INTRUSION DETECTION IN MOBILE AD HOC NETWORKS

Sevil Şen, John A. Clark

Department of Computer Science, University of York, York, UK, YO10 5DD

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

Abstract

In recent years mobile ad hoc networks (MANETs) have become a very popular research topic. By providing communications in the absence of a fixed infrastructure MANETs are an attractive technology for many applications such as rescue operations, tactical operations, environmental monitoring, conferences, and the like. However, this flexibility introduces new security risks. Since prevention techniques are never enough, intrusion detection systems (IDSs), which monitor system activities and detect intrusions, are generally used to complement other security mechanisms.

Intrusion detection for MANETs is a complex and difficult task mainly due to the dynamic nature of MANETs, their highly constrained nodes, and the lack of central monitoring points. Conventional IDSs are not easily applied to them. New approaches need to be developed or else existing approaches need to be adapted for MANETs. This chapter outlines issues of intrusion detection for MANETs and reviews the main solutions proposed in the literature.

1   Introduction

Wireless networking is now the medium of choice for many applications. In addition, modern manufacturing techniques allow increasingly sophisticated functionality to reside in devices that are ever smaller, and so increasingly mobile. Mobile ad hoc networks (MANETs) combine wireless communication with a high degree of node mobility. Limited range wireless communication and high node mobility means that the nodes must cooperate with each other to provide essential networking, with the underlying network dynamically changing to ensure needs are continually met. The dynamic nature of the protocols that enable MANET operation means they are readily suited to deployment in extreme or volatile circumstances. MANETs have consequently become a very popular research topic and have been proposed for use in many areas such as rescue operations, tactical operations, environmental monitoring, conferences, and the like.

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

Many intrusion detection systems (IDS) have been proposed in the literature for wired networks but MANETs' specific features make direct application of these approaches to MANETs impossible. New approaches need to be developed or else existing approaches need to be adapted for MANETs. In this chapter, we examine special IDS issues of MANETs and proposed IDSs for MANET-specific systems to find out how well proposed systems address these issues. In the next section, an introduction to intrusion detection systems is given. Then, intrusion detection on MANETs is discussed along with proposed IDSs. In conclusion, thoughts for practitioners and ideas for future research are given.

2   Intrusion Detection Systems

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

The *data collection component* is responsible for collection and pre-processing data tasks: transferring data to a common format, data storage and sending data to the detection module [14]. IDS can use different data sources as inputs to the system: system logs, network packets, etc. In the *detection component* data is analyzed to detect intrusion attempts and indications of detected intrusions are sent to the *response component*.

In the literature, three intrusion detection techniques are used. The first technique is *anomaly-based intrusion detection* which profiles the symptoms of normal behaviors of the system such as usage frequency of commands, CPU usage for programs, and the like. It detects intrusions as anomalies, i.e. deviations from the normal behaviours. Various techniques have been applied for anomaly detection, e.g. statistical approaches and artificial intelligence techniques like data mining and neural networks. Defining normal behaviour is a major challenge. Normal behavior can change over time and intrusion detection systems must be kept up to date. False positives – the normal activities which are detected as anomalies by IDS – can be high in anomaly-based detection. On the other hand, it is capable of detecting previously unknown attacks. This is very important in an environment where new attacks and new vulnerabilities of systems are announced constantly.

Misuse-based intrusion detection compares known attack signatures with current system activities. It is generally preferred by commercial IDSs since it is efficient and has a low false positive rate. The drawback of this approach is that it cannot detect new attacks. The system is only as strong as its signature database and this needs frequent updating for new attacks. Both anomaly-based and misuse-based approaches have their strengths and weaknesses. Therefore, both techniques are generally employed for effective intrusion detection.

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

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

3   Intrusion Detection Issues in MANETs

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

Lack of Central Points MANETs do not have any entry points such as routers, gateways, etc. These are typically present in wired networks and can be used to monitor all network traffic that passes through them. A node of a mobile ad hoc network can see only a portion of a network: the packets it sends or receives together with other packets within its radio range. Since wireless ad hoc networks are distributed and cooperative, the intrusion detection and response systems in MANETs may also need to be distributed and cooperative [28]. This introduces some difficulties. For example, distribution and cooperativeness of IDS agents are difficult in an environment where resources such as bandwidth, processor speed and power are limited. Furthermore, storing attack signatures in a central database and distributing them to IDS agents for misuse-based intrusion detection systems is not suited to this environment.

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

Wireless Links Wireless networks have more constrained bandwidth than wired networks and link breakages are common. IDS agents need to communicate with other IDS agents to obtain data or alerts and need to be aware of wireless links. Because heavy IDS traffic could cause congestion and so limit normal traf-

fic, IDS agents need to minimize their data transfers [18]. Bandwidth limitations may cause ineffective IDS operation. For example, an IDS may not be able to respond to an attack in real-time due to communication delay. Furthermore, IDS agents may become disconnected due to link breakages. An IDS must be capable of tolerating lost messages whilst maintaining reasonable detection accuracy [24].

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

Lack of a Clear Line of Defense and Secure Communication MANETs do not have a clear line of defense; attacks can come from all directions [28]. For instance, there are no central points on MANETs where access control mechanisms can be placed. Unlike wired networks, attackers do not need to gain physical access to the network to exploit some kinds of attacks such as passive eavesdropping and active interference (these require only radio contact) [28]. Furthermore, the critical nodes (servers, etc.) cannot be assumed to be secured in cabinets and nodes with inadequate protection have high risk of compromise and capture. IDS traffic should be encrypted to avoid attackers learning how the IDS works [18]. However, cryptography and authentication are difficult tasks in a mobile wireless environment since they consume significant resources. In many cases IDS agents risk being captured or compromised with drastic consequences in a distributed environment. They can send false alerts and make the IDS ineffective. IDS communication can also be impeded by blocking and jamming communications on the network.

Cooperativeness MANET routing protocols are usually highly cooperative. This can make them the target of new attacks. For example, a node can pose as a neighbour to the other nodes and participate in decision mechanisms, possibly affecting significant parts of the network.

4   Background

4.1 *Proposed IDSs*

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

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

Two different decision-making mechanisms are used in distributed and cooperative IDSs: collaborative decision-making, where each node can take active part in the intrusion detection process, and independent decision-making, where particular nodes are responsible for decision-making [12]. Both decision-making mechanisms have pros and cons. Collaborative-decision making systems are more reliable. If all nodes contribute to a decision, a few malicious nodes cannot easily disrupt the decision-making. However, if any node can trigger a full-force re-

sponse, it can affect the entire network and be vulnerable to a DoS attack [12]. A collaborative-decision making approach is also more resilient to benign failure of nodes. On the other hand, failing or compromise of particular nodes in independent decision-making systems can have drastic effects. However, these systems are less prone to spoofed intrusion attacks than collaborative decision-making systems [12].

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

4.1.1   Distributed and Cooperative IDS [28][29]

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

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

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

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

This is one of the few approaches considering mobility by monitoring node movements. This can decrease false positives resulting from the node's mobility.

However, it only reflects the local mobility not the network's mobility. Also, every node has to have a built-in GPS (Global Positioning System) to obtain this mobility data. It is emphasized that it can be applied to all routing protocols since it uses the minimal routing information. It also allows addition of new features for a specific protocol. From the security point of view the system is reliable unless the majority of nodes are compromised [28]. (These can send falsified data.) Furthermore, the collaborative detection mechanism can be prone to denial of service and spoofed intrusion attacks [12].

4.1.2   Cooperative IDS using Cross-Feature Analysis in MANETs [7][8]

Huang et al. use data-mining techniques to automatically construct an anomaly detection model [8]. They use an analysis technique that targets multiple features and which acknowledges the characteristic patterns of correlation between them. The basic assumption here for anomaly detection is that normal and abnormal events have different feature vectors that can be differentiated.

In cross-feature analysis, they train the following classification model C_i from normal data based on exploring the correlation between each feature and all other features [7]:

C_i: $\{f_1, f_2, \ldots, f_{i-1}, f_{i+1}, \ldots, f_L\} \rightarrow f_i$ where $\{f_1, f_2, \ldots, f_L\}$ is the feature set.

In practice, each feature f_i is analyzed and compared with the predicted values of f_i. Then, the average match count is evaluated by dividing the number of total true matches of all features by L and used to detect anomalies which are below the threshold. Instead of count values, probabilities can also be used. Different classification algorithms C4.5, Ripper, and NBC are investigated to calculate the probability function [7]. Since C4.5 shows better performance, it is the chosen method in their subsequent research [8].

Due to resource-constraints in MANETs, they propose a cluster-based IDS architecture. A fair and secure cluster-head assignment is presented. Cluster-heads are selected randomly, which also facilitates security. Equal service time is assigned to all selected cluster-heads.

Simple rules are also introduced to determine attack types and sometimes attackers. The rules are executed after an anomaly is detected. They are based on statistics such as the number of incoming/outgoing packets on the monitored node and are pre-computed for known attacks. For example, unconditional packet dropping of a node m is formulated as follows [8]:

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

If the denominator is not zero and FP_m is 0, it means that node m is dropping all packets. The attacker is identified by a neighbour of node m who can promiscuously overhear node m's traffic.

It is implemented on the NS-2 simulator by using traffic related and non-traffic related features. Traffic related features are packet type, flow direction, sampling periods and statistics measures (counts and standard deviations of inter-packet intervals). Non-traffic related features represent a view of network topology and routing operations and comprise information such as the number of routes added by route discovery, total route change, and absolute velocity (the physical velocity of a node). The AODV protocol is targeted and the following metrics are used for evaluation: detection rate, false positive rate, and attack type detection rate. The results are promising.

It is the first approach that uses feature correlations. They propose to investigate how computational cost can be reduced [7]. Attacker identification and attacks against the IDS (a major issue for a cluster-head architecture) are identified as future research [8].

4.1.3   Zone-Based Intrusion Detection System [22]

In [22], a non-overlapping zone-based IDS is proposed. In this architecture, the network is divided into zones based on geographic partitioning to save communication bandwidth while improving detection performance by obtaining data from many nodes. The nodes in a zone are called *intrazone* nodes, and the nodes which work as a bridge to other zones are called *interzone* (gateway) nodes. As shown in Fig 4.1 there can be more than one gateway node in a zone, for instance the nodes 1, 6, 7 are gateway nodes in zone 5. Each node in the zone is responsible for local detection and sending alerts to the interzone nodes.
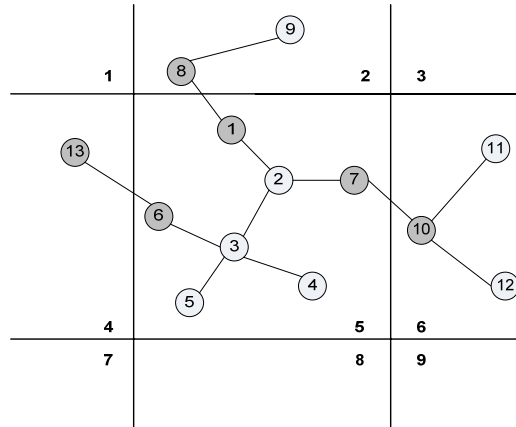
Fig 4.1 Zone-Based IDS Architecture in MANETs

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

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

One of the contributions in this paper is MIDMEF (MANET Intrusion Detection Message Exchange Format) which defines the format of information exchange between IDS agents. It is consistent with Intrusion Detection Message Exchange Format (IDMEF) proposed by the Internet Engineering Task Force (IETF) [10].

Previous work [21] analyzed how to consider mobility when designing an IDS. Link change rate is proposed to reflect different mobility levels. Suitable normal profiling and proper thresholds can then be adaptively adopted by IDS agents using this measure. Furthermore, it is shown that link change rate reflects the mobility model of the network better than the generally used mobile speed measure. Link change rate of a node is defined as [21]:

$$\frac{\left|\mathbf{N_1} - \mathbf{N_2}\right| + \left|\mathbf{N_2} - \mathbf{N_1}\right|}{\left|t_2 - t_1\right|}$$

where $\mathbf{N_1}$ is the neighbor set of the node at t_1 time and $\mathbf{N_2}$ is the neighbor set of the node at t_2 time.

The proposed IDS is simulated on the GlomoSim simulator and evaluated using the following performance metrics: false positive rate, detection rate, and mean time of first alarm (a measure of how fast intrusion is detected). The system is trained and evaluated under different mobility levels and it is shown that the anomaly-based detection performs poorly due to the irregularity of data under high mobility. Furthermore, the presence of partial victims who do not receive all falsified data because of link breakages resulting from mobility [22] is claimed to make the detection more difficult. The advantages of an aggregation algorithm using the data from both partial and full victims are emphasized: lower false positive and higher detection rate than local IDS achieves. Nevertheless, its performance can decrease with the existence of more than one attacker in the network. They also conclude that communication overhead is increased in proportion to mobility where local IDSs generate more false positives and send more intrusion alerts to gateway nodes. In addition, aggregating data and alerts at interzone nodes can result in detection and response latency, when there is sufficient data for intrusion detection even at intrazone nodes. The authors plan to investigate further attack scenarios at the routing and other layers as well as constructing further security-related features and misuse-based detection approaches.

4.1.4   General Cooperative Intrusion Detection Architecture [20]

In [20], Sterne et al. present a cooperative and dynamic hierarchical IDS architecture which uses multiple-layering clustering. Fig 4.2 shows a network with two-level clusters. The nodes annotated with "1" are the first level cluster-heads, essentially acting as a management focus for IDS activity of immediately surrounding nodes. These level 1 cluster heads can form a cluster around high level node "2", second level cluster-head. This process goes on until all nodes are assigned to a cluster. To avoid single point of failure, they propose choosing more than one cluster-head for the top-level cluster. The selection of cluster heads is based on topology and other criteria including connectivity, proximity, resistance to compromise, accessibility by network security specialists, processing power, storage capacity, energy remaining, bandwidth capabilities, and administratively designated properties [20].
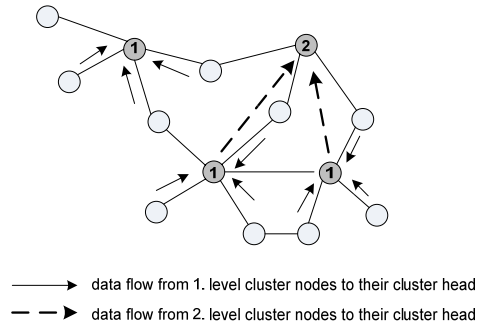
data flow from 1. level cluster nodes to their cluster head
data flow from 2. level cluster nodes to their cluster head

Fig 4.2 IDS Hierarchy with Two-Level Clusters

In this dynamic hierarchy, data flow is upward, while the command flow is downward. Data is acquired at leaf nodes and aggregated, reduced and analyzed as it flows upward. The key idea is given as detecting intrusions and correlating with other nodes at the lowest levels for reducing detection latency and supporting data reduction, whilst maintaining data sufficiency. It supports both direct reporting by participants and promiscuous monitoring for correlation purposes.

The proposed intrusion detection architecture for MANETs targets military applications. The authors claim that the dynamic hierarchy feature is highly scalable. It also reduces the communication overhead through the hierarchical architecture. However, the cost of configuration of the architecture in dynamic networks should also be considered.

Neither specific intrusion detection techniques nor the implementation of this architecture is covered. Supporting a broad spectrum of intrusion detection techniques is posed as one of the general requirements of IDS. However, applicability of these techniques to mobile ad hoc networks, which can have resource constrained nodes and no central management points, is not addressed. Examples of usage scenarios, which cover MANET-specific and conventional attacks, are presented by indicating different intrusion detection techniques on the architecture. Some attacks can be drastic in this architecture; for example the capturing of cluster-heads or a malicious node being selected as a cluster-head by sending false criteria. Ongoing areas of investigation are comparison of existing clustering algorithms and communication overhead metrics. They identify as future work the development of Byzantine-resistant techniques for clustering and for intrusion detection and correlation.

4.1.5   Intrusion Detection Using Multiple Sensors [12]

Kachirski and Guha propose an IDS solution based on mobile agent technology which reduces network load by moving computation to data. This is a significant feature for MANETs which have lower bandwidth than wired networks. A modular IDS structure is proposed that distributes the functional tasks by using three mobile agent classes: monitoring, decision-making and action-taking. The advantages of this structure are given as increased fault-tolerance, communication cost reduction, improved performance of the entire network, and scalability [12].

A hierarchical and distributed IDS architecture is given which divides the network into clusters. Cluster heads are chosen by vote, with each node voting for a node based on its connectivity. Each node in the network is responsible for local detection using system and user level data. Only cluster heads are responsible for detection using network level data and for making decisions. However, depending on the hop attribute of the clusters, network intrusion detection performance can change. For example, every node has direct connection to at least one cluster head in a one-hop clustered network, so each packet in the network can be monitored as shown in Fig 4.3(a), while three links in Fig 4.3(b) cannot be monitored by the cluster-heads in a two-hop clustered network. As the degree of monitoring increases the number of cluster heads increases too. So, choosing the hop attribute of the clusters is a trade-off between security and efficiency. However, the nodes not in a cluster head's communication range can move to the monitoring area of another cluster head due to mobility. So, having a few links that cannot be monitored by any cluster head is regarded as acceptable for highly dynamic environments.
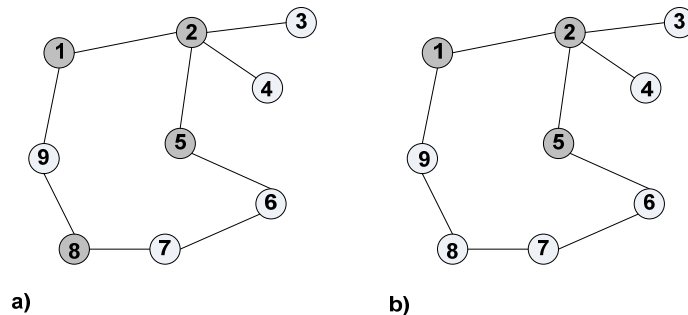

a)   b)

Fig 4.3 (a) one-hop clustered network: nodes 1, 2, 5, 8 are cluster-heads **(b)** two-hop clustered network: nodes 1, 2, 5 are cluster-heads

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

In this paper a scalable and bandwidth-efficient IDS is proposed by using mobile agents but without giving any validation via simulation or implementation. On the other hand, there are urgent security issues for mobile agents that are set to be investigated in the authors' future research. In addition, details of the anomaly-based detection method are not given, with research on more robust and intelligent cooperative detection algorithms left as future research.

4.1.6   Specification-Based IDS for AODV [25]

The first specification-based IDS in MANETs is proposed by Tseng et al. [25]. They use network monitors (NM) which are assumed to cover all nodes. Nodes moving out of the current network monitoring area are also assumed to move into range of other network monitors. Other assumptions are: i) network monitors know all nodes' IP and MAC addresses, and MAC addresses cannot be forged. ii) network monitors and their messages are secure. iii) if some nodes do not respond to broadcast messages, this will not cause serious problems.

Network monitors employ finite state machines (FSM) as specifications of the operations of AODV, especially for the route discovery process, and maintain a forwarding table for each monitored node. Each route request (RREQ) and route reply (RREP) message in the range of the network monitor is monitored in a request-reply flow. When a network monitor needs information about previous messages or other nodes not in its range, it can ask neighboring network monitors. In high mobility conditions the communication between network monitors increases since monitored nodes or/and packets frequently move out of the range of the monitoring node.

The authors also modify the AODV routing protocol by adding a new field: the *previous node*. Since RREQs are broadcast messages, it is necessary to keep track of the RREQ path. The previous node is needed to detect some kind of attacks such as sending an RREP to a node that is not on the reverse route [25].

Future work includes experimentation via NS-2 network simulation, profiling network QoS (Quality of Service) to reduce false positives by separating packet loss, packet error, and packet generation through defining reasonable thresholds for the current profile, and refining NM architecture using via a P2P (peer-to-peer) approach.

This is a promising approach that can detect both known and unknown attacks against routing protocols which have clearly defined specifications. It is claimed to detect most of the attacks with minimum overhead in real time. However, some of the assumptions accepted in this paper are not very realistic. For example, assuming the network monitors cover all network nodes and have all nodes' IP and

MAC addresses. Scalability is one of the important features on many MANET applications where the nodes can join and leave network independently and move frequently. Assuming MAC addresses cannot be easily forged is unrealistic. Moreover, dropping of some broadcast messages in the network can affect all network services if the node dropping messages is at a critical point. Furthermore, the details of the architecture are not addressed (such as the positions of network monitors in MANETs where the topology changes arbitrarily).

4.1.7   DEMEM: Distributed Evidence-driven Message Exchanging ID Model [24]

DEMEM is a distributed and cooperative IDS in which each node is monitored by one-hop neighbor nodes. In addition to one-hop neighbor monitors, 2-hop neighbors can exchange data using intrusion detection (ID) messages [24]. The main contribution of DEMEM as stated by the authors is to introduce these ID messages to help detection, which they term *evidence-driven message exchange*. Evidence is defined as critical information (specific to a routing protocol) used to validate the correctness of the routing protocol messages, for instance hop count and node sequence number in AODV. [24]. To minimize ID message overhead ID messages are sent only when there is new evidence, so it is called evidence-driven. DEMEM also introduces an ID layer to process these ID messages and detect intrusions between the IP layer and the Routing Layer without modifying the routing protocol, so it can be applied to all routing protocols.

DEMEM uses the specification-based IDS model for OLSR proposed in their previous work [23]. In OLSR [11], there are nodes called Multipoint Relays (MPRs) which serve to reduce the flooding of broadcast packets in the network. These nodes are selected by their neighboring nodes called MPR selectors. The packets of an MPR node's MPR selectors are only retransmitted by that MPR node. TC (topology control) messages are sent by each node periodically to declare its MPR selectors. The proposed specification-based system uses the following constraints of OLSR to detect intrusions:

C1: neighbors in Hello messages must be reciprocal.
C2: MPRs must reach all 2-hop neighbors.
C3: MPR selectors must match corresponding MPRs.
C4: Fidelity of forwarded TC messages must be maintained.

The authors state that the system cannot detect collaborative attacks. For example two attackers who falsely claim that they are neighbors might not be detected by the above constraints [23].

DEMEM introduces three authenticated ID messages for OLSR. The first one is ID-Evidence, which is designed for 2-hop-distant detectors to exchange their evidence concerning one-hop neighbors, MPRs and MPR selectors on OLSR. The second message, ID-Forward, is a request to forward any held ID-Evidence messages to other nodes. This means that a node can request the holder of evidence to forward it directly, rather than sending it itself, so reducing message overhead. The last message, ID-Request, is designed to tolerate message loss of ID-Evidence with low communication overhead. The false positives and delay detection due to message loss are decreased by an ID-Request message. Moreover, they specify a threshold value to decrease false positives due to temporary inconsistencies resulting from mobility. When a detector detects an intrusion, it automatically seeks to correct the falsified data.

DEMEM is simulated on the GlomoSim simulator with the random waypoint mobility model and with different speed and pause time sets for mobile nodes. The approach is very effective for mesh networks where nodes in the network do not move: there were no false positives and no false negatives with 0.05% message overhead in a network with 150 nodes and 3% overhead in a network with 10 nodes. Interestingly, the message overheads of DEMEM are decreased as the number of nodes in the network increases, because the number of Hello and TC messages is greater than ID messages in large networks [24]. The message overhead in the simulation varies between 2% and 30% depending on mobility level. They also show how detection accuracy and detection latency of the system vary with the chosen thresholds.

The applicability of DEMEM on other routing protocols especially on reactive protocols are addressed. Because reactive protocols produce fewer routing messages with generally smaller size compared to periodic routing messages of proactive protocols, IDS on reactive protocols may have a greater message overhead than proactive protocols [24]. Ongoing research includes implementation of DEMEM on AODV and implementation of a reputation-based cooperative intrusion response model.

4.1.8   Case-Based Agents for Packet-Level Intrusion Detection [5]

Guha et al. [5] proposed a case-based reasoning system for packet level monitoring based on a hierarchical IDS architecture. In the case-based reasoning approach, known attacks are formulated as cases in the case archive, which stores the features of known problems as well as the actions to solve these problems. The idea is to search for similar cases in the case archive when a problem is detected on the network. The returned similar cases are used either as direct solution to the problem or else as bases on which to formulate the new case. The case concerning the final situation, failure or success, is stored into the archive. In this paper, Snort

IDS [19] rules are used as the cases and each node has the database of these rules (which is claimed to be small in size). Since Snort rules need exact matching, this is used instead of searching for similarity in the case archive.

IDS functions (monitoring, decision making and actions) are distributed across several mobile agents. Some of them are presented on all mobile hosts, while others are distributed to only a select of group nodes [5]. All nodes have system-level and user-level monitoring that uses an anomaly-based approach. However, packet-level monitoring, which uses case-based reasoning approach, and decision-making are assigned only to cluster-heads. In their simulation, it is shown that the number of dropped packets by cluster-heads increases as the density of the network increases.

Using both anomaly-based detection for system-level and user-level monitoring, and misuse-based detection for packet-level monitoring increases effectiveness. It is also bandwidth-conscious, since it uses mobile agents. However, the security of the mobile agents still needs research.

4.1.9   An IDS Architecture with Stationary Secure Database [18]

A distributed architecture consisting of IDS agents and a stationary secure database (SSD) is proposed in [18]. All nodes have IDS agents responsible for local detection and collaborating with other agents in need. IDS agents have five components: local audit trail; local intrusion database (LID); secure communication module; anomaly detection modules (ADMs); and misuse detection modules (MDMs). The local audit trail gathers and stores local audit data – network packets and system audit data. The LID is a database that keeps information for IDS agents such as attack signatures, patterns of normal user behavior, etc. The secure communication module is used only by IDS agents to communicate securely with other IDS agents. ADMs use anomaly-based detection techniques to detect intrusions. There can be more than one ADM module in an IDS agent, for example using different techniques for different kinds of audit data. There are also MDMs responsible for misuse-based detection to detect known attacks.

The stationary secure database (SSD) maintains the latest attack signatures and latest patterns of normal user behaviors. It is to be held in a secure environment. Mobile agents get the latest information from the SSD and transfer their logs to the SSD for data mining. The SSD has more storage and computation power than mobile nodes, so it is capable of mining rules faster than the nodes in the network and can keep all nodes' logs [18]. Moreover, updating the SSD rather than all nodes in the network is easy. On the other hand, a stationary database is not suited to all kinds of networks. Military tactical environments with control centers are given as examples of the architecture suitable for SSD. However, nodes in hostile

environments may not attach to the SSD. Letting the nodes update themselves with the help of other nodes (which can consume significant bandwidth) is proposed as a solution to this problem.

Implementation and evaluation of this architecture are planned for future work. Although it seems to be an effective approach taking advantage of both anomaly-based detection using data mining techniques and misuse-based detection, it has a single point of failure, the SSD. Moreover, a stationary node goes against the nature of MANETs.

4.1.10   An IDS Model Integrating Different Techniques [9]

Huang and Lee propose an IDS model that uses both specification-based and anomaly-based detection approaches to detect interesting events [9]. A basic (routing) event is defined as the smallest set of casually related routing operations such as receiving/delivering a packet, modifying a routing parameter. An anomalous event is defined as the basic event that does not follow system specifications, such as deleting an entry in the route table, modifying route messages, etc.[9]. A specification-based approach is used to detect anomalous events that directly violate the specifications of AODV. Anomaly-based detection is used to detect events that do not violate specifications of the routing protocol directly and so require statistical measures.

In the specification-based approach extended finite state automata (EFSAs) are used to represent the specifications of AODV. Events which include only local node operations are mapped to the transitions of the automata. In the statistical-based approach, features are determined to detect anomalous events that cannot be detected by the specification-based approach, and then a set of detection rules is generated using RIPPER classifier.

The approach is evaluated using the MobiEmu simulator on some scenarios (not including high a degree of mobility). It is shown that some attacks are not detected effectively by this approach. It is concluded that these attacks cannot be detected locally [9].

The authors propose a taxonomy of attacks which decomposes an attack into a number of basic events and also propose a model to detect them. They use only local detection, since the local node is only reliable data source. That is why it cannot detect some kind of attacks which do not trigger anomalous events because of needing data from another layer such as a wormhole attack or needing other nodes such as network scan [9]. The authors plan to investigate multi-layer and global detection. Extracting features for detecting unknown attacks automatically is another issue identified as future research.

An outline of the proposed IDSs is given in Table 4.1. This shows the contribution/novelty each IDS brings and the MANET issues it does not address. However, security and limited resources issues are not shown in the table for each IDS separately, since all proposed systems usually make assumptions about these issues, or pay no attention to them.

IDS	Contribution	Other MANET IDS issues
Distributed and Co-operative IDS	first distributed and cooperative IDS consider mobility	consider only local mobility
IDS Using Cross-Feature Analysis	use cross-feature analysis construct anomaly-based detection model automatically define rules to detect attack(er)s	high computational cost consider only local mobility not consider cluster-heads' capabilities
Zone-Based IDS	use zone-based architecture define MIDMEF consider mobility based on changes of node's neighbours	cause detection and response latency even when there is enough evidence on local nodes
General Cooperative ID Architecture	use multiple-layered clustering	high-cost maintenance of the architecture under high mobility
IDS Using Multiple Sensors	use mobile agents for a scalable and bandwidth-efficient system	may not monitor each node on the network due to the hop attribute of clusters
Specification-Based IDS for AODV	first application of specification-based detection technique to MANETs	communication overhead under high mobility
DEMEM	introduce ID messages between IDS agents to help detection	may not detect some kind of distributed and collaborative attacks
Case-Based Agents for Packet-Level ID	use case-based approach and anomaly-based detection technique together	have difficulties in updating case archives in a distributed environment
IDS Architecture with Stationary Database	have a stationary secure database to keep patterns of normal user behaviors and attack signatures	have a central point
IDS Model Integrating Different Techniques	use anomaly-based and specification-based detection techniques together	carry out only local detection, may not detect distributed attacks

Table 4.1   Outline of the proposed IDSs

4.2 *Detection of Misbehaving Nodes*

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

4.2.1   Watchdog and Pathrater [15]

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

The watchdog's work is to detect misbehaving nodes by listening to nodes in promiscuous mode. When a node forwards a packet, the watchdog mechanism of that node monitors the next node to confirm that it also forwards the packet properly. It keeps sent packets in a buffer. When the packets are actually forwarded by next nodes, they are removed from the buffer. If the packets remain in the buffer longer than some timeout period, the watchdog increments the failure count of the node implicated. When the failure count of a node exceeds a threshold, the node is identified as a misbehaving node and a notification is sent to the source node. It is stated that watchdog can also detect replay attacks to some extent. However, since it uses promiscuous listening, it is stated that it might not detect misbehaving nodes in the existence of ambiguous collisions, receiver collisions, nodes that control their transmission power to deceive a listener into believing a message has truly been sent, and nodes that falsely report other nodes as misbehaving. It cannot detect partial dropping attacks and collaborative attacks involving at least two consecutive malicious nodes in a route [15].

Pathrater finds the most reliable path by using link reliability data and misbehaving nodes' information from the watchdog. In DSR, there can be many paths from source to destination, but the shortest path is selected. By using pathrater, the most reliable path is selected instead of the shortest path in the presence of misbehaving nodes. The SRR (send extra route request) extension to DSR can be added to find new paths when all paths include misbehaving nodes. Pathrater gives ratings to each node and provides a path metric based on the ratings of the nodes on the path. The authors state that ratings of the nodes should be rearranged to pre-

vent permanently excluding temporary misbehaving nodes from routing and forwarding.

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

The approach detects misbehaving nodes efficiently by using simple techniques without priori trust relationship information. Moreover, it increases the throughput of the network in the existence of misbehaving nodes, and does so with low overhead. On the other hand, it cannot detect collaborative attacks and partial dropping attacks. Additionally, it is applicable only to source routing protocols, because the watchdog needs to know where the packet is going to be forwarded by the next node. Applying the watchdog mechanism to other protocols requires adaptation. DSR needs modification for the SRR extension in the case of existence of misbehaving nodes on all paths. Finally, it rewards and reinforces malicious nodes in their behavior by forwarding their packets while they do not forward for other nodes [4].

4.2.2   Nodes Bearing Grudges [4]

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

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

The monitor (neighborhood watch) keeps a copy of recently sent packets. It can compare them with the packets forwarded by the next hop node and can detect routing and forwarding misbehaviors as deviations from normal expected behaviour. The types of misbehavior that can be detected by this system are stated to be: no forwarding, unusual traffic attraction, route salvaging, lack of error messages, unusually frequent route updates, and silent route change [4]. When a misbehaving behavior is detected, a reputation system is called for rating the misbehaving node.

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

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

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

ALARM messages are an extension to DSR and are used to distribute warning information. An ALARM message contains the type of protocol violation, the number of occurrences observed, whether the message was self-originated by the sender, the address of the reporting node, the address of the observed node and the destination address [4]. When an ALARM received, it is sent to Trust Manager to evaluate its trust level.

Assessment of this approach uses the GlomoSim simulator for evaluation and performance analysis is in progress. Moreover, the use of Game Theory for analytical evaluation is being investigated. One aim of the evaluation is to find the relation between the number of nodes in the network, the number of malicious nodes that can be tolerated, the number of friend nodes that needed for detection. In addition, they are planning to analyze the scalability, the cost/benefit ratio, the increase in the number of bits per unit of time forwarded to the correct destination minus any bits lost or retransmitted, and overheads for achieving security (an important consideration for MANETs). The effects of mobility on promiscuous monitoring (which can increase collusions) could be analyzed. Since, it uses a threshold mechanism, the effects of different threshold values for different mobility levels could usefully be assessed.

4.2.3   LiPaD: Lightweight Packet Drop Detection for Ad hoc Networks [2]

Anjum and Talpade have proposed a practical approach for detecting packet dropping attacks [2]. In this approach every node counts the packets that it receives and forwards and periodically reports these counts to a coordinator node. Promiscuous monitoring is not used since it depends on the link layer characteristics and the link layer encryption approach [2]. That's why every node is responsible for monitoring its packets in LiPaD. The algorithm executed in each node is very simple, which is good for resource-constrained nodes. On the other hand, the network bandwidth consumption can be huge, since every node sends reports of each flow defined by source IP and destination IP to the coordinator node. They suggest compressing and aggregating the reports of multiple flows instead of sending each flow in a packet. However, it still affects network traffic, especially in networks with hundreds nodes. There will be a heavy computation load on the coordinator node (which analyzes all nodes' reports). The coordinator node needs to be a powerful device and must also be secure as it can be the target of the attacks to disable the detection mechanism. For example, it can be target of DoS attacks (by overloading with reports).

Since the coordinator node analyzes the same flow through the reports from all nodes in the route, it can detect liar nodes that pass the wrong information about the statistics of their packets to the coordinator node [2]. If all the nodes on the route are cooperative and malicious, LiPaD cannot detect packet dropping attacks on this route. It is stated that LiPaD detects selective forwarding attacks. It determines a threshold value for permissible packet loss. The coordinator node also implements rewards and punishments depending on the behavior of the nodes.

It is assumed that IDS messages are encrypted and that nodes use a delivery mechanism for IDS messages to prevent them being dropped.

LiPaD is simulated on a network with 30 nodes using the OP-net simulator. It demonstrates that LiPaD detects malicious packet-dropping nodes even in the presence of non-malicious natural link-loss. On the other hand, the performance of LiPaD needs to be evaluated under high mobility and frequent link-loss. Evaluation of LiPaD performance under increased network traffic and node mobility is needed.

4.2.4   Intrusion Detection and Response for MANET [17]

Parker et al. extend snooping based methods to detect misbehavior across routing protocols. A node listens to all nodes in its transmission range, not just the packets forwarded by one of its next nodes (as in watchdog [15]). To detect a malicious node in this approach, it is stated that the node must be in the proximity of

a good node and act maliciously. It detects dropping and modification attacks which exceed the value in the threshold table for the particular attack class. However, a node moving out of range of the monitoring node before it forwards packets can be assumed to be carrying out a dropping attack. This issue will be addressed in future by the authors. Also, this approach cannot detect misrouting attacks, since it does not know the next hop of a packet that it monitors.

The intrusion detection protocol can give either a local or global response. In a local response, misbehaving nodes in the Bad Node table are isolated. It is emphasized that it is more effective in more dense networks, since more nodes detect intrusive behavior and prevent malicious nodes from utilizing network resources. In the global response, the maliciousness of node is determined by a vote by all nodes in a cluster. If the majority of the nodes agree that the node is intrusive an alert will be broadcasted. Voting is initiated by cluster heads. Cluster heads can be malicious but the likelihood of malicious nodes being elected as cluster heads is relatively small.

The approach is simulated using the GlomoSim simulator. The effect of node density (both malicious and normal nodes) on false positives is stressed. The response mechanism also affects the rate of false positives. It is claimed that global response reduces false positives due to rapid isolation of the intrusive nodes from the network.

5   Thoughts for Practitioners

Proposed IDSs for MANETs vary significantly, e.g. in terms of their detection technique, architecture, decision making and response mechanisms. All systems have advantages and disadvantages. On the other hand, every proposed system should be considered in its own context. For example, a system using a misuse-based technique is generally not suited to the very nature of MANETs, since attack databases cannot easily be updated without a central point. On the other hand, it can fit a military network which has a central location during peace-time.

Mobility, node capabilities, and network infrastructure are usually the main features examined for proposed MANET IDSs. For highly mobile networks IDSs using anomaly-detection techniques may suffer high false positive rates. Furthermore, an IDS architecture that is easy to set up should be preferred for these networks, *e.g.* IDS agents who collaborate with one-hop away nodes. Besides mobility, node capabilities should also be considered. Simple detection techniques can be more appropriate for nodes with limited resources. Trying to make the techniques simpler can be another approach. For instance, the approach in [27] uses a reduced feature set without significantly decreasing detection rate. Obvi-

ously, network infrastructure plays an important role in IDS selection. A hierarchical IDS architecture should be preferred to a multi-layered infrastructure, and distributed and cooperative architecture should be preferred for flat infrastructure [1]. Networks with central points make misuse-based and anomaly-based detection techniques easier to use by maintaining the signature database and user behaviors and analyzing them at these points. There may be an opportunity to use these techniques together in order to increase the effectiveness of the system.

The requirements of the system like high security, low bandwidth should also be satisfied by the IDS. For high secure networks, the security of IDS and IDS traffic should be considered. For example, use of mobile agents can be avoided. Moreover, IDSs that are able to detect both known and unknown attacks should be preferred. That security requirements of the system can change in different situations (e.g. peace time and war time requirements of a military network may differ) should be borne in mind while designing an IDS. For low bandwidth networks communication between IDS agents should be minimized.

None of the proposed systems are necessarily the best solution taking into account different applications. Every organization should choose the appropriate IDS for its network. Moreover, it can change the IDS according to its own requirements and characteristics. For example, it can change architecture of chosen IDS or put different intrusion detection techniques together. Therefore, defining requirements and determining characteristics of the network are very important factors in determining the most appropriate IDS solution.

6   Directions for Future Research

MANETs are a new type of distributed network whose properties are complex and ill-understood. Intrusion detection on these complex systems is still an immature research area. There are far fewer proposed IDSs for MANETs than for conventional networks. Researchers can focus on either introducing new IDSs to handle MANET specific features or can adapt existing systems. Hybrid approaches may also prove of significant use.

As stated earlier, IDS in MANETs poses special problems. Table 4.1 shows each proposed IDS reviewed in this chapter, identifying any novel contributions together with an indication of notable specific issues they do not address. In terms of these specific issues, none of the systems are complete. They usually emphasize just a few specific MANET concerns. The range of MANET issues should be considered during design to ensure effective and efficient intrusion detection suited to the environment at hand.

We make the following observations about the proposed IDSs:

- The systems generally cover restricted sets of attacks.
- The systems usually target a specific protocol.
- Some proposed IDS systems do not take into account mobility of the network.
- Inadequate acknowledgement is given to the resource constraints that many nodes are likely to be subject to, and to the likelihood of nodes with different capabilities.
- Several network architectures proposed do not sit well with the dynamic nature of MANETs.
- A more extensive evaluation of many of the systems would seem appropriate.

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

Appropriate weight should be attached to *mobility*, especially for anomaly-based IDSs. The false positive rate may be greatly affected by mobility level. The system should be aware of its mobility and current network topology. So, features having information about mobility should be included to the intrusion detection system being designed. How we get information about the mobility of the network and what features of the nodes or the network are related to mobility should be investigated.

Communication between IDS agents should be minimized due to constrained bandwidth of *wireless links*. This is one of the goals of the approach described in [24]. Other proposed systems usually do not pay attention to this issue. MANET Intrusion Detection Message Exchange Format (MIDMEF) is consistent with IDMEF and is defined in [22].

Since the nodes are the only data sources on the network, all nodes should contribute to IDS by carrying out local monitoring, detection and providing local data to other nodes when needed. However, nodes can have different computational capabilities. Moreover, some of them cannot be powerful enough for executing complex or large intrusion detection algorithms. There would appear to be insufficient research on the *limited resources* issue. Researchers can consider developing different algorithms for different nodes based on their resources and/or computa-

tional capabilities. Besides this, more intense detection algorithms can be applied in order to monitor critical nodes as proposed in [13].

Due to the *lack of clear line of defense* and *cooperativeness* features of MANETs, IDS agents can easily become the target of attackers. The proposed systems usually assume that IDS agents and communication between them are secure. Researchers should address the security of IDS. Detection of malicious IDS agents is an important research goal.

Testing IDS is an open research area for both MANETs and conventional networks. Some of the proposed systems in MANETs have not yet been implemented. Some of them are tested only on very small networks and with few attack scenarios. IDSs should be tested under different mobility levels and with different network topologies. Defining testing criteria for IDSs and preparing test datasets needs research.

7   Conclusions

MANETs are a new technology increasingly used in many applications. These networks are more vulnerable to attacks than wired networks. Since they have different characteristics, conventional security techniques are not directly applicable to them. Researchers currently focus on developing new prevention, detection and response mechanism for MANETs.

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

Abbreviations

DEMEM	distributed evidence-driven message exchanging ID model
DoS	denial of service
FSM	finite state machine
ID	intrusion detection
IDMEF	intrusion detection message exchange format
IDS	intrusion detection system
IETF	internet engineering task force
LiPaD	lightweight packet drop detection for ad hoc networks
MANET	mobile ad hoc network
MIDMEF	MANET intrusion detection exchange format
PCH	percentage of changes in the sum of hops all the routes
PCR	percentage of changed routes
RREP	route reply
RREQ	route request

Keywords

Intrusion: Any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource [6].

Intrusion Detection System (IDS): A system to detect the intrusions against computers and the network, and respond to these detected intrusions.

False Positives: Normal activities which are detected as intrusions by IDS.

Mobile Agent: A composition of computer software and data that is able to migrate from one computer to another autonomously and continue its execution on the destination computer [16].

Intrusion Detection Message Exchange Format (IDMEF): The format to define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems, and to the management systems which may need to interact with them [10].

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

Dropping Attacks: Attacks where selfish or malicious intermediate nodes drop packets that should be forwarded.

Eavesdropping Attacks: Attacks that monitor and find out information about the network. They not interfere with the network operation.

Random Waypoint Mobility Model: A mobility model used for the simulation of MANETs in which a node randomly selects a destination and moves in the direction of the destination with a speed chosen in a defined range.

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

Questions

1. How does node mobility affect IDSs in MANETs? How are wired network IDS techniques affected by mobility?
2. How do computational constraints impact on IDS techniques for MANETs? Are some techniques rendered difficult or infeasible?
3. How does the need to be power efficient impact on IDS for MANETs? Are some techniques rendered difficult or infeasible?
4. How do memory constraints impact on IDS techniques for MANETs? Are some techniques rendered difficult or infeasible?
5. A variety of architectures are possible for MANET IDS. Why might you wish to have a distributed and collaborative approach?
6. Why might you wish to have a hybrid IDS for a MANET (for example, one that uses both misuse based detection and also anomaly-based detection)?
7. What attacks on MANETs would be detectable by autonomous systems running on individual nodes (i.e. with no collaboration)?
8. What are the advantages of a collaborative approach to IDS in MANETs? What overheads are incurred by such approaches?
9. How do proposed IDSs for MANETs respond to detected intrusions? Discuss the need for different response mechanisms in different applications of MANETs.
10. What techniques are used for detecting misbehaving nodes in MANETs? How do they respond to these misbehaving nodes?

Answers

1. Since nodes move arbitrarily, a fixed IDS architecture (as is the case in wired networks) cannot be assumed in MANETs. The IDS architecture changes due to mobility in a network (e.g. roles may need to be reassigned, different cluster heads determined etc.) and construction of the IDS architecture can be costly in high mobile networks. Moreover, IDS agents can become disconnected due to link breakages, have partial data, and so effectiveness of the IDS may decrease since the consequences of mobility may become confused with the symptoms of certain types of attack.

   Because of mobility, some intrusion detection techniques may not be as effective as in wired networks. For instance, anomaly-based detection may not differentiate anomalous events from normal events in a high mobility network easily.

2. Each node on a MANET may not be able to do intensive monitoring due to computational constraints. That's why some of the proposed systems take into account nodes' different computational capacities. For example, powerful nodes may be used for high computational jobs like mining detection rules, as in [18]. On the other hand, some proposed systems do not differentiate nodes based on their computational capacities, and so for the less capable nodes IDS may incur a disproportionately high computational cost [7].

3. Nodes in MANETs generally use battery power and have different capacities. Intrusion detection can be assigned to the nodes based on their energy as in [12]. Power consumption may be affected by the complexity or regularity of processing incurred via IDS operation. Also, IDS communication overheads nay be very relevant since wireless communication is generally power hungry. As the resources available to nodes change, e.g. when power begins to run low on some nodes, reconfiguration may be needed (with less power constrained nodes taking on more of the burden). Of course, the reliance on battery power may also make a node susceptible to attack by means such as sleep deprivation attacks.

4. Effectiveness of IDS techniques can be affected by nodes' memory capacities. For example, some memory-constrained nodes may not be able to store and analyze the alarms from other nodes and so reduce effectiveness of the IDS. Limited memory may make approaches that store packets to subsequently check their forwarding difficult and attack signature databases may not be storable on at some nodes.

5. MANETs do not have any entry points such as routers, gateways, etc which are typically present in wired networks and which can be used to monitor all network traffic that pass through them. A MANET node can see only a portion of a network: the packets it sends or receives, possible together with other packets within its radio range. While some attacks can be detected locally by each node, detection of some attacks (such as network scans, distributed attacks) need to obtain global data from other nodes in MANETs. For example, routing protocols are usually cooperative in MANETs and attacks against routing protocols can affect many nodes on the network. These attacks can be detected collaboratively by the affected nodes. Moreover, a local response to a malicious node may have very limited effect. A coordinated collaborative response will be much more effective.

6. Different intrusion detection techniques have different advantages and disadvantages. For example, when the anomaly-based detection techniques can detect previously unknown attacks to the network, they can have higher false positive rates compared to misuse-based detection techniques. By using hybrid IDS, researchers aim to take advantage of the best of the individual techniques and so produce a more effective and efficient IDS.

7. Attacks which have a clear affect on a node can be detected easily by that node. However some attacks such as distributed attacks can be detected by analyzing network data. For example if intrusion detection is carried out locally on the network, *network scan* can seem normal to each node. Detecting this will likely require distributed and collaborative intrusion detection on MANETs.

8. IDS on MANETs may need to be distributed and cooperative. To detect some kind of attacks, nodes can need data from other nodes. When they observe a probability of an intrusion, they can initiate a collaborative detection by sending alerts to other nodes and make decisions collaboratively. It increases effectiveness of the IDS. On the other hand, it increases the communication and computation overhead such as processing many alerts from other nodes.

9. Some of the proposed IDSs simply raise alarms; they do not identify attackers on a network. Others give active responses to intrusions. For instance, removing the routes including malicious node(s) is a kind of response that mitigates the effects of malicious nodes on the network. There are also responses that exert control over the attacking system such as excluding attackers from the network by not giving services to them. Such approaches may be essential for some applications such as military applications.

10. Techniques that use promiscuous monitoring are usually proposed for detecting misbehaving nodes [15][4][17]. In this way, the packets sent to a node are monitored to detect if this node forwards the packets properly or not. Monitoring all packets' flows at a central point is another method proposed to detect misbehaving nodes [2]. As a response to the detection of misbehaving nodes, reputation systems which punish misbehaving nodes are generally used.

References

1. Anantvalee T, Wu J (2006) A Survey on Intrusion Detection in Mobile Ad Hoc Networks. Wirel/Mobil Netw Secur, Springer:170-196
2. Anjum F, Talpade R (2004) LiPaD: Lightweight Packet Drop Detection for Ad hoc Networks. In Proc of IEEE Veh Technol Conf (VTC) 2:1233-1237
3. Axelsson S (2000) Intrusion Detection Systems: A Survey and Taxonomy. Technical Report No 99-15, Dept. of Computer Engineering, Chalmers University of Technology
4. Buchegger S, Le Boudec J (2002) Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Network. In Proc of 10th Euromicro Workshop on Parallel, Distrib and Netw-based Process:403-410
5. Guha R, Kachirski O et al (2002) Case-Based Agents for Packet-Level Intrusion Detection in Ad Hoc Networks. In Proc of 17th Int Symp on Comput & Inf Sci:315-230
6. Heady R, Luger G, Maccabe A, Servilla M (1990) The architecture of a network level intrusion detection system. Technical Report, Computer Science Department, University of New Mexico
7. Huang Y, Fan W et al (2003) Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies. In Proc of 23rd IEEE Int Conf on Distrib Comput Syst (ICDCS):478-487
8. Huang Y, Lee W (2003) A Cooperative Intrusion Detection System for Ad Hoc Networks. In Proc of the 1st ACM Workshop on Secur of Ad Hoc and Sens Netw:135-147
9. Huang Y, Lee W (2004) Attack Analysis and Detection for Ad Hoc Routing Protocols. In Proc of Recent Adv in Intrusion Detect LNCS 3224:125-145
10. Intrusion Detection Message Exchange Format (IDMEF), http://www.ietf.org/html.charters/OLD/idwg-charter.html Accessed 30 August 2007
11. Jacquet P, Muhlethaler P et al (2001) Optimized Link State Routing Protocol for Ad Hoc Networks. In Proc of IEEE INMIC:62-68
12. Kachirski O, Guha R (2003) Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks. In Proc of the 36th IEEE Int Conf on Syst Sci (HICSS)
13. Karygiannis A, Antonakakis E et al (2006) Detecting Critical Nodes for MANET Intrusion Detection Systems. In Proc. of 2nd Int. Workshop on Secur, Priv and Trust in Pervasive and Ubiquitous Comput (SecPer)
14. Lundin E, Jonsson E. (2002) Survey of Intrusion Detection Research. Technical report 02-04, Dept. of Computer Engineering, Chalmers University of Technology
15. Marti S, Giuli TJ et al (2000) Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks. In Proc of 6th ACM Int Conf on Mobil Comput and Netw (MobiCom):255-265

16. Mobile Agent, http://en.wikipedia.org/wiki/Mobile_agent Accessed 30 August 2007

17. Parker J, Undercoffer J et al (2004) On Intrusion Detection and Response for Mobile Ad Hoc Networks. In Proc of 23rd IEEE Int Perform Comput and Commun Conf

18. Smith AB (2001) An Examination of an Intrusion Detection Architecture for Wireless Ad Hoc Networks. In Proc of 5th Natl Colloq for Inf Syst Secur Educ

19. Snort, http://www.snort.org/ Accessed 30 August 2007

20. Sterne D, Balasubramanyam P et al (2005) A General Cooperative Intrusion Detection Architecture for MANETs. In Proc of the 3rd IEEE IWIA

21. Sun B (2004) Intrusion Detection in Mobile Ad Hoc Networks. PhD Thesis, Computer Science, Texas A&M University

22. Sun B, Wu K et al (2006) Zone-Based Intrusion Detection System for Mobile Ad Hoc Networks. Int J of Ad Hoc and Sens Wirel Netw 2:3

23. Tseng CH, Song T et al (2005) A Specification-Based Intrusion Detection Model for OLSR. In Proc of the 8th Int Symp on Recent Adv in Intrusion Detect LNCS 3858: 330-350

24. Tseng CH, Wang SH (2006) DEMEM: Distributed Evidence Driven Message Exchange Intrusion Detection Model for MANET. In Proc of the 9th Int Symp on Recent Adv in Intrusion Detect LNCS 4219:249-271

25. Tseng C-Y, Balasubramayan P et al (2003) A Specification-Based Intrusion Detection System for AODV. In Proc of the ACM Workshop on Secur in Ad Hoc and Sens Netw (SASN)

26. Uppuluri P, Sekar R (2001) Experiences with Specification-based Intrusion Detection. In Proc of the 4th Int Symp on Recent Adv in Intrusion Detect LNCS 2212: 172-189

27. Wang X, Lin T et al (2005) Feature Selection in Intrusion Detection System over Mobile Ad-hoc Network. Technical Report, Department of Computer Science, Iowa State University

28. Zhang Y, Lee W (2000), Intrusion Detection in Wireless Ad Hoc Networks. In Proc of the 6th Int Conf on Mobil Comput and Netw (MobiCom): 275-283

29. Zhang Y, Lee W (2003) Intrusion Detection Techniques for Mobile Wireless Networks. Wirel Netw : 545-556