4. Security Aspects of Mobile Adhoc Networks (MANETs)

Operating in open and shared media, wireless communication is inherently less secure than wired communication. In addition, since mobile wireless devices usually have limited resources, such as bandwidth, storage space, processing capability and energy – enforcement of security is difficult. In comparison with fixed-infrastructure wireless networks, security management for wireless ad hoc networks is more challenging due to unreliable communication, intermittent connections, node mobility, and constantly changing topology. A complete security solution should include three components of prevention, detection, and reaction, and provide security properties of authentication, confidentiality, non-repudiation, integrity, and availability. It should also be adaptive enough to properly balance service performance and security performance with resource limitations.

4.1 Fundamentals of Security in Mobile Networks

There are two types of wireless networks: wireless LAN (WLAN) and wireless/mobile ad hoc network. The former requires the use of one or more access points (or base stations). Those access points connect wireless users which are one hop away and centrally control their access to Internet and the other WLANs. The ad hoc form of communications is based on radio to radio multi-hopping. Wireless/mobile ad hoc networks (simply called MANETs, since the wireless attribute is inherent to mobility) have been evolving to serve a growing number of applications, including military communications, emergency rescue operations, and disaster recoveries efforts. Benefiting from the ease of deployment, wireless ad hoc networks show great potential. Compared with WLANs, the security management in wireless ad hoc networks is much tougher due to the following characteristics:

1. **Resource Constraints**: The wireless devices usually have limited bandwidth, memory and processing power. This means costly security solutions may not be affordable in wireless ad hoc networks.

2. **Unreliable Communications**: The shared-medium nature and unstable channel quality of wireless links may result in high packet-loss rate and re-routing instability, which is a common phenomenon that leads to throughput drops in multi-hop networks. This implies that the security solution in wireless ad hoc networks cannot rely on reliable communication.

3. **Node mobility and dynamic topology**: The network topology of wireless ad hoc network may change rapidly and unpredictably over time, since the connectivity among the nodes may vary with time due to node departures, node arrivals, and the mobility of nodes. This emphasizes the need for secure solutions to be adaptive to dynamic topology.

4. **Scalability**: Due to the limited memory and processing power on mobile devices, the scalability is a key problem when we consider a large network size. Networks of 10,000 or even 100,000 nodes are envisioned, and scalability is one of the major design concerns.

Performance in wireless ad hoc networks is strongly related to the strength of security. However, without satisfactory network performance, security is meaningless. Therefore, in this chapter, we address network performance perspectives in security protocol design rather than cryptanalysis or formal verification of security protocols. The following requirements need to be considered for secure real-time communications:

**Authentication**: Authentication is the process to verify the identity of the sender of a communication. Without authentication, malicious attackers can access resource, gain-sensitive information, and interfere...
with the operation of other nodes very easily.

**Confidentiality:** Confidentiality means certain information is only accessible to authorized recipients. Participating parties to handle an emergency event need to cooperate with each other, while keeping the confidentiality of the traffic traversing the network.

**Non-repudiation:** Non-repudiation ensures that the origin of a message cannot deny having sent the message. It is useful for detection and isolation of compromised nodes.

**Integrity:** The integrity of a message is the property that the message cannot be modified without detection. Without integrity, attackers can easily corrupt and modify the data and therefore cause mobile devices to make wrong decisions based on the corrupted data.

**Availability:** Availability ensures the survivability of network services despite denial of service attacks. In unreliable wireless communications with highly dynamic topology, availability affects network performance greatly.

Ad-hoc networks are an emerging area of mobile computing. The wireless nature of communication and lack of any security infrastructure results in several security related problems. In this chapter we attempt to analyze the security aspects of ad-hoc environment by focusing on three specific areas of ad-hoc network security i.e. key-exchange and management, ad-hoc routing, and intrusion detection. The main issues concerning these areas have been addressed here.

### 4.2 Need for Intrusion Detection in Ad hoc Networks

Security is a challenging and important issue for wireless ad hoc networks. To design better security solutions, we need to correctly understand the network model and attacker model. The use of wireless links renders a wireless ad-hoc network vulnerable to malicious attacks, ranging from passive eavesdropping to active interference. In wired networks however the attacker needs to gain access to the physical media e.g. network wiring etc or pass through a plethora of firewalls and gateways. In wireless networks the scenario is quite different, there are no firewalls and gateways in place hence attacks can take place from all directions. Every node in the ad-hoc network must be prepared for dealing with the adversarial access attempts.

Each mobile node in ad-hoc network is an autonomous unit, free to move independently. This means a node with inadequate physical protection is very much susceptible to being captured, hijacked or compromised. It is difficult to track down a single compromised node in a large network. Attacks stemming from a compromised nodes are far more detrimental and much harder to detect. Hence every node in a wireless ad-hoc network should be able to work in a mode wherein it *trusts no peer*.

Ad-hoc networks have a decentralized architecture, and many ad-hoc network algorithms rely on cooperative participation of the member nodes. Adversaries can exploit this lack of centralized decision making architecture to launch new types of attacks aimed at breaking the cooperative algorithms.

Furthermore, Ad-hoc routing presents more vulnerabilities than one can imagine, since most routing protocols for ad-hoc networks are cooperative by nature. The adversary who compromises an ad-hoc node could succeed in bringing down the whole...
network by disseminating false routing information and this could culminate into all nodes feeding data to the compromised node.

Intrusion prevention techniques like encryption and authentication can reduce the risks of intrusion but cannot completely eliminate them i.e. encryption and authentication cannot defend against compromised nodes.

4.3 General overview of Intrusion Detection Techniques

In general terms “Intrusion” is defined as “any set of actions that attempt to compromise integrity, confidentiality or availability of the resource”.

The protocols and systems which are meant to provide services can be the target of attacks such as Distributed Denial of Service (DDOS). Intrusion detection can be used as a second line of defense to protect network systems because once an intrusion is detected response can be put in place to minimize the damage or gather evidence for prosecution or launch counter offensives.

Intrusion detection assumes that “user and program activities are observable “, which means that any activity which the user or an application program initiates, gets logged somewhere into system tables or some kind of a system log and intrusion detection systems (IDS) have an easy access to these system logs. This logged system/user related data is called audit data. Thus, Intrusion detection is all about capturing audit data, on the basis of this audit data determining whether it is a significant aberration from normal system behaviour, if yes then IDS infers that the system is under attack. Based on the type of audit data, IDS can be classified into 2 types i.e.

a) **Network based**: Network-based IDS sits on the network gateway and captures and examines network packets that go through the network hardware interface.

b) **Host based**: Host-based IDS relies on the operating system audit data to monitor and analyze the events generated by the users or programs on the host.

4.4 Unsuitability of the Current IDS techniques for Ad-Hoc paradigm

Wireless ad-hoc networks don’t have any fixed infrastructure. Since almost all of current network based IDS sit on the network gateways and routers and analyze the network packets passing through them, these type of network based IDS are rendered ineffective for the wireless ad-hoc networks.

In case of wireless ad-hoc networks the only available audit data is restricted to the communication activities taking place within the radio range, and any IDS meant for these types of networks should be made to work with this partial and localized kind of audit data.

Anomaly Detection models of IDS cannot be used for wireless ad-hoc networks, since the separation line between normalcy and anomaly is obscure. A node that transmits erroneous routing information (fabrication) can be either a compromised or is currently...
out of sync due to volatile physical movement. Hence in wireless ad-hoc networks it is difficult to distinguish between false alarms and real intrusions.

4.5 Novel (proposed) architecture for IDS

IDS should be both distributed and cooperative to suit the needs of wireless ad-hoc networks. As a consequence of this requirement, every node in the wireless ad-hoc network should participate in intrusion detection. Each node is responsible for detecting intrusion locally and independently but neighbouring nodes can form an association and collaboratively investigate in a broader range.

Each node within the network has its own individual IDS agent and these agents run independently and monitor user and system activities as well as communication activities within the radio range. If an anomaly is detected in the local data or if the evidence is inconclusive, IDS agents on the neighboring nodes will cooperatively participate in a global intrusion detection scheme. These individual IDS agents constitute the IDS system to protect the wireless ad-hoc network.

A Typical IDS Agent consists of following modules viz.

1) **Local Data Collection**: Local Data Collection module gathers streams of real time audit data from eclectic sources, which might include user and system activities within the mobile node, communication activities by this node as well as any communication activities within the radio range of this node and observable to this node.

2) **Local Detection Engine**: Local detection engine analyzes the local audit data for evidence of anomalies. This requires the IDS to maintain some expert rules for the node against which the audit data collected would checked. However as more and more appliances are becoming wireless, the types of planned attacks against these appliances is going to increase and this may make the existing expert rules insufficient to tackle these newer attacks. Moreover, updating these already existing expert rules is not a simple job. So any IDS meant for a wireless ad-hoc network should resort to statistical anomaly detection techniques. The normal behaviour patterns called “Normal Profiles” are determined using the trace data from a training process where all activities are normal. During the “testing” process any deviations from the normal profiles are recorded if at all any occur. A detection module is computed from the deviation data to distinguish anomalies from normalcy. There are always going to be normal activities which have not been observed and recorded before, however their deviations from the normal profile is going to be much smaller than those of intrusions.
3) **Cooperative Detection**: If a node locally detects a known intrusion with strong evidence it can very well on its own infer that the network is under attack and can initiate a response or a remedial action. However if the evidence of an anomaly or intrusion is a weak one or is rather inconclusive then the node decides it needs a broader investigation and can initiate a global intrusion detection procedure, which might consist of transmitting the intrusion detection state information among neighbours and further down the network if necessary.

The intrusion detection state information may be a mere level-of-confidence value expressed as percentage.

- With p% confidence, node A after analyzing its local data concludes that there is an intrusion.

**Fig.4.5.2 A Conceptual model for an IDS agent.**
With p% confidence, node A after analyzing the local data as well as that from its neighbours that there is an intrusion.

With p% confidence, node A, B, C,…. Collectively conclude that there is an intrusion.

To a more specific state that lists the suspects like,

With p% confidence, node A concludes after analyzing its local data that node X has been compromised.

A distributed consensus algorithm is then derived to compute the new intrusion detection state for the node under consideration, with the help of the state information recently received from the other nodes in the network. The algorithm might involve a weighted computation assuming that nearer nodes have greater effect than the far away ones.

A majority based Intrusion Detection Algorithm can include following steps:

1) The node sends to its neighbouring node an “intrusion state request”.
2) Each node, including the one which initiates this algorithm then propagates the state information, indicating the likelihood of an intrusion to its immediate neighbours.
3) Each node then determines whether the majority of the received reports point towards an intrusion, if yes then it concludes that the network is under attack.
4) Any node which detects an intrusion to the network can then initiate the remedial/response procedure.

As a rule of thumb, audit data from other nodes should not be trusted as compromised nodes might tend to send misleading data. However for compromised node sending audit data doesn’t hold any incentives, in doing so it might create a situation which would result in its expulsion from the network. Hence, unless majority of nodes are compromised, and there exists at least one valid node the remedial procedure won’t be initiated.

4.5.1 Intrusion Response

The type of intrusion response for wireless ad-hoc networks depends on the type of intrusion, the type of network protocols and the confidence in the veracity of the audit trace data. The response might range from resetting the communication channels between nodes or identifying the compromised nodes and precluding them from the network. The IDS agent can notify the end user to do his/her own investigation and take the necessary action. It also sends a re-authentication requests to all the nodes in the network, to prompt their respective end users to authenticate themselves. Only the re-authenticated nodes participate in negotiating a new communication channel and will recognize each other as legitimate nodes. Thus the malicious nodes can be excluded.
4.6 Anomaly detection in mobile ad-hoc networks

4.6.1 Detecting Abnormal Updates to Routing Tables

For Ad-hoc routing protocols, the primary concern is that false routing information generated and transmitted by a compromised node will be used by other nodes in the network, hence a good candidate for audit data would be the updates of routing information. A routing table basically holds the next hop to each destination node and the distance in terms of number of hops. A legitimate change in the routing table is caused by physical motion of the nodes or changes in the membership of the network. For a node, its own movement and the change in its own routing table are the only data it can trust and hence we use it as a basis of the trace data. The physical movement is measured by distance, direction and velocity. The routing table change is measured by Percentage of changed routes (PCR), and the percentage changes in the sum of hops of all routes (PCH). We use percentages as measurements because the number of nodes/route is not fixed due to dynamic nature of the wireless ad-hoc networks. During the “training” process, a wide variety of normal situations is simulated and the corresponding trace data is gathered for each node. The audit/trace data of all the nodes in the network are then merged together to get a set of all normal changes to the routing table for all nodes. The normal profile specifies the correlation of the physical movement of the node and the changes in the routing table. The classification algorithm classifies available trace data into ranges. Now for a particular trace data, if the PCR and/or PCR values are beyond the valid range for a particular movement (velocity, direction & distance) then it is considered to be an anomalous situation and the necessary procedures are initiated.

4.6.2 Detecting Anomalous activities in other layers

For MAC protocols, trace data could be in the form of total number of channel requests, the total number of nodes making those requests etc, for last S seconds. The class can be the range of the current requests by a node. The classifier of the trace data describes the normal profile of a request. Anomaly detection model can then be computed on the basis of the deviation of the trace data from the normal profile.

Similarly, at the Wireless Application layer can use service as the class and can contain following features – for the past S seconds, the total number of requests to the same service, total number of services requested, the average duration of service, the number of nodes that requested service, the total number of service errors etc. A classifier for each service then describes the class for each service and a normal behaviour for its requests.
4.6.3 Key Management in Wireless Networks

From security point of view, multiple lines of defense against attacks are desired. A complete security solution for wireless ad hoc networks should contain three components: prevention, detection, and reaction.

Security solutions in wireless ad hoc networks rely on key management mechanisms. In this section, we briefly introduce symmetric key management and asymmetric (public) key management.

(a) Symmetric Key Management

Symmetric key systems, like DES, AES and keyed hash functions, are based on shared key information between two parties in communications. In this case, if the sender uses the secret key to encrypt a message, the receiver uses the same secret key to decrypt the message. Symmetric key techniques are attractive due to their energy efficiency. Therefore, a number of techniques have been developed for a specific type of ad hoc networks—wireless sensors networks, since sensors are inexpensive and low-power devices.

In symmetric key cryptography, a sender and a receiver must establish a shared key before communication. In the context of sensor networks, shared keys are distributed to sensors before their deployment. It is very challenging to design key distribution schemes with the following two concerns in a large-scale sensor network under limited memory resources:

Connectivity: High percentage of the neighboring sensor nodes should share at least one secret key.

Resilience: When some nodes are compromised by an adversary, other sensors are still able to maintain secure communications.

(b) Random Key Distribution

In [10], key distribution consists of three phases: (1) key pre-distribution, (2) shared-key discovery, and (3) path-key establishment. In the pre-distribution phase,

4.7 Detecting Intrusions as Anomalies

Mobile ad hoc networks (MANETs) combine wireless networking with a high degree of node mobility. Limited-range wireless communication and high node mobility requires that the nodes cooperate with each other to provide essential networking, with the underlying network dynamically changing to ensure needs are continually met. The dynamic nature of the protocols that enable MANET operation means they are readily suited to deployment in extreme or volatile circumstances.

MANETs by their very nature are inherently more vulnerable to attack than wired...
networks. The flexibility provided by the open broadcast medium and the trust-based cooperation between the mobile devices (which have generally different resource and computational capacities, and run usually on battery power) introduces new security risks. As part of rational risk management, we must be able to identify these risks and take appropriate action. In some cases we may be able to design out particular risks cost-effectively. In other cases, we may have to accept that vulnerabilities exist and seek to take appropriate action when we believe someone is attacking us. As a result, intrusion detection is an indispensable component of security frameworks for MANETs.

Many intrusion detection systems (IDS) have been proposed in the literature for wired networks, but the peculiar features of MANETs make direct application of these approaches to MANETs impossible. In this paper, we examine special IDS issues of MANETs and proposed IDSs for MANET-specific systems to find out how well-proposed systems address these issues. In the next section, an introduction to intrusion detection systems is provided. Then, intrusion detection in MANETs is discussed along with proposed IDSs.

### 4.7.1 Conventional Intrusion Detection Systems

Intrusion is any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource [6] and an intrusion detection system (IDS) is a system for the detection of such intrusions. There are three main components of an IDS: data collection, detection and response.

**Misuse-based intrusion detection** compares known attack signatures with current system activities. It is generally preferred by commercial IDSs since it is efficient and has 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. Both anomaly-based and misuse-based approaches have their strengths and weaknesses. Therefore, both techniques are generally employed for effective intrusion detection.

The last technique is **specification-based intrusion detection.** In this approach, a set of constraints on a program or a protocol are specified and intrusions are detected as runtime violations of these specifications. It is introduced as a promising alternative that combines the strengths of anomaly-based and misuse-based detection techniques, providing detection of known and unknown attacks with a lower false positive rate [26]. It can detect new attacks that do not follow the system specifications. Moreover, it does not trigger false alarms when the program or protocol has unusual but legitimate behavior, since it uses the legitimate specifications of the program or protocol [26]. It has been applied to ARP (Address Resolution Protocol), DHCP (Dynamic Host Configuration Protocol) [25] and many MANET routing protocols. Defining detailed specifications for each program/protocol can be a very time-consuming job. New specifications are also needed for each new program/protocol and the approach cannot detect some kind of attacks such as DoS (Denial of Service) attacks since these do not violate program specifications directly [9].

When an intrusion is detected, an appropriate response is triggered according to the response policy. Responses to detected intrusions can be passive or active. Passive responses simply raise alarms and notify the proper authority. Active responses try to mitigate effects of intrusions and are divided into two groups: those that seek control over the attacked system and those that seek control over the attacking system [3]. The former tries to restore the damaged system by killing processes, terminating network connections and the like. The latter tries to prevent attacker's future attempts, which can be necessary for military applications.
4.8 Intrusion Detection Issues in MANETs

Different characteristics of MANETs make conventional IDSs ineffective and inefficient for this new environment. Consequently, researchers have been working recently on developing new IDSs for MANETs or changing the current IDSs to be applicable to MANETs. There are new issues which should be taken into account when a new IDS is being designed for MANETs.

**Mobility:** MANET nodes can leave and join the network and move independently, so the network topology can change frequently. The highly dynamic operation of a MANET can cause traditional techniques of IDS to be unreliable. For example, it is hard for anomaly-based approaches to distinguish whether a node emitting out-of-date information has been compromised or whether that node has yet to receive update information [7]. Another mobility effect on IDS is that IDS architecture may change with changes to the network topology.

**Wireless links:** Wireless networks have more constrained bandwidth than wired networks and link breakages are common. IDS agents need to communicate with other IDS agents to obtain data or alerts and need to be aware of wireless links. Because heavy IDS traffic could cause congestion and so limit normal traffic, IDS agents need to minimize their data transfers [18]. Bandwidth limitations may cause ineffective IDS operation. For example, an IDS may not be able to respond to an attack in real-time due to communication delay. An IDS must be capable of tolerating lost messages whilst maintaining reasonable detection accuracy [24].

**Limited resources:** Mobile nodes generally use battery power and have different capacities. MANET devices are varied, e.g. laptops, handheld devices like PDAs (personal digital assistants) and mobile phones. The computational and storage capacities vary too. The variety of nodes, generally with scarce resources, affects effectiveness and efficiency of the IDS agents they support. For example, nodes may drop packets to conserve resources (causing difficulties in distinguishing failed or selfish nodes from attacker or compromised nodes) and memory constraints may prevent one IDS agent processing a significant number of alerts coming from others. The detection algorithm must take into account limited resources. For example, misuse based detection algorithm must take into account memory constraints for signatures and anomaly-based detection algorithm needs to be optimized to reduce resource usage.

**Lack of a clear line of defense and secure communication:** MANETs do not have a clear line of defense; attacks can come from all directions [28]. For instance, there are no central points on MANETs where access control mechanisms can be placed. Unlike wired networks, attackers do not need to gain physical access to the network to exploit some kinds of attacks such as passive eavesdropping and active interference (these require only radio contact) [28]. Furthermore, the critical nodes (servers, etc.) cannot be assumed to be secured in cabinets and nodes with inadequate protection have high risk of compromise and capture. IDS traffic should be encrypted to avoid attackers learning how the IDS works [18]. However, cryptography and authentication are difficult tasks in a mobile wireless environment since they consume significant resources.

**Cooperativeness:** MANET routing protocols are usually highly cooperative. This can make them the target of new attacks. For example, a node can pose as a neighbor to the other nodes and participate in decision mechanisms, possibly affecting significant parts of the network.
4.9 Proposed Intrusion Detection Systems (IDSs)

IDSs on MANETs use a variety of intrusion detection methods. The most commonly proposed intrusion detection method to date is specification-based detection. This can detect attacks against routing protocols with a low rate of false positives. However, it cannot detect some kind of attacks, such as DoS attacks. There are also some anomaly-based detection systems implemented in MANETs. Unfortunately, mobility of MANETs increases the rate of false positives in these systems. There have been few misuse-based IDSs developed for MANETs and little research on signatures of attacks against MANETs. Updating attack signatures is an important problem for this approach. Some systems use promiscuous monitoring of wireless communications in the neighborhood of nodes.

Since nodes in MANETs have only local data, a distributed and cooperative IDS architecture is generally used to provide a more informed detection approach. In this architecture, every node has its local IDS agent and communicates with other nodes' agents to exchange information, to reach decisions and respond. Other IDS architectures in MANETs are stand-alone and hierarchical IDSs [1]. In stand-alone IDS architectures, every node in the network has an IDS agent and detects attacks on its own without collaborating with other nodes. Because this architecture cannot detect network attacks (network scans, distributed attacks, etc.) with the partial network data on the local node, it is generally not preferred. Hierarchical IDSs are also a kind of distributed and cooperative architecture. In this architecture, the network can be divided into groups such as clusters, zones where some nodes (cluster-heads, inter-zone nodes etc.) have more responsibility (providing communication with other clusters, zones) than other nodes in the same group. Each node in a cluster/zone carries out local detection while cluster-heads and inter-zone nodes carry out global detection. It is more suitable for multi-layered networks [1]. Distributed IDS agents (nodes) are generally divided into small groups such as clusters, zones, and one-hop away nodes, enabling them to be managed in a more efficient way, Communication between these IDS agents is provided either by exchanging data directly or by use of mobile agents.

Two different decision-making mechanisms are used in distributed and cooperative IDSs: collaborative decision-making, where each node can take active part in the intrusion detection process, and independent decision-making, where particular nodes are responsible for decision-making [12]. Both decision-making mechanisms have pros and cons. Collaborative decision making systems are more reliable. If all nodes contribute to a decision, a few malicious nodes cannot easily disrupt the decision-making. However, if any node can trigger a full-force response, it can affect the entire network and be vulnerable to a DoS attack [12]. A collaborative decision-making approach is also more resilient to benign failure of nodes. On the other hand, failing or compromise of particular nodes in independent decision-making systems can have drastic effects. However, these systems are less prone to spoofed intrusion attacks than collaborative decision-making systems.

The main proposed IDSs for MANETs in the literature are described below.

(a) Distributed and Cooperative IDS

The first IDS for MANETs proposed by Zhang and Lee is a distributed and cooperative IDS. In this architecture, every node has an IDS agent, which detects intrusions locally and collaborates with neighboring nodes (through high-confidence communication channels) for global detection, whenever available evidence is inconclusive and a broader search is needed. When an intrusion is detected, an IDS agent can trigger a local response (e.g. alerting the local user) or a global response (which coordinates actions among neighboring nodes).

Since expert rules can detect only known attacks and the rules cannot easily be updated across a wireless ad hoc network, statistical anomaly-based detection is chosen
over misuse-based detection’. The local data are relied on for statistical anomaly-based detection: the node's movement (distance, direction, velocity) and the change of routing table (PCR: percentage of changed routes, PCH: percentage of changes in the sum of hops all the routes).

A multi-layer integrated intrusion detection and response is proposed allowing different attacks to be detected at the most effective layer. It is believed to achieve a higher detection rate with a lower false positive rate.

The RIPPER and SVM-Light classification algorithms are used. In their subsequent research [29], these algorithms are evaluated on three routing protocols: AODV, DSR and DSDV using detection rate and false alarm rate metrics. SVM-Light is shown to have better performance than RIPPER. It is also shown that the protocols with strong correlation among changes of different types of information (location, routing, etc.) have better performance, so reactive (on-demand) protocols are more appropriate for this system than proactive (table-driven) protocols. Moreover, it is stated that the IDS works better with protocols which include some redundancy (such as path redundancy in DSR). However, the mobility effect is not discussed.

This can decrease false positives resulting from the node's mobility. However, it only reflects the local mobility not the network's mobility. Also, every node has to have a built-in GPS (Global Positioning System) to obtain this mobility data. From the security point of view, the system is reliable unless the majority of nodes are compromised [28]. (These can send falsified data.) Furthermore, the collaborative detection mechanism can be prone to denial of service and spoofed intrusion attacks [12].

(b) Zone-Based Intrusion Detection System

In [22], a non-overlapping zone-based IDS is proposed. In this architecture, the network is divided into zones based on geographic partitioning to save communication bandwidth while improving detection performance by obtaining data from many nodes. The nodes in a zone are called intra-zone nodes, and the nodes which work as a bridge to other zones are called inter-zone (gateway) nodes. As shown in Fig.1 there can be more than one gateway node in a zone, for instance, the nodes 1, 6, 7 are gateway nodes in zone 5. Each node in the zone is responsible for local detection and sending alerts to the inter-zone nodes.

Their framework aims to allow the use of different detection techniques in each IDS agent; however, they use only Markov chain anomaly detection in their research. Inputs to IDS agents are the routing table updates (PCR and PCH) as in [28, 29].

Intra-zone nodes carry out local aggregation and correlation, while gateway nodes are responsible for global aggregation and correlation to make final decisions and send alarms. So only gateway nodes participate in intrusion detection. The alerts sent by inter-zone nodes simply show an assessment of the probability of intrusion; the alarms generated by gateway nodes are based on the combined information received. In their aggregation algorithm, gateway nodes use the following similarities in the alerts to detect intrusions: classification similarity (classification of attacks), time similarity (time of attack happening and time of attack detection) and source similarity (attack sources). Source similarity is the main similarity used, so the detection performance of aggregation algorithm could decrease with increasing number of attackers [22].

One of the contributions in this paper is MIDMEF (MANET Intrusion Detection Message Exchange Format), which defines the format of information exchange between IDS agents. It is consistent with Intrusion Detection Message Exchange Format (IDMEF) proposed by the Internet Engineering Task Force (IETF) [10].
Previous work [21] analyzed how to consider mobility when designing an IDS. Link change rate is proposed to reflect different mobility levels. Suitable normal profiling and proper thresholds can then be adaptively adopted by IDS agents using this measure. Furthermore, it is shown that link change rate reflects the mobility model of the network better than the generally used mobile speed measure. Link change rate of a node is defined as:

\[ |N_{t2} - N_{t1}| + |N_{t1} - N_{t2}| \]

where \( N_{t1} \) is the neighbor set of the node at \( t_1 \) time and \( N_{t2} \) is the neighbor set of the node at \( t_2 \) time. The proposed IDS is simulated on the GlomoSim simulator and evaluated using the following performance metrics: false positive rate, detection rate and mean time of first alarm (a measure of how fast intrusion is detected). The system is trained and evaluated under different mobility levels and it is shown that the anomaly-based detection performs poorly due to the irregularity of data under high mobility. Furthermore, the presence of partial victims who do not receive all falsified data because of link breakages resulting from mobility [22] is claimed to make the detection more difficult. The advantages of an aggregation algorithm using the data from both partial and full victims are emphasized: lower false positive and higher detection rate than local IDS achieves.

(c) General Cooperative Intrusion Detection Architecture

In [20], Sterne et al. present a cooperative and dynamic hierarchical IDS architecture, which uses multiple-layering clustering. Fig. 2 shows a network with two-level clusters. The nodes annotated with "1" are the first-level cluster-heads, essentially acting as a management focus for IDS activity of immediately surrounding nodes. These level 1 cluster-heads can form a cluster around high-level node "2", second-level cluster-head. This process goes on until all nodes are assigned.

Fig. 2 IDS hierarchy with two-level clusters

a cluster. Single points of failure can be avoided by choosing more than one cluster-head for the top-level cluster. Criteria used for identification of cluster heads includes topology, proximity, resistance to compromise, processing power and bandwidth.

---

Security Aspects & Performance Analysis of Mobile & IP Networks  
Page 63

---

Fig. 1 Zone-based IDS architecture in MANETs
(d) Intrusion Detection Using Multiple Sensors

Kachirski and Guha [12] have proposed an IDS solution based on mobile-agent technology which distributes the functional tasks by using three mobile agent classes: monitoring, decision-making and action-taking. This architecture results in increased fault-tolerance, reduced communication cost, improved performance and scalability. The network is divided into clusters, cluster-heads are chosen by vote, with each node voting for a node based on its connectivity. Only cluster-heads are responsible for detection using network-level data and for making decisions. However, depending on the hop attribute of the clusters, network intrusion detection performance can change.

For example, every node has direct connection to at least one cluster head in a one-hop clustered network, so each packet in the network can be monitored as shown in Fig.3(a), while three links in Fig.3(b) cannot be monitored by the cluster-heads in a two-hop clustered network.

![Fig.3](a) one-hop clustered network: 1,2,5,8 are cluster-heads. (b) two-hop clustered network: 1,2,5 are cluster-heads.

As the degree of monitoring increases the number of cluster heads increases too. So, choosing the hop attribute of the clusters is a trade-off between security and efficiency. However, the nodes not in a cluster-head's communication range can move to the monitoring area of another cluster-head due to mobility. So, having a few links that cannot be monitored by any cluster-head is regarded as acceptable for highly dynamic environments.

Cluster nodes can respond to the intrusions directly if they have strong evidence locally. If the evidence is insufficient, they leave decision-making to cluster heads by sending anomaly reports to them.

(e) Specification-Based IDS for AODV

The first specification-based IDS in MANETs, proposed by Tseng et al. [25], uses network monitors (NM), which are assumed to cover all nodes. Nodes moving out of the current network monitoring area are also assumed to move into range of other network monitors. Other assumptions are: (i) network monitors know all nodes' IP and MAC
addresses, and MAC addresses cannot be forged, and, (ii) network monitors and their messages are secure.

### 4.10 Detection of Misbehaving Nodes

Nodes in MANETs rely on other nodes to forward their packets. However, these intermediate nodes can misbehave by dropping or modifying these packets. Several proposed techniques to detect such misbehaviors are given below.

(a) **Watchdog & Pathrater**

This is the primary work in detecting misbehaving nodes - nodes that do not carry out what they are assigned to do and mitigating their effects. Since ad hoc networks maximize total network throughput based on cooperativeness of all nodes for routing and forwarding, misbehaving nodes can be critical for the performance of the network as stated in [15]. In this paper, watchdog and pathrater mechanisms on DSR are proposed to improve throughput of the network in the presence of misbehaving nodes. Nodes can misbehave because they can be overloaded, selfish (wanting to save their own resources), malicious or simply malfunctioning.

Watchdog and Pathrater with/without SRR have been evaluated on the NS simulator with four different mobility levels by using throughput, overhead and false positive rates as metrics. The results show that Watchdog and Pathrater increase the throughput by 17% in the presence of 40% misbehaving nodes in moderate mobility with 9-17% overhead. Under extreme mobility, they increase throughput by 27% with 12-24% overhead.

(b) **Nodes Bearing Grudges**

This is an interesting approach proposed in [4] for detecting and responding to misbehaving nodes, inspired by the biology concept of reciprocal altruism. It detects misbehaving nodes and responds by not forwarding their packets. The aim of this approach is to increase fairness, robustness and cooperation in MANETs.

Each node is responsible for monitoring the behavior of its next-hop neighbors and detecting misbehaving nodes. Each node has a trust architecture and an FSM in each node with four main components: the monitor, the reputation system, the path manager and the trust manager.

The reputation system (node rating) keeps a local rating list and/or black list, which can be exchanged with friends. The rating of a node can change when there is enough evidence, and is based on the frequency of misbehavior occurrence [15]. The rate function also uses weights depending on the source detecting misbehavior. One's own experience has the highest weight, where observations have relatively smaller weights and reported experiences from other nodes have weight based on the trust level of these nodes. The reputation system uses only negative experience; research on positive changes and timeouts still needs attention.

The trust level of nodes is managed by the Trust Manager, which is distributed and adaptive. It is also responsible for forwarding alarm messages and filtering incoming messages from other nodes. Trust of a node plays a significant role when exchanging routing information with that node, using it for routing or forwarding, and accepting its forwarding requests.

Path manager may respond to a request from misbehaving nodes in a variety of ways, such as ignoring the request, not replying back to the node, responding to any request for a route that include misbehaving nodes by sending alerts to the source node, re-ranking paths and deleting paths including misbehaving nodes [4].

(c) **Lightweight Packet Drop Detection (LiPaD)**
Anjum and Talpade [2] have proposed a practical approach for detecting packet dropping attacks. In this approach every node counts the packets that it receives and forwards and periodically reports these counts to a coordinator node. Every node is responsible for monitoring its packets in LiPaD. The algorithm executed in each node is very simple, which is good for resource-constrained nodes. On the other hand, the network bandwidth consumption can be huge, since every node sends reports of each flow defined by source IP and destination IP to the coordinator node. They suggest compressing and aggregating the reports of multiple flows instead of sending each flow in a packet. However, it still affects network traffic, especially in networks with hundreds nodes. There will be a heavy computation load on the coordinator node (which analyzes all nodes' reports). The coordinator node needs to be a powerful device and must also be secure as it can be the target of the attacks to disable the detection mechanism. For example, it can become target of DoS attacks (by overloading with reports).

Since the coordinator node analyzes the same flow through the reports from all nodes in the route, it can detect liar nodes that pass the wrong information about the statistics of their packets to the coordinator node [2]. If all the nodes on the route are cooperative and malicious, LiPaD cannot detect packet dropping attacks on this route.

(d) Responding to Intrusion Detection

Parker et al. [17] extend snooping based methods to detect misbehavior across routing protocols. A node listens to all nodes in its transmission range, not just the packets forwarded by one of its next nodes (as in watchdog [15]). To detect a malicious node in this approach, it is stated that the node must be in the proximity of a good node and act maliciously. It detects dropping and modification attacks, which exceed the value in the threshold table for the particular attack class. However, a node moving out of range of the monitoring node before it forwards packets can be assumed to be carrying out a dropping attack.

The intrusion detection protocol can give either a local or a global response. In a local response, misbehaving nodes in the Bad Node table are isolated. In the global response, the maliciousness of node is determined by a vote by all nodes in a cluster. If the majority of the nodes agree that the node is intrusive, an alert will be broadcasted. Voting is initiated by cluster-heads. Cluster-heads can be malicious, but the likelihood of malicious nodes being elected as cluster-heads is relatively small.

4.11 Open Issues & Future Scope

MANETs are a new technology increasingly used in many applications. These networks are more vulnerable to attacks than wired networks. Since they have different characteristics, conventional security techniques are not directly applicable to them. Researchers currently focus on developing new prevention, detection and response mechanism for MANETs. Proposed IDSs for MANETs vary significantly, e.g. in terms of their detection technique, architecture, decision-making and response mechanisms. On the other hand, every proposed system should be considered in its own context.

Mobility, node capabilities and network infrastructure are usually the main features examined for proposed MANET IDSs. For highly mobile networks, IDSs using anomaly-detection techniques may suffer high false positive rates. Further, an IDS architecture that is easy to set up should be preferred for these networks, e.g. IDS agents who collaborate with one-hop away nodes. Besides mobility, node capabilities should also be considered. Simple detection techniques can be more appropriate for nodes with limited resources. For instance, the approach in [27] uses a reduced feature set without significantly decreasing detection rate. Obviously, network infrastructure plays an important role in IDS selection. A hierarchical IDS architecture should be preferred to a multilayered infrastructure, and distributed and cooperative architecture should be preferred for flat infrastructure [1].
None of the proposed systems implements the best solution taking into account different applications. Every organization should choose the appropriate IDS for its network. Moreover, it can change the IDS according to its own requirements and characteristics. For example, it can change the architecture of chosen IDS or put different intrusion detection techniques together. Therefore, defining requirements and determining characteristics of the network are very important factors in determining the most appropriate IDS solution.

4.12 Conclusions

We have presented an overview of the existing security scenario in the Ad-Hoc network environment. Key management, Ad-hoc routing and intrusion detection aspects of wireless Ad-hoc networks were discussed. Ad-hoc networking is still a raw area of research as can be seen with the problems that exist in these networks and the emerging solutions. The key management protocols are still very expensive and not fail safe. Several protocols for routing in Ad-hoc networks have been proposed. There is a need to make them more secure and robust to adapt to the demanding requirements of these networks. Intrusion detection is a critical security area. But it is a difficult goal to achieve in the resource deficient Ad-hoc environment. But the flexibility, ease and speed with which these networks can be set up implies they will gain wider application. This leaves Ad-hoc networks wide open for research to meet these demanding application.

Intrusion detection on these complex systems is an evolving, immature research area. There are far fewer proposed IDSs for MANETs than for conventional networks. Researchers can focus on either introducing new IDSs to handle MANET specific features or can adapt existing systems. Hybrid approaches may also prove of significant use.

The proposed systems seek to address the lack of central control issue on MANETs by proposing distributed and cooperative IDS architectures. Such architectures raise questions about security, communication and management aspects. Suitability of the architecture to the environment is an important consideration in designing IDS. An architecture should not introduce new weaknesses/overheads to IDS. For instance, some of the proposed architectures like cluster-based approaches are costly to build and maintain for high-mobility networks and may also have critical points of failure.

Appropriate weight should be attached to mobility, especially for anomaly-based IDSs. The false positive rate may be greatly affected by mobility level. The system should be aware of its mobility and current network topology. So features having information about mobility should be included to the intrusion detection system being designed. Since the nodes are the only data sources on the network, all nodes should contribute to IDS by carrying out local monitoring, detection and providing local data to other nodes when needed. However, nodes can have different computational capabilities and some of them cannot be powerful enough for executing complex or large intrusion detection algorithms. Insufficient research studies are currently available on the limited resources issue. Researchers may consider developing different algorithms for different nodes based on their resources and/or computational capabilities. More intense detection algorithms can be applied in order to monitor critical nodes as proposed in [13].

Testing IDS is also an open research area for both MANETs and conventional networks. Some of the proposed systems are tested only on very small networks and with few attack scenarios. IDSs should be tested under different mobility levels and with different network topologies. Defining testing criteria for IDSs and preparing test datasets needs further research.

In this paper, we have provided a survey of research on IDS for MANETs. Many MANET IDSs have been proposed, with different intrusion detection techniques,
architectures, and response mechanisms. We have focused on the contribution/novelty each brings and have identified the specific MANET issues each does not address. Proposed systems generally emphasize few MANET issues. MANETs have most of the problems of wired networks and many more besides. As a consequence, intrusion detection for MANETs remains a complex and challenging topic for security researchers.

References


5. Performance of Mobile Adhoc Networks (MANETs)

QoS is the performance level of a service offered by the network to the user. The primary goal of QoS provisioning is to achieve more deterministic behavior by proper utilization of the network resources. A network or a service provider can offer different kinds of services to the users based on a set of service requirements such as minimum bandwidth, maximum delay, maximum variance in delay, and maximum rate of packet loss. After accepting a service request from the user, the network is expected to ensure the committed service requirements of the users throughout the communication. QoS