# Intrusion Detection Techniques in Mobile Ad hoc Networks

G.L.Anand Babu, G.Sekhar Reddy, Swathi Agarwal

*Department of Information Technology, CVSR School of Engineering, Anurag Group of Institutions, Hyderabad, AndhraPradesh, India.*

***Abstract*— Mobile ad hoc networks and wireless sensor networks have promised a wide variety of applications. However, they are often deployed in potentially adverse or even hostile environments. Therefore, they cannot be readily deployed without first addressing security challenges. Intrusion detection systems provide a necessary layer of in-depth protection for wired networks. However, relatively little research has been performed about intrusion detection in the areas of mobile ad hoc networks and wireless sensor networks. In this article, first we briefly introduce mobile ad hoc networks and wireless sensor networks and their security concerns. Then, we focus on their intrusion detection capabilities. Specifically, we present the challenge of constructing intrusion detection systems for mobile ad hoc networks, survey the existing intrusion detection techniques, and indicate important future research directions.**

***Keywords*— MANETs, Intrusion detection system**.

## I. INTRODUCTION

The lack of fixed infrastructure and centralized authority makes a MANET suitable for a broad range of applications in both military and civilian environments. For example, a MANET could be deployed quickly for military communications in the battlefield. A MANET also could be deployed quickly in scenarios such as a meeting room, a city transportation wireless network, for fire fighting, and so on. To form such a cooperative and self-configurable network, every mobile host should be a friendly node and willing to relay messages for others. In the original design of a MANET, global trustworthiness in nodes within the whole network is a fundamental security assumption.

Recent progress in wireless communications and micro electro mechanical systems (MEMS) technology has made it feasible to build miniature wireless sensor nodes that integrate sensing, data processing, and communicating capabilities. These miniature wireless sensor nodes can be extremely small, as tiny as a cubic centimeter. Compared with conventional computers, the low-cost, battery-powered, sensor nodes have a limited energy supply, stringent processing and communications capabilities, and memory is scarce.

Despite the wide variety of potential applications, MANETs and WSNs often are deployed in adverse or even hostile environments. Therefore, they cannot be readily deployed without first addressing security challenges. Due to the features of an open medium, the low degree of physical security of mobile nodes, a dynamic topology, a limited power supply, and the absence of a central management point, MANETs are more vulnerable to malicious attacks than traditional wired networks are.

## II. Intrusion Detection System (IDS)

Many historical events have shown that intrusion prevention techniques alone, such as encryption and authentication, which are usually a first line of defense, are not sufficient. As the system become more complex, there are also more weaknesses, which lead to more security problems. Intrusion detection can be used as a second wall of defense to protect the network from such problems. If the intrusion is detected, a response can be initiated to prevent or minimize damage to the system.

Intrusion detection can be classified based on audit data as either host-based or network-based. A network-based IDS captures and analyzes packets from network traffic while a host-based IDS uses operating system or application logs in its analysis. Based on detection techniques, IDS can also be classified into three categories as follows:

- **Anomaly detection systems:** The normal profiles (or normal behaviors) of users are kept in the system. The system compares the captured data with these profiles, and then treats any activity that deviates from the baseline as a possible intrusion by informing system administrators or initializing a proper response.
- **Misuse detection systems:** The system keeps patterns (or signatures) of known attacks and uses them to compare with the captured data. Any matched pattern is treated as an intrusion. Like a virus detection system, it cannot detect new kinds of attacks.
- **Specification-based detection:** The system defines a set of constraints that describe the correct operation of a program or protocol. Then, it monitors the execution of the program with respect to the defined constraints.

## III. An Architecture for Intrusion Detection in MANETs

Intrusion detection and response systems should be both distributed and cooperative to suite the needs of mobile ad-hoc networks. In our proposed architecture (**Figure 1.1**), every node in the mobile ad-hoc network participates in intrusion detection and response. Each node is responsible for detecting signs of intrusion locally and independently, but neighboring nodes can collaboratively investigate in a broader range.

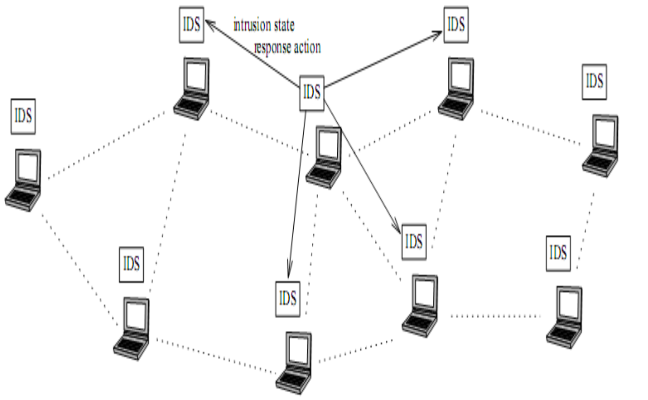

Figure 1.1: The IDS Architecture for Wireless Ad-Hoc Network

## IV. INTRUSION DETECTION TECHNIQUES

An intrusion is defined as a set of actions that compromises confidentiality, availability, and integrity of a system. Intrusion detection is a security technology that attempts to identify those who are trying to break into and misuse a system without authorization and those who have legitimate access to the system but are abusing their privileges. The system can be a host computer, network equipment, a firewall, a router, a corporate network, or any information system being monitored by an intrusion detection system.

An IDS dynamically monitors a system and users' actions in the system to detect intrusions. Because an information system can suffer from various kinds of security vulnerabilities, it is both technically difficult and economically costly to build and maintain a system that is not susceptible to attacks. Experience teaches us never to rely on a single defensive technique. An IDS, by analyzing the system and users' operations, in search of undesirable and suspicious activities, may effectively monitor and protect against threats.

Generally, there are two types of intrusion detection: misuse-based detection and anomaly based detection [1]. A misuse-based detection technique encodes known attack signatures and system vulnerabilities and stores them in a database. If deployed IDS finds a match between current activities and signatures, an alarm is generated. Misuse detection techniques are not effective to detect novel attacks because of the lack of corresponding signatures. An anomaly-based detection technique creates normal profiles of system states or user behaviors and compares them with current activities. If a significant deviation is observed, the IDS raises an alarm. Anomaly detection can detect unknown attacks. However, normal profiles are usually very difficult to build. For example, in a MANET, mobility-induced dynamics make it challenging to distinguish between normalcy and anomaly. It is, therefore, more challenging to distinguish between false alarms and real intrusions. The capability to establish normal profiles is crucial in designing an efficient, anomaly based IDS. As a promising alternative, specification based detection techniques combine the advantages of misuse detection and anomaly detection by using manually developed specifications to characterize legitimate system behaviors. Specification-based detection approaches are similar to anomaly detection techniques in that both of them detect attacks as deviations from a normal profile. However, specification-based detection approaches are based on manually developed specifications, thus avoiding the high rate of false alarms. However, the downside is that the development of detailed specifications can be time-consuming.

## V. EXISTING RESEARCH

Intrusion detection can be formulated as a pattern classification problem, in which classifiers are designed to classify observed activities as normal or intrusive. In [2], based on an identified feature set, Zhang et al. apply two well known classifiers, RIPPER and support vector machine (SVM) Light, to construct a suite of anomaly detection models. RIPPER is a decision-tree equivalent classifier for rule induction. By separating provided data into appropriate classes, RIPPER can compute rules for the system. SVM Light can produce a more accurate classifier when the data that is provided cannot be represented by the given set of features.

Because of the importance of feature selection in IDS research, Huang et al. [3] further introduce a new learning-based method to utilize cross-feature analysis to capture inter-feature correlation patterns. Suppose that L features, f1, f2, …, fL, are identified, where each fi denotes one feature characterizing either topology or route activities. The classification problem to be solved is to create a set of classification model Ci : {f1, …, fi–1, fi+1, …, fL} → fi from the training process. Here one feature fi is chosen as the target to classify. Then, the classification model Ci can be used to identify temporal correlation between one feature and all of the other features. The prediction of Ci is very likely in normal situations. However, when there are malicious events, the prediction of Ci becomes very unlikely. Based on this, normal events and abnormal events can be distinguished.

Local detection alone is not sufficient because of the distributed nature of a MANET. Huang and Lee [4] further elaborate on mechanisms in which one node can collaborate with its neighbors and initiate a detection process over a broader range. This can provide not only more accurate detection results, but also more information in terms of attack types and sources. After fairly and periodically electing a monitoring node in a cluster of neighboring MANET mobiles, a cluster-based detection scheme is proposed. Each node maintains a finite state machine, with possible states of Initial, Clique, Done, and Lost . Based on the finite state machine, a set of protocols, including a clique computation protocol, a cluster-head computation protocol, a cluster-valid assertion protocol, and a cluster recovery protocol are detailed. Resource constraint problems faced by a MANET are addressed when these protocols are designed.

Based on a specification-based approach to describe major functionality of Ad hoc On
Demand Distance Vector (AODV) routing algorithms at data layers and routing layers, Huang and Lee [6] propose an extended finite state automaton (EFSA), where transitions and states can carry a finite set of parameters. In this way, the proposed EFSA can detect invalid state violations, incorrect transition violations, and unexpected action violations. The construction of EFSA can lead naturally to a specification-based approach. Based on a set of statistical features, statistic learning algorithms are then adopted to detect abnormal patterns from anomalous basic events.

Based on Dynamic Source Routing (DSR) protocols, Marti et al. [5] propose to install extra facilities, watchdog and pathrater, to identify and respond to routing misbehaviors in a MANET. In data transmission processes, a node may misbehave by agreeing to forward packets and then fail to do so. Suppose a path exists from a source node S to a destination node D through intermediate nodes A, B, and C. Node A can overhear node B's transmissions. Node A cannot transmit directly to node C and must go through node B. To detect whether node B is misbehaving, node A can maintain a buffer of packets recently sent by node A. Node A then compares each overheard packet from node B with a buffered packet of node A to see if there is a match. A failure tally for node B increases if node A finds that node B is supposed to forward a packet but fails to do so. If the tally is above one threshold, node B is deemed to be misbehaving. Each node maintains a rating for each node it knows about in the network. Then, a path metric can be calculated by averaging the node ratings in the path. Pathrater [5] can then select the path with the highest metric. Marti et al. [5] also discuss several limitations of this approach, including limitations resulting from packet collisions, false reports of node misbehavior, and potential watchdog circumvention mechanisms.

Focusing on AODV routing protocols, Tseng et al. [6] propose a specification-based ID technique. A finite state machine (FSM) is constructed to specify correct behaviors of AODV, that is, to maintain each branch of a route request/route reply (RREQ/RREP) flow by monitoring all of the RREQ and RREP messages from a source node to a destination node. Then, the constructed specification is compared with actual behaviors of monitored neighbors. The distributed network monitor passively listens to AODV routing protocols, captures RREQ and RREP messages, and detects run-time violations of the specifications. A tree data structure and a node coloring scheme also are proposed to detect most of the serious attacks. Using a Markov chain (MC) to characterize normal behaviors of MANET routing tables. A MC-based local detection engine can capture temporal characteristics of MANET routing behaviors effectively. Because of the distributed nature of a MANET, an individual alert raised by one node must be aggregated with others to improve performance. Motivated by this, a non overlapping zone-based intrusion detection system (ZBIDS) is proposed to facilitate alert correlation and aggregation. Specifically, the whole network is divided into non overlapping zones. Gateway nodes (also called interzone nodes, i.e., those nodes that have physical connections to different zones) of each zone are responsible for aggregating and correlating locally generated alerts inside a zone. Intrazone nodes, after detecting a local anomaly, generate an alert and broadcast this alert inside the zone. Only gateway nodes can utilize alerts to generate alarms, which can effectively reduce false alarms. In a ZBIDS, the aggregation algorithm can reduce the false alarm ratio and improve the detection ratio. An alert data model conformed to intrusion detection message exchange format (IDMEF) also is presented to facilitate the interoperability of IDS agents. Based on this, gateway nodes can further provide a wider view of attack scenarios.

Considering that one of the main challenges in building a MANET IDS is to integrate mobility with IDSs and to adjust IDS behavior, demonstrate that a node's moving speed, a commonly used parameter in tuning MANET performance, is not an effective metric to tune IDS performance under different mobility models.

## VI. FUTURE RESEARCH DIRECTIONS

In this section, we discuss future research directions to construct IDSs for both MANETs and WSNs. In the system concept, IDS research for both MANETs and WSNs requires a distributed architecture and the collaboration of a group of nodes to make accurate decisions. ID techniques also should be integrated with existing MANET and WSN applications. This requires an understanding of deployed applications and related attacks to deploy suitable ID mechanisms. Attack models must be carefully established to facilitate the deployment of ID strategies. Also, solutions must consider resource constraints in terms of computation, energy, communication, and memory.

## VII. CONCLUSION

Intrusion detection systems, if well designed, effectively can identify malicious activities and help to offer adequate protection. Therefore, an IDS has become an indispensable component to provide defense-in-depth security mechanisms for both MANETs and WSNs. In this article, we provided an introduction to mobile ad hoc networks and wireless sensor networks and presented challenges in constructing IDSs for MANETs and WSNs. We then surveyed existing intrusion detection techniques in the context of MANETs and WSNs. Finally, using secure in-network aggregation for WSNs and the integration of mobility and intrusion detection for MANETs as examples, we discussed important future research directions.

## ACKNOWLEDGMENT

This work is supported by the Anurag Group of Institutions, Andhra Pradesh, India, Prof.M.Mutha Reddy, Principal, CVSR College of Engineering, Hyderabad, India.

## REFERENCES

[1] H. Debar, M. Dacier, and A. Wespi, “A Revised Taxonomy for Intrusion Detection Systems,” Annales des Telecommun., vol. 55, 2000, pp. 361–78

[2] Y. Zhang and W. Lee. Intrusion Detection Techniques for Mobile Wireless Networks. ACM/Kluwer Wireless Networks Journal, 9(5):545-556, September 2003.

[3] Y.Huang et al., “Cross-Feature Analysis for Detecting Ad-hoc Routing Anomalies,” Proc. IEEE ICDCS ’03, Providence, RI, May 2003, pp. 478–87.

[4] Y.Huang, and W. Lee, “A Cooperative Intrusion Detection System for Ad Hoc Networks,” ACM SASN ’03, Fairfax, VA, 2003, pp. 135–47.

[5] S. Marti et al., “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” ACM Mobicom 2000, Boston, MA, Aug. 2000, pp. 255–65.

[6] C.Y. Tseng et al., “A Specification-based Intrusion Detection System for AODV,” ACM SASN ’03, Fairfax, VA, 2003, pp. 125–34.