Intrusion Detection in Wireless Ad-Hoc Networks

Foong Heng Wai <hengwai.foong@nus.edu.sg>
Yin Nwe Aye <yinnweay@comp.nus.edu.sg>
Ng Hian James <nghianja@comp.nus.edu.sg>

Abstract

Wireless ad-hoc networks are increasingly being used in the tactical battlefield, emergency search and rescue missions, as well as civilian ad-hoc situations like conferences and classrooms due to the ease and speed in setting up such networks. As wireless ad-hoc networks have different characteristics from a wired network, the intrusion detection techniques used for wired networks may no longer be sufficient and effective when adapted directly to a wireless ad-hoc network. Existing methods of intrusion detection have to be modified and new methods have to be defined in order for intrusion detection to work effectively in this new network architecture. In this paper, we will first provide an introduction to wireless ad-hoc networks and thereafter an introduction to intrusion detection. We will then present various existing intrusion detection techniques that can be adapted to wireless ad-hoc networks and finally propose a hybrid intrusion detection system for wireless ad-hoc networks.

1. Introduction

A wireless ad-hoc network consists of a collection of mobile nodes that communicate with each other via wireless links without the aid of a pre-existing communication infrastructure. Nodes within each other's radio range communicate directly via wireless links, while those that are far apart rely on intermediate nodes to forward their messages. Each node can function both as a router as well as a host.

For this paper, the mobile nodes that we are focusing our discussion on are current day laptops that have sufficient processing capability and memory to support ad-hoc networking as well as intrusion detection applications. These laptops have limited battery life only when they are unplugged from a main power source. Such mobile nodes are used to setup wireless ad-hoc networks in situations like classrooms or conferences; temporary offices like a promotional booth; emergency search and rescue missions and possibly at command posts in the military.

1.1. Vulnerabilities of wireless ad-hoc networks

Despite the convenience that comes with being able to rapidly deploy wireless ad-hoc networks and being mobile, such networks have inherent vulnerabilities that make them highly susceptible to malicious attacks. The wireless link does not provide the same level of protection for data transmission as a wired link, allowing adversaries within radio transmission range to perform attacks against the transmitted data without gaining physical access to the wireless link. The dynamic and cooperative nature of ad-hoc networking without a centralized authority for authentication and monitoring is susceptible to attacks that breaks down or exploit the cooperative behavior of the ad-hoc routing. The mobile nodes that are roaming independently may have inadequate physical protection and can be captured and compromised. Adversaries using these captured nodes can perform far more damaging attacks from within the network and such attacks are much harder to detect since the captured nodes will contain the private keys and passwords used within the network.

Attacks can come in the form of a passive attack or an active attack targeted at various layers of the Open System Interconnect (OSI) model. At the link layer, a malicious node can actively jam or hoard a communication channel to cause the Media Access Control (MAC) protocol to break down in a scenario resembling a denial-of-service attack. At the network layer, the malicious node can perform passive

eavesdropping of transmitted packets or actively delete, modify, or inject erroneous message as well as impersonate another node such that the availability, integrity, authentication, or non-repudiation of the system is violated [4].

1.2. Network architecture

Wireless ad-hoc networks may be configured in basically two ways, either a flat network infrastructure or a multi-layered network infrastructure. The two different configurations will determine how well an intrusion detection system can be employed in a network as well as the architecture of the intrusion detection system. As to how well an intrusion detection scheme can be employed in a network and in what form of architecture an intrusion detection system is going to take on depend greatly on the network structure itself, we will digress a bit into the discussion of network architecture here. As each node or terminal can act both as a router and as a host, wireless ad-hoc networks may be configured in basically two ways, either a flat network infrastructure or a multi-layered network infrastructure.

In a flat network infrastructure, all nodes are considered to be equal and may participate in routing functions (figure 1) [8].

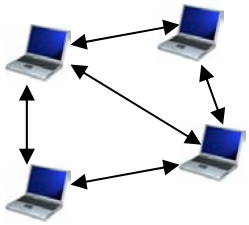

Figure 1. Flat network infrastructure

In a multi-layered network infrastructure, all nodes are not considered equal (figure 2) [8]. Nodes within transmission range are organized into a cluster, and elect a Cluster-Head (CH) node to centralize routing information for the cluster. The CH nodes will in this case be more powerful devices with better resources and they form a virtual backbone of the network. Depending on the protocol, intermediate gateway nodes may relay packets between CH nodes. Therefore, the major part of the processing in detecting intrusion can be done on the CH nodes. That is, each CH node is responsible for the cluster of devices that are communicating with it. This affects the design and implementation of an intrusion detection system in a big way as sophisticated forms of intrusion detection can be used with the CH acting as a central unit processing audit data and serving as a certification authority for providing trust among the devices.

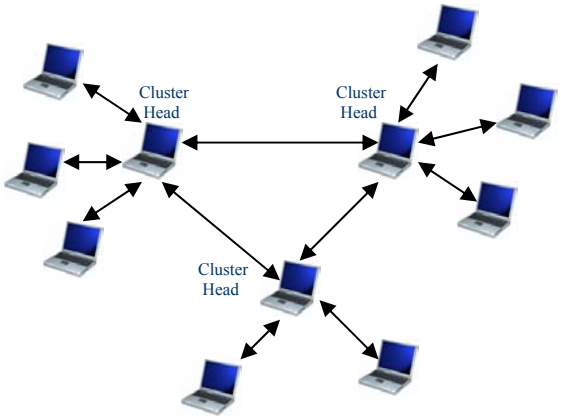

Figure 2. Multi-layered network infrastructure

The rest of our paper is organized as follows. Section 2 touches on the background and needs of intrusion detection as well as the different models of it. In section 3, we will discuss on the current intrusion techniques. In section 4, we will propose a hybrid intrusion detection system suited for the wireless ad-hoc network. Finally, in section 5, we conclude our study of the topic.

2. Intrusion detection

Intrusion detection is defined as the method to identify "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource" [13]. It is pertaining to techniques that attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Hence in the context of wireless ad-hoc network, we need to identify any malicious nodes either from outside the network trying to break into or nodes that have turned bad. Bad nodes can easily disrupt or partition the network using the various forms of attacks as seen from the previous section.

Detection of break-ins or attempts is done either manually or via software expert systems that operate on logs or other information available on the network. Humans can detect much more types of intrusions manually but we are interested in using automated systems that can study the audit data via certain mechanisms or rules. When working on intrusion detection, there are some primary assumptions to be made. Firstly, user and program activities are observable [11], that is the information regarding the usage of a system by a user or program must be recordable and analyzable. Secondly and more importantly, normal and intrusive behaviors must have distinct characteristics [11].

Why is there a need for intrusion detection in wireless ad-hoc network? Isn't intrusion prevention enough? Intrusion preventive measures such as encryption and authentication can reduce intrusion but not eliminate them [11]. Encryption and authentication cannot defend against compromised nodes and the fact that such nodes already carry private keys, which makes the network more vulnerable. The dynamic nature of the ad-hoc network also means that trust between nodes in the network is virtually non-existent. Without trust, preventive measures are unproductive and measures that rely on a certain level of trust between nodes are susceptible attacks themselves.

Another reason for not just having intrusion prevention is that it is often an after-thought during the design and development stages of computer systems. This makes room for loopholes in the system which people can exploit. As systems grow more and more complex, they become increasingly difficult to design and develop as well as maintain. The intrusion preventive measures will be inadequate as there will be more programming errors or bugs. According to Evans' Law, security risk is the product of the vulnerabilities and the number of malicious users. This works out to be about a quadrillion times worse today than in a few decades ago in terms of security problems. Hence there is the need for intrusion detection as it provides a second line of defense.

As a wireless computing device is usually of limited electrical power and intensive processing drains any stored electrical power, we have to avoid the situation whereby the device has to do more routing than other devices on the network. Hence an optimal routing algorithm has to be employed. This is made even critical as power consumption increases tremendously when the wireless transceiver is active. We do not want a device to be exhaust of electrical power faster than it is necessary, especially when it is part of an optimum or even critical routing path where such a device is not operating results in the network needing route repairs or worse, segregated. Therefore, a good intrusion detection system should not only conduct intensive processing for detecting intrusion, it will be better if the system rides on an intelligent routing protocol.

2.1. Anomaly detection vs. misuse detection

In order to detect an intrusion attack, one needs to make use of a model of intrusion. That is, we need to know what an Intrusion Detection System (IDS) should look out for. There are basically two types of

models employed in current IDS: anomaly detection (figure 3) and misuse detection (figure 4).

The first model hypothesizes its detection upon the profile of a user's (or a group of users') normal behavior. It analyzes the user's current session and compares them to the profile representing the user's normal behavior statistically. It then reports any significant deviations to a designated system administrator. As it catches sessions which are not normal, this model is hence referred to as an "anomaly' detection model.

Anomaly detection bases its idea on statistical behavior modeling and anomaly detectors look for behavior that deviates from normal system use. A typical anomaly detection system takes in audit data for analysis. The audit data is transformed to a format statistically comparable to the profile of a user. The user's profile is generated dynamically by the system (usually using a baseline rule laid by the system administrator) initially and subsequently updated based on the user's usage. Thresholds are normally always associated to all the profiles. If any comparison between the audit data and the user's profile resulted in deviation crossing a threshold set, an alarm of intrusion is declared. This type of detection systems is well suited to detect unknown or previously not encountered attacks.

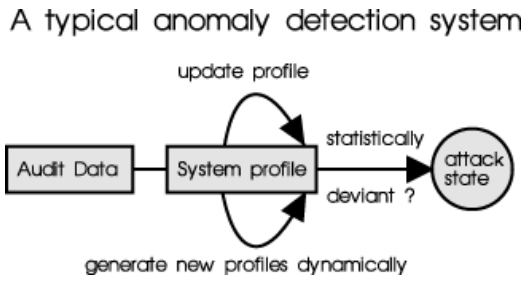

Figure 3. Example of an anomaly detection system [15]

The second type of model bases its detection upon a comparison of parameters of the user's session and the user's commands to a rule base of techniques used by attackers to penetrate a system. Known attack methods are what this model looks for in a user's behavior. Since this model looks for patterns known to cause security problems, it is called a "misuse" detection model.

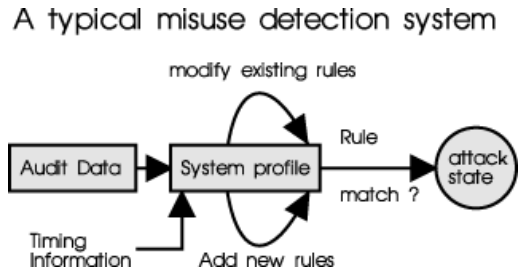

Figure 4. Example of a misuse detection system [15]

Misuse detection bases its idea on precedence and rules and misuse detectors look for behavior that matches a known attack scenario. A typical misuse detection system takes in audit data for analysis and compares the data to large databases of attack signatures. The attack signatures are normally specified as rules with respect to timing information and are also referred to as known attack patterns. If any comparison between the audit data and the known attack patterns described resulted in a match, an alarm of intrusion is sounded. This type of detection systems is useful in networks with highly dynamic behavioral patterns but like a virus detection system, it is only as good as the database of attack signatures that it uses to compare with.

2.2. Host-based vs. network-based intrusion detection

Most intrusion detection systems (IDS) take either a network-based or a host-based approach to recognizing and deflecting attacks. In either case, these products look for specific patterns that usually indicate malicious or suspicious intent. An IDS is network-based when it looks for these patterns in network traffic. It is host-based when it looks for patterns in log files.

Network-based systems (NIDS) listen on the network, and capture and examine individual packets flowing through a network. That is, they use raw network packets as the data source. They typically utilize a network adapter running in promiscuous mode to monitor and analyze all traffic in real-time as it travels across the network. They are able to look at the payload within a packet, to see which particular host application is being accessed, and to raise alerts when attacker tries to exploit a bug in such code. NIDS are typically host-independent but can also be a software package installed on dedicated workstation. A side effect of NIDS is that its active scanning can slow down the network considerably [14]. Hence usage of it on an ad-hoc network needs to be evaluated.

Host-based systems (HIDS) are concerned with what is happening on each individual host. They are able to detect actions such as repeated failed access attempts or changes to critical system files, and normally operate by accessing log files or monitoring real-time system usage. In order for a HIDS to function, clients have to be installed on every host in the network. These clients reside on the hosts as processes and perform analysis on the audit data gathered locally, at the expense of the already limited resources of the hosts. Hence care has to be taken to ensure that the HIDS client running on a host in an ad-hoc network does not drain resources more than necessary.

2.3. Online detection vs. offline detection

The classification of intrusion detection systems can be further segregated according to the timeliness of the audit data being gathered and processed. Audit data can be gathered and processed while the hosts is either online (connected to the network) or offline (disconnected from the network).

When a system is performing intrusion detection in online mode, the audit data is processed real-time continuously. A host-based system will gather information about a host as long as the host is connected to the network. A network-based system will monitor the network traffic of the hosts throughout the time they are connected. Any intrusion detected is immediately notified to other hosts.

When a system is performing intrusion detection in offline mode, the audit data is not processed real-time but periodically. A host-based system will gather information about a host even if it is not connected to the network. Even if the host is connected, detection is done as scheduled by the system. A network-based system will monitor the network traffic of the hosts periodically as can be in the case of polling. Any intrusion detected is still immediately notified to other hosts but a delay is expected. A typical technique of an offline intrusion detection system is data mining.

Table 1. Shell command records from operating system

Time	Hostname	Command	arg1	arg2
am	pascal	mkdir	dir1	
am	pascal	cd	dir1	
am	pascal	vi	tex	
am	pascal	tex	vi	
am	pascal	subject	fredd	
am	pascal	vi	progress	
am	pascal	vi	tex	

Table 2. Network connection records

Timestamp	Duration	Service	src_host	dst_host	src_bytes	dst_byets	Flag	…
1.1	0	http	spoofed_1	victim	0	0	S0	…
1.1	0	http	spoofed_1	victim	0	0	S0	…
1.1	0	http	spoofed_1	victim	0	0	S0	…
1.1	0	http	spoofed_1	victim	0	0	S0	…
1.1	0	http	spoofed_1	victim	0	0	S0	…

Given the two models (anomaly and misuse) of intrusion detection and the various approaches in implementing intrusion detection systems, there is a need to determine the sources of audit data for these systems. Audit data are information which any intrusion detection scheme can work on to determine if any intrusion has occurred. The audit data may be obtained on the host, in application or system log file by host based intrusion detection system (table 1) or from the network by network based intrusion detection system (table 2).

3. A survey of intrusion detection techniques

3.1. Problems of current intrusion detection techniques

It is difficult to apply intrusion detection techniques developed for the wired network to the wireless ad-hoc network due to the vast difference between the two networks. The main difference is that wireless ad-hoc networks do not have fixed infrastructures, and existing network-based IDSs, which rely on real-time traffic analysis, can no longer function well in the new environment. In wired networks, traffic monitoring is usually done at switches, routers and gateways. The wireless ad-hoc environment does not have such traffic concentration points where the IDS can collect audit data for the entire network and can only rely on partial, localized audit data collected from the host and from communication activities taking place within the radio range.

Besides having different network infrastructures, there is also a big difference in the communication pattern of users in the wireless mobile environment. Due to the bandwidth limitations, battery constraints and frequent disconnects, users often adopt new operations modes such as disconnected operations [12]. This suggest that existing anomaly detection models may not be able to determine that such new operations are certified and identify them as intrusions.

There also may not be a clear separation between normalcy and anomaly in the mobile environment [11]. A node that sends out false routing information could be a compromised node or merely one that is temporarily out of sync due to rigorous physical movement. Existing detection methods may find it increasingly difficult to differentiate false alarms from real intrusions.

The lack of protocol standards, an example being the lack of a standardized routing protocol makes it difficult to define intrusion attack signatures for the wireless mobile environment. Signatures are defined from the characteristics, vulnerabilities and the working topologies of the routing protocol. The lack of understanding of new applications that are being developed for the wireless mobile environment also add to the difficulty in defining attack signatures.

3.2. Reasons for choice of intrusion detection techniques

The intrusion detection techniques that will be presented in the following sections are chosen due to the suitability of the technique for anomaly detection. Anomaly detection should be the main approach for intrusion detection in the wireless ad-hoc network because it is conceivable that intrusion in this new environment will come in the form of new attacks types that are yet to be defined. These techniques can also be adapted for local and cooperative detection. The techniques can either process partial and local data on the host as well as gather more information from the neighboring hosts to perform cooperative intrusion detection.

3.3. Haystack

This algorithm [1] is a statistical anomaly detection algorithm. It works by first assuming that the audit trail generated from a host has been converted to a canonical audit trail (CAT) format. It then uses a CAT file to generate session vectors representing the activities of the users' sessions. These session vectors are then analyzed against specific types of intrusive activities to calculate "anomaly scores". If the scores cross some thresholds, warnings reports are generated. The algorithm analyzes a session vector in three steps: 1) it calculates a Bernoulli vector, 2) it calculates the weighted intrusion score, and 3) it calculates the suspicion quotient.

The Bernoulli vector is generated from the session vectors as well as some threshold vectors. It is a simple binary vector in which the values in the vector are set to one if the corresponding arbitrary counts fall outside the threshold for a particular user group. The weighted intrusion score is generated for a particular session and for a particular intrusion type. It can be used to assign a suspicion value to the session. This suspicion value, or suspicion quotient, for a session is determined by what percentage of random sessions have a weighted intrusion score less than or equal to the weighted intrusion score of the current session. It describes how closely a session resembles the intrusion type as compared to all other sessions.

The Haystack algorithm gets its name by being the algorithm implemented in the IDS called Haystack. Haystack is a host-based system which attempts to detect several types of intrusions: attempted break-ins, masquerade attacks, penetration of the security system, leakage of information, denial of service, and malicious use. It was initially developed for use in the US military network.

This algorithm is designed for use in a secured wired military network. If in a wireless ad-hoc environment, it requires a designated node to act as a central administrator and all the other nodes to allow the central administrator to retrieve audit trails from them. The central administrator can be pre-designated by the human initiator of the ad-hoc network or programmatically assigned. The audit trails requested can be submitted by the nodes themselves or by mobile agents allowed to run on the nodes.

3.4. Indra

Indra [2], named after an Indian God, is also stands for *INtrusion Detection and Rapid Action*. It is a distributed intrusion detection scheme based on sharing information between trusted peers in a network to guard the network as a whole against intrusion attempts. It is a detection tool that takes a proactive and P2P approach to network security.

The basic idea behind Indra is simple and that is cross monitoring, or simply called "neighborhood watch". In this idea, the hosts on the P2P network join together to form some sort of an immune system where each host distributes information on attempted attacks among the interested peers in the network. Such information is usually gathered by the intended victim of an attack and by notifying its adjacent hosts, an alarm can be sounded. This allows the system to react proactively or retroactively. When an alarm is sounded, subsequent attacks to other hosts are repelled straightaway as the adjacent hosts would have forewarned other hosts.

Alternatively, it is also possible for hosts in the network to detect other hosts as being under attack. This is effective if the network is a shared medium but the same effect can be achieved by having Indra installed on network gateways or on a machine attached to a "snoop" port of a network switch.

The functionality of Indra is achieved by a set of daemons. Each interested host on the network runs a special security daemon which watches out for intrusion attempts and also enforces access control based on its memory of earlier attempts. Other daemons that belong to different classes help to look out for suspicious activities, aggregate the warning notifications, or communicating with other hosts. These daemons could be configured by the system administrator for different levels of security.

Though the scheme is easy to understand, there are practical difficulties at the levels of communication, trust, and policy to overcome. Indra has gone on to address these issues.

In Indra, trust is an important issue. This is especially true in an intrusion detection system that lacks a centralized trusted authority to provide digital certificates. That is, a network without a certification authority (CA) will not have its host nodes trusting one another in order for the information-sharing idea in Indra to work. Indra requires a certain level of trust between hosts so that the daemons running on the hosts can trust the messages received from other hosts.

Unfortunately, a wireless ad-hoc network is one such network where trust is virtually non-existent. In the wireless ad-hoc environment, a host is supposed to trust no other host except itself. This poses a problem when trying to deploy Indra as the intrusion detection scheme in this type of network. Fortunately, Indra has tried to address the trusting issue. The usual decentralized alternate to central CA is the web-of-trust model. In the prototype version of Indra, certificates for hosts are gotten from trusted key servers for certifying among peers but variants of the web-of-trust model are used in real situations.

Communication in Indra is done with the use of daemons between trusted hosts. Therefore, all the hosts and subsequent hosts joining into the wireless ad-hoc network would have to have the various daemons running before they are allowed to operate in the network. So far, Indra has been investigated on several networks and models of communication. In general, Indra can be deployed on any peer-to-peer network as long as mechanisms which provide a node to propagate information to a randomized subset of its neighbors, or creating multicast trees, are present.

Policy in a wireless ad-hoc network, regardless of the intrusion detection scheme employed, has to be pre-defined and agreed upon by the hosts joining the network. Hence for Indra, the different levels of security provided by configuring the daemons and the use of the mechanism of inserting additional functionality though the use of plug-ins have to be discussed before-hand. Alternatively, all these can be set as a pre-condition for hosts belonging to the network.

3.5. Mobile agents

A global distributed and modular architecture [5] where the intrusion detection scheme is provided by local IDS (LIDS) entities, located on each node of the mobile ad hoc network (MANET) and collaborating with other LIDes through the use of mobile agents. As the lack of the centralization in MANET, some of the tasks required for the intrusion detection processes should be executed in a distributed and cooperative manner. Mobile agents are an alternative to the client-sever distribution model. Mobile agents can provide a first element of response to the problem of the scalability of the global intrusion detection process. When a node joins the network, it does so with running LIDS and a mobile agent platform. It can therefore, immediately take part in the global cooperative intrusion detection process.

This modular architecture is divided in three main processes: data collection, detection algorithm design and alert management. Each of the elements in the model; Sensor, Analyzer and Manager are related with one of the intrusion detection processes. A sensor collects data from a data source, an analyzer processes the collected data for detecting signs of events that might have security concerns and the manager stands for the management interface of whole process, besides of doing alert correlation and response initiation. Activities monitored by the sensor in the data source may be mapped in events, which are passed to the analyzer, where they are submitted to the hybrid (misuse and anomaly detection) intrusion detection algorithm. When the analyzer finds events with relevant security concerns, alert are generated to the manager.

All raw data collection and pre-processing is performed locally in the same LIDS. While executing all raw data collection and abstraction locally, node detects attacks against some of its neighbors. Thus, whenever some (high level) message needs to be processed remotely, a mobile agent is dispatched to the remote node carrying the data and possibly the code needed for the remote message processing. Mobile agents are created, received (from a remote host) and managed in the mobile agent framework. These mobile agent platforms should also provide security services (e.g. server authentication, agent and server code integrity, access control to local resources, etc) related to agent activities.

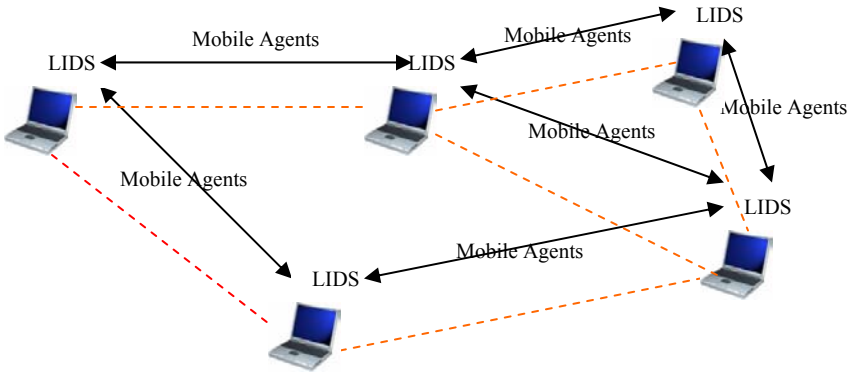

Figure 5. Intrusion detection system using mobile agents

3.6. Data mining

Data mining algorithms implemented on each mobile node can be used to analyze audit data and thereafter generate intrusion detection models. Data mining generally refers to the process of extracting useful models from large repositories of data [3]. Below are several algorithms that are particularly useful for mining audit data for anomaly detection.

Classification is the process by which a data item is mapped into one of several predefined categories. The classification algorithms normally produce "classifiers" that can be in the form of decision trees or rules. Sufficient "normal" and "abnormal" audit data must be gathered before a classification algorithm can be applied to learn a classifier that can categorize new unseen audit data as belonging to the normal class or the abnormal class.

Link analysis is used to determine relations between fields in an operating system audit record. Normal usage profile can be constructed from determining the correlation between *command* and *argument* in the shell command history data of a user [7]. A programmer, for example, may have emacs highly associated with C files.

Sequence analysis involves the analysis of frequent sequential patterns of audit data in order to gain insight into the temporal and statistical nature of many attacks as well as the normal behavior of users and programs. The statistical information collected can then be incorporated into intrusion detection models.

4. A proposed hybrid intrusion detection system

4.1. Hybrid system requirements

Our hybrid intrusion detection system is designed especially for the wireless ad-hoc network although it can also be deployed in the wired network. We take into considerations, when designing our hybrid intrusion detection system, the characteristics of the wireless ad-hoc network and the problems that existing system face when being deployed in a wireless ad-hoc environment.

The dynamic and cooperative nature of the wireless ad-hoc network suggests that the intrusion detection system should be designed to be dynamic and cooperative as well. Each node should have its own intrusion detection module since it cannot rely on other nodes that may leave the network at anytime to help it perform intrusion detection. Wireless ad-hoc networks also do not have traffic concentration points that allows for intrusion detection at a centralized location and this further emphasize the need for each to have its own intrusion detection module.

Intrusion detection should first be performed locally on each node utilizing the partial, localized audit data since this is the most reliable source of audit data for a node. Each node can then perform cooperative intrusion detection when more information is required from other nodes to confirm the intrusion. For cooperative intrusion detection, the individual node is required to work with neighboring nodes to gather more audit data for intrusion detection. This suggests that there should be a secure communication channel between the nodes participating in the cooperative intrusion detection.

The intrusion detection module on each node should be able to perform both anomaly and misuse detection but should be optimized for online anomaly intrusion detection although offline intrusion detection is needed as well. Online anomaly intrusion detection is needed to quickly identify new attacks whereas offline intrusion detection is needed to build new models that are representative of the wireless ad-hoc network. Such models can then be used by the online anomaly detection as a basis of intrusion identification.

The hybrid intrusion detection system should be interoperable with existing intrusion detection systems since a wireless ad-hoc network can be deployed in an environment (e.g. university campus) that contains different types of networks, which are interconnected and already have existing intrusion detection systems running on them. Allowing exchange of audit data and other information between the different systems may increase the overall effectiveness of intrusion detection in the entire environment.

The last requirement for the hybrid system is that it should be scalable. As wireless ad-hoc networks are becoming more mainstream, such networks in the future may contain hundreds to thousands of nodes. A scalable system will ensure that intrusion detection still continue to function effectively and efficiently under a large number of nodes.

The proposed hybrid system (figure 5) consists of the following components; data collector, detection optimizer, detection engine, response engine and secure communication module.

4.2. Data collector

The data collector collects data at the link layer, the network layer and the application layer. Information is needed from these three different layers to perform multi-layered intrusion detection [11]. Multi-layered intrusion detection is needed as certain attacks that target the upper layer may seem perfectly legitimate to the lower layers.

4.3. Detection optimizer

Due to the limited battery life that the mobile node has, we deem that intrusion detection should be done on the basis of different levels of escalation starting from the simplest and least battery consuming intrusion detection operation to more complex and CPU intensive operation. The detection optimizer preprocesses all the audit data collected from the different layers and send the most relevant audit data to the detection engine based on the mode that the mobile node is currently operating in.

4.4. Detection engine

The detection engine performs both misuse and anomaly detection. Either the Haystack or data mining algorithms can be implemented in the detection engine.

4.5. Response engine

When an intrusion is detected, the system needs to respond appropriately. It can either sound a local alarm on the host or a global alarm on the network. The nodes can then respond to the intrusion either locally or cooperatively.

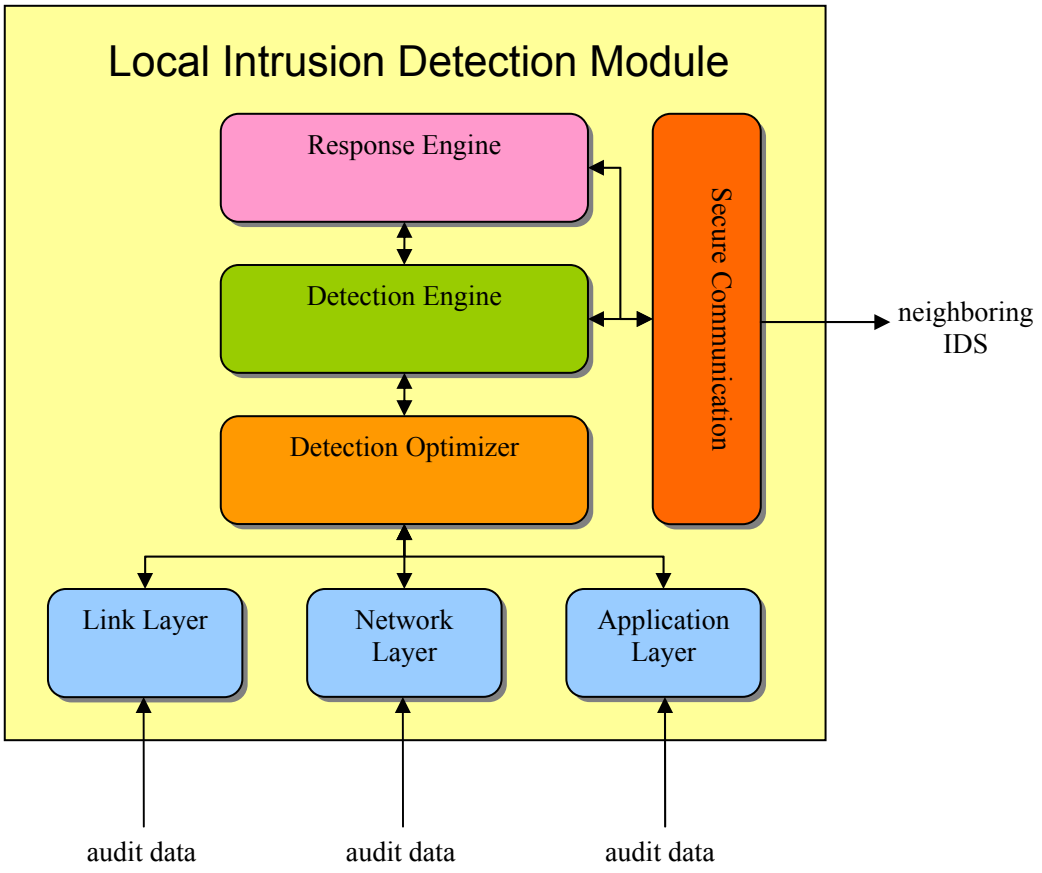

Figure 7. Hybrid intrusion detection system

4.6. Secure communication module

The secure communication module is needed when the node needs to perform cooperatively intrusion detection as well as when sounding a global alarm. Mobile agents, the Indra approach or tunneling can be implemented for this communication module.

5. Conclusion

Wireless ad-hoc networks have brought about a paradigm shift in the way we think about intrusion detection. We need to rethink methods for these new networks based on the characteristics that these networks have. In this paper, we have provided an introduction to wireless ad-hoc networks. We then proceeded to provide an introduction to intrusion detection in the context of wireless ad-hoc networking. Having understood the implications and problems in performing intrusion detection in this new environment, we performed a survey on the existing methods for intrusion detection and listed four techniques that we deemed are suitable for the wireless ad-hoc environment. We ended by proposing a hybrid intrusion detection system that allows the different techniques that we have identified to be incorporated into the system and is most suited for wireless ad-hoc networking.

References

[1] B. Mukherjee, L.Todd Heberlein, and Karl N. Levitt. *Network Intrusion Detection*. IEEE Network, May/June 1994

[2] R. Janakiraman, M. Waldvogel, and Qi Zhang. *Indra: a peer-to-peer approach to network intrusion detection and prevention*. Twelfth IEEE International Workshops, Jun 9-11, 2003

[3] Fayyad, U., Piatetsky-Shapiro, G., and Smyth, P. 1996. The KDD process of extracting useful knowledge from volumes of data. Commun. ACM 39, 11, 27-34

[4] Zhou, L. and Haas Z.,"Securing Ad Hoc Networks," *IEEE Network Magazine*, vol. 13, no. 6, November/December 1999.

[5] S. Puttini, J-M. Percher, L. Mé, O. Camp, R. de Sousa Jr., C. J. Barenco Abbas, L. J. Garcia Villalba. A Modular Architecture for Distributed IDS in MANET. In Proceedings of the 2003 International Conference on Computational Science and Its Applications (ICCSA). Springer Verlag, LNCS 2668, May 2003

[6] Kong, J., Luo, H., Xu, K., Gu, D., Gerla, M., and Lu, S.,"Adaptive Security for Multi-layer Ad-hoc Networks," *Special Issue of Wireless Communication and Mobile Computing*, 2002.

[7] Wenke Lee, Salvatore J. Stolfo. A framework for constructing features and models for intrusion detection systems. ACM Transactions on Information and System Security (TISSEC) Vol. 3, Issue 4 Nov 2000

[8] Brutch, P., Ko, C. "Challenges in Intrusion Detection for Wireless Ad-hoc Networks". Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on , 27-31 Jan. 2003

[9] Boukerche, A. "Performance Comparison and Analysis of Ad-hoc Routing Algorithms". Performance, Computing, and Communications, 2001. IEEE International Conference on. , 4-6 April 2001 Page(s): 171 - 178

[10] Zhang, Y. and Lee, W., "Intrusion Detection in Wireless Ad-Hoc Networks," In *Proceedings of the Sixth Annual International Conference on Mobile Communication and Networking*, 2000.

[11] Zhang, Y., Lee, W. and Huang Y. A., Intrusion detection techniques for mobile wireless networks. Wireless Networks, Volume 9 Issue 5, September 2003

[12] 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 Independent Computing*, Cambridge, MA (August 1993) pp. 11–28.

[13] 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).

[14] Kachirski, O. and Guha, R., " Intrusion detection using mobile agents in wireless ad hoc networks", Knowledge Media Networking, 2002. Proceedings. IEEE Workshop on, 10-12 July 2002 Page(s): 153 –158

[15] Sundaram, A., An introduction to Intrusion detection, http://www.acm.org/crossroads/xrds2-4/intrus.html