Intrusion Detection System For Adhoc Networks

1M.Narender, 2B.V.Suresh Kumar,

Abstract-The rapid proliferation of wireless networks and mobile computing applications has changed the landscape of network security. The recent denial of service attacks on major Internet sites have shown us, no open computer network is immune from intrusions. The wireless ad-hoc network is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense. The traditional way of protecting networks with firewalls and encryption software is no longer sufficient and effective. Many intrusion detection techniques have been developed on fixed wired networks but have been turned to be inapplicable in this new environment. We need to search for new architecture and mechanisms to protect wireless networks and mobile computing applications. In this paper, we examine the vulnerabilities of wireless networks and say that we must include intrusion detection in the security architecture for mobile computing environment. We have showed such architecture and evaluated key mechanisms in this architecture such as applying mobile agents to intrusion detection, anomaly detection and misuse detection for mobile ad-hoc networks.

Keywords-Intrusion, firewall, Adhoc networks, Route Discovery and Route maintenance.

I. INTRODUCTION

In the last three years, the networking revolution has finally come of age. More than ever before, we see that the Internet is changing computing, as we know it. The possibilities and opportunities are limitless; unfortunately, so too are the risks and chances of malicious intrusions. It is very important that the security mechanisms of a system are designed so as to prevent unauthorized access to system resources and data. However, completely preventing breaches of security appear, at present, unrealistic. We can, however, try to detect these intrusion attempts so that action may be taken to repair the damage later. This field of research is called Intrusion Detection.

A. Computer Security And Its Role

One broad definition of a secure computer system is given by Garfinkel and Spafford as one that can be depended upon to behave as it is expected to. It is always a point of benefit to integrate security with dependability and how to obtain a dependable computing system. Dependability is the trustworthiness of a system and can be seen as the quality of the service a system offers. Integrating security and dependability can be done in various ways. One approach is to treat security as one characteristic of dependability on the same level as availability, reliability and safety. A narrower definition of security is the possibility for a system to protect objects with respect to confidentiality, authentication, integrity and non-repudiation.

B. Threats Of Security

Threats can be seen as potential violations of security and exist because of vulnerabilities, i.e. weakness, in a system. There are two basic types of threats: accidental threats and intentional threats.

i. Accidental Threat

An accidental threat can be manifested and the result is either an exposure of confidential information or cause of an illegal system state to occur, i.e. modification of an object. Exposures can emerge from both hardware and software failures as well as from user and operational mistakes, thus resulting in the violation of confidentiality. It can also be manifested as modification of an object, which is the violation of object integrity. An object here can be both information and resource.

ii. Intentional Threat

An intentional threat is an action performed by an entity with the intention to violate security. Examples of attacks are interruption, modification, interception and fabrication of data.

C. Vulnerabilities Of Mobile Wireless Networks

The nature of mobile computing environment makes it very vulnerable to adversary’s malicious attacks. Firstly, the use of wireless links renders the network susceptible to attacks ranging from passive eavesdropping to active interfering as attacks on these links can from any direction and target at any node. This means that a wireless ad-hoc network will not have a clear line of defense, and every node has to be prepared for encounters with an adversary directly or indirectly.

Secondly, mobile nodes are autonomous units that are capable of roaming independently. Since tracking down a particular mobile node in a global scale network cannot be done easily, attacks by compromised node from within the network are more damaging and harder to detect.

Third, decision-making in mobile computing environment is sometimes decentralized and some wireless network algorithms rely on the cooperative participation of all nodes and the infrastructure. Furthermore, mobile
computing has introduced new type of computational and communication activities that seldom appear in fixed or wired environment. Applications and services in a mobile wireless network can be a weak link as well.

D. Need For Intrusion Detection

A computer system should provide confidentiality, integrity and assurance against denial of service. However, due to increased connectivity (especially on the Internet), and the vast spectrum of financial possibilities that are opening up, more and more systems are subject to attack by intruders. These subversion attempts try to exploit flaws in the operating system as well as in application programs and have resulted in spectacular incidents like the Internet Worm incident of 1988.

There are two ways to handle subversion attempts. One way is to prevent subversion itself by building a completely secure system. We could, for example, require all users to identify and authenticate themselves; we could protect data by various cryptographic methods and very tight access control mechanisms.

The history of security research has taught us a valuable lesson – no matter how many intrusion prevention measures are inserted in a network, there are always some weak links that one could exploit to break in. We thus see that we are stuck with systems that have vulnerabilities for a while to come. If there are attacks on a system, we would like to detect them as soon as possible (preferably in real-time) and take appropriate action. This is essentially what an Intrusion Detection System (IDS) does. An IDS does not usually take preventive measures when an attack is detected; it is a reactive rather than proactive agent. It plays the role of an informant rather than a police officer.

II. BACKGROUND ON INTRUSION DETECTION

In the last three years, the networking revolution has finally come of age. More than ever before, we see that the Internet is changing computing, as we know it. The possibilities and opportunities are limitless; unfortunately, so too are the risks and chances of malicious intrusions.

It is very important that the security mechanisms of a system are designed so as to prevent unauthorized access to system resources and data. However, completely preventing breaches of security appear, at present, unrealistic. We can, however, try to detect these intrusion attempts so that action may be taken to repair the damage later. This field of research is called Intrusion Detection.

A simple firewall can no longer provide enough security as in the past. Today's corporations are drafting intricate security policies whose enforcement requires the use of multiple systems, both proactive and reactive (and often multi-layered and highly-redundant). The premise behind intrusion detection systems is simple: Deploy a set of agents to inspect network traffic and look for the anomalies of known network attacks.

However, the evolution of network computing and the awesome availability of the Internet have complicated this concept somewhat. With the advent of Distributed Denial of Service (DDOS) attacks, which are often launched from hundreds of separate sources, the traffic source no longer provides reliable temporal clues that an attack is in progress. Worse yet, the task of responding to such attacks is further complicated by the diversity of the source systems, and especially by the geographically distributed nature of most attacks.

Intrusion detection techniques while often regarded as grossly experimental, the field of intrusion detection has matured a great deal to the point where it has secured a space in the network defense landscape alongside firewalls and virus protection systems. While the actual implementations tend to be fairly complex, and often proprietary, the concept behind intrusion detection is a surprisingly simple one: Inspect all network activity (both inbound and outbound) and identify suspicious patterns that could be evidence of a network or system attack.

A. Classification Of Intrusion Detection Systems

Intrusions can be divided into 6 main types

i. Attempted break-ins, which are detected by atypical behavior profiles or violations of security constraints.

ii. Masquerade attacks, which are detected by atypical behavior profiles or violations of security constraints.

iii. Penetration of the security control system, which are detected by monitoring for specific patterns of activity.

iv. Leakage, which is detected by atypical use of system resources.

v. Denial of service, which is detected by atypical use of system resources.

vi. Malicious use, which is detected by atypical behavior profiles, violations of security constraints, or use of special privileges.

We can divide the techniques of intrusion detection into two main types.

B. Anomaly Detection

Anomaly detection techniques assume that all intrusive activities are necessarily anomalous. This means that if we could establish a "normal activity profile" for a system, we could, in theory, flag all system states varying from the established profile by statistically significant amounts as intrusion attempts. However, if we consider that the set of intrusive activities only intersects the set of anomalous activities instead of being exactly the same, we find a couple of interesting possibilities: (1) Anomalous activities that are not intrusive are flagged as intrusive. (2) Intrusive activities that are not anomalous result in false negatives (events are
not flagged intrusive, though they actually are). This is a dangerous problem, and is far more serious than the problem of false positives.

The main issues in anomaly detection systems thus become the selection of threshold levels so that neither of the above 2 problems is unreasonably magnified, and the selection of features to monitor. Anomaly detection systems are also computationally expensive because of the overhead of keeping track of, and possibly updating several system profile metrics. Some systems based on this technique are discussed in Section 4 while a block diagram of a typical anomaly detection system is shown in Figure below.

### C. Misuse Detection

The concept behind misuse detection schemes is that there are ways to represent attacks in the form of a pattern or a signature so that even variations of the same attack can be detected. This means that these systems are not unlike virus detection systems -- they can detect many or all known attack patterns, but they are of little use for as yet unknown attack methods. An interesting point to note is that anomaly detection systems try to detect the complement of "bad" behavior. Misuse detection systems try to recognize known "bad" behavior. The main issues in misuse detection systems 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 activity. A block diagram of a typical misuse detection system is shown in Figure below.

### D. Network Based Intrusion Detection

The most obvious location for an intrusion detection system is right on the segment being monitored. Network-based intrusion detectors insert themselves in the network just like any other device, except they promiscuously examine every packet they see on the wire.

### E. Host Based Intrusion Detection

While network-based intrusion detectors are straightforward to deploy and maintain, there is a whole class of attacks closely coupled to the target system and extremely hard to fingerprint. These are the ones that exploit vulnerabilities particular to specific operating systems and application suites. Only host-based intrusion detection systems (the ones running as an application on a network connected host) can correlate the complex array of system-specific parameters that makeup the signature of a well orchestrated attack.

### III. ANOMALY DETECTION SYSTEMS

There have been a few approaches to anomaly intrusion detection systems, some of which are described below.

#### A. Statistical Approaches

In this method, initially, behavior profiles for subjects are generated. As the system continues running, the anomaly detector constantly generates the variance of the present profile from the original one. We note that, in this case, there may be several measures that affect the behavior profile, like activity measures, CPU time used, number of network connections in a time period, etc. In some systems, the current profile and the previous profile are merged at intervals, but in some other systems profile generation is a one-time activity.

An open issue with statistical approaches in particular, and anomaly detection systems in general, is the selection of measures to monitor. It is not known exactly what the subset of all possible measures that accurately predicts intrusive activities is. Static methods of determining these measures are sometimes misleading because of the unique features of a particular system. Thus, it seems that a combination of static and dynamic determination of the set of measures should be done. Some problems associated with this technique have been remedied by other methods, including the method involving Predictive Pattern Generation, which takes past events into account when analyzing the data.

#### B. Predictive Pattern Generation

This method of intrusion detection tries to predict future events based on the events that have already occurred. Therefore, we could have a rule $E_1 - E_2 \rightarrow \left( E_3 = 80\%, E_4 = 15\%, E_5 = 5\% \right)$ This would mean that given that events $E_1$ and $E_2$ have occurred, with $E_2$ occurring after $E_1$, there is an 80% probability that event $E_3$ will follow, a 15% chance that event $E_4$ will follow and a 5% probability that event $E_5$ will follow.

**Problem** - The problem with this is that some intrusion scenarios that are not described by the rules will not be
flagged intrusive. Thus, if an event sequence A - B - C exists that is intrusive, but not listed in the rule base, it will be classified as unrecognized.

**Solution.** The above problem can be partially solved by flagging any unknown events as intrusions (increasing the probability of false positives), or by flagging them as nonintrusive (thus increasing the probability of false negatives). In the normal case, however, an event is flagged intrusive if the left hand side of a rule is matched, but the right hand side is statistically very deviant from the prediction.

**C. Neural Networks**

Another approach taken in intrusion detection systems is the use of neural networks. The idea here is to train the neural network to predict a user's next action or command, given the window of _n_ previous actions or commands. The network is trained on a set of representative user commands. After the training period, the network tries to match actual commands with the actual user profile already present in the net. Any incorrectly predicted events actually measure the deviation of the user from the established profile.

**IV. MISUSE DETECTION SYSTEMS**

There has been significant research in misuse detection systems in the recent past. Some of these systems are explained in depth in this section.

**A. Expert Systems**

These systems are modeled in such a way as to separate the rule matching phase from the action phase. The matching is done according to audit trail events. IDES follows a hybrid intrusion detection technique consisting of a misuse detection component as well as an anomaly detection component. The anomaly detector is based on the statistical approach, and it flags events as intrusive if they are largely deviant from the expected behavior. To do this, it builds user profiles based on many different criteria (more than 30 criteria, including CPU and I/O usage, commands used, local network activity, system errors, etc.). These profiles are updated at periodic intervals. The expert system misuse detection component encodes known intrusion scenarios and attack patterns (bugs in old versions of send mail could be one vulnerability). The rule database can be changed for different systems.

**B. Keystroke Monitoring**

This is a very simple technique that monitors keystrokes for attack patterns. Unfortunately the system has several defects features of shells like `bash`, `ksh`, and `tcsh` in which user definable aliases are present defeat the technique unless alias expansion and semantic analysis of the commands is taken up. The method also does not analyze the running of a program, only the keystrokes. This means that a malicious program cannot be flagged for intrusive activities. Operating systems do not offer much support for keystroke capturing, so the keystroke monitor should have a hook that analyses keystrokes before sending them on to their intended receiver. An improvement to this would be to monitor system calls by application programs as well, so that an analysis of the program's execution is possible.

**C. Model Based Intrusion Detection**

States that are certain scenarios are inferred by certain other observable activities. If these activities are monitored, it is possible to find intrusion attempts by looking at activities that infer a certain intrusion scenario. The model-based scheme consists of three important modules. The anticipator uses the activemodels and the scenario models to try to predict the next step in the scenario that is expected to occur. A scenario model is a knowledge base with specifications of intrusion scenarios. The planner then translates this hypothesis into a format that shows the behavior, as it would occur in the audit trail. It uses the predicted information to plan what to search for next. The interpreter then searches for this data in the audit trail. The system proceeds this way, accumulating more and more evidence for an intrusion attempt until a threshold is crossed; at this point, it signals an intrusion attempt.

**V. IDS ISSUES IN MOBILE ENVIRONMENT**

Intrusion detection for traditional, wired networks has been the topic of significant research over the past few years. A problem arises, however, when taking the research for wired networks and directly applying it to wireless networks. Key assumptions are made when designing IDSs for wired networks, such as the difficulty for an attacker to penetrate the physical security of the system, the amount of network bandwidth available to the IDS, etc. Specific problems faced when building IDSs for a mobile network are addressed below.

**A. Lack of Physical Wires**

The most obvious difference when building an IDS in a wireless environment is the fact that an attacker no longer has to gain physical access to the system in order to compromise the security of the network. Potentially, it is very simple for someone to eavesdrop on network traffic in a wireless environment because they no longer have to break through any physical medium to gain access to the traffic.

**B. Bandwidth Issues**

Wireless networks have more constrained bandwidth as compared to wired networks. This problem can manifest itself in a number of different ways when an IDS is using wireless communication to convey information between parts of IDS on separate nodes. An IDS in a mobile environment must be extremely careful to limit the amount of communication that takes place between nodes. A second
problem that may possibly arise because of limited bandwidth is erroneous behavior of the IDS due to communication delay between nodes.

C. Difficulty of Anomaly/Normality Distinction

Distinguishing an anomaly from normalcy has always been somewhat difficult for wired IDSs and wireless IDSs are no different. If nodes in a network receive false or old routing information from a particular node then it is difficult to verify if that particular node has been compromised or not. An attacker could have taken the control of the node to send false information to other nodes in the network, or the node could just be temporarily out of sync due to fast movement or other processing requirements.

D. Secure Communication Between IDS Agents

It is likely that in a wireless network there will have to be portions of the IDS running on each individual node in the network. Each of these IDS agents will have to communicate with other IDS agents in the network to convey information relating to the status of the system. It is crucial that the information being passed from agent to agent be encrypted as to not allow an attacker to gain access to the communication.

E. Lack of Centralized Access/Audit Point

The lack of centralized audit points in ad hoc networks present difficult problems for intrusion detection. Most static, wired networks have specific repositories where the IDS can obtain audit data for its misuse and anomaly detection (e.g., switches, routers, gateways, etc.). Without centralized audit points, IDSs on ad hoc networks are limited to use only the current traffic coming in and out of the node as audit data. The algorithms that the IDS uses must be distributed, and take into account the fact that a node can only see a portion of the network traffic.

F. Possibility of a Node Being Compromised

Since ad hoc networks are dynamic and nodes can move about freely, there is a possibility that one or more nodes could become captured and compromised, especially if the network is in a hostile environment.

If the algorithms of the IDS are cooperative, it becomes important to be skeptical of which nodes one can trust. IDSs on ad hoc networks have to be weary of attacks made by nodes in the network itself, not just attacks from outside the network.

G. Difficulty in Obtaining Enough Audit Data

Mobile networks do not communicate as frequently as their wired counterparts. Bandwidth issues, and other issues such as battery life, contribute to this factor. This lack of communication can become a problem for IDSs attempting to define rules of normality for anomaly detection. If only a small amount of data is available to establish normal activity association rules, it is very hard to distinguish an attack from regular network use.

VI. NEW ARCHITECTURE

It is important to understand that most IDS architectural models are based on static, wired networks. These models alone are insufficient to help design an IDS in a mobile, ad hoc network environment. The architecture addressed is a distributed IDS, where each node on the network will have an IDS agent running on it. The IDS agents on each node in the network work together via a cooperative intrusion detection algorithm to decide when and how the network is being attacked. The architecture is divided into parts: the Mobile IDS Agents, which reside on each node in the network, and the Stationary Secure Database, which contains global signatures of known misuse attacks and stores patterns of each user's normal activity in a non-hostile environment.

A. Mobile IDS Agents

Each node in the network will have an IDS agent running on it all the time. This agent is responsible for detecting intrusions based on local audit data and participating in cooperative algorithms with other IDS agents to decide if the network is
being attacked. Each agent has five parts: the Local Audit Trial, the Local Intrusion Database (LID), the Secure Communication Module, the Anomaly Detection Modules (ADM s), and the Misuse Detection Modules (MDM s).

i. **The Local Audit Trial**

Each agent must constantly check the audit data to decide that an intrusion is not taking place. The Local Audit Trial will consist of specific items out of the network traffic as well as user commands to the node. The Local Audit Trial is responsible for selecting only the items it needs out of the network traffic and system audit data in order to minimize the size of the audit data collected. A audit data is collected by the Local Audit Trial, it is passed to the Misuse Detection Modules and the Anomaly Detection Modules for further analysis. The Local Audit Trial is only responsible for gathering and storing audit data, not processing it.

ii. **The Local Intrusion Database (LID)**

The LID is a local database that warehouses all information necessary for the IDS agent, such as the signature files of known attacks, the established patterns of users on the network, and the normal traffic flow of the network. The Anomaly Detection Modules and Misuse Detection Modules communicated directly with the LID to determine if an intrusion is taking place.

iii. **The Secure Communication Module**

The Secure Communication Module is necessary to enable an IDS agent to communicate with other IDS agents on other nodes. It will allow the MDM s and ADM s to use cooperative algorithms to detect intrusions. It may also be used to initiate a global response when an IDS agent or a group of IDS agents detects an intrusion. Basically, any communication that needs to occur from one IDS agent to another will use the Secure Communication Module. Data communicated via the Secure Communication Module will need to be encrypted inorder to ensure that the data received by an IDS agent is accurate and has not been tampered with. The Secure Communication module is only used by IDS agents and does not communicate any other type of information between nodes. It must share the bandwidth that the mobile device uses for normal data transmission, so it is required to be efficient, and can only use the amount of bandwidth in need. Also, the Secure Communication module must process information coming to the IDS Agent from other agents in the network. For this reason, it must be fast and efficient, so as not to take away from the processing time of the mobile unit.

iv. **The Anomaly Detection Modules (ADM s)**

Each Anomaly Detection Module is responsible for detecting a different type of anomaly. There can be one to many Anomaly Detection Modules on each mobile IDS agent, each working separately or cooperatively with other ADM s. For example, one ADM might be looking for strange network traffic patterns, while another ADM might be watching user input speed.

v. **The Misuse Detection Modules (MDM s)**

The Misuse Detection Modules function similarly to the ADM s on the IDS agent. The primary difference is that MDM s only identifies known patterns of attacks that are specified in the Local Intrusion Database. Like the ADM s, if the audit data available locally is enough to determine if an intrusion is taking place, the proper response can be initiated. It is also possible for a MDM to use a cooperative algorithm to identify an intrusion.

B. **Stationary Secure Database**

The Stationary Secure Database (SSD) in this architecture acts as a secure, trusted repository for mobile nodes to obtain information about the latest misuse signatures and to find the latest patterns of normal user activity. It is assumed that the attacker will not compromise the Stationary Secure Database, as it stored in area of high security. To ensure that the SSD will not be compromised it is kept stationary and not placed in a hostile environment where attacker attack is likely. It is also assumed that no physically compromised node will come in contact with the SSD, since the attacker will not be given physical access to the area where the SSD resides. Although these are severe restrictions, they can be accommodated through operational procedures and physical security. The mobile IDS agents will collect and store audit data while in the field, and will transfer this information when it is attached to the SSD. The SSD will then use this information for data mining of new anomaly association rules. The use of the SSD to mine new anomaly rules is beneficial to the IDS for three reasons. First, the SSD will be fixed, fast machine that is capable of mining rules much faster than on slower, mobile nodes. Second, the processing time used to mine the new rules of anomaly will not take away from the processing time of the mobile nodes.
The SSD will also be the place where the system administrator can specify the newest misuse signatures. When the IDS agents are connected to SSD, they will gain access to the latest attack signatures automatically. This will make it much easier to update all the nodes in the network to keep up with the latest attacks. Instead of manually updating the attack files in the Local Intrusion Database of each individual node, or using the Secure Communication device on each node to communicate the new signatures, the SSD will be responsible for communicating the new attack signatures to each individual IDS agent.

One of the best reasons for using the SSD to communicate the new attack signatures, and establish new patterns of normalcy, is to limit the amount of communication that must take place between IDS agents in the mobile ad hoc network. As stated earlier, the IDS agents should not use very much bandwidth, because it is limited and in use by other applications on the mobile node. The use of SSD allows the IDS agents to not continually have to share information in order to update their Local Intrusion Database. Communication between the SSD and the IDS agents will be very quick and efficient, as there should be no threat of attack. By relying on the SSD to be a trusted source of update information in order to update their Local Intrusion Database, communication between the SSD and the IDS agents will be very quick and efficient, as there should be no threat of attack. By relying on the SSD to be a trusted source of update information, the IDS agent no longer has to use cooperative algorithms to determine if the information being sent is trustworthy or not.

VII. ANOMALY DETECTION IN WIRE-LESS AD-HOC NETWORKS

In this section we discuss how to build an anomaly detection models for wireless networks. Detection based on activities in different network layers may differ in the format and the amount of available audit data as well as the modeling algorithms.

A. Building An Anomaly Detection Model

i. Framework

The basic premise for anomaly detection is that there is an intrinsic and observable characteristic of normal behavior that is distinct from that of abnormal behavior. Entropy and conditional entropy are used to describe the characteristics of the normal information flows and use the classification algorithms to build anomaly detection models. We can use a classifier trained using normal data to predict what normally the next event is given the previous n events. In monitoring when the actual event is not what the classifier has predicted there is an anomaly. When constructing a classifier features with high information gain are needed.

Using this framework we employ the following procedure for the anomaly detection.

a. Select or partition audit data so that the normal data set has low Entropy
b. Perform appropriate data transformation according to entropy measures
c. Compute classifier using training data.
d. Apply the classifier to test it.
e. Post process alarms to produce intrusion reports.

ii. Attack Models

Route logic compromise- This type of attacks behaves by manipulating routing information, either externally by parsing false route messages or internally by maliciously changing routing cache information. In particular, we consider several special cases: (a) misrouting: forwarding a packet to an incorrect node; and (b) false message propagation: distributing a false route update.

Traffic pattern distortion- This type of attacks changes default/normal traffic behavior: (a) packet dropping; (b) packet generation with faked source address; (c) corruption on packet contents; and (d) denial-of-service.

B. Areas Where Anomaly Detection Can Be Used

The two main areas where we need anomaly detection is ad-hoc networks is

· Abnormal Updates to the routing table.
· Abnormal activities in other layers.

i. Abnormal Updates to the routing table.

The two most important factors that are required for the anomaly detection are Low False positive rate High true positive rate (percentage of anomalies detected). A routing table usually contains, at the minimum the next hop to each destination node and the number of hops. The physical movement of nodes or network membership changes causes a legitimate movement in the routing table. Our objective in this study is to lead a better understanding of the important
and challenging issues in intrusion detection for ad-hoc routing protocols. First using a given set of training, testing and evaluation scenarios, and modeling algorithms, we can identify which routing protocol, with potentially all its routing information used, can result in better performing detection models. This will help answer the question “what information should be included in the routing table to make intrusion detection effective”. This finding can be used in designing more robust protocols.

ii. Abnormal Activities In other layers

At the wireless application layer, the trace data can use the service as the class (i.e., one class for each service), and can contain the following features: for the past s seconds, the total number of requests to the same service, the number of different services requested, the average duration of the service, the number of nodes that requested (any) service, the total number of service errors, etc. A classifier on the trace data then describes for each service the normal behaviors of its requests. Many attacks generate different statistical patterns than normal requests.

VIII. IMPLEMENTED APPROACHES

Following are some of the intrusion detection techniques used in wireless and ad hoc networks.

A. IEEE 802.11

The IEEE 802.11 standard provides several mechanisms intended to provide a secure operating environment. The IEEE 802.11 standard defines the physical layers and the MAC sub layers for the wireless LANs. There are three different physical layers. They are Frequency hopping Spread Spectrum Radio; direct sequence spread spectrum Radio, and Base band infrared. The MAC layer is common for all these layers.

The IEEE 802.11 defines two authentication schemes:

i. Open System Authentication.

ii. Shared Key Authentication.

i. Open System Authentication

Open system authentication is the default authentication protocol for 802.11. As the name implies, open system authentication authenticates anyone who requests authentication. A terminal announces that it wishes to associate with an access point, and typically the access point allows the association. Essentially it provides NULL authentication process.

ii. Shared Key Authentication

Shared key authentication uses a standard challenge and response along with a shared secret key to provide authentication. The shared key Authentication requires that the Wired Equivalent privacy protocol (WEP) Algorithm be implemented on both the wireless terminal and the access point. The station wishing to authenticate, the initiator, sends an authentication request management frame indicating that they wish to use “shared key” authentication. The recipient of the authentication request, the responder, responds by sending an authentication management frame containing challenge text to the initiator. The challenge text is generated by using the WEP pseudo-random number generator (PRNG) with the “shared secret” and a random initialization vector (IV). Once the initiator receives the management frame from the responder, they copy the contents of the challenge text into a new management frame body. This new management frame body is then encrypted with WEP using the “shared secret” along with a new IV selected by the initiator. The encrypted management frame is then sent to the responder. The responder decrypts the received frame and verifies that the 32-bit CRC integrity check value (ICV) is valid, and that the challenge text matches that sent in the first message. If they do, then authentication is successful. If the authentication is successful, then the initiator and the responder switch roles and repeat the process to ensure mutual Authentication.

Figure: Mutual Station Authentication Using Shared Keys

Mobiles that are allowed to connect to the network use the same shared key, so this authentication method is only able to verify if the particular mobile belongs to the group allowed to connect to the network, but there is no way to distinguish one mobile from another. Also there are no means available to authenticate the network. The IEEE 802.11 does not define any key management functions. The IEEE 802.11 defines an optional WEP mechanism to implement the confidentiality and integrity of the traffic in the network. WEP is used at the station-to-station level and does not offer any end-to-end security. Using, say, the playback attack, could easily fool the Shared Key Authentications scheme. Hence, anyway an additional authentication mechanism is needed.

iii. Secure Key Generation And Distribution
The mobile systems have constraints like minimal computational capabilities and authentication and the Secure key generation and distribution capability is required by any system, which contains cryptographic authentication, confidentiality and identification. Developing faster and more powerful hardware components, which require less Energy and changing the algorithmic and protocol design of the current system would be useful to meet the future needs.

iv. Current Approaches For The Key Generation

a. Key generation by the telephone manufacturer and distribution to the Service Provider via a backbone network

This requires the manufacturers and Service provider to develop a special distribution channel. (b) Security of keys should be ensured from the time the keys are sent to the Service provider from the manufacturer. (c) This approach is unacceptable to both the Service provider and the manufacturer.

b. Over-The-Air Phone Activation With Key Exchange

Over-the-air phone is the most preferred approach and requires a collaborative key generation and distribution between the mobile unit and the Service provider. The current over-the-air service provisioning (OTASP) uses the Diffie-Hellman key exchange between the Service provider and mobile unit to exchange a symmetric key called A-key (Authentication Key).

IX. CONCLUSION

The diligent management of network security is essential to the operation of networks, regardless of whether they have segments or not. It is important to note that absolute security is an abstract concept—it does not exist anywhere. All networks are vulnerable to insider or outsider attacks, and eavesdropping. No one wants to risk having the data exposed to the casual observer or open malicious mischief. Regardless of whether the network is wired or wireless, steps can and should always be taken to preserve network security and integrity.

We have said that any secure network will have vulnerabilities that an adversary could exploit. This is especially true for wireless ad-hoc networks. Intrusion Detection can compliment intrusion prevention techniques (such as encryption, authentication, secure MAC, secure routing, etc.) to improve the network security. However new techniques must be developed to make intrusion detection work better for the wireless networks. We have shown that an architecture for better intrusion detection in wireless networks should be distributed and cooperative by applying Mobile Agents to the network and given few of the implemented approaches for intrusion detection. Currently, the research is taking place in developing new architecture for wireless networks for better security.

X. REFERENCES

5) Wenken Lee, Dong Xiang, Informatic-Theoretic Measures for Anomaly Detection.
9) Krugel , T. Toth., Applying Mobile Agent Technology to Intrusion Detection
10) Kumar S., “Classification and Detection of Computer Intrusion “.