Intrusion Detection System For Adhoc Networks

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

GJCST Classification
C.2.0,D.4.6

***Abstract*-The rapid proliferation of wireless networks and mobile computing applications has changed thelandscape of network security. The recent denial of service attacks on major Internet sites have shown us, no open computer network is immunefrom intrusions. The wireless ad-hoc network is particularly vulnerable due to its featuresof open medium, dynamic changing topology, cooperative algorithms, lack of centralizedmonitoring and management point, and lack of a clear line of defense. The traditionalway of protecting networks with firewalls and encryption software is no longer sufficientand effective. Many intrusion detection techniques have been developed on fixed wirednetworks but have been turned to be inapplicable in this new environment. We need tosearch for new architecture and mechanisms to protect wireless networks and mobilecomputing application. In this paper, we examine the vulnerabilities of wireless networksand say that we must include intrusion detection in the security architecture for mobilecomputing environment. We have showed such architecture and evaluated keymechanisms 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 finallycome of age. More than ever before, we see that the Internet is changing computing, aswe know it. The possibilities and opportunities are limitless; unfortunately, so too are therisks and chances of malicious intrusions. It is very important that the securitymechanisms of a system are designed so as to prevent unauthorized access to systemresources and data. However, completely preventing breaches of security appear, atpresent, unrealistic. We can, however, try to detect these intrusion attempts so that actionmay be taken to repair the damage later. This field of research is called IntrusionDetection.

A. Computer Security And Its Role

One broad definition of a secure computer system is given by Garfinkel and Spafford asone 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 existbecause of vulnerabilities, i.e. weakness, in a system. There are two basic types ofthreats: accidental threats and intentional threats.

i. Accidental Threat

An accidental threat can be manifested and the result is eitheran 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 softwarefailures as well as from user and operational mistakes thus resulting in the violation ofconfidentiality. It can also be manifested as modification of an object, which is theviolation 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 withthe 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 an adversary'smalicious attacks.

Firstly, the use of wireless links renders the network susceptible to attacks rangingfrom passive eavesdropping to active interfering as attacks on these links can from anydirection 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 anadversary 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 doneeasily, attacks by compromised node from within the network are more damaging andharder to detect.

Third, decision-making in mobile computing environment is sometimes decentralized andsome wireless networkalgorithms rely on the cooperative participation of all nodes andthe infrastructure. Furthermore, mobile

[1]*M.Narender, Asst.prof. of CSE dept, HITS college of Engg, Hyderabad. Machha.narender@gmail.com*
[2]*B.V.Suresh Kumar, Asst. prof. of IT dept, MLEC, Singarayakonda Prakasam(dt), sureshkumar1239@gmail.com*

computing has introduced new type ofcomputational and communication activities that seldom appear in fixed or wiredenvironment. Applications and services in a mobile wireless network can be a weak linkas well.

D. Need For Intrusion Detection

A computer system should provide confidentiality, integrity and assurance against denialof 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 aresubject to attack by intruders. These subversion attempts try to exploit flaws in theoperating 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 subversionitself by building a completely secure system. We could, for example, require all users to identify and authenticate themselves; we could protect data by various cryptographicmethods and very tight access control mechanisms.

The history of security research has taught us a valuable lesson – no matter how manyintrusion prevention measures are inserted in a network, there are always some weaklinks that one could exploit to break in. We thus see that we are stuck with systems thathave vulnerabilities for a while to come. If there are attacks on a system, we would like todetect them as soon as possible (preferably in real-time) and take appropriate action. This isessentially what an Intrusion Detection System (IDS) does. An IDS does not usuallytake preventive measures when an attack is detected; it is a reactive rather than pro-activeagent. 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 toprevent unauthorized access to system resources and data. However, completelypreventing breaches of security appear, at present, unrealistic. We can, however, try todetect 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'scorporations are drafting intricate security policies whose enforcement requires the use ofmultiple systems, both proactive and reactive (and often multi-layered and highlyredundant). The premise behind intrusion detection systems is simple: Deploy a set ofagents to inspect network traffic and look for the —signatures" of known network attacks.

However, the evolution of network computing and the awesome availability of theInternet have complicated this concept somewhat. With the advent of Distributed Denialof 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 diversityof the source systems, and especially by the geographically distributed nature of mostattacks.

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

A. Classification Of Intrusion Detection Systems

Intrusions can be divided into 6main types

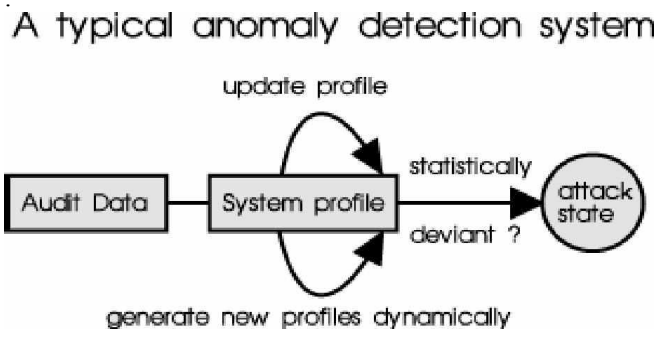
i. Attempted break-ins, which are detected by atypical behavior profiles or violations ofsecurity constraints.
ii. Masquerade attacks, which are detected by atypical behavior profiles or violations ofsecurity constraints.
iii. Penetration of the security control system, which are detected by monitoring forspecific 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 securityconstraints, or use of special privileges.

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

B. Anomaly Detection

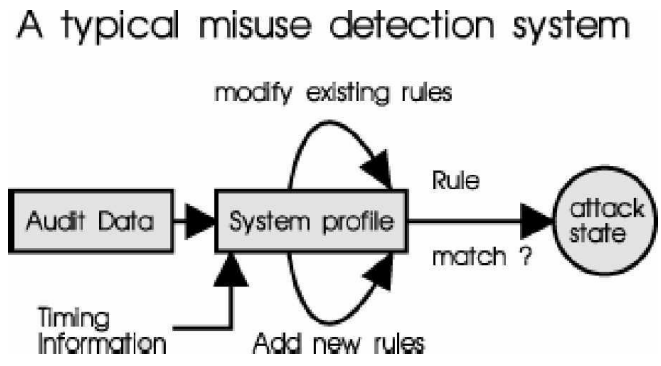
Anomaly detection techniques assume that all intrusiveactivities are necessarily anomalous. This means that if we could establish a "normalactivity profile" for a system, we could, in theory, flag all system states varying from theestablished profile by statistically significant amounts as intrusion attempts. However, ifwe consider that the set of intrusive activities only intersects the set of anomalousactivities 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) Intrusiveactivities 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 theproblem of false positives.
The main issues in anomaly detection systems thus become the selection of thresholdlevels so that neither of the above 2 problems is unreasonably magnified, and theselection of features to monitor. Anomaly detection systems are also computationallyexpensive because of the overhead of keeping track of, and possibly updating severalsystem profile metrics. Some systems based on this technique are discussed in Section 4while 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 areways to represent attacks in the form of a pattern or a signature so that even variations ofthe 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 oflittle 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 detectionsystems try to recognize known "bad" behavior. The main issues in misuse detectionsystems are how to write a signature that encompasses all possible variations of thepertinent 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 intrusiondetection system is right on the segment being monitored. Network-based intrusiondetectors insert themselves in the network just like any other device, except theypromiscuously examine every packet they see on the wire.

E. Host Based Intrusion Detection

While network-based intrusion detectors arestraightforward to deploy and maintain, there is a whole class of attacks closely coupledto the target system and extremely hard to fingerprint. These are the ones that exploitvulnerabilities particular to specific operating systems and application suites. Only hostbasedintrusion detection systems (the ones running as an application on a networkconnectedhost) 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 ofwhich are described below.

A. Statistical Approaches

In this method, initially, behavior profiles for subjects aregenerated. As the system continues running, the anomaly detector constantly generatesthe variance of the present profile from the original one. We note that, in this case, theremay be several measures that affect the behavior profile, like activity measures, CPUtime used, number of network connections in a time period, etc. In some systems, thecurrent profile and the previous profile are merged at intervals, but in some other systemsprofile generation is a one time activity.
An open issue with statistical approaches in particular, and anomaly detection systems ingeneral, 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 ofdetermining these measures are sometimes misleading because of the unique features of A particular system. Thus, it seems that a combination of static and dynamic determinationof the set of measures should be done. Some problems associated with this techniquehave been remedied by other methods, including the method involving Predictive PatternGeneration, 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 E1 - E2 --> (E3 = 80%, E4 = 15%, E5 = 5%) This would mean that given that events E1 and E2 have occurred, with E2 occurring after E1, there is an 80% probability that event E3 will follow, a 15% chance that event E4 will follow and a 5% probability that event E5 will follow.

Problem- The problem with this is that some intrusion scenarios that are not described bythe rules will not be

flagged intrusive. Thus, if an event sequence A - B - C exists that isintrusive, 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 asintrusions (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 handside is statistically very deviant from the prediction.

C. *Neural Networks*

Another approach taken in intrusion detection systems is the useof neural networks. The idea here is to train the neural network to predict a user's nextaction or command, given the window of ‗n' previous actions or commands. The networkis trained on a set of representative user commands. After the training period, the networktries 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 theestablished profile.

IV. MISUSE DETECTION SYSTEMS

There has been significant research in misuse detection systems in the recent past. Someof 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 alsodoes 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 bycertain other observable activities. If these activities are monitored, it is possible to findintrusion attempts by looking at activities that infer a certain intrusion scenario. Themodel-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 isexpected to occur. A scenario model is a knowledge base with specifications of intrusionscenarios. The planner then translates this hypothesis into a format that shows thebehavior, as it would occur in the audit trail. It uses the predicted information to planwhat 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 attemptuntil 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 directlyapplying it to wireless networks. Key assumptions are made when designing IDS s forwired networks, such as the difficulty for an attacker to penetrate the physical security ofthe system, the amount of network bandwidth available to the IDS, etc. Specific problemsfaced when building IDS 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 tothe system in order to compromise the security of the network. Potentially, it is verysimple for someone to eavesdrop on network traffic in a wireless environment becausethey 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 comparedto wired networks. This problem can manifest itself in a number of different ways whenan IDS is using wireless communication to convey information between parts of IDS onseparate nodes. An IDS in a mobile environment must be extremely careful to limit theamount of communication that takes place between nodes. A second

problem that maypossibly 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 fromnormalcy has always been somewhat difficult for wired IDS s and wireless IDS s are nodifferent. If nodes in a network receive false or old routing information from a particularnode then it is difficult to verify if that particular node has been compromised or not. Anattacker could have taken the control of the node to send false information to other nodesin the network, or the node could just be temporarily out of sync due to fast movement orother processing requirements.

D. *Secure Communication Between Ids Agents*

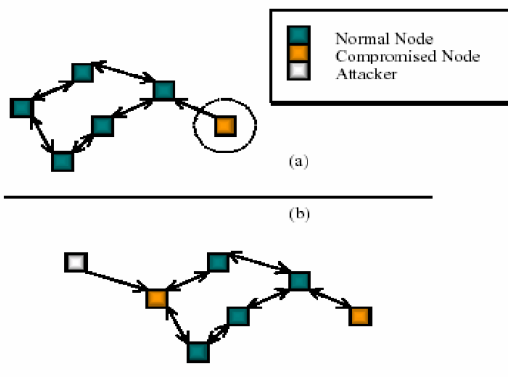
It is likely that in a wireless networkthere will have to be portions of the IDS running on each individual node in the network.Each of these IDS agents will have to communicate with other IDS agents in the networkto convey information relating to the status of the system. It is crucial that the informationbeing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

E. *Lack of Centralized Access/Audit Point*

The lack of centralized audit points in adhoc networks present difficult problems for intrusion detection. Most static, wirednetworks have specific repositories where the IDS can obtain audit data for its misuse andanomaly detection(e.g. switches, routers, gateways, etc.). Without centralized auditpoints, IDS s on ad hoc networks are limited to use only the current traffic coming in andout of the node as audit data. The algorithms that the IDS uses must be distributed, andtake 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 andnodes can move about freely, there is a possibility that one or more nodes could becaptured 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 ofwhich nodes one can trust. IDS s on ad hoc networks have to be weary of attacks madefrom nodes in the network itself, not just attacks from outside the network.

G. *Difficulty In Obtaining Enough Audit Data*

Mobile networks do not communicateas frequently as their wired counterparts. Bandwidth issues, and other issues such asbattery life, contribute to this factor. This lack of communication can become a problemfor IDS s attempting to define rules of normality for anomaly detection. If only a smallamount of data is available to establish normal activity association rules, it is very hard todistinguish an attack from regular network use.

VI. NEW ARCHITECTURE

It is important to understand that most IDS architecturalmodels are based on static, wired networks. These models alone are insufficient to helpdesign 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 intrusiondetection algorithm to decide when and how the network is being attacked. Thearchitecture is divided into parts: the Mobile IDS Agents, which reside on each node inthe network, and the Stationary Secure Database, which contains global signatures ofknown misuse attacks and stores patterns of each user‘s normal activity in a non-hostile
environment.

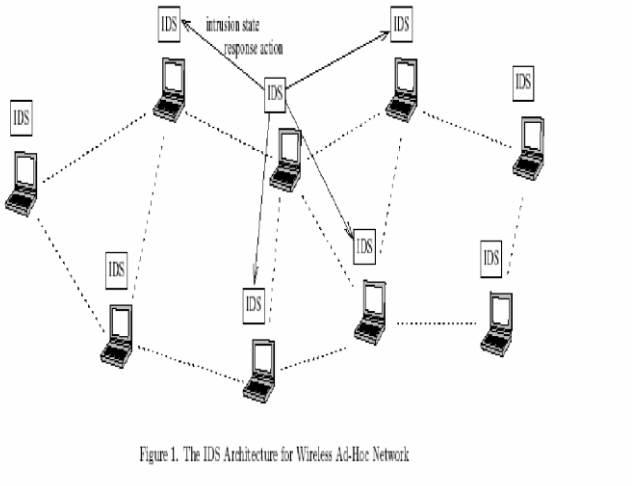


Figure 1. The IDS Architecture for Wireless Ad-Hoc Network

A. *Mobile IDS Agents*

Each node in the network will have an IDS agent running on itall times. This agent is responsible for detecting intrusions based on local audit data andparticipating in cooperative algorithms with other IDS agents to decide if the network is

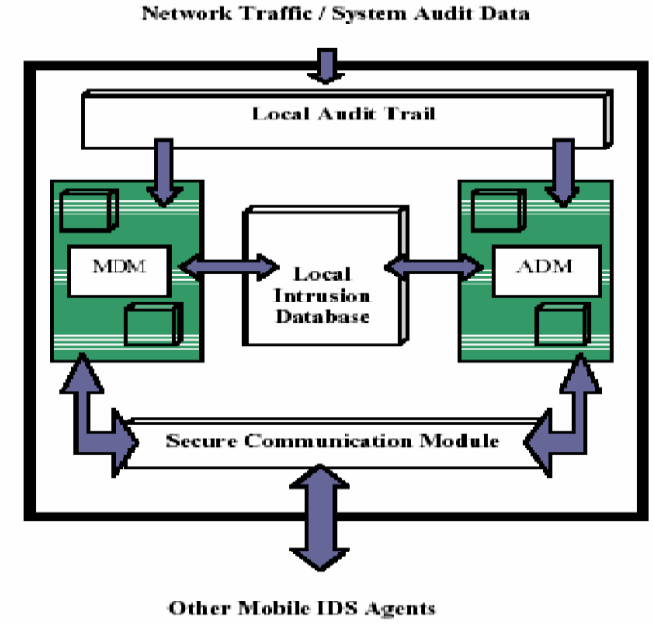
being attacked. Each agent has five parts : the Local Audit Trial, the Local IntrusionDatabase (LID), the Secure Communication Module, the Anomaly Detection Modules (ADM s), and the Misuse Detection Modules (MDM s).

i. The Local Audit Trial

Each agent must constantly check the audit data to decide thatan intrusion is not taking place. The Local Audit Trial will consist of specific items out ofthe 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 systemaudit data in order to minimize the size of the audit data collected. A audit data iscollected by the Local Audit Trial, it is passed to the Misuse Detection Modules and theAnomaly 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 warehousesall 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 thenetwork. The Anomaly Detection Modules and Misuse Detection Modules communicatedirectly 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 communicatewith other IDS agents on other nodes. It will allow the MDM s and ADM s to usecooperative algorithms to detect intrusions. It may also be used to initiate a globalresponse when an IDS agent or a group of IDS agents detects an intrusion. Basically, anycommunication that needs to occur from one IDS agent to another will use the SecureCommunication 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 beentampered with. The Secure Communication module is only used by IDS agents and doesnot communicate any other type of information between nodes. It must share thebandwidth that the mobile device uses for normal data transmission, so it is required to beefficient, and can only use the amount of bandwidth in needs.Also, the Secure Communication module must process information coming to the IDSagent from other agents in the network. For this reason, it must be fast and efficient, so asnot to take away from the processing time of the mobile unit.

iv. The Anomaly Detection Modules(ADM s)

Each Anomaly Detection Module isresponsible for detecting a different type of anomaly. There can be from one to manyAnomaly Detection Modules on each mobile IDS agent, each working separately orcooperatively with other ADM s. For example, one ADM might be looking for strangenetwork traffic patterns, while another ADM might be watching user input speed.

v. The Misuse Detection Modules (MDM s)

The Misuse Detection Modules functionssimilarly to the ADM s on the IDS agent. The primary difference is that MDM s onlyidentifies 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 istaking 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. Secondly, the processing time used to mine the new rules of anomaly will not take away from the processing time of the mobile nodes.

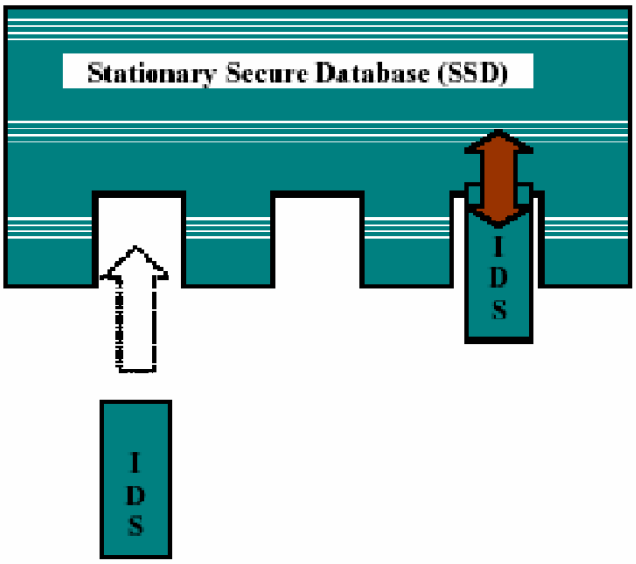


Figure: Mobile Agents Interacting with SSD

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, 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 wirelessnetworks. Detection based on activities in different network layers may differ in theformat 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 intrinsic andobservable characteristic of normal behavior that is distinct from that of abnormalbehavior. Entropy and conditional entropy are used to describe the characteristics of thenormal information flows and use the classification algorithms to build anomalydetection models. We can use a classifier trained using normal data to predict whatnormally the next event is given the previous n events. In monitoring when the actualevent is not what the classifier has predicted there is an anomaly. When constructing A classifier features with high information gain are needed.

Using this frame work we employ the following the 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 routinginformation, 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 onpacket 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 tracedata can use the service as the class (i.e., one class for each service), and can contain thefollowing features: for the past s seconds, the total number of requests to the sameservice, 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 itsrequests. Many attacks generate different statistical patterns than normal requests.

VIII. IMPLEMENTED APPROACHES

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

A. IEEE 802.11

The IEEE 802.11 standard provides several mechanisms intended toprovide a secure operating environment. The IEEE 802.11 standard defines the physicallayers and the MAC sub layers for the wireless LANs. There are three different physicallayers. They are Frequency hopping Spread Spectrum Radio; direct sequence spreadspectrum 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 defaultauthentication protocol for 802.11. As the name implies, open system authenticationauthenticates anyone who requests authentication. A terminal announces that it wishes toassociate 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)[2] . 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.

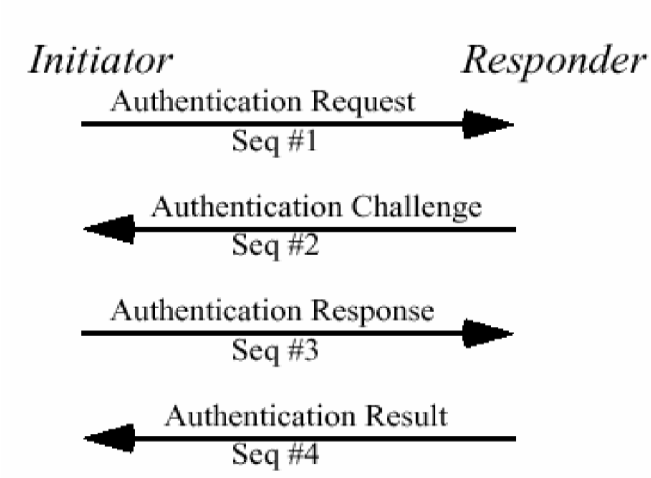


Figure: Mutual Station Authentication Using Shared Keys

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

iii. *Secure Key Generation And Distribution*

The mobile systems have constraints like minimal computational capabilities andauthentication and the Secure key generation and distribution capability is required byany system, which contains cryptographic authentication, confidentiality andidentification. Developing faster and more powerful hardware components, which requireless Energy and changing the algorithmic and protocol design of the current systemwould 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 Serviceprovider to develop a special distribution channel. (b) Security of keys should be ensuredfrom the time the keys are sent to the Service provider. from the manufacturer. (c) Thisapproach is unacceptable to both the Service provider and the manufacturer.

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

Over-the-air phone is themost preferred approach and requires a collaborative key generation and distributionbetween the mobile unit and the Service provider. The current over-the-air serviceprovisioning (OTASP) uses the Diffie-Hellman key exchange between the Serviceprovider and mobile unit to exchange a symmetric key called A-key (AuthenticationKey).

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 wirelesses, 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

1) Lidong Z., Zygmunt J. H., Securing ad hoc networks, IEEE Network, Vol. 13, No. 6, 1999, 24-30.
2) Sundaram A., "An Introduction to Intrusion Detection", http://www.acm.org/crossroads/xrds2-4/intrus.html
3) Marti S., Giuli T.J., Lai K. Baker M., —Mitigating Routing Misbehavior in Mobile Ad Hoc Networks",Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM2000, pp 255-265.
4) Arbaugh W., Shankar N., Wan Y.C.J., Your 802.11 Wireless Network Has No Clothes, Universityof Maryland, 30-Mar-2001.
5) Wenken Lee, Dong Xiang, Informatic-Theoritic Measures for Anomaly Detection.
6) Wenken Lee, Yongguang Zhang, Yi-An Huang, Intrusion Detection Techniques for Mobile wirelessnetworks.
7) Yongguang Z., Wenke L., —Intrusion Detection in Wireless Ad- Hoc Networks", Proceedings of theAnnual International Conference on Mobile Computing and Networking, MobiCom 2000, pp 275-283.
8) Andrew B.Smith, An Examination of an Intrusion Detection Architecture for Wireless Ad-HocNetworks.
9) Krugel , T.Toth. , Applying Mobile Agent Technology to Intrusion Detection
10) Kumar.S —Classification and Detection of Computer Intrusion " .