International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010
1793-8163

Real Time Intelligent Intrusion Identification in Wireless Adhoc Networks

Rajendra Prasad Mahapatra, *Member, IACSIT* and Tanvir Ahmed Abbasi

***Abstract*—Wireless Ad hoc Networks have become an important area of research in Wire-less Communications Systems. Unlike some existing networking technologies such as Internet Protocol (IP) networks or cellular systems, Wireless Ad hoc Networks have the advantage that deployment of networks does not require preexisting infrastructures. Ad hoc Networks have neither fixed topology nor centralized servers. As the recent denial of service attacks on several major internet sites have shown us on open computer network is immune from intrusion. 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 defense. Many of the intrusion detection technique developed on a fixed wired network are not applicable in this new environment. How to do it differently and effectively is a challenging research problem. In this paper we first examine the vulnerabilities of a wireless ad hoc network the reason why, we need in detection, and the reason why the current methods cannot be applied directly, that so we are describe the new intrusion detection and response mechanism that we are developing for the wireless ad hoc network.**

***Index Terms*—Wireless ADHOC Networks, Medium Access Control (MAC) Protocol, Distributed Denial-of-Services (DDOS), Intrusion Detection System (IDS).**

I. Introduction

The nature of wireless ad-hoc networks makes them very vulnerable to an adversary's malicious attacks. Unlike wired networks where an adversary must gain physical access to the network wires or pass through several lines of defense at firewalls and gateways, attacks on a wireless ad-hoc network can come from all directions and target at any node. Damages can include leaking secret information, message contamination, and node impersonation. All these mean that a wireless ad-hoc network will not have a clear line of defense, and every node must be prepared for encounters with an adversary directly or indirectly. Mobile nodes axe autonomous units that are capable of roaming independently. This means that nodes with inadequate physical protection are receptive to being captured, compromised, and hijacked. Since tracking down a particular mobile node in a large scale ad-hoc network cannot be done easily, attacks by a compromised node from within the network are far more damaging and much harder to detect. Therefore, any node in a wireless ad-hoc network must be prepared to operate in a mode that trusts no peer.

Decision-making in ad-hoc networks is usually decentralized and many ad-hoc network algorithms rely on the cooperative participation of all nodes. The lack of centralized authority means that the adversaries can exploit this vulnerability for new types of attacks designed to break the cooperative algorithm. As network-based computer systems play increasingly vital roles in modern society, they have become the targets of enemies and criminals. When an intrusion (defined as "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource" [4]) takes place, intrusion prevention techniques, such as encryption and authentication (e.g., using passwords etc.), are usually the first line of defense. However, intrusion prevention alone is not sufficient because as systems become ever more complex, while security is still often the after-thought, there are always exploitable weaknesses in the systems due to design and programming errors. Furthermore, as illustrated by recent Distributed Denial-of-Services (DDOS) attacks launched against several major Internet sites where security measures were in place, the protocols and systems that are designed to provide services (to the public) are inherently subject to attacks such as DDOS. Intrusion detection can be used as a second wall to protect network systems.

Primarily user and program activities are observable, for example via system auditing mechanisms; and more importantly, normal and intrusion activities have distinct behavior. Intrusion detection therefore involves capturing audit data and reasoning about the evidence in the data to determine whether the system is under attack. Based on the type of audit data used, intrusion detection systems (IDSs) can be categorized as network-based or host-based. A network-based IDS normally runs at the gateway of a network and "captures" and examines network packets that go through the network hardware interface. A host-based IDS relies on operating system audit data to monitor and analyze the events generated by programs or users on the host. Intrusion detection techniques can be categorized into *misuse detection* and *anomaly detection.*

Misuse detection systems, e.g., IDIOT [8] and STAT [5], use patterns of well-known attacks or weak spots of the system to match and identify known intrusions. The main advantage of misuse detection is that it can accurately and efficiently detect instances of known attacks. The main disadvantage is that it lacks the ability to detect the truly innovative (i.e., newly invented) attacks. Anomaly detection systems, for example, IDES [10], flag observed activities that deviate significantly from the established normal usage profiles as anomalies, i.e., possible intrusions. For example, the normal profile of a user may contain the averaged frequencies of some system commands used in his or her login sessions. If for a session that is being monitored, the

Manuscript received Nov 9, 2009
Rajendra Prasad Mahapatra, HOD Dept. CSE SRM University Modinagar Campus (E-mail: mahapatra.rp@gmail.com).

frequencies are significantly lower or higher, then an anomaly alarm will be raised. The main advantage of anomaly detection is that it does not require prior knowledge of intrusion and can thus detect new intrusions. The main disadvantage is that it may not be able to describe what the attack is and may have high false positive rate.

The most important difference is perhaps that the latter does not have a fixed infrastructure, and today's network based IDSs, which rely on real-time traffic analysis, can no longer function well in the new environment. Compared with wired networks where traffic monitoring is usually done at switches, routers and gateways, an ad-hoc network does not have such traffic concentration points where the IDS can collect audit data for the entire network. Therefore, at any one time, the only available audit trace will be limited to communication activities taking place within the radio range, and the intrusion detection algorithms must be made to work on this partial and localized information.

The second big difference is in the communication pattern in a wireless ad-hoc network. Wireless users tend to be stingy about communication due to slower links, limited bandwidth, higher cost, and battery power constraints. Disconnected operations [11] are very common in wireless network applications, and so is location-dependent computing or other techniques that are solely designed for wireless networks and seldom used in the wired environment. All these suggest that the anomaly models for wired network cannot be used, as is, in this new environment.

Furthermore, there may not be a clear separation between normalcy and anomaly in wireless ad-hoc networks. A node that sends out false routing information could be the one that has been compromised, or merely the one that is temporarily out of sync due to volatile physical movement. Intrusion detection may find it increasingly difficult to distinguish false alarms from real intrusions.

Following are three main objectives in developing a viable intrusion detection system for wireless ad-hoc networks:

1. To develop a good system architecture for building intrusion detection and response systems that fits the features of wireless ad-hoc networks?
2. To detect anomaly based on partial, local audit traces - if they are the only reliable audit source? And to suggest appropriate audit data source.
3. To frame work a good model of activities in a wireless communication environment that can separate anomaly when under attacks from the normalcy?

Intrusion detection and response systems should be both distributed and cooperative to suite the needs of wireless ad-hoc networks. In proposed architecture, every node in the wireless ad-hoc network participates in intrusion detection and response. Each node is responsible for detecting signs of intrusion locally and independently, but neighboring nodes can collaboratively investigate in a broader range.

It detects intrusion from local traces and initiates response. If anomaly is detected in the local data, or if the evidence is inconclusive and a broader search is warranted, neighboring IDS agents will cooperatively participate in global intrusion detection actions. These individual IDS agent collectively form the IDS system to defend the wireless ad-hoc network. Whole work for the intrusion detection & response consists of following three distinct phases.

II. Intrusion Detection System

Intrusion detection and response system should be both distributed and cooperative to suite the needs of Wireless Ad hoc Network. In our proposed architecture Figure 1,[12] every node in the wireless ad hoc network participates in intrusion detection and response. Each node is responsible for detecting signs of intrusion locally and can collaboratively investigate in a broader range. In the system aspect, individual IDS agents are placed on each and every node, each IDS agent runs independently and monitors local activities (Including user and system activities and communication activities within the radio range). It detects intrusion from local traces and initiates response. It detects intrusion from local traces and initiates response. If anomaly is detected in the evidence is inconclusive and a broader search is warranted, neighboring IDS agent will cooperatively participate in global intrusion detection system. These individual IDS agent collectively from the IDS system to define to wireless ad hoc network.IDS should be both distributed and cooperative to suit the needs of wireless ad-hoc networks. What is meant by this statement is that every node in the wireless ad-hoc network should participate in intrusion detection. Each node is responsible for detecting intrusion locally and independently but neighboring nodes can form an association and collaboratively investigate in a broader range. Each node within the network has its own individual IDS agent and these agents run independently and monitor user and system activities as well as communication activities within the radio range. If an anomaly is detected in the local data or if the evidence is inconclusive, IDS agents on the neighboring nodes will cooperatively participate in a global intrusion detection scheme. These individual IDS agents constitute the IDS system to protect the wireless ad-hoc network.

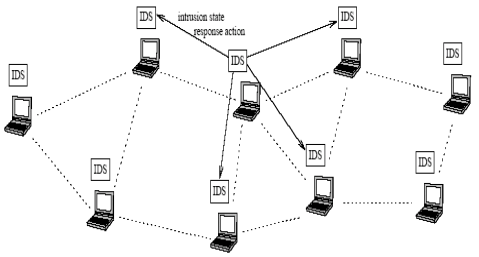

Figure 1: Block diagram of IDS

The main task of the intrusion detection system (IDS) is to discover the intrusion from the network packet data or system audit data. One of the major problems that the IDS might face is that the packet data or system audit data could be over-whelming. Some of the features of audit data may be redundant or contribute little to detection process. So the reduction in the size of data set is needed. To perform the reduction, two methods of features selection, namely, markow blanket discovery and generic algorithms are proposed. The Intrusion Detection System is distributed in nature so each node of a mobile ad hoc network equipped with an IDS system architecture of IDS comprises four

component (Figure 2):

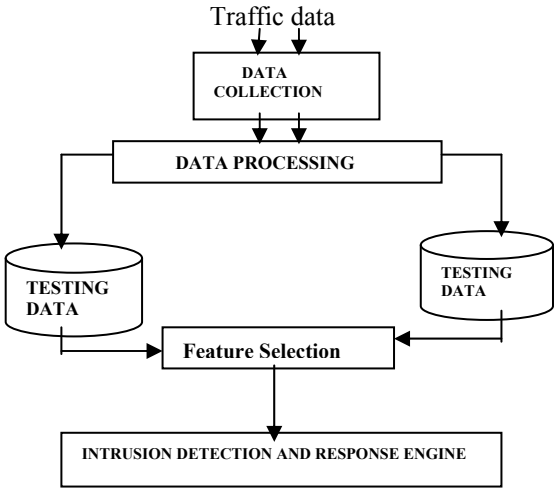

Figure 2: The IDS Architecture for Wireless Ad-hoc network

1 : Data collection module
2 : Profile module
3 : Feature selection module
4 : Detection and Response module

A. Data collection module

The module collects audit data for each node. The proposed system considers unknown attacks. So the IDS need normal behavior of the system (normal profile) and violation of normal behavior (attack profile).Normal profile is created using the collection during scenario. Attack profile is created by simulating the attacks

B. Profile module

In this module audit data is transported into appropriate format for the detection process. From the attack data, training data set is created to train the Bayesian classifier. Training data consists of labeling of events whether it is a normal event or an attack. Test data is collected under simulated attack environment and it is given to the Bayesian classifier to identify as event whether it is an attack or normal.

C. Feature selection module:

Feature selection is the process of selecting important features from the large data set. The selected features are relevant to the detection process. In order to perform this operation two features selection methods are proposed.

1) Markow blanket Discovery

The selection of markov blanket is based on the d-separation rule of the Bayesian network. Given a specific attribute, which is represented as a node in a the Baysian network markov blanket is discovered. Markov blanket is the set of nodes composed of the attribute's parents. Its children's parents of Bayesian network. When using a Bayesian classifier on complete data, the markov blanket are detected from the Bayesian.

2) Generic Algorithm:

GA-based features selection algorithm is based on the wrapper model. In the adopted algorithm, the search component is a GA and the evaluation component is a Bayesian network. The initial population is randomly generated. Every individual of the population is represented by means of genes, each of which represents a feature. If the feature value is '1', it is used during constructing of Bayesian network if it is '0' that feature is not used.

D. Intrusion Detection and Response module:

This module detects deviation from the norm. In order to detect the anomalies Bayesian classifier is used. Classifier will be trained by the training data. The test data will be given as input to the trained Bayesian classifier. Any deviation from the threshold level is considered level as anomalies. Once all the attacks are indentified then the notification will be given to all the nodes in the ad hoc environment.

III. A Conceptual Model for an IDS Agent

A Typical IDS Agent consists of following modules viz.

1) Local Data Collection: Local Data Collection module gathers streams of real time audit data from eclectic sources, (Figure 3)[13].which might include user and system activities within the mobile node, communication activities by this node as well as any communication activities within the radio range of this node and observable to this node.

2) Local Detection Engine: Local detection engine analyzes the local audit data for evidence of anomalies. This requires the IDS to maintain some expert rules for the node against which the audit data collected would checked. However as more and more appliances are becoming wireless, the types of planned attacks against these appliances is going to increase and this may make the existing expert rules insufficient to tackle these newer attacks. Moreover, updating these already existing expert rules is not a simple job. So any IDS meant for a wireless ad-hoc network should resort to statistical anomaly detection techniques. The normal behavior patterns called "Normal Profiles" are determined using the trace data from a "training " process where all activities are normal. During the "testing" process any deviations from the normal profiles are recorded if at all any occur. A detection module is computed from the deviation data to distinguish anomalies from normalcy. There are always going to be normal activities which have not been observed and recorded before, however their deviations from the normal profile is going to be much smaller than those of intrusions.

3) Cooperative Detection: If a node locally detects a known intrusion with strong evidence it can very well on its own infer that the network is under attack and can initiate a response or a remedial action. However if the evidence of an anomaly or intrusion is a weak one or is rather inconclusive then the node decides it needs a broader investigation and can initiate a global intrusion detection procedure, which might consist of transmitting the intrusion detection state information among neighbors and further down the network if necessary.

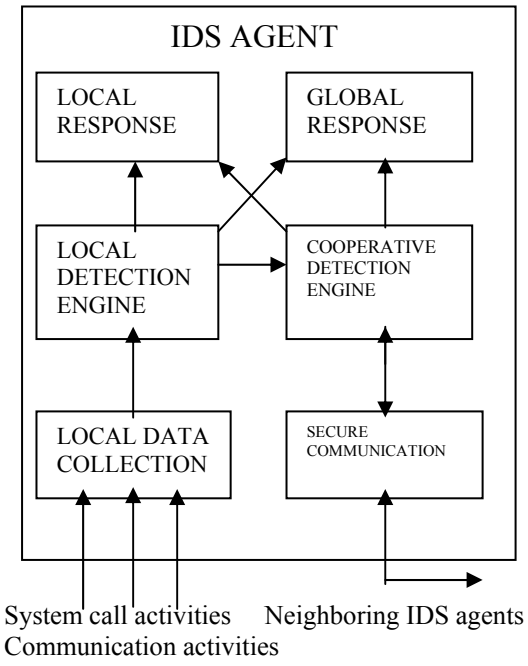

Figure 3: A Conceptual model for an IDS agent

The intrusion detection state information may be a mere level-of-confidence value expressed as percentage.

- With p% confidence , node A after analyzing its local data concludes that there is an intrusion.
- With p% confidence , node A after analyzing the local data as well as that from its neighbors that there is an intrusion.
- With p% confidence , node A, B, C,…. Collectively conclude that there is an intrusion.

To a more specific state that lists the suspects like,

- With p% confidence, node A concludes after analyzing its local data that node X has been compromised.

A distributed consensus algorithm is then derived to compute the new intrusion detection state for the node under consideration , with the help of the state information recently received from the other nodes in the network. The algorithm might involve a weighted computation assuming that nearer nodes has greater effect than the far away ones.

A majority based Intrusion Detection Algorithm can include following steps:

- The node sends to its neighboring node an "intrusion state request".
- Each node , including the one which initiates this algorithm then propagates the state information, indicating the likelihood of an intrusion to its immediate neighbors.
- Each node then determines whether the majority of the received reports point towards an intrusion, if yes then it concludes that the network is under attack.
- Any node which detects an intrusion to the network can then initiate the remedial/response procedure.

As a rule of thumb, audit data from other nodes should not be trusted as compromised nodes might tend to send misleading data. However for compromised node sending audit data doesn't hold any incentives , in doing so it might create a situation which would result in its expulsion from the network. Hence , unless majority of nodes are compromised, and there exists at least one valid node the remedial procedure won't be initiated.

IV. Intrusion Detection & Response

The intrusion detection starts analyzing the local data traces gathered by the local data collection module for evidence of anomalies. It is believed that the IDS for a wireless ad-hoc network should mainly use statistical anomaly detection techniques. In general, the procedure of building such an anomaly detection model is the following:

- the normal profiles (i.e., the normal behavior patterns) are computed using trace data from a "training" process where all activities are normal;
- the deviations from the normal profiles are recorded during a "testing" process where some normal and abnormal activities (if available) are included;
- a detection model is computed from the deviation data to distinguish normalcy and anomalies; although there will always be "new" normal activities that have not been observed before, their deviations from the normal profiles should be much smaller than those of intrusions.

In the work on fixed wired networks [7], we have developed efficient data mining algorithms for computing normal traffic patterns from TCP/IP trace data (i.e., *tcpdump* [6] (output), as well as classification techniques for building misuse and anomaly detection models. The main challenges here are how to define the trace data, and how to determine the types of patterns that best describe the normal behavior. While there are many anomaly detection models for user behavior and system activities (e.g., [2, 3, 9]), our focus here is on new models for wireless ad-hoc networks
The intrusion detection state information can range from a mere level-of-confidence value such as

- "With p% confidence, node A concludes from its local data that there is an intrusion"
- "With p% confidence, node A concludes from its local data and neighbor states that there is an intrusion"
- "With p% confidence, node A, B, C ... collectively conclude that there is an intrusion" to a more specific state that lists the suspects, like
- "With p% confidence, node A concludes from its local data that node X has been compromised" or to a complicated record including the complete evidence.

As a next step, we can derive a distributed consensus algorithm to compute a new intrusion detection state for this node, using other nodes' state information received recently.

The algorithm can include a weighted computation under the assumption that nearby nodes has greater effects than far

away nodes.

For example, a majority-based distributed intrusion detection procedure can include the following steps:

- the node sends to neighboring node an "intrusion (or anomaly) state request";
- each node (including the initiation node) then propagates the state information, indicating the likelihood of an intrusion or anomaly, to its immediate neighbors;
- each node then determines whether the *majority* of the received reports indicate an intrusion or anomaly; if yes, then it concludes that the network is under attack;
- *any* node that detects an intrusion to the network can then initiate the response procedure.

Intrusion Response

The type of intrusion response for wireless ad-hoc networks depends on the type of intrusion, the type of network protocols and applications, and the confidence (or certainty) in the evidence. For example, here is a few likely response:

- Re-initializing communication channels between nodes (e.g, force re-key).
- Identifying the compromised nodes and re-organizing the network to preclude the promised nodes.

V. Anomaly Detection Models

The 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. The main requirement of an anomaly detection model is low false positive rate, calculated as the percentage of normalcy variations detected as anomalies, and high true positive rate, calculated as the percentage of anomalies detected. We need to first determine the trace data to be used that will bear evidence of normalcy or anomaly. For ad-hoc routing protocols, since the main concern is that the false routing information generated by a compromised node will be disseminated to and used by other nodes, we can define the trace data to describe, for each node, the normal (i.e., legitimate) updates of routing information. Hence, the data shall be used on the node's physical movements and the corresponding change in its routing table as the basis of the trace data. The physical movement is measured by distance, direction, and velocity (this data can be obtained by a built-in GPS device). The routing table change is measured by the percentage of changed routes (PCR), and the (positive or negative) percentage of changes in the sum of hops of all the routes (PCH). During the "training" process, where a diversity of normal situations are simulated, the trace data is gathered for each node. The trace data sets of all nodes in the training network are then aggregated into a single data set, which describes all normal changes in routing tables for all the nodes. A detection model which is learned from this aggregated data set will therefore be capable of operating on any node in the network.

A normal profile on the trace data in effect specifies the correlation of physical movements of the node and the changes in the routing table. We can use the following scheme to compute the normal profile:

- denote PCR the *class* (i.e. *concept),* and distance, direction, velocity, and PCH the *features* describing the concept;
- use n classes to represent the PCR values in n ranges, for example, we can use 10 classes each representing 10 percentage points - that is, the trace data belongs to n classes;
- apply a classification algorithm to the data to learn a classifier for PCR;
- repeat the above for PCH, that is, learn a classifier for PCH;

A classification algorithm, e.g., RIPPER [1], shall use the most discriminating feature values to describe each concept. For example, when using PCR as the concept, RIPPER can output classification rules in the form of: "if (distance 0.01 AND PCH _~ 20) then PCR = 2; else if ...". Each classification rule (an "if") has a "confidence" value, calculated as the percentage of records that match both the rule condition and rule conclusion out of those that match the rule condition. The classification rules for PCR and PCH together describe what are the (normal) conditions that correlate with the (amount of) routing table changes. We shall use these rules as the normal profiles. One 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 (e.g., with RIPPER as the classification algorithm for protocol trace data and "nearest neighbor" as the clustering algorithm for deviation scores), we can identify which routing protocol, with potentially all its routing table information used, can result in better performing detection models. This will help answer the question "what information should be include in the routing table to make intrusion detection effective." This finding can be used to design more robust routing protocols. Next, using a given routing protocol, we can explore the feature space and algorithm space to find the best performing model. This will give insight to the general practices of building intrusion detection for wireless networks.

Anomaly detection for other layers of the wireless networks, e.g., the MAC protocols, the applications and services, etc., follows a similar approach.

VI. Multi-Layer Integrated Intrusion Detection and Response

Traditionally, IDSs use data only from the lower layers: network-based IDSs analyze TCP/IP packet data and host based IDSs analyze system call data. This is because in wired networks, application layer firewalls can effectively prevent many attacks, and application-specific modules, e.g., credit card fraud detection systems, have also been developed to guard the mission-critical services.

Given that there are vulnerabilities in multiple layers of wireless networks and that an intrusion detection module needs to be placed at each layer on each node of a network, we need to coordinate the intrusion detection and response efforts. We shall use the following integration scheme:

- if a node detects an intrusion that affects the entire network, e.g., when it detects an attack on the ad hoc routing protocols, it initiates the re-authentication process to exclude the compromised/malicious nodes from the network;
- if a node detects a (seemingly) local intrusion at a higher layer, e.g., when it detects attacks to one of its services, lower layers are notified. The detection modules there can then further investigate, e.g., by initiating the detection process on possible attacks on ad hoc routing protocols, and can respond to the attack by blocking access from the offending node(s) and notifying other nodes in the network of the incident.

In this approach, the intrusion detection module at each layer still needs to function properly, but detection on one layer can be initiated or aided by evidence from other layers. As a first cut of our experimental research, we allow the evidence to flow from one layer to its (next) lower layer by default, or to a specific lower layer based on the application environment.

The multi-layer integration enables us to analyze the attack scenario in its entirety and as a result, we can achieve better performance in terms of both higher true positive and lower false positive rates. For example, a likely attack scenario is that an enemy takes control of the mobile unit of a user (by physically disable him or her), and then uses some system commands to send falsified routing information. A detection module that monitors user behavior, e.g., via command usage, can detect this event and immediately (i.e., before further damage can be done) cause the detection module for the routing protocols to initiate the global detection and response, which can result in the exclusion of this compromised unit. As another example, suppose the users are responding to a fire alarm, which is a rare event and may thus cause a lot of unusual movements and hence updates to the routing tables. However, if there is no indication that a user or a system software has been compromised, each intrusion report sent to other nodes will have a "clean" vector of upper layer indicators, and thus the detection module for the routing protocols can conclude that the unusual updates may be legitimate.

Currently, we are continuing our investigation in the architecture issues, the anomaly detection model, and the multilayer integration approach. For architecture study, we are refining its design and plan to implement it and study its performance implications. For anomaly detection model, we are studying the effectiveness and scalability of our approach for building anomaly detection models for ad-hoc routing protocols and for other layers of wireless networking. In particular, focus on two questions about ad-hoc routing: what information a routing protocol should include to make intrusion detection effective, and what is the best anomaly detection model for a given routing protocol. We will study the effectiveness gain (i.e., in detection rate) with the multi-layer integration approach, as well as its performance penalties.

VII. Conclusion

We have argued that any secure network will have vulnerability that an adversary could exploit. This is especially true for wireless ad hoc network. Intrusion detection can compliment intrusion prevention technique (such as Encryption, Authentication, Secure MAC, Securing routing, etc) to improve the network security. However new technique must be developed to make intrusion detection work better for the wireless ad hoc environment. Through our continuing investigation, we have show that architecture for better intrusion detection in wireless ad hoc network should be distributed and cooperative. A statistical anomaly detection approach should be used. The trace analysis and anomaly detection should be done locally in each node and possibly through cooperation with all node in the network. Further intrusion detection should take place in all networking layers in an integrated cross layer manner. Currently, we are continuing our investigation in the architecture issues the anomaly detection model, and the multilayer issues, the anomaly detection model and the multilayer integration approach for architecture study, we are refining its design and plan to implements it and study its performance implications. For anomaly detection model, we are studying the effectiveness and scalability of our approaches for building anomaly detection models for ad hoc routing protocol for other layers of wireless networking in particular we will first focus on two questions about ad hoc routing. What information a routing protocol should include to make intrusion detection effective, and what is the best anomaly detection model for a given routing protocol. Finally, we will study the effectiveness, best gain (i.e in detection rate) with the multilayer integration approach as well as its performance penalties.

References

[1] W. W. Cohen. Fast effective rule induction. In *Machine Learning: the 12th International Conference,* Lake Taho, CA, 1995. Morgan Kaufmann.

[2] S. Forrest, S. A. Hofmeyr, A. Somayaji, and T. A. Longstaff. A sense of self for Unix processes. In *Proceedings of the 1996 IEEE Symposium on Security and Privacy,* pages 120-128, Los Alamitos, CA, 1996. IEEE Computer Society Press.

[3] A. K. Ghosh and A. Schwartzbard. A study in using neural networks for anomaly and misuse detection. In *Proceedings of the 8th USENIX Security Symposium,* 1999.

[4] R. Heady, G. Luger, A. Maccabe, and M. Servilla. The architecture of a network level intrusion detection system. Technical report, Computer Science Department, University of New Mexico, August 1990.

[5] K. Ilgun, R. A. Kemmerer, and P. A. Porras. State transition analysis: A rule-based intrusion detection approach. *IEEE Transactions on Software Engineering,* 21(3):181-199, March 1995.

[6] V. Jacobson, C. Leres, and S. McCanne. *tcpdump.* available via anonymous ftp to ftp.ee.lbl.gov, June 1989.

[7] W. Lee, S. J. Stolfo, and K. W. Mok. A data mining framework for building intrusion detection models. In *Proceedings of the 1999 IEEE Symposium on Security and Privacy,* May 1999.

[8] S. Kumar and E. H. Spafford. A software architecture to support misuse intrusion detection. In *Proceedings of the 18th National Information Security Conference,* pages 194-204, 1995.

[9] T. Lane and C. Brodley. Temporal sequence learning and data reduction for anomaly detection. *ACM Transactions on Information and System* Security, 2(3), August 1999.

[10] T. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P. Neumann, H. Javitz, A. Valdes, and T. Garvey. A real-time intrusion detection expert system (IDES) - final technical report. Technical report, Computer Science Laboratory, SRI International, Menlo Park, California, February 2004.

[11] M. Satyanarayanan, J. J. Kistler, L. B. Mummert, M. R. Ebling, P. Kumar, and Q. Lu. Experiences with disconnected operation in a mobile environment. In *Proceedings of USENIX Symposium on Mobile and Location Independant Computing,* pages 11-28, Cambridge, Massachusetts, Aug. 1993.

[12] Ioanna Stamouli, Patroklos G, and Argyoudis IEEE international symposium a world of wireless mobile 2005 *Real time intrusion detection for* ad *hoc network*

[13] Yongguang Zang and wenke lee 2000 Sixth Annual international Conference on mobile computing and networking(Mobicomm 2000) *Intrusion* detection *wireless ad hoc network.*