A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks

Adnan Nadeem member IEEE and Michael P. Howarth

***Abstract*—In the last decade, mobile ad hoc networks (MANETs) have emerged as a major next generation wireless networking technology. However, MANETs are vulnerable to various attacks at all layers, including in particular the network layer, because the design of most MANET routing protocols assumes that there is no malicious intruder node in the network. In this paper, we present a survey of the main types of attack at the network layer, and we then review intrusion detection and protection mechanisms that have been proposed in the literature. We classify these mechanisms as either point detection algorithms that deal with a single type of attack, or as intrusion detection systems (IDSs) that can deal with a range of attacks. A comparison of the proposed protection mechanisms is also included in this paper. Finally, we identify areas where further research could focus.**

***Index Terms*—Intrusion detection and prevention, mobile ad hoc networks, network layer attacks, securing ad hoc networks.**

I. Introduction

The concept of mobile wireless devices working together was proposed in the 1990s, since when a significant amount of research has been conducted on mobile ad hoc networks (MANETs). The IETF established the Mobile Ad hoc Networks Working Group [1] in 1997, with the aim of standardizing routing protocols for MANETs. They developed two standard track routing protocol specifications, namely the reactive and proactive MANET protocols. Another IETF working group, called Ad Hoc Networks Autoconfiguration (autoconf) [2], had as its main aim considering the issues in the addressing model for ad hoc networks. MANETs use IEEE 802.11 architecture components as described in [3]. The Basic Service Set (BSS) defines an architecture in which all stations can communicate between themselves using IEEE 802.11 wireless LAN technology. A BSS consists of an access point (AP) and all the stations associated with it. Figure 1 shows the alternative ad hoc network architecture using the IEEE 802.11 independent basic service set (IBSS). In this mode no access point is required, and nodes communicate in a distributed peer-to-peer manner. The minimum requirement for IBSS operation is that two nodes be within radio range of each other.

MANETs have wide applications in various fields. For example, they have been used in a military context since the 1970s to ensure the timely flow of information and command in battle, contributing to the success of a mission. Given their desirable characteristic of fast and easy deployment, MANETs are also ideal for establishing communication networks and providing rescue services following natural disasters such as earthquakes or floods. Another major application of MANETs is on-the-fly collaborative computing outside an office environment, for example during fieldwork, in a team project

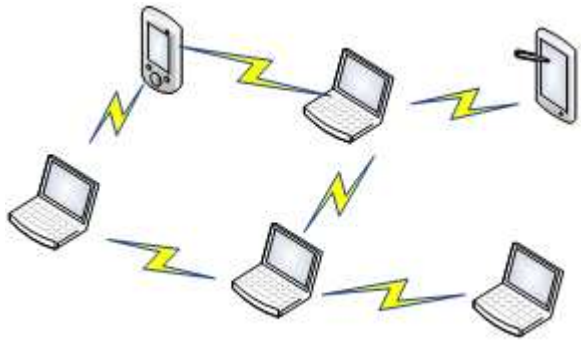


Fig. 1. Ad hoc architecture using IEEE 802.11 IBSS

offsite, or during an offsite meeting. Researchers are also investigating the technicalities of application scenarios for MANETs in commercial areas. For example, MANETs can be used in communication dispatch systems for taxis in a town to inform individual taxis about passenger pickups, route directions, weather conditions etc. Finally, they can also be used in personal networking: for example, PDAs, notepads, and cell phones can form an ad hoc network to communicate and achieve other networking capabilities using IEEE 802.11.

Noting these wider applications of MANETs, much research has been conducted since 1990 on various aspects such as routing, security, quality of service, IP addressing, multiple access, and management of these networks. A significant part of the research work has focused on providing security services for MANETs, because security is the main obstacle for the widespread adoption of MANET applications. MANETs are vulnerable in their functionality: intruders can compromise the operation of the network by attacking at any of the physical, MAC or network layers. The network layer, especially the routing protocol, is vulnerable because of the use of cooperative routing algorithms, the limited computational ability of nodes, the exhaustible node batteries, a lack of clearly defined physical network boundary and the transient nature of services in the network. Standard information security measures such as encryption and authentication do not provide complete protection, and, therefore, intrusion detection and prevention (IDP) mechanisms are widely used to secure MANETs.

IDP systems have been used for the last three decades as one of the main layers of security in organizational networks. Research in this area started with Anderson's paper [4] in 1980. Since then, a significant number of intrusion detection system prototypes and proposals have been published, 92 of which have been recorded by Sobirey [5]. The authors in [6][7] presented a comprehensive taxonomy of intrusion detection

systems (IDSs) for fixed networks, and classified existing IDS proposals. Although the networking technology has since evolved and the networking paradigm has shifted from fixed to wireless networks in the last decade, intrusion detection and prevention is still considered as one of the basic layers of defence. Indeed, in infrastructure-less wireless networks such as MANETs where network firewall implementation is complex, intrusion detection and prevention is now considered as the first layer of defence [7][8].

Intrusion detection (ID) in MANETs is more complex and challenging than in fixed networks, because of the difficulty in fulfilling the requirements of IDS (namely the ability to collect audit data from the network, and apply ID techniques to detect intrusion with a low rate of false positives and an effective response to intrusion) and because some characteristics of MANETs create operational and implementation complexities. Additional challenges for IDSs in MANETs are as follows:

- MANETs lack concentration points where monitoring and audit data collection can be performed
- MANET routing protocols require nodes to cooperate and act as routers, creating opportunities for attacks
- Due to the nodes' mobility, the network topology is dynamic and unpredictable, making the process of intrusion detection complicated
- IDSs in MANETs are more complex because of the limited computational ability of most of the nodes

To cover the wide range of intrusion detection and prevention techniques in MANETs, in this paper we divide the techniques into two categories: those that are designed to deal with a single type of attack (which we call point detection algorithms), and those that can identify a range of attacks, which we consider to be true IDSs. In addition, this paper only considers network layer attacks. Consequently, given the importance of security services in MANETs and the challenges of protecting them from different types of attacks, in this paper we present a survey of network layer attacks, a critical review of their protection mechanisms and their classification as point detection algorithms or intrusion detection systems.

A number of surveys of intrusion detection for MANETs have been published. For example, [9] discussed the challenges of IDSs and presented a survey of a number of IDS proposals in both MANETs and WSNs. In [10], a description of network layer attacks and a survey of defence mechanisms for specific attacks were given. The authors of [11] presented a survey of anomaly-based intrusion detections systems (ABID) for MANETs. They compared eight ABID systems, considering detection techniques, attack types addressed and simulation environment, and discussed the advantages and disadvantages of the proposed mechanisms. In [12] the authors presented a survey of MANET IDSs that deal with specific attacks, and analyzed some of the challenges of IDSs. The authors of [13] surveyed countermeasures proposed for various network layer attacks, structuring their survey by attack type. In [14] the authors presented a survey of IDSs in MANETs and wireless mesh networks, mostly from the preceding four years. They compared IDSs based on the type of attack addressed and their underlying architecture. They also suggested that IDS needs a scalable architecture based on cross-layer design to detect these attacks effectively. [15] surveyed and classified IDSs in MANETS based on their architecture and the addressed type of attack. A number of mechanisms for detecting black hole attacks were reviewed in [16]. Our paper extends all the above work and draws on the significant amount of research that has been conducted since these papers were published, to provide an up to date view of the current state of the art in MANET intrusion detection. In particular, as we have noted, we classify the defence mechanisms as either point detection algorithms that deal with single types of attack, or as IDSs that deal with a wide variety of attacks.

The rest of our paper is organized as follows. In Section II we present a classification of network layer attacks and then illustrate some of the main types. Section III reviews the point detection algorithms that have been proposed to secure MANETs from specific network layer attacks. Section IV then considers proposals that detect a range of attack types; the section first introduces the main categories of intrusion detection systems, then describes the challenges of implementing IDSs in MANETs, and finally reviews proposed IDSs and their architectures. Finally, Section V presents a summary, considers some open questions and suggests future research directions.

II. Attacks In MANETs

Various types of network layer attacks or intrusions are known for MANETs. In this Section we first present a classification of major network layer attacks and introduce some individual attacks. We then illustrate some major network layer attacks.

A. Classification of Network Layer Attacks

Network layer attacks in MANETs can be divided into two main categories, namely passive attacks and active attacks, as shown in Figure 2.

1) Passive Attacks : Passive attacks are those where the attacker does not disturb the operation of the routing protocol but attempts to seek some valuable information through traffic analysis. This in turn can lead to the disclosure of critical information about the network or nodes such as the network topology, the location of nodes or the identity of important nodes. Some examples of passive attacks are as follows:

Eavesdropping

Because of the wireless links in MANETs, a message sent by a node can be heard by every device equipped with a transceiver and within radio range, and if no encryption is used then the attacker can get useful information. The sender and receiver usually have no means of knowing that this attack has taken place. Although in most cases eavesdropping is not considered to be a severe attack, it could provide vital information in some scenarios and therefore researchers have focused on minimizing it. For example in [92] the authors analyzed the risk of eavesdropping as a function of the transmission range of the nodes and their geographical distribution.

Traffic Analysis and Location Disclosure

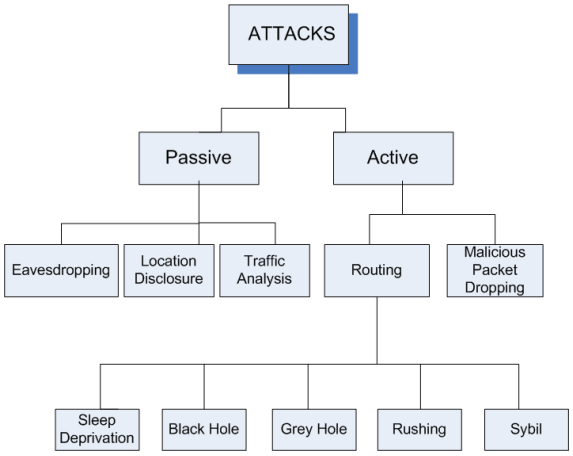


Fig. 2. Classification of network layer attacks in MANETs

Attackers can listen to the traffic on wireless links to discover the location of target nodes by analyzing the communication pattern, the amount of data transmitted by nodes and the characteristics of the transmission. For example, in a battlefield scenario, a large amount of network traffic normally flows to and from the headquarters. Traffic pattern analysis therefore allows an intruder to discover the commanding nodes in the network. Even if the data in a message is protected by encryption, traffic analysis can still be performed to extract some useful information. Although passive attacks do not directly affect the network' functionality, in some MANET application scenarios, such as military communication, important information disclosure through traffic analysis or simply eavesdropping could prove costly. Examples of work on analysis and protection against these attacks can be found in [92][17][18].

2) Active Attacks : In active attacks, intruders launch intrusive activities such as modifying, injecting, forging, fabricating or dropping data or routing packets, resulting in various disruptions to the network. Some of these attacks are caused by a single activity of an intruder and others can be caused by a sequence of activities by colluding intruders. Active attacks (as compared to passive attacks) disturb the operations of the network and can be so severe that they can bring down the entire network or degrade the network performance significantly, as in the case of denial of service attacks. Therefore, in this paper we have focused on active network layer attacks. Active attacks can be further divided into malicious packet dropping attacks and routing attacks, as shown in Figure 2.

Malicious Packet Dropping

A path between a source node and a destination node in a MANET is established using a route discovery process. Once this has been done, the source node starts sending the data packet to the next node along the path; this intermediate node identifies the next hop node towards the destination along the established path and forwards the data packet to it. This process continues until the data packet reaches the destination node. To achieve the desired operation of a MANET, it is important that intermediate nodes forward data packets for any and all source nodes. However, a malicious node might decide to drop these packets instead of forwarding them; this is known as a data packet dropping attack, or data forwarding misbehaviour. In comparison to deliberately malicious behaviour, in some cases nodes are unable to forward data packets because they are overloaded or have low battery reserves; alternatively the nodes may be selfish, for example saving their battery in order to process their own operations. Packet dropping attacks differ from black hole and grey hole attacks (see below) because there is no attempt to "capture" the routes in the network.

Routing Attacks

Both the reactive and proactive routing protocols are vulnerable to routing attacks because they route based on the assumption that all nodes cooperate to find the best path. Consequently, a malicious node can exploit the vulnerabilities of the cooperative routing algorithms and the lack of centralized control to launch routing attacks. In particular, the on-demand (reactive) MANET routing protocols, such as AODV [19] and DSR [20], allow intruders to launch a wide variety of attacks. In the following we give examples of how different intrusive activities can cause various attacks in MANETs, illustrating them with AODV as the routing protocol.

Sleep Deprivation Attack

Sleep deprivation (SD) [21] is a distributed denial of service attack in which an attacker interacts with the node in a manner that appears to be legitimate, but where the purpose of the interaction is to keep the victim node out of its power-conserving sleep mode. In [22] the authors consider an intruder that can cause SD of a node by exploiting the vulnerability of the route discovery process of the protocol through malicious route request (RREQ) flooding in the following ways:

Malicious RREQ Flooding 1: an intruder broadcasts a RREQ with a destination IP address that is within the network address range but where the corresponding node does not exist. This compels all the nodes to forward this RREQ because no one will have the route for this destination IP address.

Malicious RREQ Flooding 2: After broadcasting a RREQ an intruder does not wait for the ring traversal time, but it continues resending the RREQ for the same destination with higher TTL values. This is a significant denial of service attack when we consider the energy constrained operations of MANETs.

Black Hole Attack

Intruders can exploit the vulnerability in route discovery procedures of on-demand routing protocols, such as AODV and DSR, when a node requires a route towards the destination. The node sends a RREQ and an intruder advertises itself as having the fresh route. By repeating this for route requests received from other nodes, the intruder may succeed in becoming part of many routes in the network. The intruder, once chosen as an intermediate node, drops the packets instead of forwarding or processing them, causing a black hole (BH) [23] in the network. The way the intruder initiates the black hole attack and captures the routes may vary in different routing protocols. For example, in AODV, the destination sequence number (dest_seq) is used to represent the freshness of the route. A higher value of dest_seq means a fresher

route. On receiving a RREQ, an intruder can advertise itself as having the fresher route by sending a Route Reply (RREP) packet with a new dest_seq number larger than the current dest_seq number. In this way, the intruder becomes part of the route to that destination. The severity of the attack depends on the number of routes in the network the intruder successfully becomes part of.

Grey Hole Attack

A grey hole attack (GH) [24] is a special case of the BH attack, in which an intruder first captures the routes, i.e. becomes part of the routes in the network (as with the BH attack), and then drops packets selectively. For example, the intruder may drop packets from specific source nodes, or it may drop packets probabilistically or drop packets in some other specific pattern. As we noted above, BH and GH attacks are different in nature from packet dropping attacks, where the attacker simply fails to forward packets for some reason. BH and GH attacks on the other hand comprise two tasks: the attacker first captures routes and then either drops all packets (BH attack) or some packets (GH attack).

Rushing Attack

In order to limit the control packet overhead, an on-demand protocol only requires nodes to forward the first RREQ that arrives for each route discovery. An attacker can exploit this property by spreading RREQ packets quickly throughout the network to suppress any later legitimate RREQ packets. For example, in AODV an intruder can forge and forward a rushed RREQ, assigning a higher source sequence (src_seq) number to it; the intruder will also transmit the packet earlier than specified in the AODV protocol (this is the sense in which it is a "rushing" attack). This causes any later legitimate RREQ to be suppressed, and increases the probability that routes that include the intruder will be discovered instead of other valid routes. Hu et al. [25] first described the rushing attack, and proposed its prevention through a set of generic mechanisms such as secure neighbour detection, secure route delegation and randomized RREQ forwarding.

Sybil Attack

Each node in a MANET requires a unique address to participate in routing, through which nodes are identified. However, in a MANET there is no central authority to verify these identities. An attacker can exploit this property and send control packets, for example RREQ or RREP, using different identities; this is known as a sybil attack (SY) [26]. This is an impersonation attack where the intruder could use either random identities or the identity of another node to create confusion in the routing process, or to establish bases for some other severe attack.

In summary, we note that the motivation of intruders behind launching either packet dropping or routing attacks is to achieve a certain goal such as denial of service (i.e. making certain resources or services, such as applications, web access, printing, or routing, unavailable to the intended users). In addition, other goals of intruders might include partitioning the network, creating routing loops, discovering valuable information, or theft of resources.

B. Illustration of Network Layer Attacks

In this subsection we illustrate the operation of some of the major network layer attacks that were introduced in subsection A.

1) Sleep Depriviation Attack Illustration: We start with the sleep deprivation attack defined in section II.A, using AODV as the routing protocol as an example to illustrate in detail the ways this attack can be introduced in the network.

When a node needs a route towards a destination, it initiates a route discovery process by broadcasting a RREQ with its current destination sequence number. If an intermediate node that receives the RREQ knows the route, it unicasts a RREP back to the source node, otherwise it rebroadcasts the RREQ packet. To control the dissemination of RREQs, AODV uses an expanding ring search technique, where the source node first sends a RREQ with its Time to Live (TTL) field set to some initial value, TTL_start. The source then waits for the ring_traversal_time. If this time expires without receiving a RREP the source node may send a RREQ again with increased TTL value. This process can be repeated until the TTL value reaches some value TTL_threshold, where TTL_threshold > TTL_start. Now consider Figure 3, which shows a snapshot of the network, where circles represent nodes and the dotted lines show direct links between the nodes. Suppose that node v_6 is an intruder, and suppose it launches a SD attack using malicious RREQ flooding as follows:

- v_6 generates a RREQ with a destination IP address for some non-existent node $v_{25,}$ (i.e. the IP address is within the network's address range but the node does not exist). Intruder v_6 broadcasts this RREQ (we assume here that the TTL value is sufficiently large to allow the RREQ to propagate across the network). Figure 4 shows the network after this initial broadcast. Nodes v_2 , v_1 , v_5 and v_9, which are within the radio range of v_6, will receive the RREQ (the solid arrows show the RREQ flow), and check their routing table entries for routes to the destination node v_{25}.
- Because nodes v_2, v_1, v_5 and v_9 do not have the route for node v_{25}, they will rebroadcast the RREQ initiated by the intruder.
- Nodes that receive RREQs from v_2 , v_1 , v_5 or v_9 will first check whether they have processed earlier copies of these requests; if not, then they will also broadcast this malicious RREQ further.
- Since no nodes know the route for this destination node, this process continues across the network.

Figure 5 shows the state of the network after the RREQ has been broadcast for three hops. The part of the network shown in the figure is flooded with malicious RREQs, and eventually the entire network will be flooded with these RREQs. Nodes processing these unnecessary packets drain their batteries and, hence, may no longer be able to provide services in the network.

In [27], the authors proposed neighbour supervision as a solution to this problem. Here, the neighbours maintain a priority queue of incoming RREQs and reduce the probability of processing RREQs from a node if a high number of

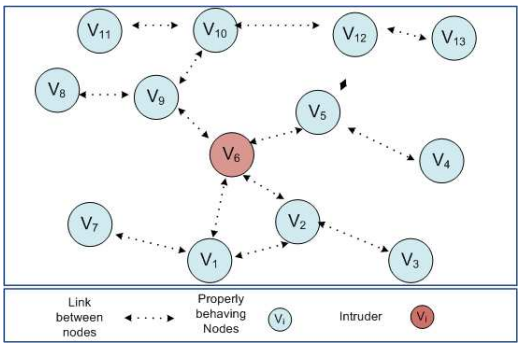


Fig. 3. Snapshot of the network without any attack

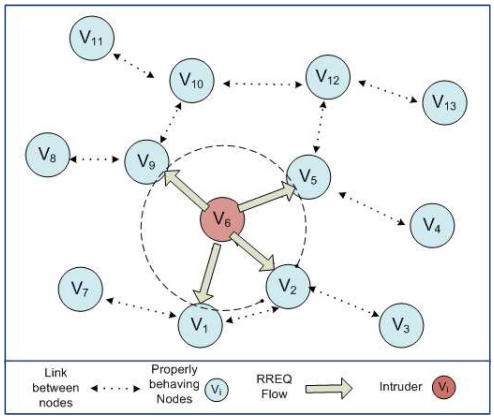


Fig. 4. Snapshot of the network after an intruder generates a malicious RREQ (after one hop)

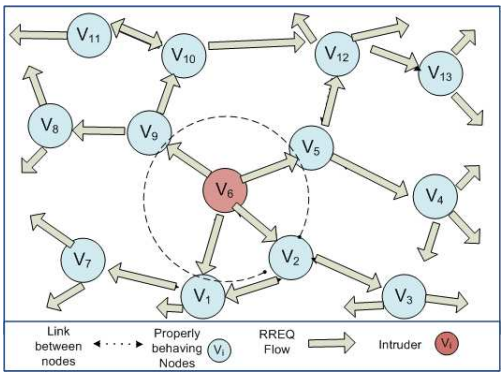


Fig. 5. Snapshot of the network with malicious RREQ flooding

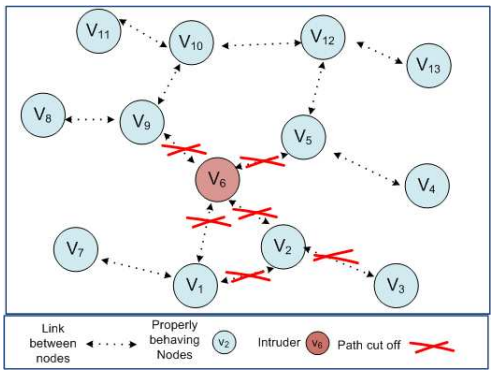


Fig. 6. Prevention of malicious RREQ flooding [27]

incoming RREQs are received from this node. If the number of RREQs received from a node exceeds a threshold the node neighbours cut off the path. For example, in Figure 6 if the number of RREQs received by the neighbours of node v_6 exceeds a threshold, each neighbour ignores $v_6$and cuts off the path. However, in some applications of MANETs, such as in networks formed for a seminar, some nodes might reasonably generate more data, for example if node v_2 is the seminar chair. Yet the method proposed in [27] based on a static threshold will cut off the path of node v_2 as shown in Figure 6. Node mobility will further degrade the performance of this approach; for example if intruder v_6 after a few broadcasts moves and continues the attack from another location, it can easily bypass this protection mechanism.

2) Black Hole Attack Illustration: We now consider the network in Figure 7 and illustrate how an intruder can launch a black hole or grey hole attack. We suppose that nodes v_9 and v_4 each need routes to nodes v_{13} and v_7 respectively. Therefore, nodes v_9 and v_4 broadcast RREQs and the initial flow of RREQs is shown in Figure 8. Now assume node v_6 is an intruder and wants to capture the routes in the network to cause either a black or grey hole attack, by using false RREP packets in the following way:

The two RREQs from nodes v_9 and v_4 will be heard by node v_6, which then checks its current destination sequence numbers for v_{13} and v_7.

- Intruder v_6 prepares RREP packets for these RREQs with destination sequence numbers higher than the current destination sequence number for nodes v_{13} and v_7.
- v_6 sends these false RREPs back to the source nodes v_9 and v_4 as shown in Figure 9.

After receiving the false RREPs, source nodes v_9 and v_4 will select the route through v_6, since the received RREPs suggest that v_6 has the freshest routes. By repeating this process, intruder v_6 can successfully capture other routes in the network and force most of the network traffic flow through itself. Now the intruder v_6 is in control of the network data traffic and can drop data packets to cause either black hole or grey hole attacks. For instance, source nodes v_9 and v_4 will send data packets to their destination node which will reach node v_6; instead of forwarding these data packets, v_6 can drop them all, causing a black hole attack as shown in Figure 10.

3) Grey Hole Illustration : Figure 11 shows an example of a grey hole attack, where intruder v_6 decides to drop packets for v_{13} and forward all other packets as shown.

4) Rushing Attack Illustration: In a rushing attack the intruder exploits the property of an on-demand routing protocol, according to which nodes are only allowed to forward the first RREQ that arrives for each route discovery and are required to discard RREQs later received for the same route. An intruder will "rush" (i.e. transmit early) the RREQ to suppress any later legitimate RREQs. We again consider the network in Figure 7 as an example. Suppose that node v_9 broadcasts a RREQ for node v_{13} and node v_{12} knows the freshest route to v_{13}. Now, on hearing the RREQ, intruder v_6 rushes the RREQ to suppress the later legitimate RREQ in the following way.

- Intruder v_6 ignores the request forwarding delay (this is

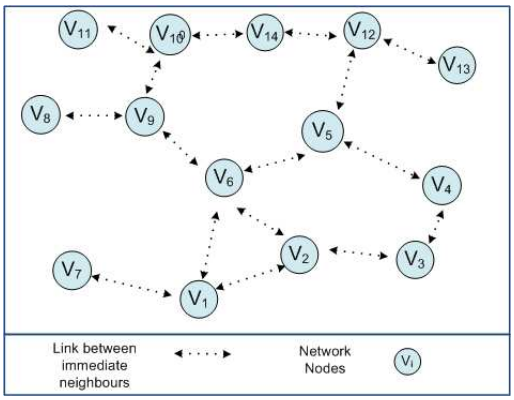


Fig. 7. Snapshot of the network without any attack

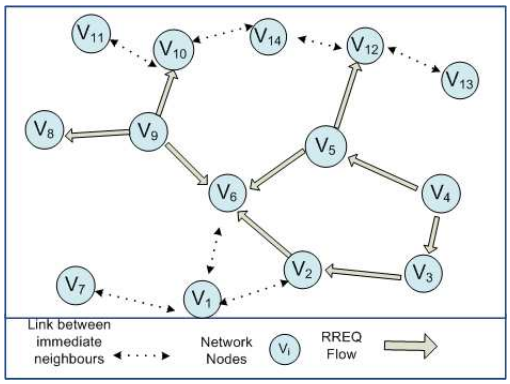


Fig. 8. Snapshot of the network: after route discovery from node v_9 & v_4

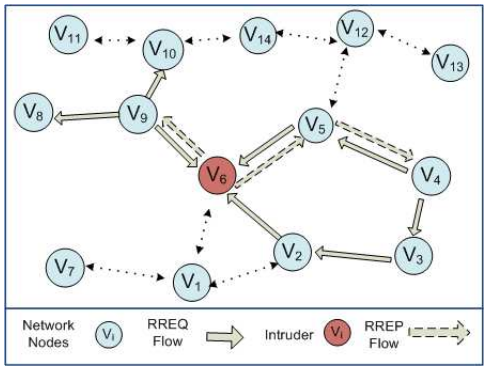


Fig. 9. Snapshot of the network: intruder sending false RREP to source node v_9 & v_4

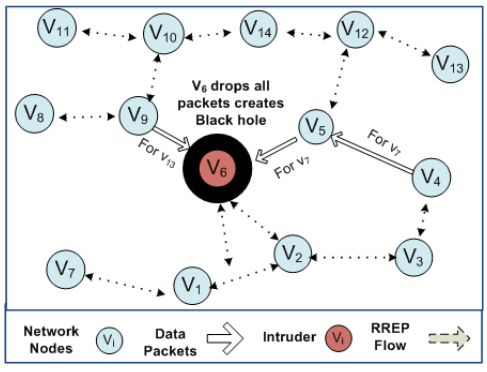


Fig. 10. Snapshot of the network: intruder v_6 drops all data packets to create a black hole

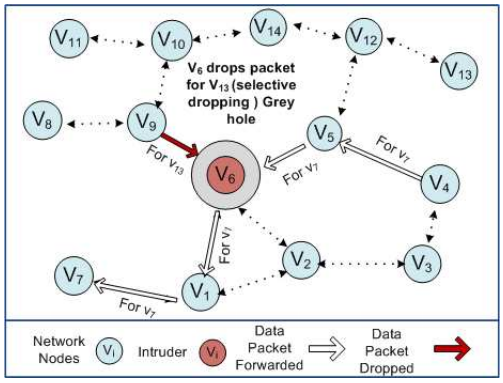


Fig. 11. Snapshot of the network: intruder v_6 drops packets selectively to create a grey hole

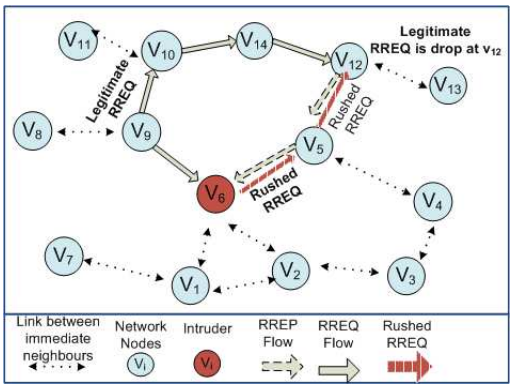


Fig. 12. Snapshot of the network with rushing attack

a randomized delay used by the routing protocol to avoid collision of broadcast packets).

- Intruder v_6 rushes (i.e. transmits without delay) the RREQ with a higher source sequence number.

This rushed RREQ from intruder v_6 arrives first at node v_{12}, and therefore node v_{12} will discard the legitimate RREQ from v_9 when it arrives later via v_{10} and v_{14}, as shown in Figure 12. This will not only suppress the legitimate route discovery but will also increase the probability that routes that include the intruder will be discovered rather than other valid routes. This then allows the intruder to perform its attack on other routes.

III. Point Detection Algorithms

In Section II we classified and illustrated major network layer attacks. In this Section, the focus moves to the review of algorithms and mechanisms that have been proposed in the literature to protect from these attacks. We categorise all the intrusion detection mechanisms reviewed in this paper according to the taxonomy of network layer protection mechanisms given in Figure 13. We initially divide the mechanisms according to the number of attack types they can identify. We define point detection algorithms as those that can detect a single category of network layer attacks, and general intrusion detection systems (IDSs) as those that can detect a range of attack types. Within the point detection algorithms we classify them according to the type of attack that they protect: these

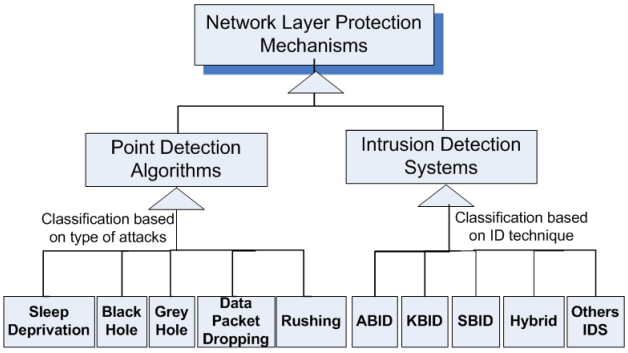


Fig. 13. Taxonomy of network layer protection mechanisms

algorithms are reviewed in the remainder of this Section. Intrusion detection systems will be reviewed in Section IV.

A. Protecting Against Data Packet Dropping

Significant research has been conducted in studying and protecting against data packet dropping attacks. For example in [28], the authors propose a protection scheme against a data packet dropping attack based on the cooperative participation of nodes. This scheme requires every node in the network to monitor the behaviour of its neighbours; when it detects packet dropping it invokes a distributed approach to investigate the attack. After detecting a node that is dropping packets the scheme then uses a trust collector function to gather trust values from the neighbours of the suspicious node. If a majority of the nodes has a low trust value for the suspicious node, they then inform all the nodes about the attacker by raising a global alarm. The authors compare the performance of this scheme against the watchdog algorithm proposed in [29] and show an improvement in terms of low false alarm rates.

Some other approaches based on Neighbour Watch System (NWS) have been proposed to detect malicious nodes that drop packets [30][31]. Packet forwarding misbehaviour detection based on the principle of flow conservation is proposed in [32] and [33], where nodes continuously monitor their neighbours, maintain the list of nodes they hear and check the behaviour of the nodes periodically. Misbehaving nodes are detected by comparing the estimated percentage of packets dropped with a pre-established misbehaviour threshold. An adaptive policy-based version of this algorithm was proposed in [34]. Adaptation is achieved in two ways. First the authors propose a method for the calculation of a misbehaviour detection threshold. Second, the adaptability of the protection mechanism is achieved using policies that consider changing network conditions and the management objectives. In SCAN [35], the authors proposed a self organized network layer protocol for secure packet delivery in MANETs. They assume that nodes can overhear packets received by their neighbour and have a copy of the neighbour's routing table. So, when a neighbour receives a packet it finds the next hop through its routing table. It considers the packet as dropped if the monitoring node does not overhear the packet being forwarded from the neighbouring node. To mitigate the effect of packet dropping in MANETs, Marti et al. [29] proposed a mechanism consisting of two parts: watchdog and pathrater. Watchdog uses promiscuous listing to identify the nodes that drop packets and pathrater maintains the path of every node and decreases its rating when it learns its packet dropping behaviour from watchdog. To mitigate the effect of packet dropping, pathrater selects the path based on the nodes' rating.

B. Protecting Against Sleep Deprivation Attacks

We now review protection mechanisms against a SD attack. Yi et al. [27] considered a route request (RREQ) flooding attack in MANETs. They proposed a RREQ flooding prevention mechanism based on neighbour's supervision that maintains a priority queue of the incoming RREQs. This mechanism reduces the priority of RREQs generated by a specific node if a higher rate of incoming queries from that particular node is observed. However, as we noted in Section II, in some applications of MANETs there can be specific nodes that generate more traffic than average; for example, in on-the-fly networks during a seminar, and yet the method of Yi et al. will in all cases remove requests above a certain incoming request rate. In [36] the authors proposed an analytical model which detects flooding attacks in MANETs using flow based detection features. In [37] the authors described three ways by which an attacker can drain the batteries of wireless devices, such as PDAs and notepads, in a mobile computing environment, for example through repeated requests for services or by forcing nodes to do energy hungry tasks. To analyze the impact of this attack they experimented with an IBM Thinkpad T23 notepad, a Compaq iPAQ 37600 PDA and a Compaq Itsy. Their results showed that the average power consumption of the IBM Thinkpad and Compaq iPAQ increased by approximately 15% and 30% respectively under sleep deprivation attack. Then they proposed a power secure architecture with the aim of defending against these attacks by guaranteeing a minimum battery life even when the device is under attack. The architecture employs two features: energy signature monitoring and multilayer authentication. The authors of [38] considered a sleep deprivation attack through injecting packets and proposed a lightweight inter-layer protocol to detect this in MANETs. Similarly, Yu and Ray [39] described sleep deprivation attacks that used two types of traffic injection attack in ad hoc networks, namely query flooding and data packet injection. They investigated these two attacks from the attacker's point of view and theoretically analyzed the probability of cases where the attacker can successfully launch these attacks without being detected. Then, assuming nodes that can authenticate each other through a public key mechanism, they proposed a query flooding attack detection mechanism using neighbour monitoring. On receiving a route request each node checks conditions, such as the legality of the source and the destination, request id, the time the request was received previously, and whether any node in the route is already marked as a bad node. However, the authors did not identify the cases where the intruder bypasses these checks by using the malicious RREQ flooding 1 and 2 mechanisms illustrated in section II.A.

C. Protecting Against Black Hole Attacks

To guard MANETs against black hole attacks several mechanisms have been proposed using different strategies. In [16] Tseng et al. surveyed existing solutions for detecting black hole attacks and classified these proposals as identifying either single (i.e. a single attacker launches the attack in the network) or cooperative black hole attacks (i.e. two or more nodes collaborate to launch the attack). TOGBAD [40] is an example of a black hole detection mechanism. It detects the attack using a topology graph, looking at the number of neighbours a node claims to have and the actual number of neighbours according to the graph. TOGBAD was developed for the OLSR proactive routing protocol, where topology information can be obtained; however it would not be effective for reactive routing protocols, where acquiring complete topology information is not operationally feasible. In [41] the authors proposed a black hole detection method for AODV in which, on receiving a reply, the receiver node initiates a judgement process about the replier. Neighbours share their opinion about the replier. A decision is made based on number (a fixed threshold) such that if a node receives many packets but does not send a certain number of packets then it is considered to be malicious. In our opinion, considering the dynamic environment of MANETs, such mechanisms based on fixed thresholds to detect black hole attacks suffer from high false alarm rates since they have no means to adapt to changes caused by node mobility. In [42] Zhang et al. proposed a black hole detection scheme based on sequence number checking of the RREP packets. They considered a scenario where an intermediate node is an attacker and suggested that, whenever a node sends a RREP back to a source node, the intermediate node should also generate a request for a sequence number to the destination node. The destination node responds by sending a packet containing its sequence number to the source node. The source node then checks the freshness of the route by comparing the sequence number of the RREP received from the intermediate node (suspect) with the sequence number reply packet from the destination node; it consequently detects an attack if the comparison fails. However, the introduction of two new packets with every reply not only increases the routing overhead but also the nodes have to ensure that the attacker does not drop or modify these sequence request and sequence reply messages.

D. Protecting Against Grey Hole Attacks

Xiaopeng and Wei [43] proposed a grey hole detection scheme for the DSR routing protocol. This requires each node to produce evidence on forwarding packets using an aggregated signature algorithm. Then a checkup algorithm detects whether packets have been dropped or not; finally, a source node uses a diagnostic algorithm to trace the malicious node. They slightly modified their proposal in [44], using a Distributed Certificate Authority (DCA) to update key management information, facilitating the detection process that uses the aggregate signature algorithm. Another mechanism for grey hole detection in AODV was proposed in [24], which requires all nodes to maintain their neighbours' data forwarding information. After a certain time, each node checks any neighbour with whom it has not communicated recently, and initiates the detection procedure for that node. The initiator performs a local detection by checking the number of RTS (request to send) and CTS (clear to send) messages; if this node is found to be suspicious then it asks other neighbours of the suspected node to check and finally it makes a decision about the suspected node.

E. Protecting Against Rushing Attacks

In [25], Hu et al. analyzed how an attacker can launch a rushing attack (RU) in DSR and proposed a rushing attack prevention mechanism for MANETs. They described ways an intruder can use it to launch the attacks; for example an attacker can rush a RREQ by using a higher than normal radio range using a higher power level or a higher gain antenna to suppress later legitimate RREQs. They assumed negligible MAC protocol delays. They proposed a secure neighbour detection mechanism through a mutual authentication protocol that uses tight delay timing to ensure that other node is within the communication range. To integrate their rushing prevention with the routing protocol they ensure that before sending or forwarding a RREQ a node first performs a secure neighbour detection exchange with the previous hop node. In [46] the authors proposed a Secure Message Transmission (SMT) protocol that ensures a secure end-to-end data forwarding protocol. They suggested that SMT can be used mainly for protecting the data forwarding operation, while route discovery procedures that are vulnerable to routing attacks such as rushing attacks can be secured using the Secure Routing Protocol (SRP) [47], an Internet Draft earlier proposed by the same authors in an attempt to mitigate the effects of misbehaving nodes in routing operations. However, they did not evaluate the effectiveness of SRP against routing attacks. In [48] Rawat et al. examined the possibility of a rushing attack on SRP and concluded that SRP can withstand the attacks.

F. Protecting Against Sybil Attacks

The use of trusted certificates through a certificate authority is by far the most commonly cited solution for sybil attacks. Douceur claimed [49] that using trusted certificates is the only way of completely eliminating sybil attacks from MANETs. Piro et al. showed in [26] that mobility could be used to identify sybil identities in MANETs. They proposed that a single node could detect a sybil attack by keeping track of the identity (i.e. the IP or MAC address) of nodes it hears transmitting. Groups of nodes that are heard together could be identified as possible attackers. They also suggested that multiple trusted nodes could share their observations to increase the accuracy of detection. In [50] Monica et al. claimed that radio resource tests of devices would allow the detection of sybil identities in the network. They assessed the power and performance of different radio resource tests including simultaneous sender test, optimized simultaneous sender test, simultaneous receiver test and forced collision test.

G. Comparison

We now compare the point detection algorithms described above. We first analyze them based on parameters such as the detection technique, addressed attack type, routing protocol used, response to attack and architecture. Table 1 provides a summary of the main point detection algorithms, where sufficient details are given in the original paper. The architecture of most of the proposed algorithms is either distributed or hierarchical, reflecting the distributed nature of the MANET itself. A hierarchical approach is used by the authors of these algorithms to provide some level of scalability, where information has to be gathered from across the network in order to detect the specific attack, and where the aim is not to impose a significant processing overhead on a single node in the network. The hierarchical architectures organize nodes in tiers and assign different roles to each tier level. Clustering techniques are extensively used to organize nodes in MANETs in a hierarchy. The hierarchical approach generally has a lower overhead compared to the flat distributed approaches because nodes communicate with a smaller set of nodes (such as cluster heads) than in the fully distributed case. We also note from the "Source of Data" column in Table 1 that monitoring of transmissions to or from neighbouring nodes is a particularly popular mechanism for data gathering (this is also known by some authors as promiscuous monitoring); in this case some node X is within range of another node Y and overhears the communications to and from Y even if those communications do not directly involve X. The principal alternative, direct reporting, is where data is collected directly from the nodes themselves. In this case, nodes transmit observed data to other nodes using special packets. The advantage of monitoring by neighbours is that it provides an independent source of data for the algorithms (unless two neighbouring nodes are colluding in an attack); whereas data reported directly from nodes may be susceptible to compromise. On the other hand, the nature of wireless transmissions means that some transmissions may not be overheard, even for two nodes that are in close proximity, and algorithms that use neighbour monitoring therefore have to deal with a degree of uncertainty in the data they are using. We also note that most of the mechanisms use detection techniques that are so specific that they require a particular routing protocol to identify a particular attack. For example, [27] uses priority queues of incoming RREQs to deal with malicious RREQ flooding for AODV. Clearly, this reduces the general applicability of these algorithms. Some of the point detection algorithms attempt to respond to a detected attack, usually by isolating the intruding node so that its traffic and data are removed from the network and the network traffic is routed around the intruder (see "Response of Attack" column). In other cases the response to intrusion is not considered by the authors. A general comment about all the point detection algorithms in Section III is the observation that since one algorithm can only detect one class of attack it means that: (a) a large number of algorithms would need to be implemented in a MANET to provide a wide range of intrusion coverage; (b) interactions between different point detection algorithms would need to be considered in building a robust intrusion detection environment that can cope with many different attack types [10]; (c) a wide range of differing algorithms will impose a significant overhead on the MANET in terms of network traffic, processing overhead and administration; and (d) discovery of further classes of attacks will require further research on specific algorithms. We are not aware of any research that has been conducted on the interactions between the various algorithms. In addition, it seems sensible for the network to have a consistent defined response to intrusion, and as we have commented above, the attack response is not considered by all the algorithms. Although it could be argued that some of the algorithms discussed in this Section have been optimised to detect their named attacks with high efficiency (or to identify the attacks quickly, or for the algorithms themselves to be robust against attacks or collusion between multiple nodes, etc.), all these points suggest that a more general intrusion detection system may provide a better solution to the protection of MANETs.

IV. INTRUSION DETECTION SYSTEMS

In this Section we consider IDSs that can identify a range of attacks. We first introduce the concepts and background knowledge of intrusion detection systems (IDSs). Secondly, we describe challenges faced by MANET intrusion detection systems, and finally, we review MANET intrusion detection system proposals, including intrusion response systems.

A. Intrusion Detection Techniques

Intrusion Detection Systems can be split into three main classes based on the detection approach employed: (1) anomaly-based intrusion detection (ABID), also known as behaviour-based intrusion detection; (2) misuse detection, also known as knowledge-based intrusion detection (KBID); and (3) specification-based intrusion detection (SBID), which has been proposed recently. Figure 13 gives our taxonomy of network layer protection mechanisms. For the division that covers mechanisms that can deal with a range of different attacks (i.e. intrusion detection systems), we classify them according to the intrusion detection technique they use: either ABID, KBID, SBID, or a hybrid of these, or some other mechanism. Before we review the systems that have been proposed in the literature, we start by reviewing the three main intrusion detection techniques.

1) Anomaly-Based Intrusion Detection : Anomaly-based intrusion detection (ABID) systems flag as anomalous observed activities that deviate significantly from the normal profile. ABID systems are also known as behaviour-based intrusion detection, in which the model of normal behaviour of the network is extracted, and then this model is compared with the current behaviour of the network to detect intrusion in the network. A diagram illustrating the basic ABID process is shown in Figure 14. Anomaly detection systems typically consist of two phases of operation: training and testing.

Training is the process of modelling the normal or expected behaviour of the network or of the users. The model also acts as a profile of user or network behaviour. For any anomaly-based IDS to be effective, it must therefore have a consistent

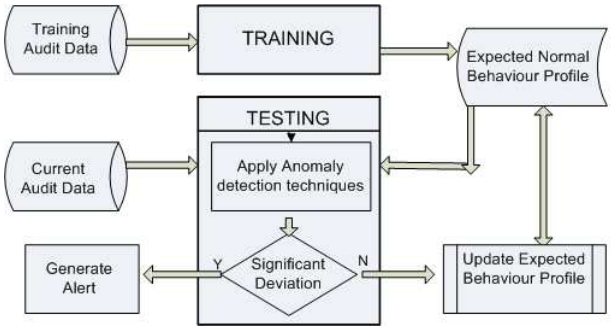


Fig. 14. Anomaly-based intrusion detection process

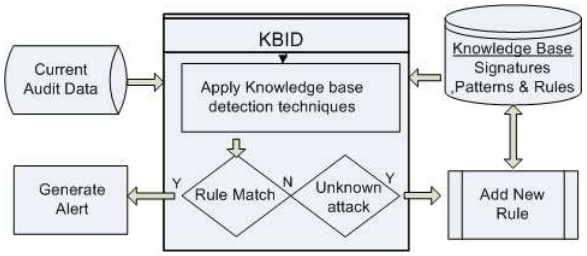


Fig. 15. Knowledge-based intrusion detection process

and stable profile that characterizes this behaviour. A profile consists of information about the list of parameters which are specifically geared to the target being monitored. Constructing an effective profile involves gathering information on behaviour and activity that is considered acceptable for the network.

Testing for intrusion involves comparing the normal or expected behaviour model derived during the training phase with the current model of the network or users. The detection techniques usually involve statistical or mathematical approaches to flag any significant deviation between two models. For anomaly detection techniques to be effective, they must have mechanisms that keep the false alarm rate low. ABID systems extensively use statistical methods [51] [52] to estimate the deviation between the expected and the current behaviour to detect an intrusion in the network. Statistical probabilistic techniques including the chi-square test, Hotelling's T2 test, decision trees and Markov chains are employed in ABID systems. Neural network algorithms [53] have also been used to learn and model the behaviour of the users in the network. The key advantage of ABID systems is that they can detect attempts to exploit new unforeseen vulnerabilities, because ABID looks for deviations from the normal expected behaviour. ABID systems can also provide early warnings of potential intrusions in the network. However, they are prone to generate false alarms.

2) Knowledge-Based Intrusion Detection: Knowledge-based intrusion detection systems maintain a knowledge base that contains signatures or patterns of well-known attacks and looks for these patterns in an attempt to detect them. In other words, KBID systems have knowledge about specific attacks and look for attempts to use them. A KBID system triggers an alarm when such an attempt is detected. A diagram illustrating the basic KBID process is shown in Figure 15. KBID relies on knowledge about attacks so anything not explicitly recognized as an attack based on existing knowledge is declared as non-intrusive or acceptable. However, the case of an event or a series of events that has degraded the network performance can be identified as an unknown attack because it does not match the existing rules of attacks, and the system can update the knowledge base by adding a new rule. KBID systems use various methods for constructing and modelling the knowledge for intrusion detection, some of which are described below.

Some KBID systems use expert systems [54][55] for intrusion detection. An expert system maintains the knowledge of known attacks in a knowledge base in the form of a set of rules. Captured audit data from a monitoring network are translated into facts and then an inference engine uses these facts and a set of rules in the knowledge base to detect an intrusion in the network.

State transition modelling can alternatively be used for intrusion detection where the attack is represented as a series of state transitions and defined attack states. The state transition models that represent attacks are normally maintained in a knowledge base and the state transition model is applied in real time to identify an intrusion in the network. Signature analysis is also used by KBIDs, where the attacks are modelled through a sequence of events or patterns, which are then compared with the generated audit trails to indicate intrusion. Some KBIDs have also applied rule-based approaches [56] to model the knowledge of known attacks in the form of a set of rules which is obtained through observation or by considering attack scenarios. The KBID checks the audit data by applying rules of known attacks, either using forward or backward chaining techniques in search of evidence of an attack. The main advantage of KBID systems is that they generally have very low false positive rates of detection (especially when compared to ABID) simply because they trigger alarms only when the exact match of a known attack signature, pattern, or sequence of events occurs. They are therefore best suited to scenarios where the network is highly vulnerable to certain known attacks. However, KBID systems have some drawbacks: in particular, they can only detect attacks whose signatures or patterns are in the knowledge base, and gathering the required information about attacks and keeping them up to date is a demanding task.

3) Specification-Based Intrusion Detection : Generally, specification-based intrusion detection systems (SBIDs) first explicitly define specifications as a set of constraints. They then use these specifications to monitor the routing protocol operations or network layer operations to detect attacks in the network. The basic process of SBID is shown in Figure 16. The first step extracts the specifications, which define the correct operation of (for example) the network or the MAC layer protocol through a set of constraints. The system then monitors the execution of the protocol with respect to the given specification, deviations from the specification being treated as intrusion [57]. Syntax- and semantic-based approaches have also been proposed for network based intrusion detection system in fixed networks [58].

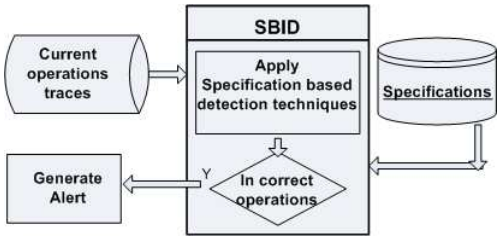


Fig. 16. Specification-based intrusion detection process

B. Challenges of Intrusion Detection Systems in MANETs

Intrusion detection systems developed for fixed networks are not directly implementable in the wireless network environment, and therefore research in the last few years has focused on securing MANETs with IDSs. Intrusion detection in MANETs is more complex and challenging than in fixed networks for reasons that we now discuss.

Unlike fixed networks, MANETs lack concentration points where monitoring and audit data collection can be performed. For example, in fixed networks, traffic is monitored at network gateways whereas in an infrastructureless MANET a node can only observe other nodes within its radio range; attackers outside this radio range can therefore escape easily. Consequently, the network-based IDS (NIDS) proposals used in fixed networks are not directly implementable in MANETs. Realizing this difficulty, researchers have proposed cooperative approaches of audit data collection and the application of intrusion detection techniques using network clustering [59][60][61][62].

Moreover, MANETs introduced a new set of routing protocols, which are significantly different from those used in fixed networks. These protocols require nodes to cooperate and act as routers; but it also means that the network's routing infrastructure is not under the control of a single management entity. This has created opportunities for attackers to identify vulnerabilities and find new ways to launch attacks, as explained in Section II.

Attacks in MANETs differ from those in fixed networks and therefore most detection methods used in fixed networks are not directly applicable; hence alterations to existing techniques and the introduction of new methods for intrusion detection have been considered by researchers.

Due to the nodes' mobility, the topology of the network is dynamic and unpredictable and this makes the entire process of intrusion detection complicated. First, it makes it difficult to capture and gather audit data; then, it is hard to accurately characterize the normal behaviour of the network; and, finally, the detection phase has to accommodate the dynamics of MANETs.

ID in MANETs is more demanding because some of the MANETs' characteristics such as the nodes' limited computational ability limit the effectiveness of host-based intrusion detection systems (HIDS), where the IDS is deployed in a distributed architecture on each host. Additionally, because the geographical territory of the network is not defined in MANETs, it is difficult to physically secure a node. The limited bandwidth of MANETs in contrast to wired networks additionally makes it challenging to transfer large amount of intrusion detection data and therefore MANET IDSs have to limit the volume of data transfer required for intrusion detection.

To sum up, every phase of intrusion detection in MANETs presents additional challenges as compared to fixed networks.

C. Proposed IDSs for MANETs

From the discussion of Section IV.B we can see the extra challenges and complexities that IDSs have to overcome in MANETs. To overcome these, researchers have, as with the point detection algorithms, tended to use either distributed (peer-to-peer) or hierarchical (clustered) architectures for IDS. Following our taxonomy of Figure 13, we now review MANET intrusion detection systems that have been proposed in the literature, classifying them under the headings of ABID, KBID, SBID, Hybrid IDS or other proposals.

1) Anomaly-Based Intrusion Detection Proposals: Anomaly detection approaches appear to hold more promise than knowledge-based approaches, since they utilize learning techniques to enable adaptation to the ever-changing MANET environment. This is important for MANETs where the overall behaviour of the network changes with time because of nodes periodically entering or leaving the network. In addition, anomaly-based detection is simpler in operation because it needs to first establish a normal expected behaviour and then compare it with the current behaviour to detect intrusion, as explained in Section IV.A. Researchers have proposed anomaly-based detection techniques based on different training and testing approaches. Some of these approaches are discussed below.

In [63] Cretu et al. proposed an anomaly detection approach for MANETs in which they model device behaviour, which peers can then use to determine the trustworthiness of other nodes. They examine their approach through an anomalous payload detector: the training phase observes payloads and then aggregates them from different nodes to build profiles which are compared by forming a similarity matrix. However, exchanging models among all nodes in a MANET could produce a significant processing and communication overhead, and devices in the networks can have different behaviour depending on the application of the MANET. In [64], Liu et al. proposed a game theoretic framework for intrusion detection in MANETs. They model the intruder and the defender as a two player Bayesian game. They propose Bayesian hybrid detection approaches which monitor the network in two different ways, namely in lightweight and heavyweight monitoring systems. The lightweight monitoring system consumes less energy and thus it is always on, whereas the heavyweight monitoring system uses ABID to build a normal profile and compare it against the tested data in order to detect intrusion.

Markov chain classifiers are also used in anomaly detection. For example, Jiang and Wang [65] proposed an anomaly detection algorithm based on Markov chains for wireless ad hoc networks. The algorithm consists of two parts: the construction of a Markov chain table and the construction of a classifier using a Markov model. The audit data traces are

first converted into sequences of symbols and a Markov chain table with state transitions is constructed. The second part consists of constructing a classifier using the Markov chain model that checks whether the current transition follows the Markov property by using a uniform distribution to calculate trace values and set the threshold to detect anomalies. Markov chain classifiers have also been used in fixed networks by Jha et al. [66], who used a sequence of system calls corresponding to each process as the traces of system activity. These traces of different sets of events were recorded in a Linux environment, and test suites and classifiers were constructed to detect anomalies. In [67] Sun et al. modified the Markov chain classifier for detecting routing disruption attacks of falsified RREPs in AODV MANETs. Similarly, in [68], the authors proposed using a Markov chain model and Hotelling's T2 test approach to detect local intrusion in MANETs. They argue that the nodes' mean speed does not accurately reflect the MANET's dynamics, and so it is not an efficient parameter to adjust the impact of mobility on IDS. They proposed instead that each local IDS agent periodically use link rate change to accommodate the effect of mobility.

Statistical probabilistic techniques are extensively used for anomaly detection. For example, research using probabilistic techniques for anomaly detection was conducted by Ye et al. [51]. They conducted a comprehensive investigation of the frequency and ordering property of audit data by applying probabilistic techniques including Hotelling's T2 test, the chi square multivariate test, a Markov chain approach and decision trees as a pattern recognition technique for detecting intrusion into the information system in fixed networks. To test the performance of these techniques they gathered one sample of both normal and intrusive activities by monitoring and collecting computer audit data from a Sun SPARC workstation running the Solaris operating system, which has a Basic Security Module (BSM) to record audit events. The second sample of normal and intrusive activities was taken from MIT Lab, which was produced by a US Air Force project. After testing, they concluded that anomaly detection through a chi square test based on frequency property provides good intrusion detection performance, and a Markov model based on the ordering property can provide additional advantages for detecting intrusion in an information system. After [51], Ye and Chen proposed an anomaly detection scheme in [52], based on only the chi-square test for detecting intrusion into information systems in fixed networks. In this paper, they used the same sample MIT audit data of normal events that they used in [51], and split that sample into two groups, one to be used for training a normal profile and the other to be used for testing. They considered some intrusion scenarios, built audit data of intrusive events and applied the chi square test. They observed a promising performance for intrusion detection in terms of high detection and low false alarm rate. We consider that their proposal could be applied with modifications in MANETs for detecting denial of service attacks. In [22] we proposed an anomaly-based intrusion detection protocol (AIDP), which uses a combination of the chi square goodness of fit test and control charts to detect, identify and isolate an intruder causing a sleep deprivation attack.

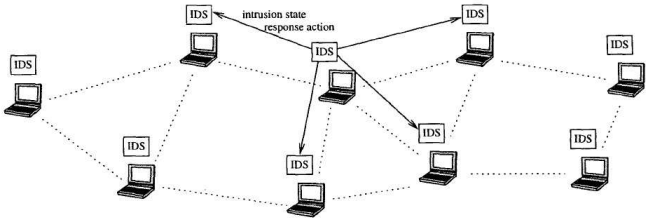


Fig. 17. The IDS peer-to-peer architecture for MANETs [69]

Zhang and Lee [69] proposed an intrusion detection system architecture in which an IDS agent runs on each mobile node, as shown in Figure 17. The agent collects local data by gathering real-time audit data from various sources and performs local detection through an engine: this analyses the local data traces from the data collection module for anomalies and uses anomaly detection to detect abnormal updates to the routing table. A cooperative detection and global response is then triggered when an intrusion is reported by a node. In [70], Zhang et al. extended and implemented the IDS architecture proposed in [69] in a simulation study. Kurosawa and Jamalipour [23] also proposed a black hole detection mechanism, this time for AODV, where three feature vectors are used to model normal states of the network and an ABID discrimination module is used to identify the black hole attack.

Albers et al. in [71] proposed a Local Intrusion Detection System architecture (LIDS) which uses a MIB (Management Information Base) agent, a SNMP (Simple Network Management Protocol) agent and a local intrusion detection agent that work together to detect intrusion.

Sterne et al. in [59] proposed a cooperative IDS architecture which is organized as a dynamic hierarchy, as shown in Figure 18, where the nodes annotated with 1 and 2 represent first and second level cluster nodes respectively. In this hierarchical architecture, data is acquired at leaf nodes through either promiscuous monitoring or direct reporting. After the data is acquired, it is then analysed as it flows upwards towards cluster head nodes. The cluster head applies ABID techniques in a detection module to detect nodes that intentionally drop a significant amount of data packets. The authors claimed that routing attacks such as the modification of RREQ packets can be detected, but this was not demonstrated in the paper because the main purpose was to propose an architecture that can meet the challenges of IDSs.

In [72], Kachirski and Guha proposed distributed intrusion detection based on mobile agent technology for wireless ad hoc networks. This IDS uses a mobile agent framework, where three types of agent (monitoring agent, action agent and decision making agent) run on network nodes as shown in Figure 19. They used a distributed algorithm that selects nodes in the network which will run the monitoring agent to observe and analyze network packets and the decision making agents to make decisions on network level intrusion. In addition, host monitoring and action agents are implemented on all the nodes in the network for monitoring system and application level activities on each host and for taking action to respond

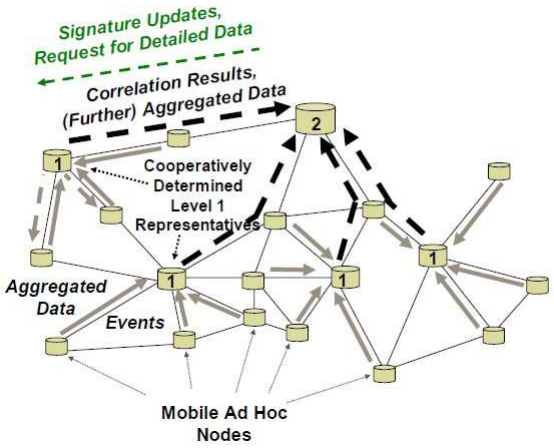


Fig. 18. The IDS dynamic hierarchical architecture for MANETs [59]

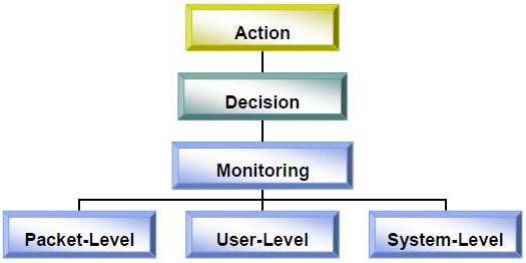


Fig. 19. Layered mobile agent architecture for a distributed IDS[72]

to intrusion on a host respectively. The paper focused on presenting the distributed mobile agent architecture from an implementation perspective. However, it also considered intrusion (attack) scenarios to validate the proposed mechanism's effectiveness under various network layer attacks.

Neural network algorithms [73] have also been used for intrusion detection. In [74] the authors proposed an intrusion detection engine for MANETs that used a neural network and watermarking techniques. They use self-organizing maps in conjunction with machine learning and watermarking techniques [75] to design an intrusion detection engine. The architecture of the proposed mechanism is shown in Figure 20: it first extracts MAC layer features, then it performs data collection and intrusion detection using an engine, and finally it applies the appropriate intrusion response. Each node creates a map that represents its security status, and distributes it to neighbouring nodes. Once a node has received all maps from its neighbours it then generates a global map which helps the node to estimate how secure the MANET is and how to perform routing securely and efficiently by avoiding the paths that include nodes which are comprised or under attack from the intruders. Watermarking is used to maintain the integrity and authenticity of these self-organized maps. The authors claim this method can detect various types of attacks but did not specify the attack scenarios against which it had been tested. Similarly, in [76], the authors proposed an ABID system that used neural networks to detect DoS attacks in MANETs. In another example, Huang and Lee [60] proposed

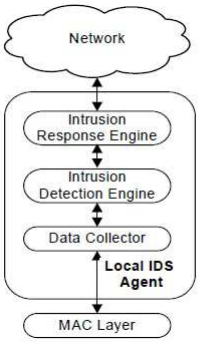


Fig. 20. Intrusion detection architecture [74]

a cooperative intrusion detection system for ad hoc networks. They developed a clustered IDS using a cluster formation protocol that ensures only each cluster leader performs ID. They proposed a cluster head assisted anomaly detection cross feature analysis to detect various attacks.

2) Knowledge-Based Intrusion Detection Proposals: Knowledge-based approaches have an advantage of very low false alarm rates as compared to ABID systems because they maintain a knowledge base containing signatures or patterns of attacks and only look for these specific attacks. As mentioned in Section IV.A, KBID systems use different techniques to model the knowledge about attacks. KBID systems can use state transition modelling; for example, STAT ("state transition analysis") [77] maintains the knowledge attacks in fixed networks as a sequence of states. This approach models intrusion using a state transition diagram as a series of state changes from an initial secure state to a final compromised state. In [78], the authors used the concepts of STAT [77] to design an intrusion detection tool, AODVSTAT, to detect packet dropping and spoofing attacks in MANETs. Signatures are represented by using an event model and the events are either data or AODV routing packet exchanges in the network. They assume that each node is equipped with an AODVSTAT sensor. This sensor performs a state analysis of the packet stream that the node has observed either by monitoring its neighbour or through updates from its neighbour's observations to detect signs of attacks. In [79] the authors focused on services to propose a detection framework for MANETs that identifies nodes that are not authorized for specific services.

A study to analyse the effectiveness in ad hoc networks of KBID using signature detection of known attacks was conducted in [80]. The authors assumed they knew the attack signature and that the node could execute an intrusion detection process to detect an attack on the ad hoc routing protocol. They considered a very simple scenario with an intruder node as part of the initial path between source and destination, and estimated the probability of detecting this intruder with and without node mobility. They concluded that a MANET using a reactive routing protocol is less effective at detecting an attack than one with proactive routing. In [81] the authors proposed a peer-to-peer KBID IDS architecture, a distributed intrusion detection architecture based on a static database. The architecture has two parts. First, an IDS mobile

agent resides on each node in the network, and is responsible for detecting local intrusions based on local audit data and participating in cooperative algorithms with other IDS agents to make decisions about potential intrusions. The second part is a secure stationary database that contains known misuse attack signatures. However, the assumption made in this paper is that the stationary database is accessible to all the nodes, which in a decentralized MANET architecture is difficult to achieve.

3) Specification-Based Intrusion Detection Proposals: The SBID approach was introduced and tested in fixed networks in [57] [82] [83]. In MANETs, SBIDs describe the correct operation of the protocol by defining a set of constraints, and monitor the execution of the protocol with respect to the defined constraints to detect anomalies in the network. For example, in [45] the authors proposed a SBID system for the AODV routing protocol. They use a finite state machine to define the correct operation of AODV in terms of the RREQ-RREP flow, including a suspicious state. Monitoring nodes are selected to monitor the RREQ-RREP flow according to the defined specification. They indicate an anomaly if the suspicious state is reached. Tseng et al. [86] proposed a SBID approach for the optimized link state routing (OLSR) protocol. They proposed a finite state automata model that defines a correct operation of the OLSR node by defining a set of constraints, for example how the OLSR node handles control traffic. Then nodes (using a distributed architecture) monitor a neighbour's behaviour according to the defined specifications. The nodes detect intrusion by comparing the neighbour's behaviour with defined specifications. Similarly, in [84] an extended finite state machine (EFSM) was used in a SBID system for OLSR-based networks. The authors manually derived the set of constraints from the IETF's specification for OLSR [85] in the form of message sent and received traces. The EFSM compares a network's traces with the specification, using backward tracking to identify intrusion. In [87], the authors proposed a specification synthesis to model and analyze MANET routing protocols. They focused on the flow of traffic to extract specifications in the form of directed graphs where nodes represent the protocol configuration and edges show how the protocol evolves from one configuration to another. They use this specification to detect run time anomalous behaviour, and have constructed and validated specifications for DSR and AODV through a simulation-based case study.

4) Hybrid Intrusion Detection Proposals: In some proposals the authors have used a combination of ABID and KBID techniques; we refer to these as hybrid approaches. In [88], CRADS, a cross layer approach, was proposed that uses a non linear detector based on a support vector machine (SVM) [89] to detect packet dropping, spoofing, modification and rushing attacks on the proactive routing protocol OLSR. As shown in Figure 21, CRADS consists of three modules: a) data collection, which collects data from the network, MAC and physical layers, b) data reduction, which reduces the number of features and events in the training data set, and c) a learning module, which uses the SVM classification model to differentiate between benign and malicious events.

In an extension of the original ABID system, AIDP [22],

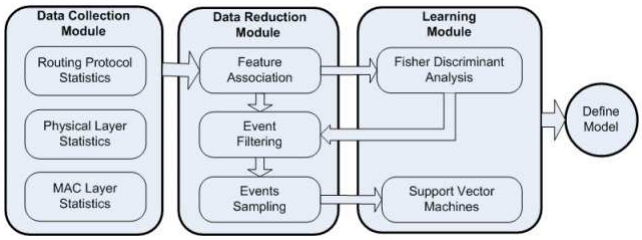


Fig. 21. CRADS architecture [88]

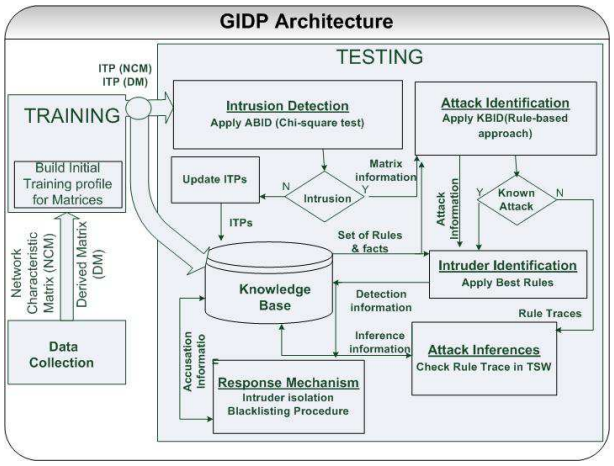


Fig. 22. GIDP architecture [90]

a generalized intrusion detection and prevention mechanism (GIDP) was proposed in [90]. GIDP uses a combination of both anomaly- and knowledge-based intrusion detection techniques to protect a MANET from a wide variety of network layer attacks including simultaneous multiple attacks. Figure 22 shows the architecture of GIDP, which consists of three phases: 1) data collection, 2) training and 3) testing. In the first phase, the network layer characteristics and a performance matrix are collected from the network nodes, and in the second phase the training module uses this information to build training profiles. Finally, the testing module is invoked periodically to detect intrusion, identify any attack(s) and identify intruding nodes, and respond to a detected intrusion. The ABID module detects an intrusion, and the KBID module helps the system to identify the specific attack from its set of rules.

5) Other Intrusion Detection Proposals: In the literature there are examples of intrusion detection mechanisms that can detect a range of attack types but where the authors have not explicitly mentioned the type of ID techniques they used. In [91], Hijazi and Nasser studied and analysed the feasibility of mobile agents for MANET intrusion detection and concluded that many mobile agents' features satisfy the requirements for MANET IDS. They believe that mobile agents (autonomous executing programs) that execute without being affected by the originating node status have direct relevance to the challenges faced in MANETs, such as reducing network load, conserving bandwidth, and having robust and fault-tolerant behaviour. However, they also point out that mobile agents have inherited

security vulnerabilities, which is one of the reasons why they are still not used extensively for ID.

In [62] Yi et al. presented a clustered detection approach where periodically a single node is elected as the monitoring node; it then monitors the cluster and performs both local and global detection. They abstracted the correct behaviour of the nodes based on the DSR routing protocol specification and constructed a finite state machine (FSM). The monitor node checks every node's behaviour and indicates an attack if a certain node behaviour is not verified through the FSM. Some other researchers have proposed approaches that are more general than the point detection algorithms of Section III but which are not based on ABID, KBID or SBID. For example, ARAN [93] is a hop-by-hop authenticated routing mechanism that can protect MANETs against a number of attacks from external malicious nodes. The authors first define vulnerabilities in terms of the modification and fabrication of routing packets in the AODV and DSR routing protocols, and spoofing. They note that modifying or fabricating certain routing packets can cause denial of service, route redirection, tunnelling and routing loops. ARAN detects these attacks by introducing authentication, integrity and non-repudiation in a MANET by using a certification process. A similar approach, Ariadne [94], has been proposed for end-to-end authentication based on shared key pairs. Karyotis et al. [95] performed a vulnerability analysis of wireless ad hoc networks through a probabilistic model. They evaluated various strategies used by attackers to launch different attacks and used simulations to analyze the impact of an attack. In another example, SEAD was proposed in [96] as a secure routing protocol that uses a one-way hash function to provide authentication for the proactive routing protocol DSDV against attacks caused by modification of routing packets, advertising false routing packets, reply attacks and wormhole attacks.

6) Comparison : Table 2 provides a summary of some of the MANET IDS mechanisms surveyed in this section, where sufficient information is available in the original papers, using the same parameters as Table 1. We can see from Table 2 that the IDS mechanisms generally use either ABID, KBID or SBID techniques to identify intrusions, but hybrid techniques, for example GIDP [90] and CRADS [88], have been developed in some cases to deal with network layer attacks. In addition, we observe that there are mechanisms that deal with multiple attacks by implementing cryptographic techniques, such as ARAN and SEAD. We furthermore notice ("Intrusion Response" column) that most of the proposals do not consider the response to an attack. Yet, interestingly enough, we have shown in [97] that the careful selection of the intrusion response can optimise the network's operation: for example, for a minor intrusion, the impact of isolating the intruder may be worse than the impact of the intrusion itself.

As with the point detection algorithms of Section III and Table 1, the IDSs of Table 2 generally use either distributed or hierarchical architectures, and for the same reasons. The "Source of Data" column shows that in Table 2 a wider range of data sources is typically used compared to the point detection algorithms. Given the greater level of complexity of the analysis performed by the IDSs this is not surprising.

The "Routing Protocol" column in Table 2 shows that more IDS algorithms claim to have general applicability, independent of the MANET's routing protocol, as compared to the protocol-specific point detection algorithms in Table 1. For example [90][22][59][60][93] are general IDS mechanisms that happen to have been tested using AODV. Finally, we observe that ABID is the most popular technique for IDSs, presumably because of its general applicability and its ability to identify new unforeseen attacks. But, one drawback of ABID is its training phase: one needs to have confidence that there are no attacks taking place during the training period. We might however expect standard profiles to become available once MANETs become commonplace and the technology matures.

V. Conclusions And Future Work

The distributed nature of MANETs means that it is vital to protect them from modern sophisticated network layer attacks. In this paper we have presented a survey of significant network layer attacks, and we have reviewed intrusion detection mechanisms that have been proposed in the literature. We find that the protection mechanisms can be classified as either point detection algorithms or as IDSs that can deal with a wide range of attacks. In comparing the main proposals in Tables 1 and 2 we have highlighted a number of key similarities and differences between the various mechanisms.

However, history shows that intruders often find new ways to attack and cause damage to computer systems and networks. Therefore, we consider that enabling a protection mechanism to learn from experience and use the existing knowledge of attacks to infer and detect new intrusive activities (attacks) is an important and potentially fruitful area of future research. We also believe that the development and deployment of network security policies are vital in networks with a dynamic environment such as are found in MANETs; this is a further potential area of research. Finally, the attacker may try to attack an existing protection scheme; therefore the protection mechanisms need to be robust enough to protect themselves and not introduce new vulnerabilities into the system.

VI. Acknowledgement

The authors are grateful to the anonymous reviewers for providing valuable feedback. The work is partially funded by the Higher Education Commission, Pakistan.

References

[1] IETF Mobile Ad-Hoc Networks Working Group (MANET), IETF website www.ietf.org/dyn/wg/charter/manet-charter.html

[2] IETF Ad-Hoc Networks Autoconfigurations (autoconf) Working Group, IETF website http://datatracker.ietf.org/wg/autoconf/charter/

[3] IEEE Std 802.11-2007, IEEE standard for information technology-Telecommunication and information exchange between systems- Local and metropolitan area network-Specific requirement, Part 11 Wireless LAN medium access control and physical layer specifications, June 2007.

[4] J. Anderson "Computer Security, Threat monitoring and surveillance", Fort Washington PA, James P, Anderson & Co, 1980.

[5] Michael Sobirey, "Intrusion Detection Systems Bibliography", available at http://www.cse.sc.edu/research/isl/mirrorSobireys.shtml

TABLE I
COMPARISON OF POINT DETECTION ALGORITHMS

Author	Algorithm Name	Architecture	Attack Type Addressed	Detection technique	Response to Attack	Routing Protocol	Source of Data	Contribution
Sen et al. [28]	None	Distributed	Data packet dropping	Trust-based approach	Isolate attackers	Not specified	Promiscuous monitoring	Claims to show improvement over algorithm in [29]
Yang et al.[35]	SCAN	Distributed	Data packet dropping	Information cross validation	Isolate attackers	AODV	Collaborative monitoring	Provides secure packet delivery in MANETs
Gonzalez et al. [32] [33]	None	Hierarchical	Data packet dropping	Principle of flow conservation	Isolate attackers	AODV	Promiscuous monitoring	Application of flow conservation
Marti et al. [29]	None	Distributed	Data packet dropping	Watchdog and Pathrater	Isolate attackers	DSR	Promiscuous listing	Detects packet dropping behaviour using watchdog & pathrater
Yi et al. [27]	None	Distributed	Sleep deprivation by malicious RREQ flooding	Priority queue incoming RREQs	Isolate attackers	AODV	Promiscuous monitoring	Malicious RREQ flooding prevention mechanism
Yu & Ray [39]	None	Distributed	Sleep deprivation	Neighbours checks certain conditions	Not Considered	DSR	Neighbouring nodes' RREQs packets	Mechanism to protect against sleep deprivation through traffic injection
Hsu et al. [38]	LIP	Not specified	Sleep deprivation	Local broadcast authentication	Not considered	Not specified	Node's information	Lightweight interlayer protocol to prevent packet injection
Martin et al. [37]	None	Not Specified	Sleep deprivation	Multi level authentication & power signature	Not considered	Not considered	Service requests on SSH server through ipaq	Analyzes impact of SD attack on real system & proposes power secure architecture
Padillia et al.[40]	TOGBAD	Hierarchical centralized	Black hole	Comparing claimed number of neighbours with topology graph	Not considered	OLSR	Topology graph	Black hole detection for OLSR
Zhang et al. [42]	None	Distributed	Black hole	Checking RREP sequence numbers	Not specified	AODV, SAODV	Sequence no of RREPs from intermediate nodes	Black hole detection mechanism
Medadian et al. [41]	None	Distributed	Black hole	Finding safe route	Not considered	AODV	Neighbours supervision	Combats BH through neighbour supervision
Xiaopeng & Wei [43]	None	Distributed	Grey hole	Creating proof & check up algorithm	Not specified	DSR	Evidence from forwarded packets	Grey hole detection scheme for DSR
Sen et al. [24]	None	Hierarchical	Grey hole	Monitoring behaviour in terms of RREP	Isolate attackers	AODV	Neighbour data collection module	Grey hole detection for AODV
Hu et al. [25]	None	Distributed	Rushing attack	Mutual authentication protocol	Not specified	DSR	Transmitted RREQ packets radio range	Rushing attack prevention mechanism for MANETs
Douceur [49]	None	Centralized	Sybil	Using trusted certificate	Not considered	Not specified	Certificate managed by CA	Showed that without a logically centralized authority it is difficult to eliminate sybil identities.
Piro et al. [26]	PASID	Distributed	Sybil	Recording identities & mobility pattern	Not considered	AODV	Promiscuous monitoring	Showed that mobility can be used to identify sybil identities in MANETs.

TABLE II
COMPARISON OF IDS MECHANISMS

Author	Algorithm Name	Architecture	Attack Type Addressed	Intrusion Detection Technique	Intrusion Response	Routing Protocol	Source of Data	Contribution
Zhang & Lee [69]	None	Distributed peer-to-peer	Various network layer attacks	ABID	Not considered	AODV, DSR	System events	Agent-based IDS architecture
Albers et al. [71]	LIDS	Hierarchical clustered	Not specified	ABID	Isolate attackers	Not specified	SNMP data in MIB	Local IDS architecture based on mobile agent
Sterne et al. [59]	None	Hierarchical, Clustered	Data packet dropping	ABID	Not considered	General, but tested on AODV	Nodes reporting to clusters directly	Dynamic IDS hierarchical model for MANETs
Kachirski & Guha [72]	None	Distributed	Not specified	ABID	Not considered	Not specified	Mobile agent monitoring events	Distributed mobile agent architecture
Nadeem & Howarth [22]	AIDP	Hierarchical, clustered	DoS attacks	ABID	Isolate attackers	General, but tested on AODV	Routing information	ABID for detecting DoS attacks in MANETs
Kurosawa et al. [23]	None	Distributed	DoS, Black hole	ABID	Not considered	AODV	Feature vector	Anomaly-based detection using feature vector
Cretu et al. [63]	None	Distributed peer-to-peer	Anomalous behaviour of devices	ABID	Does not cooperate with attackers	Not Specified	Experimental testbed	Anomaly detection model exchange for MANETs
Huang & Lee [60]	None	Hierarchical, clustered	Multiple Attacks	ABID	Not specified	General, but tested on AODV	Features	Clustered IDS that can detect various attacks in MANETs
Liu et al. [64]	None	Distributed	DoS	ABID (Bayesian game theoretic)	Not considered	Not specified	Data from two type of monitoring systems	Model intrusion using Bayesian game theoretic framework
Sun et al. [67]	None	Distributed	Routing disruption attacks	ABID (Markov chain classifier)	Not considered	AODV	Audit data sources	Markov chain anomaly detection algorithm
Mitrokosta et al. [74]	None	Distributed collaborative	Various attacks	ABID (Neural Network)	Avoiding routes that include attackers	Not Specified	MAC layer features	IDS engine based on neural network & watermarking
Jabbehdari et al. [76]	None	Not specified	DoS attacks	ABID (Neural Network)	Not considered	Not Specified	Neural network elements maping	Uses neural network for MANET ABID
Smith [81]	None	Distributed	Not specified	KBID	Not considered	General	Audit data trails	KBID using mobile agents
Vgina et al. [78]	AODVSTAT	Distributed collaborative	Packet dropping, resource depletion	KBID	Not considered	AODV	Data & AODV routing packets	ID tool for packet dropping attack using STAT [77]
Nadeem & Howarth [90]	GIDP	Hierarchical, clustered	Various network layer attacks	Hybrid ID	Isolate attackers	General, but tested using AODV	Network characteristics & performance matrix	Generalized IDP mechanism with attacker isolation
Joseph et al. [88]	CRADS	Not specified	Packet drop, spoofing, rushing	Hybrid ID	Not considered	OLSR	MAC, Network Physical layer statistic	Cross layer approach using non linear detector
Tseng et al. [86]	None	Distributed	DoS attacks	SBID (FSM)	Not considered	OLSR	Specifications of OLSR	SBID for OLSR
Orset et al.[84]	None	Distributed	Fabrication, modification & Sybil	SBID (extended FSM)	Not considered	OLSR	OLSR IETF specifications [85]	SBID with extended FSM for OLSR
Tseng et al. [45]		Distributed	Not specified	SBID	Not considered	AODV	RREQ-RREP flow Specifications	FSM that defines specifications for AODV operations
Stakhanova et al.[87]	None	Not specified	Claim to deal with various behaviour	SBID	Not considered	AODV, DSR	Specification of network traffic flow	SBID mechanism for AODV and DSR
Hu et al.[96]	SEAD	Distributed	Multiple attacks	Other IDS	Not considered	General but tested on DSDV	Routing information	A secure routing protocol for DSDV
Sanzgiri et al.[93]	ARAN	Centralized	Multiple attacks	Other IDS	Not considered	General but tested on DSR AODV	Routing information	Certification process provides authentication, integrity & non repudiation
Yi et al. [62]	None	Hierarchical, clustered	DoS attacks, routing loop	Other IDS	Send alarm	DSR	DSR routing specifications	FSM to detect attacks in DSR without signature
Hijazi & Nasser [91]	None	Distributed	Not Specified	Mobile agent feasibility for ID	Not considered	Not Specified	Not Specified	Analyzes feasibility of using mobile agent for ID in MANETs

[6] H. Debar, M. Dacier and A.Wespi, “Towards a Taxonomy of Intrusion Detection Systems”, Computer Network Journal, special issue on Computer Network Security, Vol.31, No.8, pp 805-822, April 1999.

[7] H. Debar, M. Dacier and A.Wespi, “A Revised Taxonomy for Intrusion Detection Systems”, Annals of Telecommunications, Vol.55, No.7, pp 361-378, July 2000.

[8] G.A. Jacoby, R.Marchany and N.J. Davis, “Battery-based intrusion detection as first line of defense”, Proc. Annual IEEE Information Assurance Workshop, pp 272-279, 2004.

[9] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks," IEEE Wireless Communications Magazine, special issue on Security in Wireless Mobile Ad Hoc and Sensor Networks, Vol.14, No.5, pp. 56-63, Oct. 2007.

[10] G.S.Mamatha and S.C. Sharma, “Network Layer Attacks and Defence Mechanisms in MANETs - A Survey”, International Journal of Computer Applications, Vol.9, No.9, Nov. 2009.

[11] D. Kheyri and M. Karami, “A comprehensive survey of anomaly based intrusion detection systems in MANETs”, Journal of Computer and Information Science, Vol. 5, No. 4, pp. 132-139, 2012.

[12] S. Sahu and K. Shandilya, “A Comprehensive Survey on Intrusion Detection in MANET”, International Journal of Information Technology and Knowledge Management, Vol.2, No. 2, pp. 305-310, 2010.

[13] M.Ghonge, P.M.Jawandhiya and M.S.Ali, “Countermeasures of Network Layer Attacks in MANETs”, International Journal of Computer Applications, Special Issue on Network Security and Cryptography, NSC, 2011.

[14] N. Deb, M.Chakraborty and N. Chaki, “A state-of-the-art survey on IDS for mobile ad-hoc networks and wireless mesh networks”, Proceedings International Conference on Parallel, Distributed Computing Technologies and Applications, PDCTA 2011, pp. 169-179, 2011.

[15] S.Gangwar, “Mobile Ad Hoc Networks: A Comprehensive Study and Survey on Intrusion Detection”, International Journal of Engineering Research and Applications (IJERA), Vol.2, No.1, pp 607-612, 2012.

[16] F.Tseng, L. Chou and H.Chao, “A Survey of Black Hole Attacks in Wireless Mobile Ad Hoc Networks”, Journal on Human-Centric Computing and Information Sciences, Springer, Vol.1, No.4, pp. 1-16, 2011.

[17] T. He, H. Wang and K.W. Lee, “Traffic analysis in anonyms MANETs”, Proc. IEEE Military Communication Conference MILCOM, November 2008.

[18] J. Kong, X. Hong and M. Gerla, “A new set of passive routing attacks in Mobile ad hoc networks”, Proc. IEEE Military Communication Conference MILCOM, October 2003.

[19] E. Perkins and M. Royer, “Ad Hoc On Demand Distance Vector Routing”, Sun MicroSystem Laboratories Advance Development Group, Proceeding of the IEEE MOBICOM, pp 90-100, 1999.

[20] B. Johnson and A. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks”, Proc. Mobile Computing Journal, Vol.353, pp 153-181, 1996.

[21] M. Pirrete and R. Brooks, “The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defence”, International Journal of Distributed Sensor Networks, Vol.2, No.3, pp 267-287, 2006.

[22] A.Nadeem and M.Howarth, “Adaptive Intrusion Detection & Prevention of Denial of Service Attacks in MANETs”, Proc. ACM International Wireless Communication and Mobile Computing Conference (IWCMC 09), Leipzig Germany, June 2009.

[23] S. Kurosawa and A. Jamalipour, “Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning method”, International Journal of Network Security, Vol.5, No.3, pp 338-345, November 2007.

[24] J.Sen, M.Chandra, S.G. Harihara, H.Reddy and P.Balamuralidhar, “A Mechanism for Detection of Gray Hole Attacks in Mobile Ad Hoc Networks”, Proc. IEEE International Conference on Information Communication and Signal Processing ICICS, Singapore, Dec. 2007.

[25] Y.Hu, A. Perrig and B. Johnson, “Rushing Attack and Defence in Wireless Ad Hoc Networks Routing Protocol”, Proc. ACM Workshop on Wireless Security, pp. 30-40, 2003.

[26] C.Piro, C.Shields and B.Levine, “Detecting the Sybil Attack in Mobile Ad hoc Networks”, Proc. IEEE International Conference on Security and Privacy in Communication Networks, Aug-Sep. 2006.

[27] P.Yi, Z.Dai, Y. Zhong and S.Zhang, “Resisting Flooding Attack in Ad Hoc Networks”, Proc. IEEE International Conference on Information Technology Coding & Computing ITCC, April 2005.

[28] J. Sen, M. Chandra, P. Balamurlidhar, S.G. Harihara and H.Reddy, “A Distributed Protocol for Detection of Packet Dropping Attack in Mobile Ad hoc Networks”, Proc. IEEE Conference on Telecommunication and Malaysian International Conference on Communication (ICT-MICC), 2007

[29] S. Marti, T.J. Giuli, K.Lai and M. Baker, “Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks”, Proc. International Conference on Mobile Computing and Networking, pp 255- 265, 2000.

[30] S.B. Lee and Y.H. Choi, “A Resilient Packet Forwarding Scheme against Maliciously Packet Dropping Nodes in Sensor Networks”, Proc. ACM workshop on Security of Ad Hoc and Sensor Networks (SANS 2006),pp 59-70, USA, Oct. 2006.

[31] P. Papadimitratos and Z.Haas, “Secure Data Communication in Mobile Ad Hoc Networks”, IEEE Journal on Selected Areas in Communications, Vol.24, No.2, pp 343-356, Feb. 2006.

[32] O.F. Gonzalez-Duque, M. Howarth and G. Pavlou, “Detection of Packet Forwarding Misbehaviour in Mobile Ad hoc Networks”, Proc. International Conference on Wired/Wireless Internet Communications (WWIC 2007), pp 302-314, Portugal, June 2007.

[33] O.F. Gonzalez-Duque, G. Ansa, M. Howarth and G. Pavlou, “Detection and Accusation of Packet Forwarding Misbehaviour in Mobile Ad hoc Networks”, Journal of Internet Engineering, Vol.2, No.8, pp 181-192, June 2008.

[34] O.F. Gonzalez-Duque, A.M. Hadjiantonis, G. Pavlou and M. Howarth, “Adaptive Misbehaviour Detection and Isolation in Wireless Ad Hoc networks Using Policies”, Proc. IFIP/IEEE International Symposium on Integrated Network Management (IM 2009), pp 242- 250, NY, USA, June 2009.

[35] H. Yang, J. Shu, X. Meng, and S. Lu, “SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks,” IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp. 261-273, 2006.

[36] Y. Guo and S. Perreau, "Detect DDoS Flooding Attacks in Mobile Ad Hoc Networks," International Journal of Security and Networks, Vol. 5, No.4, pp. 259 - 269, 2010.

[37] T. Martin, M. Hsiao, H. Dong and J. Krishnaswami, “Denial-of-Service Attacks on Battery Powered Mobile Computers”, Proc. IEEE International Conference on Pervasive Computing and Communications (PerCom), March 2004.

[38] H. Hsu, S. Zhu, and A. R. Hurson, "LIP: a Lightweight Interlayer Protocol for Preventing Packet Injection Attacks in Mobile Ad Hoc Networks," International Journal of Security and Networks, Vol. 2, Nos. 3/4, pp. 202 - 215, 2007.

[39] W.Yu and K.Ray, “Defense Against Injecting Traffic Attack in Cooperative Ad Hoc Networks”, Proc. IEEE GLOBECOM, St. Louis, Missouri, USA, Dec. 2005.

[40] E.Padilla, N.Aschenbruck, P.Martini, M.Jahnke and J.Tolle, “Detecting Black Hole Attack in Tactical MANETs using Topology Graph”, Proc. IEEE Conference on Local Computer Networks, 2007.

[41] M. Medadian, M.H. Yektaie and A.M. Rehmani, “Combat with Black Hole Attack in AODV Routing Protocol in MANETs”, Proc. IEEE Asian Himalayas International Conference on Internet, Nov. 2009.

[42] X.Y. Zhang, Y. Sekiya and Y. Wakahara, “Proposal of a Method to Detect Black Hole Attack in MANETs”, Proc. IEEE International Symposium on Autonomous Decentralized System ISADS, 2009.

[43] G.Xiaopeng and C.Wei, “A Novel Grey Hole Attack Detection Scheme for Mobile Ad-Hoc Networks”, Proc. IFIP International Conference on Network and Parallel Computing, 2007.

[44] C. Wei, L. Xiang, B. Yuebin and G.Xiopeng, “A New Solution for Resisting Grey Hole Attack in Mobile Ad Hoc Networks”, Proc. IEEE Conference on Communication and Networking, China 2007.

[45] C.Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, “A Specification Based Intrusion Detection for AODV”, Proc. ACM Workshop on Security of Ad Hoc and Sensor Networks,2003.

[46] P. Papadimitratos and Z.J. Haas, “Secure Message Transmission in Mobile Ad Hoc Networks”, Elsevier Journal of Ad Hoc Networks, Vol.1, No.1, pp 193-209, 2003.

[47] P. Papadimitratos, Z.J. Haas and P. Samar, “The Secure Routing Protocol (SRP) for Ad Hoc Networks”, IETF Internet Draft , December 2002, available at http://www.ietf.org/proceedings/56/I-D/draft-papadimitratos-secure-routing-protocol-00.txt.

[48] A. Rawat, P.D. Vyavahare and A.K. Ramani, “Evaluation of Rushing Attack on Secure Message Transmission (SMT/SRP) Protocol for Mobile Ad Hoc Networks”, Proc. International Conference on Personal Wireless Communications (ICPWC), Jan. 2005.

[49] J. Douceur, “The Sybil Attack”, Proc. International Workshop on Peer-to-Peer Systems (IPTPS), March 2002.

[50] D.Monica, J. Leitao, L. Rodrigues and C.Riberio, “On the use of Radio Resource Test in Wireless Ad Hoc Networks”, Proc.Workshop on Recent Advances in Intrusion Tolerant Systems, Portugal, June 2009.

[51] N.Ye, X.Li, Q.Chen, M.Emran and M.Xu, “Probabilistic Techniques for Intrusion Detection Based on Computer Audit Data”, IEEE Transactions on Systems, Man, and, Cybernetics, Vol. 31, No. 4, July 2001.

[52] N.Ye and Q.Chen, “An Anomaly Detection Technique based on a CHI-SQUARE Statistics for Detecting Intrusion into Information System”, International Journal of Quality and Reliability Engineering International, Vol.17, No.6, pp 105-112, 2001.

[53] H. Debar, M. Becker and D. Siboni, “A Neural Network Component for an Intrusion Detection System”, Proc. IEEE Computer Society Symposium on Security and Privacy, Oakland, May 1992.

[54] D.S. Bauer, F.R. Eichelman, R.M. Herrera and A.E. Irgon, “Intrusion Detection an Application of Expert Systems to Computer Security”, Proc. IEEE International Conference on Security Technology, 1989.

[55] T. Lunt and R. Jagannathan, “A Prototype Real Time Intrusion Detection Expert System”, Proc. IEEE Symposium on Security and Privacy, Oakland, April 1988.

[56] N. Habra, B. L. Charlier, A. Mounji and I. Mathie, “Asax_ Software Architecture and Rule Based Language for Universal Audit Trail Analysis”, Proc. European Symposium on Research in Computer Security ESORICS, France, November 1992.

[57] P. Uppuluri and R. Sekar, “Experiences with Specification-Based Intrusion Detection,” Proc. Recent Advances in Intrusion Detection, (RAID), 2001.

[58] W. Scheirer and M. Chuah, "Syntax vs. Semantics: Competing Approaches to Dynamic Network Intrusion Detection”, International Journal of Security and Networks, Vol. 3, No. 1, pp. 24 - 35, 2008.

[59] D.Sterne, P.Balasubramanyam, D.Carman, B.Wilson, R. Talpade, C.Ko, R. Balupari, C.-Y. Tseng, T.Bowen, K.Levitt and J.Rowe, “A General Cooperative Intrusion Detection Architecture for MANETs”, Proc. IEEE International Workshop on Information Assurance (IWIA 05), 2005.

[60] Y. Huang and W. Lee, “A Cooperative Intrusion Detection System for Ad Hoc Networks”, Proc. ACM Workshop on Security of Ad Hoc and Sensor Networks, New York, USA, 2003.

[61] B. Pahlevanzadeh and A. Samsudin, “Distributed Hierarchical IDS for MANET over AODV”, Proc. IEEE International Conference on Telecommunications, Malaysia, May 2007.

[62] P. Yi, Y. Jiang, Y. Zhong and S. Zhang, “Distributed Intrusion Detection for Mobile Ad Hoc Networks”, Proc. IEEE Application and Internet Workshop, 2005.

[63] G.F.Cretu, J.Parekh, K.Wang and S.J.Stolfo, “Intrusion and Anomaly Detection Model Exchange for Mobile Ad-Hoc Networks”, Proc. IEEE Consumer Communication and Networking Conference, 2006.

[64] Y. Liu, C. Comaniciu and H. Man, "Modelling Misbehaviour in Ad Hoc Networks: a Game Theoretic Approach for Intrusion Detection”, International Journal of Security and Networks, Vol. 1, Nos.3/4, pp. 243 - 254, 2006.

[65] H.Jiang and H.Wang, “Markov Chain Based Anomaly Detection for Wireless Ad-Hoc Distribution Power Communication Networks”, Proc. IEEE Power Engineering Conference, 2005.

[66] S.Jha, K.Tan and R.A.Maxion, “Markov Chains, Classifier, and Intrusion Detection”, Proc. IEEE Computer Security Foundations Workshops, 2001.

[67] B. Sun, K. Wu and U.W. Pooch, “Routing Anomaly Detections in Mobile Ad Hoc Networks”, Proc. IEEE International Conference on Computer Communication and Networks ICCCN, 2003.

[68] B.Sun, K.Wu, Y.Xiao and R.Wang, “Integration of Mobility and Intrusion Detection Wireless Ad Hoc Networks”, Journal of Communication Systems, Wiley International, Vol. 20, No. 6, pp. 695-721, 2007.

[69] Y.Zhang and W.Lee, “Intrusion Detection in Wireless Ad-Hoc Networks”, Proc. ACM International Conference on Mobile Computing and Networking(MobiCom), pp 275-283, Boston, US, 2000.

[70] Y. Zhang, W. Lee, and Y. Huang, “Intrusion Detection Techniques for Mobile Wireless Networks,” ACM Wireless Networks, Vol. 9, No. 5, pp. 545–56, Sep. 2003.

[71] P.Albers, O.Camp and R.Puttini, “Security in Ad-Hoc Networks: A General ID Architecture Enhancing Trust Based Approaches”, Proc. IEEE International Workshop on Wireless Information Systems, 2002.

[72] O.Kachirski and R. Guha,.“Effective Intrusion Detection Using Multiple Sensors in Wireless AdHoc Networks.” Proc. IEEE Hawaii International Conference on System Sciences (HICSS’03), 2003.

[73] P.Tai, H.A Ryaciotaki-Boussalis and D.Hollaway, “Neural Network Implementation to Control Systems: a Survey of Algorithm and Techniques”, Proc. IEEE International Conference on Signals, Systems and Computers, Nov. 1991.

[74] A.Mitrokosta, N.Komninos and C.Douligeris, “Intrusion Detection with Neural Networks and Watermarking Techniques for MANETs”, Proc. IEEE International Conference on Pervasive Services, pp 118-127, July 2007.

[75] V.M.Potdar, S.Han and E.Chang, “A Survey of Digital Image Watermarking Techniques”, Proc. IEEE International Conference on Industrial Informatics, Aug. 2005.

[76] S.Jabbehdari, S.H. Talari and N.Modiri, “A Neural Network Scheme for Anomaly Based Intrusion Detection Systems in Mobile Ad Hoc Networks”, Journal of Computing, Vol. 4, No. 2, pp-61-66, 2012.

[77] K.Ilgun, R.A.Kemmerer, and P.A.Porras, “State Transition Analysis: a Rule Based Intrusion Detection Approach”, IEEE Transactions on Software Engineering, Vol.21, No.3, pp-181-199, March 1995.

[78] G. Vgina, S. Gawalani, K. Srinivasan, M. Belding-Royer and A. Kemmerer, “An Intrusion Detection Tool for AODV Based Ad Hoc Wireless Networks”, Proc. IEEE Annual Computer Security Application Conference ACSAC,2004.

[79] N.Komninos, D. Vergados and C.Douligeris, “Detecting Unauthorized and Compromised Nodes in Mobile Ad Hoc Networks”, Journal of Ad Hoc Networks, Elsevier, Vol. 5, No. 3, pp 289–298, April 2007.

[80] F. Anjum, D. Subhadrabandhu and S. Sarkar, “Signature Based Intrusion Detection for Wireless Ad Hoc Networks: a Comparative Study of Various Routing Protocols”, Proc. IEEE Vehicular Technology Conference (VTC), Oct 2003.

[81] A.B.Smith, “An Examination of Intrusion Detection Architecture for Wireless Ad-Hoc Networks”, Proc. National Colloquium for Information System Security Education, May 2001.

[82] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, and S. Zhou, “Specification-Based Anomaly Detection: a New Approach for Detecting Network Intrusions”, Proc. ACM Conference on Computer and Communications Security CCS ’02, 2002.

[83] R. Sekar and P. Uppuluri, “Synthesizing Fast Intrusion Prevention/Detection Systems from High-Level Specifications”, Proc. Usenix Security Symposium, 1999.

[84] J.-M. Orset, B. Alcalde, and A. R. Cavalli, “An EFSM-Based Intrusion Detection System for Ad Hoc Networks”, Proc. International Conference on Automated Technology for Verification and Analysis, pp 400–413, 2005.

[85] T. Clausen and P. Jacquet. IETF RFC 3626: Optimized Link State Routing Protocol (OLSR). http://www.ietf.org/rfc/rfc3626.txt, 2003.

[86] H. Tseng, T.Song, P. Balasubramanyam, C.Ko and K.Levitt, ”A Specification-Based Intrusion Detection Model for OLSR,” Proc. International Symposium on Recent Advances in Intrusion Detection (RAID), pp. 330-350, 2005.

[87] N. Stakhanova, S. Basu, W. Zhang, X. Wang, and J. Wong, “Specification Synthesis for Monitoring and Analysis of MANET Protocols,” Proc. International Symposium on Frontiers in Networking with Applications, 2007.

[88] J.Joseph, A.Das, B.Seet and B.Lee, “CRADS: Integerated Cross Layer approach for Detecting Routing Attacks in MANETs”, Proc. IEEE Wireless Communication and Networking Conference (WCNC), 31st March -3rd April 2008.

[89] V.N.Vapnik, ”Statistical Learning Theory”. 1998: Wiley.

[90] A.Nadeem and M.Howarth, “A Generalized Intrusion Detection and Prevention Mechanism for Securing MANETs”, Proc. IEEE International Conference on Ultra Modern Telecommunications and Workshops, St Petersburg Russia 2009.

[91] A.Hijazi and N.Nasser, “Using Mobile Agent for Intrusion Detection in Wireless Ad-Hoc Networks”, Proc. IEEE Wireless Communication and Networking Conference WCNC, March 2005.

[92] J.C. Kao and R. Marculescu, “Eavesdropping Minimization via Transmission Power Control in Ad Hoc Wireless Networks”, Proc. IEEE Sensors and Ad hoc Communication and Networks SECON, 2006.

[93] K.Sanzgiri and M.Belding-Royer, “A Secure Routing Protocol for Ad Hoc networks”, Proc. IEEE International Conference on Network Protocol (ICNP’ 02), 2002

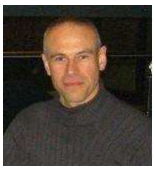
[94] Y.Hu, A.Perrig and B.Johnson, “A Secure On Demand Routing Protocol for Ad Hoc networks”, Proc. ACM/ IEEE International Conference on Mobile Computing (MobiCom), Atlanta, Georgia, USA, pp 23-28, Sep. 2002.

[95] V. Karyotis, S. Papavassiliou, M. Grammatikou, and V. Maglaris, "A Novel Framework for Mobile Attack Strategy Modelling and Vulnerability Analysis in Wireless Ad Hoc Networks," International Journal of Security and Networks, Vol. 1, Nos.3/4, pp. 255 - 265, 2006.

[96] Y.Hu, B. Johnson and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks”, International Journal of Ad hoc Networks, Vol.1, pp 175-192, 2003.

[97] A.Nadeem and M.Howarth, “Protection of MANETs from a range of attacks using an intrusion detection and prevention system”, Telecommunication Systems Journal, Springer, In Press, DOI 10.1007/s11235-011-9484-6, July 2011.

Adnan Nadeem received his bachelor’s degree BSc and master’s degree MCS in computer science, both from the Faculty of Science, University of Karachi. He gained his PhD from the Centre for Communication Systems Research (CCSR) at the University of Surrey, UK. His principal research interests include security issues in mobile ad hoc networks, intrusion detection & prevention, and routing in Body Area Sensor Networks. He is an assistant professor in the Department of Computer Science, Federal Urdu University of Arts Science & Technology, Pakistan. He is a member of the IEEE and a fellow of the Higher Education Academy, UK.



Michael Howarth received his bachelor’s degree in engineering science and a DPhil degree in electrical engineering, both from Oxford University, and his MSc in telecommunications from the University of Surrey. Prior to joining the University of Surrey, he worked for several networking and IT consultancies. He is a lecturer in the Centre for Communication Systems Research (CCSR) at the University of Surrey His research interests include traffic engineering, quality of service, security and privacy, applied in fixed Internet, wireless and satellite networks. He is a chartered electrical engineer and a member of the UK IET.