# Comparative Analysis of IDS and Techniques in Mobile Ad-hoc Networks

Ganesh Kumar Wadhwani*
Heena Khera**

**Abstract**

Intrusion Detection System is a type of security management system for computers and networks. An Intrusion Detection System gathers and analyzes information from various areas within a computer or a network to identify possible security breaks, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).It sometimes uses vulnerabilities assessment (known as scanning), which is a technology developed to assess the security of a computer system or network. The process through which Intrusion Detection is achieved is called Intrusion Detection System. An IDS keeps the information or record of activities taking place in the system to determine and find if there is any activity that is quite different from usual activities that are taking place in the system or any activity that is violating the security rules. In this paper we are doing comparison of Distributive IDS, Cooperative IDS, Hierarchical IDS, Zone Based IDS, Agent Based Anomaly IDS, Local IDS, and Standalone IDS. We are also comparing Intrusion Detection Techniques including Anomaly, Misuse and Specification.

**Keywords:** NBIDS, HBIDS, Intrusion, MANET, Attacks.



## Introduction

Any attempt to compromise the integrity, confidentiality and availability of information and resources. There is no such system that is totally secure. If we have the ability to detect the attack, once it comes into the network, we can stop it from doing any damage to the system or any data. Here is where intrusion detection system comes in.

## Intrusion Detection System

- ❖ Intrusion: The act of wrongfully entering upon, seizing, or taking possession of the property of another. (Dhangar, Kulhare & Khan, 2013)
- ❖ Detection: The act of discovering or determining the presence, existence or fact of.
- ❖ Intrusion Detection: The act of discovering or determining the presence, existence or fact of .the wrongfully entering upon, seizing, or taking possession of the property of another.

**Ganesh Kumar Wadhwani***
IITM, New Delhi

**Heena Khera****
IITM, New Delhi

Intrusion Detection can be defined as a process of monitoring activities in a system, where system can be a standalone computer or any network system. The process through which Intrusion Detection is achieved is called Intrusion Detection System. An IDS keeps track on all activities taking place in the system to determine and find if there is any activity that is quite different from usual activities that are taking place in the system or any activity that is violating the security rules. Once an IDS determines such unusual activity or an activity that is known to be an attack, it than generates an alarm to alert the security administrator. IDS can also give a proper response to the malicious activity. Although there are several intrusion detection techniques for wired networks, but they are not suitable for wireless ad hoc networks

## Characteristics of a Good Intrusion Detection System

- Continuous autonomous execution
- Fault tolerance
- Minimal Overhead
- Not easily deceived

## Intrusion Detection System in MANET

An intrusion detection system is a defense system that detects unusual activities in a network and then tries to prevent such activities that may compromise system security. Intrusion Detection system achieve detection by continuously monitoring the network for unusual activity. Prevention part in IDS may include issuing alerts, taking direct preventive measures such as blocking the suspected connection. Intrusion Detection System is a process of identifying and responding to malicious activity targeting at computing and networking resources.

**IDS Tools** are capable of identifying insider originating from inside the network and external attacks. Intrusion Detection System comes when an intrusion has already occurred. That is why Intrusion Detection System are called second line of defense.

**Limitation of MANET** routing protocol, nodes in MANETs assume that all nodes cooperate with each other to send data. Due to this assumption attacker gets an opportunity to achieve significant impact on network with just one or two compromised nodes.IDS act as the second layer in MANETs.

## Classification of Intrusion Detection System

Monitor, detect and respond to any unauthorized activity are the characteristics of Intrusion Detection System.

**Base on Data Monitoring**: Intrusion detection can be classified based on monitoring data as either:

1. Host Based Intrusion Detection System (HIDS)
2. Network Based Intrusion Detection System(NIDS)

## Host Based Intrusion Detection System (HIDS):

It operates on single workstation. It monitors traffic on its host machine by utilizing the resources of its host to detect attacks.

## Network Based Intrusion Detection System (NIDS):

It operates as stand-alone devices in a network. It monitors traffic on the network to detect attacks such as denial of service.

## Based on the Network Infrastructure

MANET can be configured as flat or multilayered. An efficient IDS architecture for the MANET depends on the network infrastructure itself. There are six main architectures on network:-

Standalone IDS
Distributive and Collaborative IDS
Hierarchical IDS
Mobile Agent for intrusion detection
Local IDS
Zone based IDS

**Table 1: Difference between NBIDS and HBIDS**

| Network Based Intrusion Detection System | Host Based Intrusion Detection System |
|---|---|
| Resides on the computer or application connected to a part of organization network and monitors network traffic on that segment looking for on-going or successful attacks. | Resides on particular computer or server known as host and monitors activity that occurs on that system looking for any malicious programme running. |
| NIDS uses monitoring port, when placed next to a networking device like hub, switch. The port views all the traffic passing through the device. | Capable of monitoring system configuration databases such as windows registers, and stored configuration files like .ini, .cfg, and .dat files. |
| Works on the principle of signature matching .i.e. comparing attack patterns to known signatures in their database. | Work on the principle of configuration and change management. An alert is generated when file attributes change, new files created, or existing files deleted. |
| NIDS are suitable for medium to large scale organization due to their volume of data and resources. So many smaller companies hesitant in deploying IDS. | Most HIDS has common architectures that is most host systems work as host agents reporting to a central console. |

## Standalone IDS

In this architecture intrusion detection system runs on each node to identify intrusions independently [3]. Each node takes its own decision based on the information it has collected by itself. There is no interaction among the nodes present in the network and no data is exchanged between them. Though nodes are in same network they don't know anything about each other. It is suitable in a network where not all nodes are capable of running intrusion detection system. It is more suitable for flat networks than for multilayered networks infrastructure. Because of its limitation that each node maintains only its own information and does not know anything about other nodes in the network, they might not be able to detect all intrusions. Therefore this architecture is not chosen in most of the IDS for MANETS.

## Distributive and Collaborative IDS

In this architecture there is a rule that every node has to participate in intrusion detection and response by using IDS agent running on them. The IDS agent is responsible for detecting and collecting local events and data to identify possible intrusions and responding them individually. In this architecture neighboring IDS agents cooperatively participate in finding intrusions globally.

## Hierarchical IDS

It is an extended version of distributed and collaborative IDS architecture. This architecture is used where network is divided into clusters therefore it uses multi layered network. It consists of cluster heads that act as control points which are similar to switches, routers, or gateway in wired network.

## Mobile Agent for IDS

It uses mobile agents to perform specific tasks on a node. It allows distribution of intrusion detection tasks. Because it has the ability to move around the large network therefore each mobile agent is assigned one specific task to perform and then one or more mobile agents are distributed into each node in the network. This is how intrusion detection task is distributed. It helps to reduce the consumption of power which is hard to find in mobile ad hoc network.

## Zone Based Intrusion Detection System

ZBIDS is a distributed IDS, in which two levels of hierarchical structure is defined. It simultaneously collects node-tracing data and network traffic information to construct anomaly-based IDS. ZBIDS can detect not only the simple intrusion without sequence characters by a pre-classifier but also with the special sequence characters by a Markov-chain-based classifier.

## Comparative Analysis of IDS

Distributed IDS introduced by R.Nakkeeran consider only local mobility issues; it is Anomaly Based Intrusion Detection System, it uses anomaly based technique to find misbehaving nodes and attacks. It handles attacks like Distributed Denial of Service. Architecture of Distributed IDS is modular and distributed. It uses Mobile Agent Based Algorithm to deal with attacks. Cooperative IDS introduced by Y.Haung is also anomaly based intrusion detection system i.e. it uses anomaly based method and consider only local mobility issues. It deals with DDOS (distributed denial of service) Attack. It uses cluster based distributed algorithm and it consist of hierarchical architecture. Zone Based IDS introduced by B.Sun, K.Wu, and H.W Pooch causes detection and response latency even when there is enough evidence on local nodes. It uses Aggregation algorithm. Architecture of Zone Based IDS is Distributed and Collaborative. It is an anomaly based intrusion detection system; it uses anomaly techniques to identify attacks and to find misbehaving nodes. Agent Based IDS introduced by Rosa Cano is a Signature Based Intrusion Detection System i.e. it uses signature based technique or misuse technique to identify malicious nodes and attacks. It fails to address security issues. Layout of Zone Based IDS is distributed, Hierarchical multi-agent form. It uses Agent Based cooperative and distributive algorithm to deal with attacks. LIDS (local intrusion detection system) instigated by L.Portnoy uses both misuse and anomaly ID method to find misbehaving nodes. It cannot identify the attacker efficiently. It uses Density Based Algorithm and its architecture is distributed and collaborative.

**Table 2: Comparative Analysis of IDS**

| Topic | Author | Architecture | ID Method | Issues | Algorithm | Attacks |
|---|---|---|---|---|---|---|
| 1) Distributed IDS | R.Nakkeeran | Modular and Distributed | Anomaly Based | Consider only local mobility | Mobile Agent Based(independently & cooperatively) | Distributed Denial Of Service |
| 2) Cooperative IDS | Y.Haung | Hierarchical | Anomaly Based | Consider only local mobility | Cluster Based distributed scheme | Distributed Denial Of Service |
| 3) Zone Based IDS | B.Sun, K.wu & H.W Pooch | Distributed & Collaborative | Anomaly Based | Cause detection and response latency even when there is enough evidence on local nodes | Aggregation Algorithm | Routing Disruption Attack |
| 4) Agent Based Anomaly Detection | Rosa Cano | Distributed & Hierarchical multi-agent | Signature Based | It fails to address security issues | Agent Based Cooperative and Distributive | Sql Injection Attack |
| 5) Local IDS | L Portnoy | Distributed & Collaborative | Misuse, Anomaly Based | Cannot identify the attacker efficiently | Density Based Algorithms | Denial Of Service, Penetration Attack |
| 6) Hierarchical IDS | Hou Young, Fieng Zheng | Hierarchical | Anomaly | sensor node selfishness | Quantum Clustering Algorithm, Potential Function Algorithm | Node Replication Attack |
| 7) Standalone IDS | Manoj Rameshchandra Thakur | Standalone | Anomaly | No communication between nodes therefore no alert information is passed | Standalone Algorithm | Novel Attacks |



## Intrusion Detection Techniques

There are three types of Intrusion Detection Techniques:

Anomaly Detection
Misuse Detection
Specification-Based Detection

## Anomaly Detection

In anomaly detection system a baseline or normal activity is created. Any activity in the system if deviate from the baseline or normal activity than that activity is treated as an intrusion. Anomalies also known as outliers, exceptions are patterns in data that do not conform to a well-defined concept of normal behavior of a system. (Karthikeyan & Rana, 2010)

A simple example showing anomalies $O_1$, $O_2$, $O_3$ that differ from normal behavior $N_1$ and $N_2$.

Anomaly detection technique is designed to uncover the patterns whose behaviour is different from the normal and that deviates from it. Then that pattern is marked as possible intrusion. Anomaly Detection Technique can be categorized into:

- Static
- Dynamic

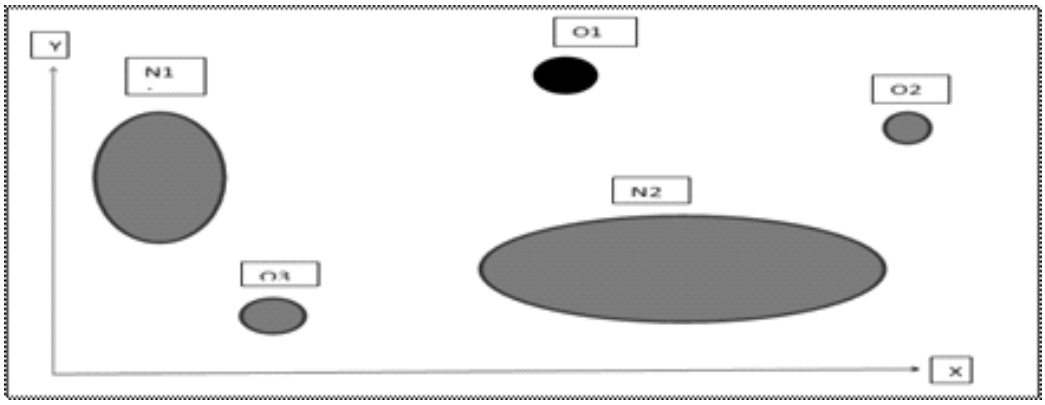


**Fig. 1: Example of Anomaly**

**Static Anomaly Detector:** A portion of the monitored system remains constant or static. The static portion of the system consist of two parts

- The system code
- The portion of system data that remains constant

Static portion of the system can be a set of strings (such as files) that if deviates from its original form, either an error has occurred or an intruder has altered the static portion of the system. Static anomaly detectors are used to check the data integrity.

**Dynamic Anomaly Detector:** In this system behavior is defined as a sequence of distinct events. The system may depend on parameters that are set during initialization to reflect the uncertain behavior. Initial behavior of system is assumed to be normal.

In anomaly based intrusion detection every node in the ad hoc network participates in intrusion detection and response to it. Every node is responsible for finding signs of intrusion locally and independently by observing the activities of user and system and the communication activities within the radio range.

## Procedure for Anomaly Detection:

- Select or partion the audit data so that the normal data set has low chaos.
- Perform suitable data transformation
- Compute the classifier
- Testing of data is done by classifier
- Use alarms to produce intrusion reports.

The major requirements of anomaly based intrusion detection model are FPR(false positive rate), and high TPR (true positive rate). Parameters used for these requirements are :

- True Positive
- True Negative
- False Positive
- False Negative

**True Positive (TP):** This occurs when IDS generates true alerts on a detected malicious traffic. TP is total malicious activity detected.

**True Negative (TN):** This occurs when no malicious activity occurs in the network and no alarm is generated by IDS.

**False Positive (FP):** This occurs when an IDS wrongly raises a false alarm over a authorized activity in the network.

**False Negative (FN):** This occurs when IDS fails to detect the malicious activity in the network.

**False Positive Rate (FPR):** This shows the proportion of exceptions which were not intrusions but then also alarm was generated for them. FPR is obtained using the following formula;

FPR=FP/FP+TN

**True Positive Rate (TPR):** This shows how good IDS is in detection intrusions in the network. It is also known as Detection Rate. Obtained as:

TPR=TP/TP+FN

The best IDS is one that have FPR less than 1% and TPR .

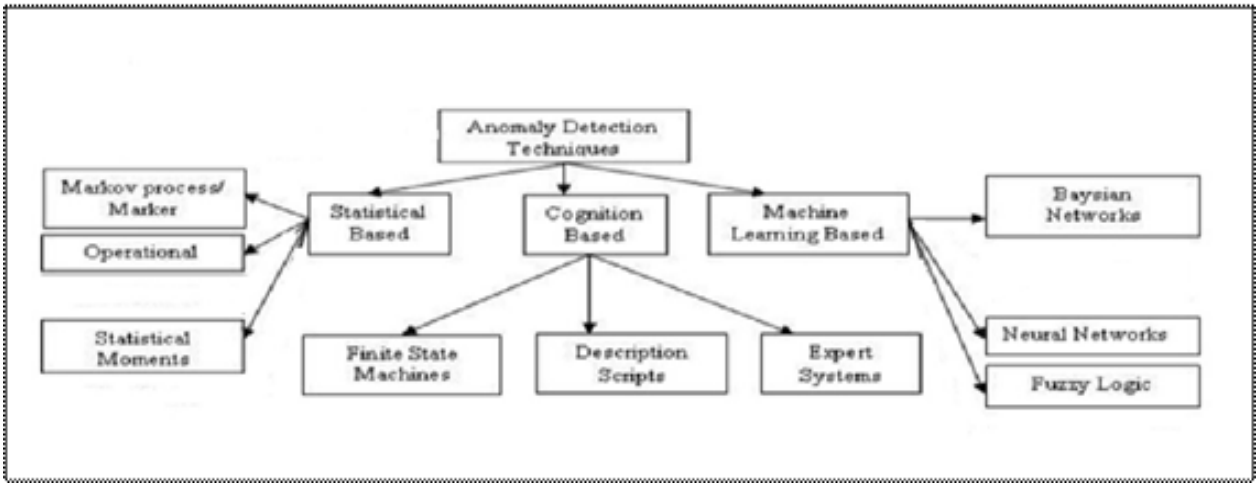


**Fig. 2: Classification of Anomaly Based Intrusion Detection**

## Classification of Anomaly Based Intrusion Detection:

**Statistical Anomaly Based Intrusion Detection:** A normal TCP traffics follow three way handshake process for connection setup, data transfer phase, and then completes the connection drop down. In the absence of attacks different types of TCP packets are balanced. Statistical anomaly based IDS captures this behavior and differentiates between the long term and short term observations in a protected environment to avoid false alarms to be generated while normal traffic changes.

**Operational Model:** The number of events that occur over a period of time determines the alarm to be raised if less than 'm' or more than 'n' events occur. For example executable files size is restricted in some organization about 4mb. The difficulty in this sub model is determining 'm' and 'n'.

**Markov Process/ Marker Model:** In this model intrusion detection is done by investigating the system at fixed intervals and keeping track of its state. Probability of each state at a given time interval say Is .When an event occurs there is a change in the state of the system and its behavior is considered anomaly if the probability of occurrence of that state is low.

**Statistical Moment:** Any co-relation is said to be moment. If the event that falls outside the set interval above or below the moment is said to be anomalous. There are major two advantages over operational model. First prior knowledge is not required for determining the normal activity in order to set limits. Second determining the intervals depends on observed user data as it varies from user to user. In this model higher weight is given to recent activities.

**Cognition Based Detection Technique:** Also known as **Knowledge Based or Expert Based.** It is used to classify audit data based on set of rules. It involves three steps.

1) Different attributes and classes are identified from training data
2) Set of classification rules
3) Parameters and Procedures are derived

**Finite State Machine:** It models attacks as a network of states and transitions (matching events). A state contains information of the past, i.e. any changes made in the input are noted and based on it transition take place. An action is a description of an activity that is to be performed at given moment. Several actions are performed like entry action, exit action, and transition action.

Every observed event that represent attack scenario is applied to the finite state machine. Any machine that reaches its final state indicates an attack.

**Description Scripts:** In this scripting languages which can describe signature of attacks on computer and network are given by the intrusion detection community. These scripting languages are capable of

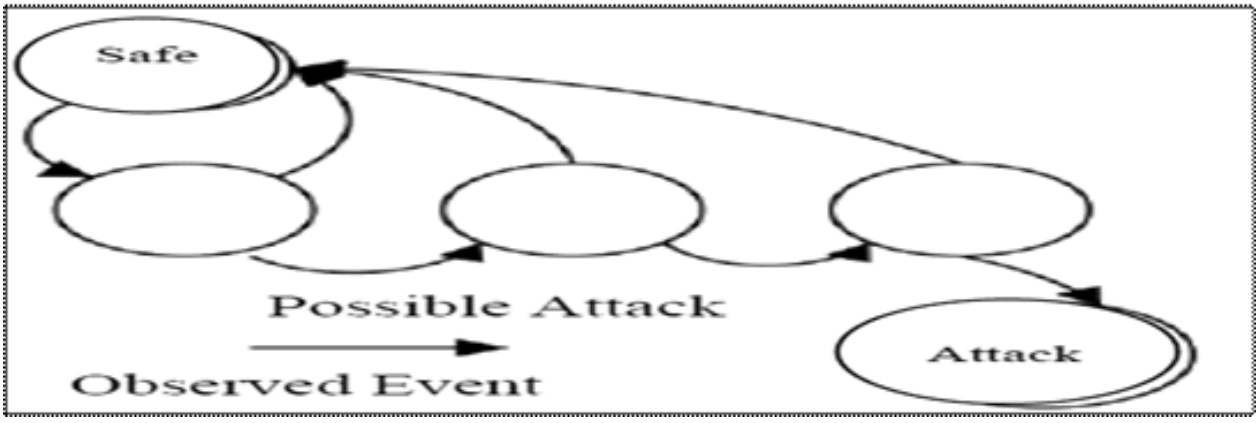


**Fig. 3: Finite State Machine**

identifying the sequences of specific activities that point out attacks.

**Adapt System:** In this system human expertise is used for problem solving. It solves uncertainties by consulting one or more human experts. They are efficient in certain problem domain and are also considered as a class of artificial intelligence (AI) problems. Adept Systems are trained based on extensive knowledge of patterns associated with known attacks provided by human experts.

**Machine Learning Based Detection Techniques:** It is used to find outliers in data set. It uses small subsets to find unknown attributes of test points. It allows patterns to be analyzed and categorized based on implicit or explicit model. The major drawback of this technique is their resource expensive nature.

**Bayesian Networks:** It is a probabilistic model. It helps in solving the problem that requires the prediction of the outcome of the system consisting of high number of interrelated variables. It goes through the training period in which it learns the behavior of the model after which it is able to predict its outcome. Successful applications of Bayesian networks include for example email classification for spam detection (Yang et al., 2006), failure detection in industrial production lines (Masruroh & Poh, 2007), reconstruction of trafûc accidents (Davis &Pei, 2003) (Davis, 2006).

**Neural Networks:** The goal for using neural networks for intrusion detection it to be able to generalize from incomplete data and to classify whether the data is normal or intrusive. It consists of collection of processing elements that are highly interconnected. In this we are given a set of inputs and a set of desired output. The transformation from input to output is done by the weights associated with the processing elements which are interconnected. By modifying these interconnections, the network is able to get desired output. Its ability of high tolerance for learning by example makes neural networks flexible and powerful in intrusion detection system.

It can easily represent linear and non-linear relationships between input data and output data. Even if the data is incomplete neural networks are able to correctly find the different data classes taken from the network other sources.

**Fuzzy Logic:** It is difficult to predict normal and intrusive activities in networked computer as boundaries are not well defined. This prediction process may generate false alarms in anomaly based intrusion detection systems. It reduces the false alarm rate in while determining intrusive activities. It can detect both misuse and anomaly attacks. It consists of fuzzy rules that can be applied to determine normal and abnormal behavior in computer networks. The main problem with this process is to make good fuzzy classifiers to detect intrusions.

## Misuse Detection

In this system Legal or Illegal behavior is defined and then the observed behavior is compared accordingly in. If the behavior of the activity does not matches with the normal activity behavior than that activity is

treated as an intrusion. It is able to detect attacks based on predefined signatures or patterns, a set of events that match a predefined pattern. Signature based detection technique are effective in detecting attacks without too many false alarms , but at the same time this technique is unable to detect common attacks whose signatures are unknown.

In this technique we know signatures of attacks and some or all nodes in the system execute intrusion detection logic; such nodes are said to enact as intrusion detection subsystem.

The objective or goal of any intruder in any network is to deliver malicious packets at the end point and harm the destination point. The intrusion detection system tries to find out occurrence of such packets while the transmission taking place between source node and destination node to take corrective actions. Routing protocols will have an effect on the intrusion detection capabilities in network. In ad hoc network with many nodes there may be repetitious paths between a given source node and destination nodes. The routing protocols might switch packets while they are being transferred from source node to destination node. Because of this it may become difficult even to detect those attacks whose signature is known. Therefore this technique is inefficient and is not possible in many cases where resource constraints are applied.

**Rule Based Languages:** This is the most widely used approach in misuse detection. The patterns of known attacks are specified as rule sets, and a forward-chaining expert system is usually used to look for signs of intrusions. Here we discuss two rule-based languages, rule-based sequence evaluation language (RUSSEL) (Mounji, Charlier, Zampunieris, &Habris, 1995) and production-based expert system tool set (P-BEST) (Lindqvist&Porras, 1999). Other rule-based languages exist, but they are all similar in the sense that they all specify known attack patterns as event patterns.

## RUSSEL

RUSSEL is the language used in the advanced security audit trail analysis on UNIX (ASAX) project (Mounji, Charlier, Zampunieris, & Habris, 1995). It is a language specifically tailored to the problem of searching arbitrary patterns of records in sequential files. The language provides common control structures, such as conditional, repetitive, and compound actions. Primitive actions include assignment, external routine call, and rule triggering. A RUSSEL program simply consists of a set of rule declarations that are made of a rule name, a list of formal parameters and local variables, and an action part. RUSSEL also supports modules sharing global variables and exported rule declarations.

When intrusion detection is being enforced, the system analyzes the audit records one by one. For each audit record, the system executes all the active rules. The execution of an active rule may trigger (activate) new rules, raise alarms, write report messages, or alter global variables, for example. A rule can be triggered to be active for the current or the next record. In general, a rule is active for the current record because a prefix of a particular sequence of audit records has been detected. When all the rules active for the current record have been executed, the next record is read and the rules triggered for it in the previous step are executed in turn. User-defined and built-in C-routines can be called from a rule body.

RUSSEL is quite flexible in describing sequential event patterns and corresponding actions. The ability to work with user-defined C-routines gives the users the power to describe almost anything that can be specified in a programming language. The disadvantage is that it is a low-level language. Specifying an attack pattern is similar to writing a program, although it provides a general condition trigger framework and is declarative in nature. The feature that rules can share global variables introduces the possibility of bugs along with the convenience of sharing information among different rules.

## P-BEST

P-BEST was developed for the multiplexed information and computing service (Multics) intrusion detection and alerting system(MIDAS) and later employed by the intrusion detection expert system (IDES), NIDES, and the event monitoring enabling responses to anomalous live disturbances

(EMERALD) (Lindquist Y Porras, 1999). The P-BEST toolset consists of a rule translator, a library of runtime routines, and a set of garbage collection routines. Rules and facts in P-BEST are written in production rule specification Language. The rule translator is then used to translate the specification into an expert system program in C language, which can then be compiled into either a stand-alone, self-contained executable program or a set of library routines that can be linked to a larger software framework. The P-BEST language is quite small and intuitive. In P-BEST, the user specifies the structure of a fact (e.g., an audit record) through a template definition referred to as a pattern type. For example, an event consisting of four field sæevent_type (an integer), return code (an integer), username (a string), and hostname (a string) can be defined as ptype [event event type: int, return code: int, username: string, hostname: string].Thus, P-BEST does not depend on the structure of the input data. One important advantage of P-BEST is that it is a language pre-processor (i.e., it generates a precompiled expert system) and can extend its ability by invoking external C functions. However, it shares a similar problem with RUSSEL: It is a low-level language. Specification of attack patterns in P-BEST is time consuming. When many related rules are included in a system, correctness of the rules is difficult to check due to the interaction of these rules.

## Specification-Based Detection

A set of constraints are defined in this system that describes the correct operation of the program or protocol and then monitors the program with respect to the defined constraints. This technique provides the capability of detecting previously unknown attacks.

## Comparative Analysis between Anomaly, Misuse and Specification

Cost of Anomaly based ids is comparatively less than Misuse based ids where as cost of Specification ids are much higher than both. Anomaly based technique identifies attacks based on behavior, Misuse based technique identifies attack if that attack is already identified before by matching the attacks and Specification based technique defines the

**Table 4: Comparison of ID Techniques**

| Anomaly IDS | Misuse IDS | Specification IDS |
|---|---|---|
| recognize a typical behavior | recognize known attacks | Describes the desirable behavior of the system |
| Cost is less | Costly than anomaly | Expensive |
| Define a set of metrics for the system | Define a set of attack *signatures* | Define a set of specifications |
| Build a statistical model for those metrics during "normal" operation | Detect actions that match a signature | Detect specifications that does not match with the specified system's specification |
| Detect when metrics differ significantly from normal | Add new signatures often | Sequence of operations executed outside of the system's specifications is considered to be a security violation |
| Examples: MIDA(Modular Interactive Data Acquisition) | Examples: Cyber Cop, GRIDS(Global Resource Information Database), Stalker, Tripwire | Examples: SHIM(System Health and Intrusion Monitoring) |

specifications for the system and if anything goes out of that specification than that is considered as attack.

## Conclusion

Only intrusion detection techniques are not sufficient for securing wireless network but there is also need of good Intrusion Detection System. In this paper we have analysed various IDS and their techniques. According to the nature of mobile ad hoc networks, almost all of the intrusion detection systems (IDSs) uses anomaly based technique to identify malicious nodes and attacks.

## References


1. Dhangar Kiran, Kulhare Deepak and Khan Arif (2013), "Intrusion Detection System (A Layered Based Approach for Finding Attacks)." *International Journal of Advance Research in Computer Science and Software Engineering,* 3(5).
2. Karthikeyan K.R, A.Indra (2010). "Intrusion Detection Tools and Techniques - A Survey". *International Journal of Computer Theory and Engineering,* 2(6), 901-906.
3. Tamilarasan S, Aramudan, (2011)."A Performance and Analysis of Misbehaving Node in Manet Using Intrusion Detection System". *IJCSNS International Journal of Computer Science and Technology,* 11(5), 258-264.
4. Yang, Zhen, et al. (2006) "An Approach to Spam Detection by Naive Bayes Ensemble Based on Decision Induction", Intelligent Systems Design and Applications, in Proc. of Sixth International Conference, 861-866.
5. Masruroh N. A. and Poh K. L. (2007) "A Bayesian Network Approach to Job-shop Rescheduling," *International Journal of Computational Science* 1(2), 162-178.
6. Davis, Pei Jianping (2006). "Speed as a Risk Factor in Serious Run-off-road Crashes: Bayesian Case-Control Analysis with Case Speed Uncertainty", *Journal of Transportation and Statistics,* 9(1), 17-28.
7. Ning, Peng, and Jajodia Sushil. (2003). "Intrusion Detection Techniques." The Internet Encyclopedia.
8. Mounji, Charlier, Zampunieris, & Habris, "Distributed Audit Trail Analysis" In D.Baleson and R.Shrey (Eds), Proceedings of ISOC'95 Symposium on Network and Distributed System Security, IEEE computer Society, 102-112.
9. Lindqvist and Porras Y. "Detecting Computer and Network Misuse Through the Production Based Expert System Tools", Proceeding of the IEEE 1999 Symposium on Security and Policy, 146-161.