A Survey on Some Currently Existing Intrusion Detection Systems for Mobile Ad Hoc Networks

Mnar Saeed Alnaghes
Department of Electrical and Computer Engineering
University of Victoria
Victoria, Canada
manar@uvic.ca

Fayez Gebali
Department of Electrical and Computer Engineering
University of Victoria
Victoria, Canada
fayez@uvic.ca

Abstract
Mobile Ad-Hoc Network (MANET) is one of the most promising technologies that have applications in military, environmental, space exploration and forestry industry areas. This type of network has attractive features such as its low transmission power to conserve energy, increase throughput, and reduce delay. However, it suffers from many constraints, including limited resources, and the use of insecure wireless communication channels. Due to the lack of defense, the security of these networks is a worthy concern, particularly for the applications where confidentiality has prime importance. Thus, any kind of intrusions should be detected before attackers can harm the network in order to operate MANET in a secure way. In this article, we present a survey of the state-of-the-art in Intrusion Detection Systems (IDSs) that are proposed for MANETs. This is followed by a comparison of each scheme along with their advantages and disadvantages. This survey is concluded by highlighting open research issues in the field.

Keywords Security, Network security, Mobile Ad-Hoc Network, MANET, Intrusion Detection System, IDS.

1 Introduction
Traditional wired networks are relatively more secure compared to wireless networks. Wireless ad hoc network integrates with multiple wireless systems such as wireless local area network (WLAN), wireless personal area network (WPAN), and wireless metropolitan area network (MAN), in order to improve its performance. It also provides communication between various devices (nodes) using a shared wireless channel. However, unlike more conventional wireless networks, nodes in ad-hoc networks communicate without the assistance of a fixed network infrastructure. It uses collaborative store-and-forward strategy to provide connectivity beyond transmit/receive range. Nodes within one another’s radio range can communicate through wireless links, and, often these nodes are mobile, they dynamically change their locations. This type of networks is suited for situations where rapid network coverage is required or it is highly costly to deploy and manage a network infrastructure.

Wireless ad-hoc networks are vulnerable to threats because the wireless medium is insecure, and, the domain of attacks is transient in nature as are the wireless networks themselves. Thus, it needs efficient routing protocol and design particular detection and strategies prevention techniques in order to secure this network. For the importance of securing such a network, there has been much work in intrusion detection system for traditional wired networks, but, it is a bit different for Ad hoc networks. The key reason is the differences of architectural features, most notably the lack of a fixed infrastructure. The lack of certified or trusted nodes and lack of centralized audit points, such as routers, switches, and gateways, makes it difficult to collect audit data for the entire network. Intrusion detection system, which monitors system activities and detects intrusions, must work with localized partial information. An IDS is generally used to complement other security mechanisms, and, it is a complex and difficult task due to Ad-hoc network’s features.

The rest of the paper is organized as follows: In Section II, an introduction of IDSs is reviewed. Section III includes a brief discussion of IDSs proposed for MANETs, followed by their classifications in Section IV. Then, a detailed literature review on MANETs IDSs is provided along with comments on their prominent and lacking features. Finally, this paper is concluded by comparing existing approaches.

2 Intrusion Detection System In General
Intrusion is any attempts to compromise the integrity, confidentiality, or availability of a resource and an intrusion detection system (IDS) is a system which
detects such intrusions [2]. There are three main components of an IDS. First, data collection which is responsible for collecting data and preprocessing its tasks; data storage, data format, and sending data to the detection module. IDSs are able to use different sources for data as inputs to the system such as system logs, network packets, etc. [3]. Second, detection, at this level, data is analyzed to detect intrusions. Third, response where the action will be taken after receiving indications of detected intrusions from detection component.

There are three basic intrusion detection techniques as discussed in the following subsection [18]:

2.1 Anomaly-based intrusion detection:

The parameters of the system such as CPU usage for programs are profiled. Intrusions are recognized as variations from the normal behaviors. The challenge is to define the normal behaviors. A block diagram of a typical anomaly detection system is shown in Figure 1. After monitoring system activity and profiling it, the patterns are saved in the system profile where they can be updated. The overhead of updating several system profile metrics make anomaly IDS computationally expensive. Additionally, false positive can be high in anomaly-based detection. On the other hand, it is capable of detecting previously unknown attacks.

![Figure 1: a typical anomaly detection system](image)

2.2 The Misuse-based or signature-based intrusion detection:

Known attack signatures are compared with current system activities. This system is efficient and has a low false positive rate thus it is preferred by commercial IDSs. However, Misuse-based intrusion detection cannot detect new attacks. This needs continuous updating for new types of attacks. A block diagram of a typical misuse detection system is shown in Figure 2 below. Detection rules are generated based on specific attack’s signatures. These rules are saved and updated in the system profile. The main issues here are how to write a signature that encompasses all possible variations of the pertinent attack, and how to write signatures that do not also match non-intrusive activities.

![Figure 2: a typical misuse detection system](image)

2.3 Specification-based intrusion detection:

There is a specified set of constraints on a program or a protocol, and, intrusions are detected as runtime violations of these specifications. This approach combines the strengths of anomaly-based and misuse-based detection techniques. Thus, it can detect known and unknown attacks with a lower false positive rate. It can discover a new attack that does not follow the system specifications. Further, specification-based intrusion detection does not lead to false alarms when the program or protocol has unusual but legitimate actions, since it uses the legitimate behaviors of the program or protocol [4]. Also, this approach cannot detect some kind of attacks such as Denial of Service (DoS) attacks since these do not violate program specifications directly.

3 Intrusion Detection System for MANET

A fairly usable analysis of MANET’s risks by identifying assets, threats, and vulnerabilities will be helpful to provide good security solutions [7]. Besides, MANET’s features should be considered when a new IDS is being designed for this network. Without a centralized authority, the algorithms used for intrusion detection must be distributed in nature, yet it must be kept in mind that attacks may be made from nodes inside the network, this means that node which is participating in a collaborative intrusion detection algorithm may be a malevolent node. Further, nodes of a mobile ad hoc network can only see the packets that they send or receive together within their radio range. Furthermore, because of the wireless ad hoc network is distributed and cooperative, the intrusion detection system in MANET should also be distributed and cooperative, which shows certain difficulties. The highly dynamic feature of this network makes intrusion detection system’s traditional techniques become unreliable. The IDS needs a scalable architecture to collect sufficient evidences to detect the attacks effectively.

Mobile nodes typically consume battery power, and, they have different capacities. These devices are varied, and their computational and storage capacities vary too. This variety affects the efficiency of IDS agents they support. For instance, nodes may drop packets to conserve resources causing difficulties in distinguishing failed or selfish nodes from attacker. Thus, it is very important for a detection algorithm to be considered the limited resources problem. Besides, Ad Hoc Networks usually have highly cooperative routing protocols which makes them the target of new attacks. MANET,s have more constrained bandwidth, and, the link breakages are common. An IDS agent needs to communicate with other IDS agents with a view to gain data or alerts and needs to be aware of wireless links. Due to the heavy traffic of intrusion detection systems, congestion could be caused. Intrusion detection systems agents will need to decrease their data transfers [1].
4 Intrusion Detection System Classification

The existing IDS architectures for MANET consider under three basic categories [9]:

(a) Stand-alone architecture which uses an engine installed at each node utilizing only the node’s local audit data. This fact limits the Stand-alone IDS in terms of detection accuracy and the type of attacks that it could detect [14].

(b) Cooperative architecture which processes each host’s audit data locally. It is similar to standalone architecture, but it also uses collaborative techniques to detect more accurately a large list of attacks. Thus, the majority of the most recent IDS for MANET are based on them and the Hierarchical architectures as well [14].

(c) Hierarchical architecture which is an extended version of the cooperative architectures [14]. This architectures reach to a multilayer approach by dividing the network into clusters. Specific nodes are selected as cluster-heads and undertake various responsibilities and roles in intrusion detection, which are different from those of the simple cluster members.

(d) Intrusion Detection System architecture with mobile agent which uses mobile agents that can move through large networks. It allows the distribution of the intrusion detection tasks. Each agent is assigned to do a specific task and then one or more agents are distributed into each node in the network.

5 Existing Intrusion Detection System for MANET

As it is clear, it is difficult to build a completely secure MANET system in spite of using a complex cryptographic technique or so-called secured routing protocols. Some of the existing IDS algorithms that have been introduced for MANETs are explained as follows:

5.1 Bayesian Game Approach IDS [6]

A game theoretic framework using a Bayesian formulation which can analyze the interactions between pairs of attacking and defending nodes was introduced in a flat Ad-hoc network. The achievable equilibrium strategies was investigated for the attacker and defender game in both static and dynamic scenarios. In these games, players try to maximize their payoff. The motivation behind the Bayesian game formulation is that generally an attacker/defender game is an incomplete information game where the defender is uncertain about the type of his opponent whether it’s a regular node or malicious. A Bayesian game formulation provides a framework for the defender to select his strategies based on his belief on the type of his opponent [13]. In the proposed static game, the defender always assume fixed prior probabilities about the types of his opponent throughout the entire game period. On the other hand, a more realistic model, the dynamic game, allows the defender to update his belief about his opponent’s type based on new observed actions and the game history. Additionally, a Bayesian hybrid detection approach in the dynamic game in which a lightweight monitoring system is used for the defender, as it shown in Figure 3, to estimate his opponent’s actions, and a heavyweight monitoring system acts as a last resort of defense. The simulation’s results show that by adding the very simple coarse-grained node-to-node analysis system in front of the association-rule analysis system will reduce the probability of false alarm for the overall equivalent IDS.

![Figure 3: The Bayesian hybrid detection framework](image)

5.2 Acknowledgment-Based Approach IDS[10]

The 2-ACK scheme forwards two hop acknowledgment packets in the opposite direction of the routing path. This approach is an add-on method for routing schemes to detect and mitigate the effect of such routing misbehavior. The 2-ACK transmission is carried out for every set of three nodes along with the path from the source to the destination. Figure 4 shows the operation of the 2ACK scheme, N1, N2, and N3 are three consecutive nodes along a route, S and D are the source and destination nodes. By acknowledging every data packet transmitted over every three successive nodes along the route, 2ACK is able to predict malicious links. This scheme overcomes several problems including ambiguous collisions, receiver collisions, and limited transmission powers comparing to some other schemes. The simulation shows that the 2ACK scheme maintains up to 91 percent packet delivery ratio even when there are 40 percent misbehaving nodes in the MANETs. The regular Dynamic Source Routing (DSR) scheme is able only to offer a packet delivery ratio of 40 percent.

![Figure 4: 2-ACK Scheme](image)
5.3 Ex-Watchdog Approach IDS [11]

The proposed intrusion detection system is an extension of Watchdog so the used system is the Route-guard as the response system, and the IDS function is also detecting intrusion from malicious nodes and reports this information to the response system. The authors declared this technique in view to overcome one of the weaknesses in watchdog which is the false misbehaviour node. In the simulation, the metrics of throughput and overhead were used in order to evaluate the Ex-Watchdog performance with some malicious nodes that falsely report other nodes as misbehaving. The benefit of their technique is that it decreases the overhead comparing with Watchdog, however, it does not increase the throughput obviously.

5.4 Classification-Based Approach IDS [12]

In this paper, intrusion detection system models using supervised classification algorithms are presented. The used classification algorithms are Multi-Layer Perceptron (MLP), the linear classifier, the Gaussian Mixture Model (GMM), the Naive Bayes and Support Vector Machines (SVM). They assume that the IDS architecture composed of multiple local IDS agents that are responsible for detecting possible intrusions locally. They used features from the network layer and evaluated the performance of these algorithms for the detection of four serious attacks in MANETs, the Black hole, Forging, Packet Dropping and Flooding attack. In results, the easiest attack to be detected is the Flooding attack, while the most difficult attack to detect is the Packet Dropping attack. The most efficient classifier for detecting all four types of attacks simultaneously is the SVM classifier for multiclass classification although the MLP classifier presents a satisfying Detection Rate (DR) and also a quite high False Alarm (FA) rate. Further, the highest the number of malicious node in the network the easiest to detect intrusions.

5.5 Zone-Based Approach IDS [8]

The proposed intrusion detection system is a non-overlapping zone-based framework. The use of different detection techniques is pliable in their IDS agents, but technically they only use Markov chain anomaly detection in their research. Based on geographic partitioning, the network is divided into zones in order to save bandwidth. The performance is improved by obtaining data from many nodes. An intra-zone node is a regular node in a zone, and an inter-zone node is a gateway node which work as a bridge to other zones. Each node in the zone is responsible for local detection and sending alerts to the inter-zone nodes. The alert is generated and sent by inter-zone nodes based on the combined information received. The detection performance of the algorithm could be decreased with the increasing of the number of attackers. From simulation, the local anomaly detection model works well in low mobility environment. However, it is shown that the anomaly-based detection performs poorly because the data are unstable under high mobility. The benefits of the aggregation algorithm generally are lower false positive and higher detection rate than local IDS achieves. One of the contributions is MANET Intrusion Detection Message Exchange Format (MIDM EF) which declares information exchange's format between IDS agents.


This paper introduces the first application of specification-based detection technique for MANETs. It is assumed that all nodes are covered using network monitors which have nodes IP addresses. All these monitors and their messages are secure, and, MAC addresses are not rigged. Each Network Monitor uses finite state machines as operations specifications of AODV in order to correct AODV routing behavior and distributed network monitors for detecting run-time violation. All RREQ and RREP messages in the range of the network monitors are monitored in request reply flows. The algorithm uses a tree structure of data which can detect most of known and unknown attacks against routing protocols efficiently in real time and with minimum overhead since these attacks have clearly defined specifications. However, network services can be affected by dropping certain broadcast messages if this action is happened at a critical point. Also, according to MANET characteristics, nodes can independently join and leave network and frequently move, it is non-pragmatic to assume that network monitors can cover all nodes and have all their IP and MAC addresses which are non-forged.

5.7 Fuzzy Logic Approach IDS [15]

The proposed intrusion detection system uses fuzzy logic, this fuzzy logic works to handle imprecise information in order to help the IDS to detect malicious behavior and identify the attacks. Fuzzy logic is a computational paradigm that provides a mathematical tool to deal with the uncertainty and the imprecision which is involved in human reasoning. Fuzzy logic's features, which is the capability to express knowledge in a linguistic way, makes fuzzy logic-based systems attractive for applications like medical diagnosis. After detecting intrusion in MANET, fuzzy Logic approach is used for three types of symptoms. First symptom, when the number of packets dropped is greater than threshold. Second symptom, when the number of packets dropped is greater than threshold and the number of packets dropped for the particular destination is greater than another threshold value which called DestThreshold. Third symptom, when the number of packets drop is greater than threshold and the number of packets drop for the particular source is greater than DestThreshold. The main aim behind this method is to detect the malicious nodes locally at each node. Thus, each node has its local IDS which monitors the nodes traffic. From simulation results, the output of a fuzzy-based IDS could be a more accurate input since the output of an IDS is normally used as input to a routing protocol for isolating malicious nodes from the network. Additionally, analyzing the level of intrusion in the network using the fuzzy logic is more accurate than when it is not used.
5.8 Elliptic Curve Cryptography-Based Enhanced Adaptive Acknowledgment IDS [16]

An acknowledgment-based IDS named Elliptic Curve Cryptography Based Enhanced Adaptive Acknowledgment (ECC-EAAC) is proposed. It demonstrates higher rates for malicious behavior detection in certain situations while does not greatly affect the network performances. It has a strong and light-weight Intrusion detection mechanism called EAACK which requires less hardware cost. Acknowledgment (ACK), secure ACK (S-ACK) and misbehavior report authentication (MRA) are the three major parts of EAACK. All the three parts rely on acknowledgment packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. ACK is basically an end-to-end acknowledgment scheme, which acts as a part of the hybrid scheme in EAACK in order to reduce network overhead when no network misbehavior is detected. If the receiver node does not send the ACK within predefined period, then ACK assumes malicious may attend, as a consequence, it switch to S-ACK part to detect malicious nodes. In S-ACK, for every three successive nodes in the route, the third one is required to send an S-ACK acknowledgment packet to the first node. The objective of starting S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. When a malicious node is found, then MRA part suggests alternate path to the destination. The source node will not immediately trusts the misbehavior report because EAACK requires the source node to switch to MRA node and confirm this misbehavior report. This is a vital step to detect false misbehavior report in their proposed scheme. An improved Cryptographic technique was used in view to improve intrusion detection results in MANET, ensure the secure communication of packets, increase security and convenience, and provide digital signatures that cannot be forged. After simulation, the results show positive performances which make this approach suitable to be implemented in MANETs.

5.9 Cross Layer-Based Approach for IDS [17]

In this paper, a cross layer-based detection system is presented to detect the black-hole attack in MANETs. This cross layer technique incorporating IDS leads to an escalating detection rate in the number of malicious behavior of nodes increasing the true positive and reducing false positives in the MANET. In this approach, the decision to detect malicious nodes is made by the network layer, MAC layer and physical layer on the basis of the parameters passed by the physical and the link layer to the network layer using cross layer design, and then the best path is selected among the various paths between the source node and the destination node. Each layers is designed separately with the services it implements, with the help of the well-defined interfaces through which these layers communicate with each other. In the layered architecture, UDP packets are sent to and from the network layer to the application layer over the transport layer. This communication causes some delay which decreases the overall network performance. If it is possible to design a direct application layer- network layer interface bypassing the transport layer, the end to end delay is saved and hence the overall network performance is improved. Performance can be optimized by using the available information across many protocol layers. One of the vital methods of cross layer design is sharing of the database between the different layers hence the parameters could be available at different layers of the protocol stack. The nodes were simulated with random mobility model, and, a black hole attack was simulated with malicious nodes. As a simulation result, the throughput, which is the number of successfully delivered packets from the source to destination, and packet delivery ratio which Ratio, which is the parameter which tells how successfully the packets are delivered to the destination, of the proposed technique shows better results than that of the standard AODV under attack.

6 Comparison of Existing IDSs’ approaches

We have followed a critical analytical comparison to compare the discussed intrusion detection techniques since they have different routing protocols. Unluckily, these approaches are not entirely ideal. However, Specification-based Approach IDS [4] would be considered in terms of reducing the overhead rate and covering many of different routing attacks. The findings are summarized in Table 1.

7 Conclusion

Since mobile ad hoc networks has become widely used, the importance of securing these network has increased. Due to prevention techniques alone are not sufficient and new intrusions continually attack such a network, an IDS is a necessary component of a security system. IDS is basically used to detect possible violations of a security policy by monitoring system activities. The IDS perform some tasks which are monitoring the network, analyzing collected data, identifying intruders, generating alarms, and tracking intruders to prevent such attacks in the future. All these functionalities are in order to identify either an outside intrusion or an inside intrusion.

Designing a powerful IDS that support the network performance is in fact a complicated task because of the MANETs Features. In this survey paper, we present brief details of various available intrusion detection techniques. The basic idea behind all of the above discussed IDSs is comparing their techniques in order to cope up with the limitations of IDSs. It is noticed that almost all intrusion detection systems are distributed and have a cooperative architecture. And, the specification detection is more powerful among the various detection methods used. However, IDS itself may be attacked and the study of the defense to such attacks should also be explored.
| No. | IDS Method                                      | Architecture              | Routing Protocol | Type of Attacks                                      | Technique                           | Protocol | Overhead | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type | Overhead Type |
|-----|-----------------------------------------------|---------------------------|------------------|------------------------------------------------------|-------------------------------------|----------|----------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|
| 1   | Bayesian Game Approach [6]                    | Cooperative and Hierarchical | Identified       | Sneak Attack                                        | Game Theoretic Scheme               | AODV     | YES      | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            |
| 2   | Acknowledgment-Based Approach [10]            | Cooperative               | Identified       | Selfish, Sneak, and Routing Disruption              | Cooperative Network Monitors        | AODV     | YES      | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            |
| 4   | Classification Based Approach [12]             | Cooperative               | Identified       | Selfish, Sneak, and Routing Disruption              | Cooperative Monitor                | AODV     | YES      | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            |
| 5   | Zone Based Approach [8]                       | Cooperative               | Identified       | Selfish, Sneak, and Routing Disruption              | Cooperative Monitor                | AODV     | YES      | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            |
| 7   | Fuzzy Logic Approach [15]                     | Cooperative               | Identified       | Selfish, Sneak, and Routing Disruption              | Cooperative Monitor                | AODV     | YES      | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            |
| 8   | Elliptic Curve Cryptography Based Approach [16] | Cooperative               | Identified       | Selfish, Sneak, and Routing Disruption              | Cooperative Monitor                | AODV     | YES      | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            |
| 9   | Cross Layer Based Approach [17]                | Hierarchical              | Identified       | Selfish, Sneak, and Routing Disruption              | Cooperative Monitor                | AODV     | YES      | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            | YES            |

Table 1: Intrusion Detection Systems’ Comparison
References