# Comparative Study of Intrusion Detection Techniques for Mobile Ad-Hoc Networks

[1]Gulshan Singla, [2]Hari Singh, [3]Sukhvir Singh
[1]Singhania University, Jhunjunu, Rajasthan, India
[2,3]N. C. College of Engg., Panipat, Haryana, India

**Abstract**
The rapid proliferation of wireless local area networks has changed the landscape of network security. The traditional way of protecting networks with firewalls and encryption software is no longer sufficient and effective. There are number of new techniques available for detecting the intruders in Wireless LAN. In this paper, we examine the comparative study of these techniques for detecting the vulnerabilities in wireless local area. This paper gives an overview of the existing intrusion detection techniques, including anomaly detection and misuse detection , and identifies techniques related to intrusion detection in Wireless LAN. Topics covered include Specification-Based Technique, Radio Frequency Fingerprinting (RFF) Based Technique, A Swarm-Intelligence-Based Technique, Immune System Technique, Adaptive Hierarchical Agent-Based Technique, Distributed Technique, Layered Technique, Statistical Approach, Battery-Based Technique, Honeypots Technique, Text Categorization Techniques And Dependency-Based Distributed Technique etc.

**Keywords**
About four key words or phrases in alphabetical order, separated by commas. For a list of suggested keywords, send a blank e-mail to keywords@ieee.org or visit http://www.ieee.org/organizations/pubs/ani_prod/keywrd98.txt

## I. Introduction

Intrusion detection continues to be an active research field. Even after years of research, the intrusion detection community still faces several difficult problems. Despite new security enhancements, the risk of intrusion is still a legitimate concern because preventive measures may be circumvented, cost prohibitive, or not practiced at all. As a result, intrusion detection systems for wireless LAN environments have emerged to detect unauthorized access. Detecting unauthorized access affords an opportunity to respond to the intrusion and curtail the potential damage to preserve the privacy and integrity of the network.

Intrusions are the activities that violate the security policy of the system, and intrusion detection is the process used to identify intrusions. Intrusion detection techniques for Wireless LAN have been traditionally classified into one of two methodologies: anomaly detection (based on the normal behavior of a subject) or misuse detection (based on characteristics of known attacks or system vulnerabilities).

This paper starts with an overview of current intrusion detection techniques. Next, it reviews the various types of anomaly detection methods, such as statistical models and machine learning methods, followed by an overview of various types of misuse detection methods, including rule-based languages, the colored Petri-net-based method, and the abstraction-based method. The section following that discusses additional techniques for intrusion detection in distributed systems, including distributed IDSs, network-based IDSs, and interoperation between (heterogeneous) IDSs.

Intrusion detection is based on the assumption that it is impossible to avoid security breach in the long run. All defensive security mechanism may, at some point fail. Traditionally, a defensive technique was used to block the attacker. Intrusion detection is trying to identify, preferably in real time, attacks and assess damage caused. It is also based on the assumption that the "exploitation of a system's vulnerabilities involve abnormal use, of the system; therefore, security violations could be detected from abnormal patterns of system usage". How to measure and detect these "abnormal patterns" is not an easy straightforward task. Today, intrusion detection is gaining a lot of research attention.

Stallings stress the importance of using some form of intrusion detection techniques for Wireless LAN: "Inevitably, the best intrusion prevention system will fail. A system's second line of defense is intrusion detection"[5[. At the same time, intrusion detection grabs a good deal of resources: A powerful system being able to parse huge amount of network traffic, some intelligent logging facilities, and some human interaction is usually required. These are resources corporate firms may not have.

Dorothy Denning was one of the first to present an intrusion detection model in the classical IDS paper "Intrusion Detection Model" . Lunt later redefined Denning's model and implemented the "intrusion detection expert system" (IDES) in WLAN. Denning says the arguments for developing intrusion detection are motivated by following factors:

- Most system has security flaws, and fixing them all is not always an option due to technical or economical reasons.
- Developing totally secure systems is not possible.
- Even the most secure Wireless network is vulnerable to abuse by insider who misuses their privileges.

## II. Classification of Intrusion Detection Techniques

There are traditionally two main classifications of intrusion detection systems [1]. Porras divide intrusion detection into two main types: statistical and rule-based. The other classification is between host based and network based intrusion detection.

### A. Statistical Anomaly Detection Techniques

The statistical approach uses various statistical methods to extract metrics that model the behaviour of a user. Porras further split this category into threshold and profile based detection. Threshold detection defines global threshold independent of users. Profile based detection tries to build a profile for normal behaviour for each users.

Anomalies detection has the advantages of detecting new attacks, since it is not based on predefined rules. The limitations are that statistical detection require huge amount of statistical data, often data that are attack free, to build the threshold/profiles.

### B. Rule-Based Intrusion Detection Techniques

A rule based approach [2-3] has a set of rules that defines normal behaviour. Porras further specified this into anomalies and expert systems.A rule based anomalies system is similar to statistical anomaly detection. A huge amount of data is parsed and rules are created based on previous behaviour pattern. A lot of challenges

must be met by rule based anomalies: What is to be monitored? How do initial rules for a new user get installed? Using some sort of "basis-rules"? A period of "learning-time"? But a learning time require an attack-free period. How could an attack free learning time be simulated?

A rule-based expert (penetration) system, also called signature based, uses pre-defined signatures to recognize attacks. Signature based detection is based on the assumption that all attacks leave their own unique signature that can be detected [6, 7]. The problem here is that it becomes a "race" between rule-writers and attackers; when a new attack is discovered, a new rule must be written, distributed and installed.

### 1. Specification-Based Technique

A specification-based approach for intrusion detection is proposed in a Wireless LAN [12]. The idea is to use traces, ordered sequences of execution events, to specify the intended behaviors of concurrent programs in a network. A specification describes valid operation sequences of the execution of one or more programs, collectively called a (monitored) subject. A sequence of operations performed by the subject that does not conform to the specification is considered a security violation. Each specification is called a trace policy. A grammar called parallel environment grammars (PE-grammars) was developed for specifying trace policies.

The advantage of this approach is that in theory, it should be able to detect some new types of attacks that intruders will invent in the future. The drawback of this approach is that substantial work is required to specify accurately the behavior of the many privileged system programs, and these specifications will be operating-system specific. To address this issue, C. Ko proposed the use of inductive logic programming to synthesize specifications from valid traces [13]. The automatically generated specifications may be combined with manual rules to reduce the work involved in specification of valid program behaviors.

Wagner and Dean further advanced the specification-based technique [12]. The basic idea is to automatically generate the specification of a program by deriving an abstract model of the programs from the source or binary code. Wagner and Dean studied several alternative models, including the call-graph model and the abstract stack model. Central to these models is the control flow graph of a program; these models adopt different ways to represent the possible system call traces according to the control flow graph. Attractive features of this approach are that it has the potential to detect unknown patterns of attacks and it has no false alerts, although it may miss some attacks.

### 2. Radio Frequency Fingerprinting (RFF) Based Technique

The Radio Frequency Fingerprinting (RFF) approach [8] incorporates radio frequency fingerprinting (RFF) into a wireless intrusion detection system (IDS), for detecting Media access control (MAC) address spoofing attack which can result in the unauthorized use of network resources. RFF technique is used to uniquely identify a transceiver based on the transient portion of the signal it generates. The success rate of a wireless IDS is also improved by correlating several observations in time, using a Bayesian filter. Simulation results, with an average success rate of (94-100%), support the feasibility of employing RFF and Bayesian filtering techniques to successfully address the aforementioned problem.

### 3. A Swarm-Intelligence-Based Technique

A Swarm-intelligence-based intrusion detection technique is developed in order to reduce the misjudgment & misdetection and increase the real-time response in the existing intrusion detection techniques for WLAN. Separating a huge and complicated intrusion detection system into severer independent detection units with unique function so that the amount of detection data processing and the complexity of detection signature selecting, which are the main factors affecting the application performance of existing intrusion detection techniques, are reduced significantly. Moreover, by utilizing the information from each independent detection unit, the complicated intrusion of the entire intrusion detection system can be detected. The key techniques for the implementation of the system include the user trace under the environment of network, the interception and detection of real-time system calls, and the efficient access of shared information base.

The swarm-intelligence-based intrusion detection technique better solves the problems by means of decomposing of detection functions, corresponding separation of data traffic and mutual information exchanging and sharing among detection units. In fact, confront to the more and more serious problem of network security, the distribution and cooperation may be utterly adoptable solution. Its essence is just "swarm intelligence", which is also consistent with the current hot technology——distribute computation & active wireless network.

### 4. Immune System Technique

Immune System Technique offer an in-depth review of work relating to the application of AISs (Artificial immune systems) to the problem of intrusion detection in WLAN. The use of artificial immune systems in intrusion detection is an appealing concept for two reasons. Firstly, the human immune system provides the human body with a high level of protection from invading pathogens, in a robust, self-organised and distributed manner. Secondly, current techniques used in Wireless LAN are not able to cope with the dynamic and increasingly complex nature of wireless networks and their security. It is hoped that biologically inspired approaches in this area, including the use of immune-based systems will be able to meet this challenge. Here we collate the algorithms used, the development of the systems and the outcome of their implementation. It provides an introduction and review of the key developments within this field, in addition to making suggestions for future research.

### 5. E. Adaptive Hierarchical Agent-Based Technique

The Adaptive Hierarchical Agent-based Intrusion Detection Technique employs a fully distributed, multi- agent framework. The major components in this framework are Director Agents, Manager Agents, Tool agents, and Surrogate agents. In this framework, which is based loosely on the agent architecture, Director agents are responsible for detecting intrusive action on a collection of systems and network segments. In a large-scale network, multiple levels of Directors can exist. At each level in this hierarchical arrangement, Directors are responsible for a subset of the systems for which its immediate supervisor is responsible. Associated with each Director agent is a Surrogate agent. This surrogate resides on another part of the network, and its role is to assume the Director's responsibilities in the event that the Director fails. The use of surrogates partially mitigates the inherent shortcomings of hierarchical arrangements (i.e. the existence of single points of failure), while retaining much of the inherent advantages of

hierarchical arrangements. The lowest–level Director agents supervise a set of Manager agents, each of which is responsible for detecting intrusive activities on possibly overlapping subsets of the systems for which the Director is responsible.Manager agents detect intrusive activity on the system for which they are responsible by employing a dynamically changeable set of Tool agents. Tool agents are low-level, lightweight, but fully functional, intrusion detection systems. The determination, by the Manager agents, of the most suitable number and type of Tool agents to employ, at any given time, is one of the most important responsibilities of Manager agents. The above framework provides detection adaptation in three specific areas. First, it supports adaptation by adjusting the amount of system resources devoted to the task of detecting intrusive activities. There will always be a tradeoff between the amounts of system resources devoted to perform useful work (functionality) vs. that which is devoted to securing the system. For example, there are periods when, due to a perceived low degree of threat, that only a small proportion of system resources should be devoted to detecting intrusive activities. On the other hand, during period of perceived high threat, significantly more resources should be devoted to this task. There is direct support within the framework for the reasoning process necessary to determine the appropriate level of system resources for accomplishing the intrusion detection task. Second, the adapts by dynamically invoking new combinations of low-level detection agents in response to changing circumstances. As the conditions in a given network change, resulting in increased or decreased resources levels for intrusion detection, so does the need for varying types of low-level intrusion tools. For instance, if the rates of a specific type of attack were expected to increase, then it would clearly be sensible for IDS to use tools that are designed to detect that type of attack. This framework provides explicit support for this form of adaptation. Finally, it adapts by adjusting the confidence metric that it associates with the low-level detection agents. All IDS can generate both false positives and false negatives. Unfortunately, these rates are not always known a priori. One way to improve the overall IDS which uses these tools would be to keep track of the performance of the low level tools and maintain a confidence metric.

## 6. Distributed Technique

Most of today's Wireless LAN are distributed because of the need to share system resources. Currently available security techniques are not able to cope with the dynamic and increasingly complex nature of the attacks on distributed networks. An automated and adaptive defensive tool is imperative for distributed computer networks. Alongside the existing techniques for preventing intrusions such as encryption and firewalls, a promising solution is emerging in the Distributed Intrusion Detection System (DIDS) which is able to detect unauthorized access, misuse and abuse of networks by both the internal users and external offenders. This technology still faces some challenges such as arbitrary definitions of abnormal activities and ineffective coordination between the DIDS modules. This technique is a review of Intrusion Detection Technology for distributed computing networks. The review is followed by a proposal to use data mining techniques to assist the hierarchical DIDS to construct essential features from raw data and dynamically create normal user behavior profiles. This model will overcome some limitations of the current approaches in distributed computer networks.

## 7. Layered Technique

A layered technique to intrusion detection is worth considering. A single type or layer of intrusion detection alone cannot be considered to be secure enough. A Layered approach involves developing and deploying multiple layers of security with each layer contributing to the overall security. A simple truism is "The more the layers, the more secure". The first requirement for a layered approach is to have a well defined security policy. The policy should categorically state and define the different security mechanisms deployed, address issues such as user privacy and activity monitoring and define a contingency/incident-response plan.

The first system layer should be a firewall. Firewalls are filtering tools and will help the other layers such as intrusion detection or auditing. Firewalls should use the security policy to decide which traffic should be allowed into and out of the network. The firewall rules should be carefully designed and tested to ensure their effectiveness. The second layer can be the intrusion detection system. Here issues such as number of systems and their placement in the network should be addressed. If the network is too large then a NIDS might become a bottleneck because of its processing limitations. Deploying multiple NIDS at different network points will help reduce this bottleneck, but will result in more systems that need to be maintained. Finally host-based systems especially those which detect misuse attacks must be deployed on all systems or at least the important systems. Just because a system is not important doesn't mean that it should not be secured as it can be used to attack other important systems. A layer which can be considered common to all the detection layers is the logging and auditing layer. Human intervention plays an important part in this layer. Logs and audit trails should be monitored periodically and discrepancies addressed. The security and the correctness of the logs should also be ensured. The number of layers or their deployment is subject to the organization's policies and infrastructure.

## 8. Statistical Approach

Statistical-Based systems use statistical models to detect malicious packets. Statistical models are primarily used to relate information regarding occurrence and variables related to factors that influence occurrence. Statistical systems adapt to different system behaviors or occurrences and try to develop a usage pattern. Then they monitor pre-defined variables over a time period and calculate a test value. If this value is above the user-defined threshold then they trigger an alert. This approach does not require any predefined attack patterns and is capable of detecting new attacks. Also depending upon the number of variables processed it can detect evasion attacks or slow attacks. Like behavior based approaches the system must "learn". So the effectiveness of the system depends on the learning process. Another concern with statistical approach is the fact that it will not pinpoint the attack or the problem. It will only flag a packet as being anomalous and either drop the packet or trigger an alert. The administrator will then have to perform the necessary analysis on it and will require reasonable amount of expertise.

## 9. Battery-Based Technique

This technique is an efficacious early warning system via a mobile host- based form of intrusion detection that can alert security administrators to protect their corporate network(s) by a novel technique that operates through the implementation of smart battery-based intrusion detection (B-bid) on wireless networks. A host intrusion detection engine (HIDE) monitors power behavior

to detect potential intrusions by noting consumption irregularities and serves like a sensor to trigger other forms of protection. HIDE works in conjunction with a Scan Port Intrusion Engine (SPIE) that ascertains the IP and port source of the attack and with a Host Analysis Signature Trace Engine (HASTE) that determines the energy signature of the attack and correlates it to a variety of the most common attacks to provide additional protection and alerts to both mobile hosts and their network.

## 10. Honeypots Technique

A honeypot is "an information system resource whose value lies in unauthorized or illicit use of that resource". This methodology has been used to study attackers and types of attacks in depth, providing valuable information about tools, tactics, and motives of attackers. To learn more about malware, we use low-interaction honeypots such as Nepenthes and high-interaction honeypots such as GenIII honeynets. Low-interaction honeypots emulate services or operating systems. They allow an attacker a limited interaction with the target system and allow us to learn mainly quantitative information about attacks. Since low-interaction honeypots use simulation, they construct a controlled environment and thus the risk involved is limited. We give a more detailed introduction to low-interaction honeypots in the following section.

In contrast, high-interaction honeypots do not emulate any services, functionality, or operating systems. Instead, they provides real systems and services, allowing us to capture extensive information on threats. Several honeypots can be combined into a network, called a honeynet. We can capture the exploits of attackers as they gain unauthorized access, monitor their keystrokes, recover their tools, or learn what their motives are. The disadvantage to high-interaction solutions is that they have increased risk: Because the attackers can potentially fully access the operating system, they can potentially use it to harm other nonhoneypot systems.

A honeynet creates a fishbowl environment that allows attackers to interact with the system, while giving the operator the ability to capture all of their activity. This fishbowl also controls the attacker's actions, mitigating the risk of them doing harm to any nonhoneypot systems. The key element to a honeynet deployment is called the Honeywall, a layer-two bridging device that separates the honeynet from the rest of the network. This device miti- gates risk through data control and captures data for analysis. Tools on the Honeywall allow for analysis of an attacker's activities. Any inbound or outbound traffic to the honeypots must pass through the Honeywall. Information is captured using a variety of methods, including passive net- work sniffers, IDS alerts, firewall logs, and the kernel module known as "Sebek". The attacker's activities are controlled at the network level, with all outbound connections filtered through both an intrusion preven- tion system and a connection limiter. Neither of these two approaches is superior to the other; each has unique advantages and disadvantages.

## 11. Text Categorization Techniques

A new approach [ 9 ] , based on the k-Nearest Neighbor (kNN) classifier, is used to classify program behavior as normal or intrusive. Short sequences of system calls have been used by others to characterize a program's normal behavior before. However, separate databases of short system call sequences have to be built for dif- ferent programs, and learning program profiles involves time-consuming training and testing processes. With the kNN classifier, the frequencies of system calls are used to describe the program behavior. Text categorization techniques are adopted to convert each process to a vector and calculate the similarity between two pro- gram activities. Since there is no need to learn individual program profiles separately, the calculation involved is largely reduced. Preliminary experiments with 1998 DARPA BSM audit data show that the kNN classifier can effectively detect intrusive attacks and achieve a low false positive rate.

## 12. Datamining Techniques

There are number of techniques available on Anomaly-Detection based Intrusion Detection System. The goal was to try out various data mining approaches and analyze the results of the same when used for Anomaly Detection. Schemes such as Outlier Detection for Network based IDS and Prediction of system calls for Host based IDS, were tried out. These techniques detect anomalies using both host-based and network-based approaches. We used Anomaly Detection for both Host-based as well as Network-based IDS approaches. A Network-Based the problem of use of Data mining approaches for Intrusion Detection [4, 10] is a much-researched one.

## 13. Dependency-Based Distributed Technique

In Dependency-Based Distributed Technique hosts are clustered into regions based on network proximity and dependency, and communication among them becomes more efficient. To capture the dependency, we apply different intrusion detection techniques within regions and across regions.

Distributed network intrusion detection has attracted much attention recently. In this techniqueis on zero-day, slow-scanning worms, of which no existing signatures are available. We organize end hosts into regions based on network knowledge, which we posit is positively correlated to the dependency structure. Lever- aging on this organization, different intrusion detection techniques within and across regions. We use a Hidden Markov Model (HMM) within a region to capture the dependency among hosts, and use Sequential Hypothesis Testing (SHT) globally to take advantage of the independence between regions.

## 14. Some Other Techniques

Bayesian network based techniques are used in to imbue end hosts with probabilistic graphical models. With random messaging to gossip state among the lo- cal detectors, they show that such a system is able to boost the weak local detectors to detect slowly propagating worms. Sequential Hypothesis Testing (SHT) was first adapted to intrusion detection by Jung. The original algorithm was centralized, with detection performed at the gateway. It was decentralized where hosts exchange their information, and perform the inference individually in parallel. We identify two issues with this technique. First, it assumes independence among intrusion attempts and, second, it cannot deal with the case when a worm interleaves the intrusion traffic with non-intrusion traffic. In our work, we assume dependence among hosts within a region, and assume independence between regions. To address this dependence/ independence, we use a Hidden Markov Model (HMM) to detect intrusion within a region and SHT globally between regions. The HMM allows us to incorporate our dependency assumption into the regional aggregations, and SHT depends on our assumption of independence between regions. Machine learning has been applied to intrusion detection in various aspects. For example, Agosta designed an adaptive mechanism that adjusts the threshold of anomaly based on traffic . This does not seem to handle alternating traffic either. Our use of the HMM approach allows us to handle such interleaving, because it learns both transition and emission probabilities from observations, since neither is known a priori.

## III. Conclusion

Intrusion detection is based on the fairly reasonable assumption that, no matter how well you configure your systems, you cannot be utterly certain that an intrusion will never take place or that it will never go undetected. A good intrusion detection policy is often the one that is most strongly tailored to fit your network. Not all techniqus will be suitable for your requirements, and you will ultimately need to decide if you need all your network traffic monitored or if you can get away with only scanning key systems that initially need protection. The amount of network traffic intrusion detection package introduces can be phenomenal, so expect your network to significantly drop in efficiency after you've implemented a tough intrusion detection policy. Bear in mind that not all systems should be treated with equal rigour, and define certain "exclusion areas" which are not scanned all the time but which can be scanned when needed - for example, immediately after your intrusion detection system has announced a potential intruder. Review Stage.

## References

[1] H. Altunbasak, H. Owen,"Alternative Pair-wise key exchange protocols for robust security networks", IEEE 802.11i in wireless LANS, SoutheastCon, 2004, Proceedings IEEE, pp. 77-83.

[2] W.A. Arbaugh," An inductive chosen plaintext attack against WEP and WEP2, IEEE 802.11 working group, Task Group I (Security), 2002.

[3] W.A. Arbaugh, N. Shankar, Y.C.J. Wan, K.Zhang," Your 802.11 wireless network has no clothes", IEEE Wireless Communications, pp. 44-51, 2002.

[4] W.A. Arbaugh," Wireless security in different computers", Vol. 36, Iss. 8 pp. 99-101, 2003.

[5] N. Borisov, I. Goldberg, D.Wanger,"Intercepting mobile communications: The insecurity of 802.11", 7th Annual International Conference on Mobile Computing and Networks, 2001.

[6] M. Carli, A. Rosetti, A. Neri, "Integrated security architecture for WLAN Telecommunications, ICT, Vol. 2, pp. 943-947, 2003.

[7] C. Candolin, H.H. Kari,"A security architecture for wireless Ad-Hoc networks, MILCON 2002, Proceedings, Vol. 2, pp. 1095-1100, 2002.

[8] I. Chlamtac, M. Conti, J. Liu, "Mobile Ad-Hoc networking: imperatives and challenges. Ad-Hoc Networks, pp. 13-64, Elsevier, 2003.

[9] Y.M. Erten,"A layered security architecture for corporate 802.11 wireless networks. Wireless Telecommunications Symposium, pp. 123-128, 2004.

[10] H. Feil, "802.11 Wireless Network Policy Recommen-dations for usage within unclassified Government Networks", The Aerospace Corporation, pp. 832-838, 2003.

[11] V. Gupta, S. Gupta,"Securing the wireless internet", Communications Magazine, IEEE, Vol. 39, Iss. 12, pp. 68-74, 2001.

[12] D.Wagner, R.Dean,"Intrusion Detection via static analysis", Security and Privacy, pp. 156-168, Proceedings, 2001 IEEE.

[13] C. Ko,"Logic induction of valid behavior specification for intrusion detection", 0-7695-0665-8, pp. 1-12, 2000 IEEE.