An Examination of an Intrusion Detection Architecture for Wireless Ad Hoc Networks*

Andrew B. Smith, Undergraduate
Department of Computer Science, Mississippi State University
Box 9637, Mississippi State, MS 39762
absmith@cs.msstate.edu

Abstract- Because all vulnerabilities of a network cannot be realized and penetration of the system cannot always be prevented, Intrusion Detection Systems (IDS s) have become necessary to ensure the security of a network. A great deal of research has been conducted on intrusion detection in a wired environment; however, new issues arise when trying to implement an IDS in a mobile, ad hoc environment. This paper discusses considerations when designing an IDS for a mobile, ad hoc network and describes an architectural model for IDS s that takes into account these and other pre-existing considerations.

I. INTRODUCTION

Any computer system, regardless of the amount of effort put into the design of the system, can have its security compromised. Authorized users who are trusted by the system can misuse their privileges and unauthorized users can deliberately penetrate the system. Even with the latest advances in security technology, if an attacker tries hard enough, they will eventually succeed in infiltrating the system. Because of this, it is important to constantly (or at least periodically) monitor what is taking place on a system and look for suspicious behavior. Intrusion Detection Systems (IDS s) do just that: monitor audit data, look for intrusions to the system, and initiate a proper response (e.g., email the Systems Administrator, start an automatic retaliation, etc.) [4].

The first IDS s were based at the *host level* and monitored the operating system s audit data on a single host. As networks became more popular, *network level* IDS s became more common, monitoring not only the audit data on the hosts in the network, but also examining network traffic for any type of suspicious activity [7]. Both host and network level IDS s normally use two techniques to detect intrusions: *misuse detection* and *anomaly detection*.

Misuse detection is when an IDS attempts to identify intrusions by recognizing known patterns of attacks [8]. For example, the IDS might identify the password crack attack when a certain user fails to supply the correct password after 3 attempts. One advantage of using misuse detection is the ability to be very certain when a known attack is taking place. This could allow the system to initiate prevention techniques to counter the attack. In this example, it may be wise to lock the account temporarily to prevent a cracker program from obtai ning the user s password through a brute force attack. Misuse detection fails, however, when the attack pattern is not known by the IDS or if the attacker is creative in disguising what they are attempting to do.

Anomaly detection attempts to identify patterns of normal behavior for users and then identify an intrusion when a user deviates from their established pattern. This technique is very useful in detecting new attacks that are not already known by the misuse detection system. It is, however, very difficult to pattern a user s normal behavior, typically leading to a large number of false alarms (false positives) [10].

Research has demonstrated that having one mechanism at a single place in the network doing anomaly and misuse detection might not be the ideal way to detect intrusions [6]. The idea of having mobile software agents, programs that work autonomously and can communicate with other agents, is currently being explored and seems promising as an effective way to identify intrusions [6,3].

The use of mobile software agents to accomplish misuse and anomaly detection can be applied to mobile, ad hoc networks. With the recent popularity

* This research is supported in part by grants from The National Science Foundation (CCR-0085749 and CCR-9988524) and The Army Research Laboratory (DAAD17-01-C-001).

This paper is sponsored by Dr. Ray Vaughn and Dr. Susan Bridges, Computer Science Department, Mississippi State University

of wireless communication technology, the ability to detect an intrusion in a wireless network has become very important. Mobile networks are susceptible to a new variety of intrusions in addition to attacks that wired networks are vulnerable to. Mobile IDS s also face additional difficulties as compared to those of wired IDS s. Even more difficulties result when attempting to provide intrusion detection on ad hoc, wireless networks. This problem is especially critical to the Department of Defense as the use of wireless, mobile technologies continues to increase in tactical applications on the battlefield.

This paper will discuss some of the problems that are encountered when attempting to build an IDS for a mobile network. Then, it will address some problems faced by IDS s on ad hoc networks. Finally, based on these new problems, a new architectural model for building an IDS on a mobile, ad hoc network will be presented.

II. 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 IDS s 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 an IDS for a mobile network are now addressed below:

A. Lack of Physical Wires

Perhaps 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 [5]. 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. Eavesdropping of network traffic is not just a problem for wireless security in general. When building an IDS for wireless networks, traffic from parts of the IDS on each individual host (node) in the network must communicate with one another. This IDS traffic must be protected against eavesdropping because if an attacker can read and understand the traffic, they may be able to learn information about how the IDS works, allowing them to develop ways to penetrate the network undetected by the IDS.

Since no physical access has to be accomplished, it seems possible that an attacker could block or jam communication between nodes of the network very easily by inserting noise into the wireless channel [5]. This could quite easily be directed toward a specific, targeted network or directed to a large geographical region. In either case a denial of service attack results. If nodes are unable to communicate with one another because the network is being jammed, it is very obvious that the availability of the network will be compromised. The same is true for IDS inter-communication. If IDS communication from node to node can be blocked by the attacker, individual components of the IDS on each node of the network will not be able to connect with each other to share vital intrusion detection information, making the entire IDS less useful.

Perhaps even worse than eavesdropping or jamming, it may be possible for an attacker to interject messages or signals into the network traffic, conceivably from a large distance away, that would disrupt or compromise the security mechanisms of the network [5]. If messages passing from node to node could be tampered with undetected, it may be impossible for the IDS s to work properly, leaving the mobile network unable to detect a security breach and creating a false sense of security.

B. Bandwidth Issues

Wireless networks have more constrained bandwidth as compared to hardwired networks [2]. This problem can manifest itself in a number of different ways when an IDS is using wireless communication to convey information between parts of the 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. With the bandwidth of the wireless network already being starved by the normal communication between wireless nodes, the IDS must only send messages when required, and send them with the maximum efficiency possible. Too much communication by the IDS can cause congestion, hindering normal communication between nodes, and even worse, hindering the efficiency of the IDS to communicate that the network is being attacked.

A second problem that may possibly arise because of limited bandwidth is erroneous behavior of the IDS due to communication delay between nodes. Take for example the case that one node is far away from other nodes. If the distant node is trying to send an

intrusion alert, the other nodes in the network may not receive that message until it is too late to identify it as an attack or to correlate it with other messages that would indicate an attack. If an IDS on one node is trying to contact a distant node, it might think that there is an attack taking place when communication from the distant node is slower than the communication from the other nodes. These are just a few examples of how bandwidth restrictions might affect the design or functionality of IDS s on wireless networks. There are certainly many others.

C. Difficulty of Anomaly/Normality Distinction

Distinguishing an anomaly from normalcy has always been somewhat difficult for wired IDS s, and wireless IDS s are no different. In fact, it might be said that determining anomaly on a wireless channel is more difficult. In [10], an example is given of the problem of determining an anomaly from normal behavior. 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 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.

Efficiently encrypting communication in a wireless environment is a very difficult task in and of itself. Wireless devices have less electrical power and less computing power compared to their wired counterparts, making it unsuitable to encrypt IDS communication with a public-key encryption algorithm [9]. Also, any type of encryption will take processing time at the sending and receiving ends, adding overhead to an already relatively slow communication link.

Even disregarding the communication delay caused by the encryption, encoding is not a fix-all to secure IDS communications. If one of the nodes in a wireless network can be captured, an attacker might be able to transmit and receive information from other IDS agents without even knowing the encryption algorithm. In this case, encryption would do nothing to protect the information passing from IDS agent to IDS agent.

There are other problems to address as well. For example, spoofing may be an easier attack to mount in a wireless environment than in a wired network. Killing a mobile host and introducing a false replacement can be a plausible attack. Similarly, mounting a man-in-the-middle attack could become a threat unless the wireless configuration is closely monitored. This problem is more carefully examined in the section below.

III. IDS ISSUES IN AN AD HOC ENVIRONMENT

An ad hoc network consists of several mobile nodes that communicate with each other in the absence of base stations or fixed hosts [11]. The network is constantly changing its topology, that is, the nodes can move in and out of the network at random. If a node is out of range because of distance separation, other nodes in the network can work together to route messages to that node. These features present new problems when designing an IDS for an ad hoc environment. They also represent a realistic view of what a mobile, tactical computing environment will have to look like on the battlefield of the 21st Century.

A. Lack of Centralized Access/Audit Point

The lack of centralized audit points in ad hoc networks presents 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.) [10]. Without centralized audit points, IDS s 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 [10].

Research that has been conducted using independent software agents might be useful to combat this problem [3,6]. These software agents can monitor audit data at different points in the system and communicate information to each other without a commanding agent. Placing mobile IDS agents on each node in the network could extend this idea of software agents to a mobile, ad hoc environment. Using this approach, one agent could be placed on

every node in the ad hoc network, and could communicate with the other agents in the network to identify intrusions. No centralized audit point is necessary, as each agent will monitor the audit data that it can obtain. The disadvantage to this approach, however, is the diminished ability to correlate intrusion data.

B. 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 of the nodes could be 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. IDS s on ad hoc networks have to be weary of attacks made from nodes in the network itself, not just attacks from outside the network [11]. For example, if one node of the network is captured, the attacker who has taken control of that node can send false information to the IDS s on the other nodes.

A scenario illustration of this problem can be seen in the following. IDS s on a mobile ad hoc network are communicating with a certain encryption algorithm. Once an attacker compromises the security of one node in the network, it can send a message to all of the neighboring nodes conveying the need to change the encryption algorithm because of an attack. Since the compromised node is communicating with the authorized encryption algorithm, the other nodes in the network trust the compromised nodes decision, and change the encryption algorithm for the network. This could lead to a type of availability attack on the network. While the nodes are busy trying to change encryption keys, the IDS takes up a lot of the communication bandwidth between nodes, making the other, regular communication between nodes very slow.

Figure 1 shows how the availability attack described above could also result in another type of attack. While the network is slowed because of heavy IDS communication, another attacker could target the network at another point. Because the network is running slower than normal, it will take longer for the IDS to respond to the new attack. For time critical maneuvers, such as military strikes, this time could be crucial to the effectiveness of the mission.

One way to avoid the forcing of the re-key is to assume that a majority of the nodes in the ad hoc network will not be captured. With this assumption, a node may not be able to trust one given node, but can trust a group of nodes. But, not being able to trust one node makes it hard for the IDS to react quickly to an intrusion, since more than one node has to verify the attack to prove an intrusion has taken place.

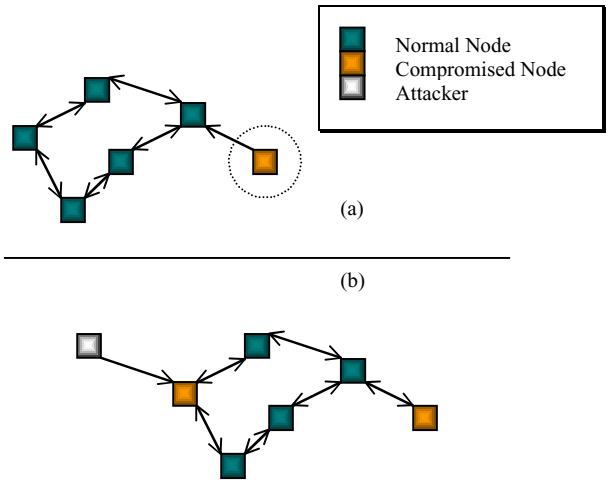

Figure 1: (a) An attacker has compromised a node of the network and forces other nodes to do a re-key. (b) While the network is slowed, another attacker attacks a different node, causing it to be compromised.

C. Difficulty Obtaining Enough Audit Data

Mobile networks do not seem to 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 IDS s 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 [2, 10].

In order to establish a pattern of normalcy, a substantial amount of data and time is required. Since mobile, ad hoc networks have limited communication, and can potentially only see a small amount of the network at a time, it is very difficult to get this large amount of data. And, without a large amount of data, it is extremely difficult to be able to perform accurate anomaly detection or intrusion detection in ad hoc environments.

IV. ARCHITECTURAL MODEL

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 environment. Taking into account the issues described earlier in this paper, as

well as other basic IDS issues, a new architecture is proposed herein to help develop IDS s in this relatively new environment.

The architecture now 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 two 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 users normal activity in a non-hostile environment.

A. Mobile IDS Agents

Each node in the network will have an IDS agent running on it at all times. 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 Trail, the Local Intrusion Database (LID), the Secure Communication Module, the Anomaly Detection Modules (ADM s), and the Misuse Detection Modules (MDM s).

1. The Local Audit Trail

Each agent must constantly check audit data to decide that an intrusion is not taking place. The Local Audit Trail will consist of specific items out of the network traffic as well as user commands to the node. The Local Audit Trail 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.

As audit data is collected by the Local Audit Trail, it is passed to the Misuse Detection Modules and the Anomaly Detection Modules for further analysis. The Local Audit Trail is only responsible for gathering and storing the audit data, not processing it.

2. 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 communicate directly with the LID to determine if an intrusion is taking place.

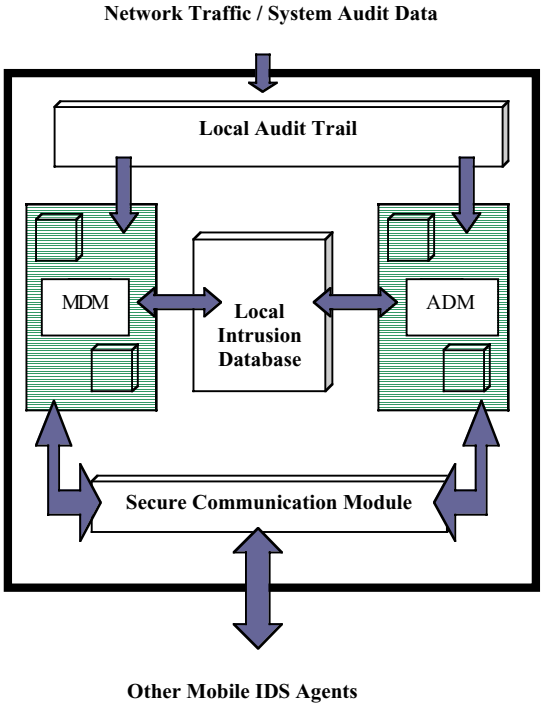

Figure 2: **A Graphical Representation of a Proposed Mobile IDS Agent**

3. 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 the 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 in order 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 the 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 needs.

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. Although this is currently a technology challenge, there are products emerging in the commercial market that will address this issue (e.g., Secure Wireless LAN Card by Harris Corporation).

4. *The Anomaly Detection Modules (ADMs)*

Each Anomaly Detection Module is responsible for detecting a different type of anomaly. There can be from 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.

If an ADM can identify an anomaly based solely on the data in the Local Intrusion Database, then it can initiate a local and global response to the intrusion. An example of a local response could be to shut down the node, rendering it useless to an attacker. A possible global response would be to use the Secure Communication module to alert other IDS agents, allowing them to reconstitute a network while excluding the compromised node.

If the amount of data in the Local Intrusion Database is not sufficient to determine if the present activity should be classified as an intrusion, then it is possible for the ADM to use the Secure Communication module to query other nodes in the network to get help in identifying an intrusion. An example of a cooperative algorithm that discusses this type of intrusion detection in detail can be found in [10], and is not further discussed in this paper.

5. 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 the MDM s only identify 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. If a MDM needs more information from other IDS agents on other nodes, it would be expected to use the Secure Communication module to interact with them. Using the information given by other IDS agents, the MDM might be able to predict an intrusion with more accuracy.

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 is stored in an 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 commonly practiced in military tactical environments associated with command posts and control centers.

The mobile IDS agents will collect and store audit data (such as user commands, network traffic, etc.) 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 (see [1] for a more detailed description of this research). The use of the SSD to mine new anomaly rules is beneficial to the IDS for three reasons. First, the SSD will be a 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. The SSD puts the task of creating new rules for anomaly detection on the wired server and away from the mobile nodes. And thirdly, the SSD is capable of having much more storage capacity to store an abundance of audit data collected from the nodes. It is very likely that the mobile nodes will not have enough storage to store substantial amounts of audit data, but by uploading audit data to the SSD, no data is deleted because of lack of storage space.

The SSD will also be the place where the system administrator can specify the newest misuse signatures. When the IDS agents are connected to the 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.

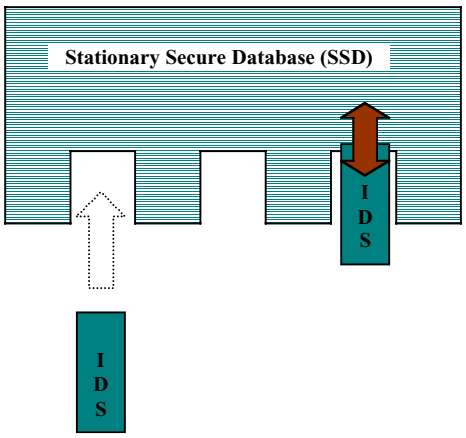

Figure 3: Mobile IDS Agents interacting with SSD

Perhaps one of the best reasons for using the SSD to communicate 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 in the paper, 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 the 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 to it is trustworthy or not.

It is feasible to think that the SSD could have other functions besides updating the intrusion detection information on each IDS agent. Perhaps the SSD could be a place where the mobile nodes could charge their batteries while receiving the latest IDS information for example. This way, the time spent at the SSD would be more efficient and not be used for just intrusion detection.

Despite all the benefits of having a SSD in a mobile IDS architecture, there are a few disadvantages of relying on a stationary database to provide vital IDS information. If a SSD is used, mobile nodes will have to be attached to the non-mobile database periodically to stay up-to-date with the latest intrusion information. This may not be an option for some mobile, ad hoc environments. Also, since the SSD must be a trusted source, it cannot be taken on-site without significant risk. If a mobile IDS agent detects a new intrusion while in a hostile environment, it cannot be attached to the SSD in order to communicate the new attack pattern. And, even if it could, other nodes would be in the hostile environment and would not be able to attach to the SSD right away to get the new signature. However, these problems might be solved if the IDS agents can communicate new patterns of attacks to each other via the Secure Communication module while in the hostile environment. This way, only information that has to be communicated right away will be sent over the wireless channels, and less time sensitive information can be gathered later at the SSD when time permits. Use of this architecture might, for example, be very appropriate for unmanned remote vehicle operations.

V. OTHER MOBILE AD HOC ARCHITECTURES

Research in this field is very limited, but an example of an IDS architecture that uses cooperative statistical anomaly detection in a wireless, ad hoc network is presented in [10]. However, this architecture makes key assumptions and does not address some of the issues presented earlier in this paper. One problem not addressed in [10] is the large amount of data that must be passed over the wireless environment to update the local database of anomaly and misuse rules. Bandwidth constraints and low battery life make this process impractical. In the architecture described previously, the use of the Stationary Secure Database keeps the IDS agents on each node up-to-date without using the already starved bandwidth of the mobile network.

Another issue not addressed in [10] is how to obtain enough audit data to establish normal patterns of use. Without this audit data, it becomes next to impossible to do accurate anomaly detection. The architecture proposed in this paper requires that each individual IDS agent store all relevant audit data, and uploads it to the Stationary Secure Database when it is docked to it. Using this technique, the SSD can retain large amounts of audit data, and continually use this data to obtain new anomaly association rules.

Also, the issue of secure communication between nodes is not discussed in [10]. This is very important to the IDS on the mobile network. The communication between IDS agents must be encrypted so

enemies cannot read or tamper with communication between IDS agents. The use of encryption will most likely make the IDS communication process slower, and this should be taken into consideration when designing the IDS. Because IDS communication will be slowed due to encryption, it becomes vital to only communicate between mobile IDS agents when absolutely necessary.

Finally, the use of basic, statistical anomaly detection might not be the best way to detect anomalies. Current research has shown that using artificial intelligence techniques, such as fuzzy data mining, are very successful in detecting anomalies in wired environments [1]. If a large amount of data can be stored on the SSD, genetic algorithms can use these fuzzy techniques to develop anomaly association rules [1], and these rules can be placed on each mobile IDS agent.

VI. CONCLUSIONS AND FUTURE RESEARCH

This paper has discussed several new issues and ideas that must be addressed when designing Intrusion Detection Systems for mobile, ad hoc networks. Research that has been done on wired, static IDS s can be helpful when designing an IDS for wireless networks, but the ideas discussed in this paper must be addressed when applying them to this new environment. Also, a basic architecture was described that took into account some of the ideas presented earlier in the paper. This architecture might prove helpful in networks that are dynamic in nature, such as a group of tanks roaming in the desert, emergency response teams, and law enforcement.

Future work includes implementation of such an IDS architecture and testing its effectiveness in mobile, ad hoc environments.

VII. ACKNOWLEDGEMENTS

I wish to acknowledge the encouragement and assistance provided by Dr. s Ray Vaughn and Susan Bridges of the Computer Science Department of Mississippi State University and to the research group they lead in the area of intelligent intrusion detection.

REFERENCES

[1] Bridges, S., R. Vaughn. 2000. "Fuzzy Data Mining and Genetic Algorithms Applied to Intrusion Detection". *23d National Information Systems Security Conference*. October 2000, Baltimore, Maryland.

[2] Corson, M., J. Macker, G. Cirincione. 1999. Internet-Based Mobile Ad Hoc Network - ing . In *IEEE Internet Co mputing*. Vol. 3, No. 4, July/August 1999. pp. 63-70.

[3] Crosbie, M., G. Spafford. 1996. Defen ding a Computer System using Autonomous Agents. Technical Report No. 95-022, Dept. of Computer Sciences, Purdue University, March 1996.

[4] Gollmann, D. 1999. *Computer Security*. West Sussex, England: John Wiley & Sons Ltd.

[5] Harrington, J., D. Pritchard. 1997. Co n-cepts and applications of wireless security systems for tactical, portable, and fixed sites . In *Proceedings of The Institute of Electrical and Electronics Engineers 31st Annual 1997 International Carnahan Conference on Security Technology*. pp. 133 —139.

[6] Jansen, W., P. Mell, T. Karygiannis, D. Marks. 2000. Mobile Agents in Intrusion Detection and Response . In *Proceedings of the 12th Annual Canadian Information Technology Security Symposium.* June 2000, Ottawa, Canada.

[7] Kim, J., P, Bentley. 1999. "The Artificial Immune Model for Network Intrusion Detection". In *7th European Congress on Intelligent Techniques and Soft Computing (EUFIT'99). Aachen, Germany. September 13- 19.*

[8] Lee, W., S. Stolfo. 1999. A Framework for Constructing Features and Models for Intrusion Detection Systems . In *Proceedings of the 1999 IEEE Symposium on Security and Privacy.*

[9] Wu, H., S. Yang, Y. Lin. 2000. The Sharing Session Key Component (SSKC) Algorithm for End-to-End Secure Wireless Communication. In *Proceedings of the IEEE 34th Annual International Carnahan Conference on Security Technology.* pp. 242-250.

[10] Zhang, Y., W. Lee. 2000. Intrusion Detection in Wireless Ad-Hoc Networks. In *Proceedings of The Sixth International Conference on Mobile Computing and Networking (MobiCom 2000)*. Boston, MA. August 2000.

[11] Zhou, L., J. Zygmunt. 1999. Securing Ad Hoc Networks . In *IEEE Network*. November/December 1999.