of routing algorithms. These vulnerabilities of MANETs are summarized in the following section.

2.1. 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 [27]. 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 [6]”. Furthermore, the introduction of more

security features into the network increases the computation, communication and management load [33]. This is a challenge for networks that are already resource-constrained.

2.2. 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. In this section we describe the operation of AODV to understand better the routing attacks explained subsequently. We aim to illustrate principles of attacks. Other protocols may be susceptible to these or similar attacks, but may also be vulnerable to further protocol specific attacks. Moreover the consequences of attacks can have different impacts in different routing protocols (*e.g.* in proactive vs. reactive routing protocols).

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" [26]. It is claimed that AODV can handle low, moderate, and relatively high mobile rates, together with a variety of data traffic loadings [26]. 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" [26]. The methods for a node to control its connectivity to its active next hops on AODV are:

- link layer notification using control packets such as link layer acknowledgement messages (*e.g.* ACK or RTS-CTS);
- passive acknowledgement: notification by listening on the channel to determine if the next node forwards the packet or not; and
- 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.

3. 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. *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. Because new routing protocols introduce new forms of attacks on MANETs, we mainly focus on network layer attacks in this chapter.

Layer	**Attacks**
Application Layer	data corruption, viruses and worms
Transport Layer	TCP/UDP SYN flood
Network Layer	hello flood, blackhole
Data Link Layer	monitoring, traffic analysis
Physical Layer	eavesdropping, active interference

Table 1. *Some Attacks on the Protocol Stack*

3.1. 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 [2]. 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. In this paper, we mainly concentrate on attacks carried out by *malicious* nodes who intentionally aim to disrupt the network communication.

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:

- *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.
- *Node Isolation:* isolating a node or some nodes(s) from communicating with other nodes in the network, partitioning the network, etc.
- *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 [5]. 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 [45]. This sort of distinction may affect the ability to eavesdrop, to jam a network effectively, and to escape destruction (e.g. a single powerful jammer can easily be taken out, distributed jamming is harder to extinguish).

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 [28] Sun et al defined this phenomenon as being a "partial victim". Moreover they have stated that even if it reduces the damage caused by the attacker, it makes detection more difficult since the symptoms of an attack and those arising due to the dynamic nature of the network are difficult to distinguish. In conclusion, the impact of mobility on detection is a complex matter.

Degree of physical access (including node capture ability and ability to carry out physical deconstruction)

Given the agile nature of MANETs determining an applicable adversary model is difficult. However, systems can be evaluated against a range of representative threat models.

3.2. Attacks

We can classify attacks as passive or active.

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 [3].

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 $t+\epsilon$ are likely to be from the same packet flow [1]. 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).

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. It might also reduce the network performance by causing data packets to be retransmitted, new routes to the destination to be discovered, and the like.

Unfortunately most routing protocols (DSR is an exception [2]) have no mechanism to detect whether data packets have been forwarded or not. However, they can be detected by neighbouring nodes through passive acknowledgement or hop-by-hop acknowledgement at the data link layer.

An attacker can choose to drop only some packets to avoid being detected; this is called a ***selective dropping attack***. Besides data packets or route discovery packets, an attacker can also drop route error packets, causing the source node to be unaware of failed links (thus interfering with the discovery of alternative routes to the destination).

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. It is especially effective in routing protocols that use advertised information such as remaining energy and nearest node to the destination in the route discovery process. 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 [4].

Fabrication Attacks: Here the attacker forges network packets. In [5], 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. It causes route disruption by causing messages to be sent to a non-existent node or putting the attacker itself into the route between two endpoints of a communication channel if the insider attacker has already have a

route to the destination. Figure 2 shows an example of a forge reply attack defined in [5]. The best route (with minimum hop) from node S to node D is S-I1-I2-D. Malicious node M forges a RREP message to the source node S through node I1. The message claims to come from the destination node D with higher destination sequence number to suppress the existing route. The faked message results in the updating of the route entry to the destination node in the routing tables of node S and I1. Node I1 forwards data packets to the malicious node instead of node I2 since node M seems to have a fresh route to node D, so the new route becomes S-I1-M-I2-D.

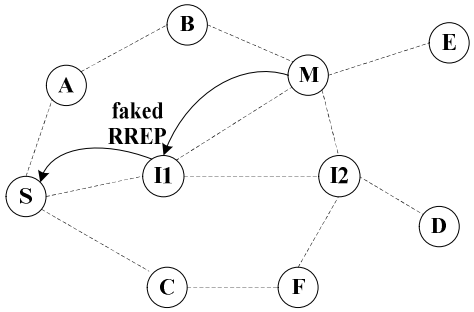

Figure 2. *A Forge Reply Attack*

Attackers can initiate frequent packets to cause denial of service (DoS). Example DoS attacks that exploit MANETs' features are sleep deprivation torture attacks, routing table overflow attacks, ad hoc flooding attacks, rushing attacks, and the like**.** The ***sleep deprivation torture*** attack consumes a node's battery power and so disables the node. It does so by persistently making service requests of one form or another. This attack was introduced by Stajano et al. [6] who emphasized that it is more powerful than better known DoS attacks such as CPU exhaustion, since most mobile nodes are run on battery power. The ***ad hoc flooding attack***, introduced in [7], is another DoS attack against on-demand protocols, in which nodes send Route Request messages when they need a route. The attacker exploits this property of Route Discovery by broadcasting many Route Request messages to a node that is not in the network. Another attack at the Route Discovery phase is the ***routing table overflow attack***. Here the attacker sends a lot of route advertisements for nodes that do not exist. Since proactive protocols update routing information periodically before it is needed, this attack, which results in overflowing the victim nodes' routing tables and preventing new routes from being created, is more effective in proactive protocols than in reactive protocols [8].

Another interesting fabrication attack on MANETs is ***the routing cache poisoning attack*** [8]. 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*** [9] 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. So, if the Route Request forwarded by the attacker arrives first at the destination, routes including the attacker will be discovered instead of valid routes. 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 [9]. The ***hello flood attack*** [10] is another attack that makes the adversary attractive for many routes. In some routing protocols, nodes broadcast Hello packets to detect neighbouring nodes. These messages are received by all one-hop neighbour nodes, but are not forwarded to further nodes. The attacker broadcasts many Hello packets with large enough transmission power that each node receiving Hello packets assumes the adversary node to be its neighbour. It can be highly effective in both proactive and reactive MANET protocols.

A further significant attack on MANETs is the collaborative ***wormhole attack***. Here an attacker receives packets at one point in the network, tunnels them to an attacker at another point in the network, and then replays them into the network from this final point [11]. Packets sent by tunneling forestall packets forwarded by multi-hop routes as shown in Figure 3 and it gives the attacker nodes an advantage for future attacks. Since the packets sent over tunneling are the same as the packets sent by normal nodes, it is generally difficult to detect wormhole attackers by software-only approaches such as IDS [11]. That is why *packet leashes* (any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance [11]) have been introduced for preventing wormhole attacks.

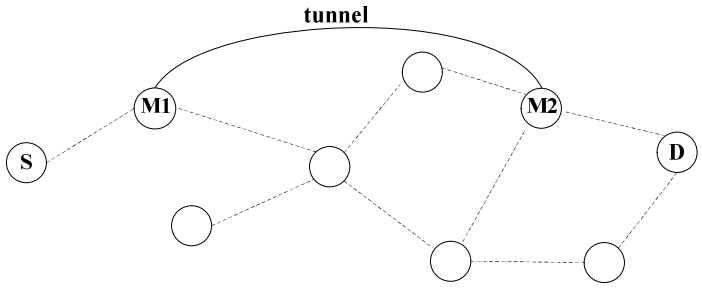

Figure 3. ***Wormhole Attack***

4. Countermeasures

In general, we prevent compromise where we can (proactive solutions), but seek to detect and deal with it when prevention does not work (reactive solutions). In this section we discuss proactive and reactive solutions proposed for MANETs.

4.1. Prevention Techniques: Secure Routing

Many of the attacks described above could be avoided by including authentication techniques in the routing protocol [34], [35], [36]. The main idea here is to guarantee that all nodes wishing to participate in the routing process are authenticated nodes; i.e., trusted network elements that will behave according to the protocol rules. Authentication should be enforced during all routing phases, thus preventing

unauthorised nodes (including attackers) from participating in the routing and so from launching routing attacks. Authentication can be provided based either on public-key or symmetric cryptography. In the former case, nodes issue digital signatures associated with the routing messages. Signatures can be verified by any other node, providing a secure proof of the identity of the sender. Digital evidence with similar properties can be constructed using secret-key cryptography, such as MACs (Message Authentication Codes).

The use of cryptography comes hand in hand with an associated problem: the necessity of a mechanism for issuing, exchanging, and revoking keys. Key management in MANETs is generally more difficult than in classical wired networks due to the absence of any infrastructure or central administrative authorities. There is no obvious point(s) where services such as certification authorities (CA) or key servers (KS) can be placed, and the great majority of the solutions proposed so far rely on schemes where the whole key management system is spread out to a subset of the mobile nodes.

Schemes proposed so far are mostly distributed key agreement protocols, such as the classical two-party Diffie-Hellman (DH) scheme [37]. Some works have extended the basic protocol towards n-party versions, in such a way that n nodes can establish a common key for group communications (see *e.g.* [38]). Encrypted Key Exchange (EKE) protocols [39] have also been adopted in MANETs. These schemes were proposed with the goal of allowing two parties to generate a long-term common key from a shared password (typically of low entropy and therefore vulnerable to guessing attacks). A common feature of all these approaches (DH, general DH, EKE, etc.) is that some initial values must be shared by all nodes before the protocol can be used. This is generally known as the "bootstrapping" problem and it has received a fair amount of attention in recent years.

The development of public-key infrastructures (PKI) especially tailored for MANETs has been a hot research topic during the last years. The majority of the solutions rely on a distributed CA based on threshold cryptography [40]. For example, in the scheme proposed in [41], a subset of nodes known as "servers" act collectively as a CA. Each public key belonging to a network node is divided into n shares and distributed among the n servers. A number $k<n$ of servers are required to sign a certificate. Each server generates its partial signature and collects the partial signatures generated by other servers. In global terms, the scheme is robust against any adversary who can compromise no more than k-1 nodes. MOCA (Mobile Certificate Authority) [42] is a similar solution which incorporates a number of criteria (physical location, computational characteristics, security measures deployed, etc.) for choosing which nodes will act as servers.

4.2. Intrusion Detection

Since prevention techniques are limited in their effectiveness and new intrusions continually emerge, an intrusion detection system (IDS) is an indispensable part of a security system. An IDS is introduced to detect possible violations of a security policy by monitoring system activities and responding to those that are apparently intrusive. If we detect an attack once it comes into the network, a response can be initiated to prevent or minimize the damage to the system. An IDS also provides information about

intrusion techniques, enhancing our understanding of attacks and informing our decisions regarding prevention and mitigation.

Although there are many intrusion detection systems for wired networks, they do not find simple application to MANETs. Different characteristics of MANETs make conventional IDSs ineffective and inefficient for this environment. Consequently, researchers have been working recently on developing new IDSs for MANETs, or on modifying current IDSs to be applicable to MANETs.

Next, we give a summary of the different intrusion detection techniques proposed for MANETs. Attacks detected by each technique are identified too.

Specification-Based Intrusion Detection

One of the most commonly proposed intrusion detection techniques for MANETs is specification-based intrusion detection, where intrusions are detected as runtime violations of the specifications of routing protocols. This technique has been applied to a variety of routing protocols on MANETs such as AODV[14], OLSR[13][17], DSR[17]. In [13] each network monitor employs a finite state machine (FSM) to state the specifications of AODV, especially for the route discovery process, and maintains a forwarding table for each monitored node. Each RREP and RREQ message in the range of the network monitor is monitored in a request-reply flow which checks the situations such as if route request packets are forwarded by next node or not, if route reply packets are modified on the path or not, and the like. When a network monitor needs information about previous messages or other nodes that are not in its range, it can ask neighbouring network monitors.

In DEMEM [13], a distributed and cooperative IDS is described in which each node is monitored by 1-hop neighbour nodes for the OLSR routing protocol. In addition to 1-hop neighbour monitors, 2-hop neighbours can exchange data to have sufficient evidence about intrusions. The main contribution of DEMEM, as stated by the authors, is to introduce specific IDS messages to help detection.

Specification-based IDSs have been generally used to detect modification and forge attacks. However, this technique cannot detect attacks that do not violate protocol specifications directly. (Various DoS attacks come in this category.) For that reason Huang *et al* [15] have proposed an IDS which uses a specification-based technique for attacks that violate the specifications of AODV directly and an anomaly-based technique for other kinds of attacks such as DoS. In [17] the authors propose adding a signature analysis tool in the future to detect DoS attacks that cannot be detected by the extended finite state machine based IDS for the OLSR routing protocol.

Anomaly-Based Intrusion Detection

This technique profiles the symptoms of normal behaviours of the system, such as usage frequency of commands, CPU usage for programs, and the like. It detects intrusions as anomalies, i.e. deviations from the normal behaviour patterns. Various techniques have been applied for anomaly detection, e.g. statistical approaches, and artificial intelligence techniques like data mining and neural networks. The

biggest challenge is defining normal behaviour. Normal behaviour can change over time and IDS systems need to adapt accordingly. That's one of the reasons false positives – the normal activities which are detected as anomalies by IDS – can be high in anomaly-based detection. On the other hand, it is capable of detecting unknown attacks. This is important in an environment where new attacks and new vulnerabilities of systems are announced constantly.

The first proposed IDS for MANETs uses statistical anomaly-based detection [27]. In that research, each node has an IDS agent responsible for local detection, and collaborates with neighbouring nodes for global detection whenever the evidence is inconclusive and a broader search is needed. SVM Light and RIPPER classifiers are employed on three popular routing protocols (DSR, AODV, DSDV) and compared. The research focuses on two attack types: route logic compromise (*e.g.* misrouting) and traffic pattern distortion (*e.g.* dropping, modification, DoS attacks). This is also one of the few approaches to consider mobility data by monitoring node movements using built-in GPS functionality on each node.

Another proposed anomaly-based detection approach for MANETs [28] is Zone-Based IDS, where the network is divided into zones based on geographic partitioning. The nodes in a zone are grouped into intrazone nodes and interzone nodes (which work as bridges to the other zones). Each node in a zone is responsible for local detection and sending alerts to interzone nodes which make the final decisions. They use a Markov-chain based local anomaly detection model and evaluate it on route disruption attacks. Link change rate is used to reflect different mobility levels of the system.

Constructing an anomaly-detection model automatically by extracting the correlations among monitored features is proposed in [29]. They introduce simple rules to determine attack types and sometimes attackers. The rules are executed after an anomaly is detected. They are based on statistics such as the number of incoming/outgoing packets on the monitored node and are pre-computed for known attacks. For example, unconditional packet dropping of a node m is formulated as follows [29]:

$$FP_m(\text{forward percentage}) = \frac{\text{packets actually forwarded}}{\text{packets to be forwarded}}$$

Blackhole and dropping attacks are used to evaluate the performance of this approach. They observe that MANETs have strong feature correlations in normal behaviour patterns. For instance, the correlation packet dropping and route entries updating (while packet dropping is drastically increasing on the network, there is an obvious change in routing updates.) are highly correlated.

Misuse-Based Intrusion Detection

Misuse-Based IDSs compare known attack signatures with current system activities. They are generally preferred by commercial IDSs since they are efficient and have a low false positive rate. The drawback of this approach is that it cannot detect new attacks. The system is only as strong as its signature database and this needs frequent updating for new attacks.

There has been little research on signatures of new attacks against MANETs, so few misuse-based IDSs have been proposed so far. One of them is based on a stateful misuse detection technique and defines state transition programs for known attacks such as spoofing, dropping, and resource depletion attacks on AODV [18].

In [19], known attacks are formulated as cases for exact/similarity matching on the packet level. However Snort rules are used as the cases instead of signatures of MANETs' specific attacks. In [20] another misuse-based IDS for MANETs is proposed with descriptions of two attack signatures using Finite State Machines (FSMs). One of the attacks is a network level attack against the OLSR routing protocol and the other one is application level "*stepping stone attack*". They evaluated these attacks on a small network. Adding an anomaly detection module to broaden spectrum of detected attacks has been suggested in both cases [19][20].

A different approach which creates signatures of some known attacks against MANETs automatically is given in [30]. In this research, intrusion detection rules to detect dropping, flooding, and route disruption attacks on AODV are evolved by using evolutionary computation techniques. The performance of evolved programs is demonstrated on simulated networks under varying mobility and traffic levels, and the results are quite promising. In addition, trade-offs between intrusion detection ability of evolved programs (rules) and their energy usage are identified leading to the creation of power-aware programs for such resource-constrained environment in their subsequent research [31].

Promiscuous Monitoring Based Intrusion Detection

Since wireless nodes can overhear traffic in their communication range, promiscuous monitoring is a popular method used to detect misbehaviour of nodes such as dropping and modification of packets on MANETs. However this technique might not detect misbehaving nodes in the presence of ambiguous collisions, or receiver collisions.

The primary work on detecting misbehaving nodes and mitigating their performance effect proposed *Watchdog and Pathrater* mechanisms on the DSR [21]. Routing control packets in DSR carry all routing path information between nodes on the path. When a node forwards a packet, the Watchdog mechanism of that node monitors the next node to confirm that it also forwards the packet properly. When the number of dropping packets by a node exceeds a threshold, the node is considered as a misbehaving node and a notification is sent to the source node. With the Pathrater, the most reliable path is selected (instead of the shortest path as in DSR) in the presence of misbehaving nodes by using link reliability data and data from the Watchdog.

An approach which uses a reputation mechanism to respond to malicious nodes is given in [22]. Each node is responsible for monitoring the behaviour of its next hop neighbours and detecting misbehaving nodes as in [21]. When a misbehaving behaviour is detected, the reputation system is called to rate the misbehaving node. The system keeps a local rating list and/or blacklist which can be exchanged with

friend nodes. The rating of a node is based on the times of misbehaviour occurrence as in [21]. The rate function also uses weights depending on the source detecting the misbehaviour.

In [23] Parker et al. extend the method using promiscuous listening to detect misbehaviour in a wide variety of routing protocols (not just DSR). A node listens to all nodes in its transmission range, not just the packets forwarded by the next node as in [21]. It detects dropping and modification attacks that exceed the threshold value in the threshold table for the particular attack class. However, a node moving out of range of the monitoring node before it forwards the packets it should can be assumed to be carrying out a dropping attack.

There are also a few cooperative approaches proposed to detect misbehaving nodes. In [24], every node counts the packets that it receives and forwards and periodically reports these counts to a coordinator node. Promiscuous monitoring is not used since it depends on the link layer characteristics and the link layer encryption approach [24].

Another approach for detecting dropping attacks on MANETs is presented in [25]. The algorithm only differentiates dropping attacks from the faults due to broken links. Malicious behaviour is defined as the dropping of data packets starting at some random time and continuing from that time onwards. The idea behind the algorithm is based on associating the route error messages of the DSR routing protocol with TCP timeouts. In the DSR protocol a route error control message is sent back to the source node if an intermediate node cannot forward the packet to the next hop. TCP timeout occurs when the sender does not receive an acknowledgement within a specific interval. All route error messages on a per flow basis are collected at the source node. When a TCP timeout occurs at this node it is controlled if there are any route error messages for this flow within the detection interval or not. If there are, they are associated with a broken link, and otherwise with malicious dropping.

Communication between the IDS agents has also been provided by the use of mobile agents [19][20][43] besides promiscuous monitoring or by exchanging data directly between nodes in the literature.

5. Future Directions for Research

Given their flexibility MANETs are very attractive for military and disaster recovery applications. Moreover mobile devices are getting smaller, cheaper, more powerful and more mobile every day. In the future MANETs will likely be a part of our lives. There has been much research on this promising new networking. Security is one of the hot topics in the area due to new security threats MANETs have introduced. The threats to MANETs have been examined in many research papers. However more research needs to be done on identifying new security threats. We believe that with the increase in the use of MANETs, new intrusions are going to emerge continuously.

Since conventional security solutions are not easily applicable to MANETs, new solutions have been proposed for the last decade, which is far fewer than proposed approaches for conventional networks.

None of the proposed systems are necessarily the best solution taking into account different applications which they can have their own requirements and characteristics. They also usually consider few specific attacks and target a specific routing protocol. Furthermore they emphasize just a few specific MANET features. For instance the consequences of having limited resources is generally little explored.. Some solutions might not be suitable for some nodes which can have limited computational capabilities and resources. Researchers can develop solutions considering different characteristics of these nodes. Cooperation and communication between nodes is another area need to be explored. Proposed network architectures should not introduce new weakness/overheads to the system. To conclude, researcher should focus on developing solutions suitable to MANETs' specific features.

6. Conclusions

In this chapter 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. Firstly we have presented specific vulnerabilities of this new environment. Then we have surveyed the attacks exploit these vulnerabilities and, possible proactive and reactive solutions proposed 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. In this chapter we summarize secure routing approaches proposed for MANETs. The difficulty of key management on this distributed and cooperative environment is also discussed. Furthermore we have surveyed intrusion detection systems with different detection techniques proposed in the literature. Each approach and technique is presented with attacks they can and cannot detect. To conclude, MANET security is a complex and challenging topic. To propose security solutions well-suited to this new environment, we recommend researchers investigate possible security risks to MANETs most horoughly.

References

1. Kong J., Hong X., Gerla M., "A New Set of Passive Routing Attacks in Mobile Ad Hoc Networks", In IEEE MILCOM, 2003

2. 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

3. 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

4. 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

5. 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

6. Stajano F., Anderson R., "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", In Proc. of Int. Workshop on Security Protocols, Springer, 1999

7. Yi P., Dai Z., Zhang S., Zhong Y., "A New Routing Attack in Mobile Ad Hoc Networks", Int. Journal of Information Technology, vol. 11, No. 2, pp. 83-94, 2005

8. 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

9. 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

10. Karlof C., Wagner D., "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Ad Hoc Networks, pp. 293-315, 2003

11. Hu Y.-C., Perrig A., Johnson D.B., "Packet Leashes: A Defence against Wormhole Attacks in Wireless Ad Hoc Networks", In Proc. of INFOCOM, 2003

12. Li Y., Wei J., "Guidelines on Selecting Intrusion Detection Methods in MANET", In Proc. of Information Systems Educators Conference, 2004

13. Tseng C.H., Wang S.H., Ko C., Levitt K., "DEMEM: Distributed Evidence Driven Message Exchange Intrusion Detection Model for MANET", RAID 2006, LNCS 4219, Springer, pp. 249-271, 2006

14. Tseng C.-Y., Balasubramayan P., Ko C., Limprasittiporn R., Rowe J., Levitt K., "A Specification-Based Intrusion Detection System for AODV", In Proc. of the ACM Workshop on Security in Ad Hoc and Sensor Networks, 2003

15. Huang Y., Lee W., "Attack Analysis and Detection for Ad Hoc Routing Protocols", RAID 2004, LNCS 3224, pp. 125-145, Springer, 2004

16. Yi P., Zhong Y., Zhang S., "A Novel Intrusion Detection Method for Mobile Ad Hoc Networks", EGC 2005, LNCS 3470, pp. 1183-1192, Springer, 2005

17. Orset J.-M., Alcalde B., Cavalli A., "An EFSM-based Intrusion Detection System for Ad Hoc Networks", 3rd Int. Symp. Automated Technology for Verification and Analysis, LNCS 3707, pp. 400-413, Springer, 2005

18. Vigna G., Gwalani S., Srinivasan K., Belding-Royer E. M., and Kemmerer R. A., "An intrusion detection tool for aodv-based ad hoc wireless networks", In Proc. of the 20th Annual Computer Security Applications Conference, pp.16-27, IEEE Computer Society, 2004

19. Guha R., Kachirski O., Schwartz D.G., Stoecklin S., Yilmaz E., "Case-Based Agents for Packet-Level Intrusion Detection in Ad Hoc Networks", In Proc. of 17th Int. Symp. on Computer & Information Sciences, 2002

20. Puttini R.S., Percher J-Mr., Me L., Camp O., Sousa Jr. R., Abbas C.J.B., Garcia-Villalba L.J., "A Modular Architecture for Distributed IDS in MANET", In Proc. of the 2003 Int. Conf. on Computational Science and Its Applications, LNCS 2669, pp. 91-113, Springer, 2003.

21. Marti S., Giuli T.J., Lai K., Baker M., "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks", In Proc. of ACM Int. Conf. on Mobile Computing and Networking, MOBICOM, pp. 255-265, 2000

22. Buchegger S., Le Boudec J., "Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Network", In Proc. of Parallel, Distributed and Network-based Processing, pp. 403-410, 2002

23. 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

24. Anjum F., Talpade R., "LiPaD: Lightweight Packet Drop Detection for Ad hoc Networks", In Proc. of IEEE Vehicular Technology Conference, pp. 1233-1237, 2004

25. Gavini, S., "Detecting Packet-Dropping Faults in Mobile Ad-Hoc Networks", Master of Science Thesis, School of Electrical Engineering and Computer Science, Washington State University, 2004

26. 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

27. Zhang Y., Lee W., "Intrusion Detection Techniques for Mobile Wireless Networks", Wireless Networks, pp. 545-556, Springer, 2003

28. 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

29. Huang Y., Lee W., "A Cooperative Intrusion Detection System for Ad Hoc Networks", In Proc. of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003

30. Sen S., Clark J.A., "A Grammatical Evolution Approach to Intrusion Detection on Mobile Ad Hoc Networks", In Proc. of the 2nd ACM Conference on Wireless Network Security, pp. 95-102, 2009

31. Sen S., Clark J.A., Tapiador J.E., "Power-Aware Intrusion Detection on Mobile Ad Hoc Neworks", In Proc. of the 1st International Conference on Ad hoc Networks , 2009

32. Denning D., "An Intrusion-Detection Model", IEEE Transactions on Software Engineering, vol. 13, no 2, pp. 222-232, 1987

33. 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.

34. Hu Y.-C. , Perrig A. and Johnson D.B., "Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks", In Proc. of the 8th International Conference on Mobile Computing and Networks, pp. 12-23, 2002

35. K. Sanzgiri et al., "A Secure routing Protocol for Ad Hoc Networks", In Proc. of the 10th IEEE Conference on Network Protocols, 2002

36. B. Awerbuch et al, "An On Demand Secure Routing Protocol Resilient to ByzantineFailures", In Proc. of the ACM Workshop on Wireless Security, 2002

37. W. Diffie and M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, IT-22(6):644-654, 1976

38. M. Steiner, Tsudik G., and Waidner M., "Diffie-Hellman Key Distribution Extended to Group Communication", In Proc of the ACM Conference on Computer and Communication Security, pp. 31-37, 1996

39. Bellovin S.M., Merritt M., "Encrypted Key Exchange: Password-based Protocols Secure Against Dictionary Attacks", In IEEE Symposium on Security and Privacy, pp. 72-84, 1992

40. Shamir A., "How to Share a Secret", Communications of the ACM 22(11), pp. 612-613, 1979

41. Zhou L., Haas Z.J., "Securing Ad Hoc Networks", IEEE Network 13(6), pp. 24-30, 1999

42. Yi S., R. Kravets. "MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks", In the 2nd Annual PKI Research Workshop, 2003

43. Kachirski O., Guha R., "Effective intrusion detection using multiple sensors in wireless ad hoc networks", In Proc. of the 36th IEEE International Conference on System Sciences, 2003

44. Mobile Agent, http://en.wikipedia.org/wiki/Mobile_agent, accessed 01 September 2009

45. Chivers H., Clark J. A., "Smart dust, friend or foe?--Replacing identity with configuration trust", Computer Networks 46(5), pp. 723-740, 2004

Keywords

Intrusion: Any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource [32].

Intrusion Detection System (IDS): A system to detect possible violations of a security policy by monitoring system activities and responding to those that are apparently intrusive.

Promiscuous monitoring: The monitoring all packets in a node's transmission range regardless of their destinations in wireless networks.

Denial of Service: Attacks that aim to make computer/network resources unavailable to the intended users.

Routing Attack: Attacks that seek to manipulate the operation of routing layer and aim to disrupt the routing mechanism of a network.

Mobile Agent: Compositions of computer software and data that is able to migrate from one computer to another autonomously and continue its execution on the destination computer [44].

Authentication: The verification of claims about the identity of a source of information.

Cryptography: The study and practice of protecting information by data encoding and transformation techniques.

Key management: The process of generating, distributing, using, exchanging, and updating keys in a cryptography system design.

Questions

1. Distinguish active and passive modes of attacks on MANETs, and give examples.
2. What new forms of attack are possible in MANETs that do not occur in wired networks?
3. What features of MANETs and MANET routing protocol operation make new attacks possible?
4. For AODV write a concise description of dropping attacks and ad hoc flooding attacks.
5. For the attacks in question 4 above what countermeasures have been proposed?
6. Why do security solutions for MANETs usually prefer to have a distributed and collaborative approach?
7. What attacks on MANETs would not be detectable by autonomous systems running on individual nodes (i.e. with no collaboration)?
8. What is the main difficulty of adapting conventional prevention techniques to MANETs?
9. What attacks on MANETs are detectable by promiscuous monitoring?
10. Identify the attacker goals for selfishness and traffic analysis.

Answers

1. In the *passive mode,* an attacker node just monitors and aims to find out information about the network. He does not cause any direct damage to the network. Passive attacks can be launched by insider or outsider attackers. Traffic analysis which aims to reveal the location of nodes is an example of a passive attack. On the other hand, in the *active mode*, attackers cause unauthorised state changes in the network, such as denial of service, modification of packets, and the like. Active attacks are generally launched by insider attackers who have authorisation to operate within the network. For example sink hole is an active attack where the attacker attracts traffic through a

victim node by forging falsified routing packets into the network. He changes the operation of the routing mechanism.

2. The sleep deprivation torture attack is a DoS attack on MANETs. It aims to consume a node's battery power and effectively disables the node since mobile nodes generally run on battery power. The wormhole is another interesting attack where an attacker receives packets at one point in the network and tunnels them to an attacker at another point. There are also other attacks that exploit the vulnerabilities of routing protocols on MANETs. For example a blackhole attack attracts traffic through itself by advertising falsified routing information.
3. The use of wireless links makes MANETs particularly susceptible to attacks such as eavesdropping and active interference. The cooperative nature of routing protocols allows an attacker to become a part of the routing mechanism easily and disrupt network communications by disobeying the protocol specifications. Furthermore resource-constrained nodes can be the target of new attacks such as sleep deprivation torture.
4. In *dropping attacks* malicious or selfish nodes deliberately drop all packets which are not destined for them and aim to disrupt network communication. In ad hoc flooding attacks the attacker floods the network with many route request packets and aims to consume the network's resources.
5. In the literature solutions using promiscuous monitoring techniques have usually been proposed to detect dropping attacks. When a node forwards a packet to its next node, it checks whether the next node (in the case it is not the destination node) also forwards the packet or not. There are other approaches such as using active acknowledgement from other nodes or associating route error packets with the lack of TCP acknowledgements. Ad hoc flooding is a DoS attack. Anomaly-based intrusion detection techniques are proposed to detect this attack. There is also an attempt to automatically discover intrusion detection rules for this attack. Defining the attack's signature manually is another approach.
6. MANETs do not have any entry points such as routers, gateways, etc which are typically present in wired networks and which can be used to monitor all network traffic that pass through them. A MANET node can see only a portion of a network: the packets it sends or receives, possible together with other packets within its radio range. While some attacks can be detected locally by each node, detection of some attacks (such as network scans, distributed attacks) need to obtain global data from other nodes in MANETs. For example, routing protocols are usually cooperative in MANETs and attacks against routing protocols can affect many nodes on the network. These attacks can be detected collaboratively by the affected nodes. Moreover, a local response to a malicious node may have very limited effect. A coordinated collaborative response will be much more effective.
7. Attacks which have a clear affect on a node can be detected easily by that node. However some attacks (such as distributed attacks) can be detected only by analyzing the network data. For example if intrusion detection is carried out locally on the network, *network scan* can seem normal to each node. Detecting this attack will likely require distributed and collaborative intrusion detection on MANETs.

8. Key management in MANETs is a challenging topic due to the absence of any infrastructure or central administrative authorities. There is no obvious point(s) where services such as certification authorities (CA) or key servers (KS) can be placed. So the great majority of the solutions proposed for MANETs so far rely on schemes where the whole key management system is spread out to a subset of the mobile nodes.
9. Techniques that use promiscuous monitoring [21][22] [23] are usually proposed for detecting misbehaving nodes who carry out attacks such as dropping and misrouting attacks. In this way, the packets sent to a node are monitored to detect if this node forwards the packets properly or not.
10. The main motive for selfish behaviour of a node is to preserve its resources. They avail themselves of the services of the other nodes, but do not reciprocate. By traffic analysis attacker can reveal some information about the network such as the existence and location of nodes, the communications network topology, the roles played by nodes and the like. Then he can use this information to carry out further attacks.