Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2007

Intrusion Detection System (IDS) Techniques and Responses for Mobile Wireless Networks

Krishnun Sansurooah
Edith Cowan University

Originally published in the Proceedings of 5th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, December 4th 2007
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/39

Intrusion Detection System (IDS) Techniques and Responses for Mobile Wireless Networks

Krishnun Sansurooah
School of Computer and Information Science (SCIS)
Edith Cowan University
Perth, Western Australia.
ksansuro@student.ecu.edu.au

Abstract

In recent years, the rapidly expanding area of mobile and wireless computing applications was definitely redefined the concept of network security. Even though that wireless had opened a new and exiting world with its advancing technology it is no doubt that it is popularity is on the rise. However, the biggest concern with either wireless or mobile computing applications in security. It can no longer be effective in the traditional way of securing networks with the use of firewalls and even with the use of stronger encryption algorithm keys. The need to develop and research for new structures and methods to protect and define the wireless networks and the mobile computing applications is becoming more and more evident. In this report, we will conduct an in-depth analysis of the weaknesses of the wireless networks and hence proved why the use of an intrusion detection system is of great importance in securing the backbone of mobile computing field. This would also involve detecting anomalies in the mobile ad-hoc network including inconsistencies in the routing tables and activities on other layers.

Keywords

Intrusion Detection Systems (IDS), wireless and mobile intrusion response, active countermeasures and anomaly detection and misuse detection.

INTRODUCTION

The definition of an intrusion can be defined as a set of events and actions that unfortunately lead to either a modification or an unauthorized access to a particular system. The purpose of an Intrusion Detection System (IDS) is to constantly perform monitoring of the computer network and also where possible in detecting any intrusions that have been perpetrated and hence altering the concerned person after the intrusion have been detected and recorded.

Following a report that Moore (2001) published, the Code Red worm caused a total chaos in infecting over 359,000 hosts within less than 14 hours as illustrated in Figure 1.

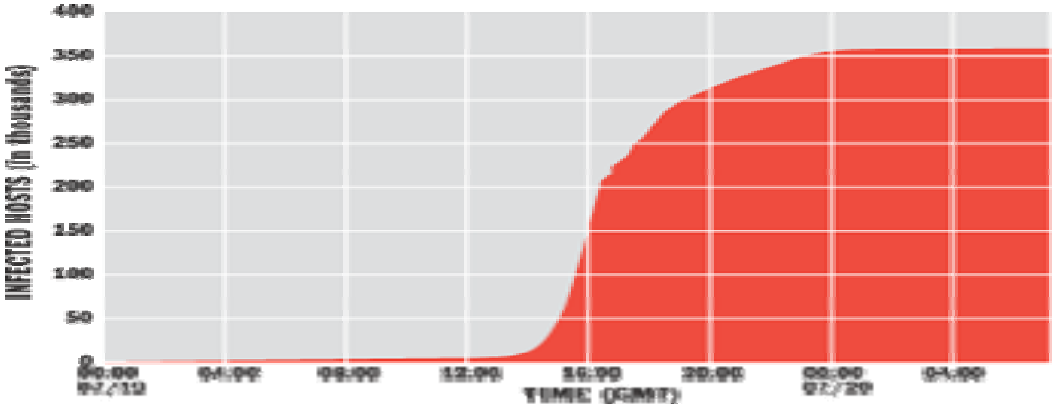

Figure 1 Illustration of the propagation of the Code Red Worm

Therefore, the traditional way of securing networks with firewalls or by making use of stronger encryption algorithm keys prove to be on longer effective. As per figure 1, this internet worm mostly known as Code Red was intended to cause a disruption of service among Window-based server. However, it was not at its first incident as it has been detected and caught in different occasion due to the use of mobile computers of several business travelers who have access to laptops while going onto the different conferences hence making use of wireless access to the Internet which does have an extremely high probability of being infected by the worm.

When, at a later stage, these laptops returned to their original base – i.e. when they are connected back to their company network, the worm can spread from within thus leaving the firewall to be of absolute gimmick.

Also with the mobile ad-hoc network commonly described as (MANET) is known to be a short of self-configuring network that comes together automatically by a collection of mobile nodes without having to rely on a fixed infrastructure. This therefore include that each node is equipped with a wireless transmitter and receiver to allow communication flow with each node.

The main concern of IDS is its responsibility in gathering and collecting activity information which then is put to analysis to determine whether there has been any intrusion(s) which has cause any rules to be infringed. Once the IDS are certain that an irregularity has occurred or such as an unusual activity has been recorded, it then alerts the concern person – i.e. the system administrator. Even with the numerous intrusion detection techniques that have been developed for wired networks, they still do not adjust onto the wireless networks due their different trails.

INTRUSION DETECTION SYSTEM (IDS)

An Intrusion Detection System (IDS) can therefore be defined as a system that inspects all inbound and outbound network activities and identifies suspicious patterns that may indicate either a system or network attack from an intruder attempting to break into or to comprise a system.

Past historical events have proved that intrusion prevention techniques by itself such as either authentication or encryption which are usually considered as the first line of defense is not enough. Nowadays, systems are more complex thus; more weaknesses and vulnerabilities are found which lead to one particular problem which is security. Intrusion detection systems should therefore be used as a second layer of defense to securely protect the networks and thus mitigating disruption to a system.

Intrusion detection system can hence be categorized into 3 different sectors as illustrated below based on audit data.

Misuse detection v/s Anomaly detection

In misuse detection, the IDS analyze the information that it has collected and then compares it to a large database of known attack signatures. Eventually, the IDS will look for a specific attack that has already been recorded and documented. In anomaly detection, the system administrator will have to indicate the baseline, or normal, state of the networks traffic load, breakdown, protocol and typical packet size. Therefore the anomaly detector controls the network segment to compare their state to the normal baseline and to look for anomalies.

Network-base (NIDS) v/s host-based system (HIDS)

In a network based system, or NIDS, the individual packet flowing through the network are scrutinized and also analyzed. The NIDS can detect malicious packets that have been designed to be ignored by a firewall's filtering rules. In a host-based system, the IDS would examine the activities on each individual host or computer

Passive v/s Reactive

Passive, the IDS detects a potential security breach, will keep track by logging the information and triggering an alert whereas in a reactive system, the IDS will have to react to the suspicious activity by logging off a user or by either reprogramming the firewall to block network traffic from the un-trusted source.

WEAKNESSES OF MOBILE WIRELESS NETWORKS

Mobile wireless network environment is greatly vulnerable to malicious attacks due to the fact of the use of wireless links that unfortunately contribute to make these attacks more and more real. Compared to a wired network if an intruder would like to gain unauthorized access to the system, there are various levels of security that s/he would have to bypass, as gaining access to network wires would include to bypass firewalls and gateways whereas on a mobile wireless network, attacks could come from anywhere and hence any node on the wireless network could be targeted. Such implication could definitely result in lack of information which could be very costly to the organization. The bottom line of using mobile wireless ad-hoc network is that there is not a clear defense line of security and that every node or access points must be ready and prepared in terms of securing the network to encounter direct or indirect attacks from outsiders.

Another issue with mobile access points (APs) or nodes are that they are uncontrolled units and able to operate on their own. Meaning if those units do not have the adequate physical protection, they are very much proved to be attacked, captured, compromised or hijacked. Zhang et al (2003) mentioned that tracking down a particular

node in a global scale network is not an easy task to perform and attacks by a node that has been compromised within the network are far more damaging and even much harder to trace out. Therefore all mobile APs or nodes must be adjusted to behave in such a way that no peer is trusted.

Finally a gigantic security issues does arise when it comes to decision making in mobile wireless computing environment which most of times if not 9 times out of 10 are decentralized and leaving some of the wireless network keys to depend on all the other nodes of the structure. This deficiency in relying upon decentralized infrastructure makes the system more vulnerable to attacks which would be more focused on breaking the general algorithms.

A very obvious example would be relating to the MAC protocols used in the wireless channel are attackable even with the numerous of MAC protocols the very basic principle operate similarly. Each AP will compete to be able to get the control of the transmission channel each and every time that a message is sent out in a contention based methods where the nodes will have to follow pre-defined protocols to avoid any collision whereas in a contention free method, each node will have to request from all the other nodes an undisputed exclusive use of the channel resource when transmitting and this regardless of the MAC protocols used or in place thus sometimes resulting in a Denial of Service (DOS) attack. However, this would never occur in a wired network because of the MAC layer and the physical layer is segregated from the outside world which hence occurs and operates at the layer 3 of the gateway or firewall. This is definitely not the case with mobile wireless ad-hoc network where every mobile node is completely isolated and unprotected in the wireless communication medium.

With the advances in technology, mobile computing has been reformed by introducing new ways of communication that is rarely present in wired network environment. However, users of mobile wireless networks tend to complain about the limitations of the communication due to limited bandwidth, higher cost rates, slower connection speed and mechanism like disconnected operations mentioned by Kistler et al. (1993) and location – dependent operations only appear to mobile wireless networks.

Another reason why applications in mobile wireless networks can be viewed as a weak point is that these networks are often making used of proxies and also using software agents that are run in the base-stations (BS) and for those in-between nodes to attain the performance gain this should be performed through traffic shaping caching or through content transcoder. Attacks could therefore target these proxies or software agents in order to steal the sensitive information or simply coordinating a DOS attack by overflowing the cache with poor or fake reference or by simply forcing the content transcoder to compute futilely.

Hence to recapitulate, mobile wireless network is exposed to attacks because of its inability to effectively secure is medium of communication, its inadaptability to manage a central monitoring, and also due to its dynamic damaging network topology choices. Therefore, it can be deduced that further in-depth research is needed to be able to cover these weaknesses in the mobile wireless network.

ARCHITECTURES OF IDS FOR MOBILE WIRELESS NETWORKS

The structure for the wireless mobile network can be used and configured depending of the applications. According Brutch & Ko (2003), the optimal IDS architecture for a mobile network will totally depend on the network infrastructure itself. In a flat network infrastructure, all the nodes are to the same level of priorities and suit applications such as conferences whereas on multi-layered network infrastructure some nodes may be separated into different clusters each having a cluster head to allow communication process.

STAND-ALONE IDS

With stand-alone IDS, the architecture is normally based upon running each node separately in order to locate the intrusions if perpetrated. Hence every decision is based and focused upon all the information that is collected at each and every node as all the nodes are independent and work individually as per its name itself “stand-alone”. Beside being totally isolated, the nodes on the same network do not know anything about the different nodes or the same network as no data is exchanged hence no alert information is passed on. Even though restricted by its limitations, more adaptable in situation when each node can run an IDS on their own or have IDS installed it is much more preferred for a flat network architecture which will unfortunately not suitable for wireless mobile network.

COOPERATIVE & DISTRIBUTED IDS

Zhang & Lee (2003) mentioned that wireless mobile networks have to adapt a cooperative and distributed intrusion detection system architecture. This is achieved by the IDS agent running on top of the nodes. Yet the

IDS agent can however be complex but when analyzed closely, the IDS agent can be broken into six different modules. Figure 2 below gives a clear illustration of the 6 different components of the IDS agent.

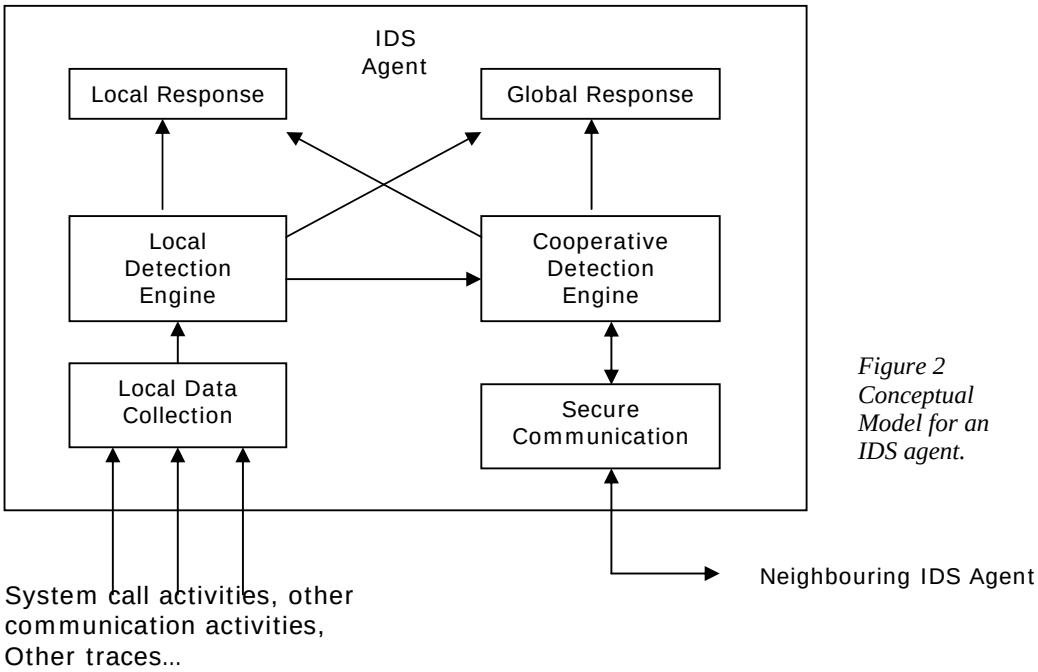

Figure 2 Conceptual Model for an IDS agent.

So in the cooperative and distributed network mentioned by Zhang & Lee (2003), every single node has a crucial role to play, each node has the responsibility for detecting any signs of intrusion and is responsible for contributing individually or entirely onto the network. This can hence be achieved through the different parts of the IDS agent illustrated in Figure 2 where the "local data collection" would be collecting real-time data this would definitely include both user and system activities within radio transmission range. The IDS also triggers response if intrusion is detected. However, if an anomaly in the local data is xx or detected on the boarder search, then the neighboring IDS agents will collectively associate themselves into the global intrusion detections actions. We certainly do note that these isolated IDS agents are entirely link together to form the IDS system defending the mobile wireless network.

In figure3 below is a detailed outline of the IDS architecture for wireless mobile networks with each node bundled with the IDS Agent which is responsible as mentioned earlier of the intrusion state and the response action.

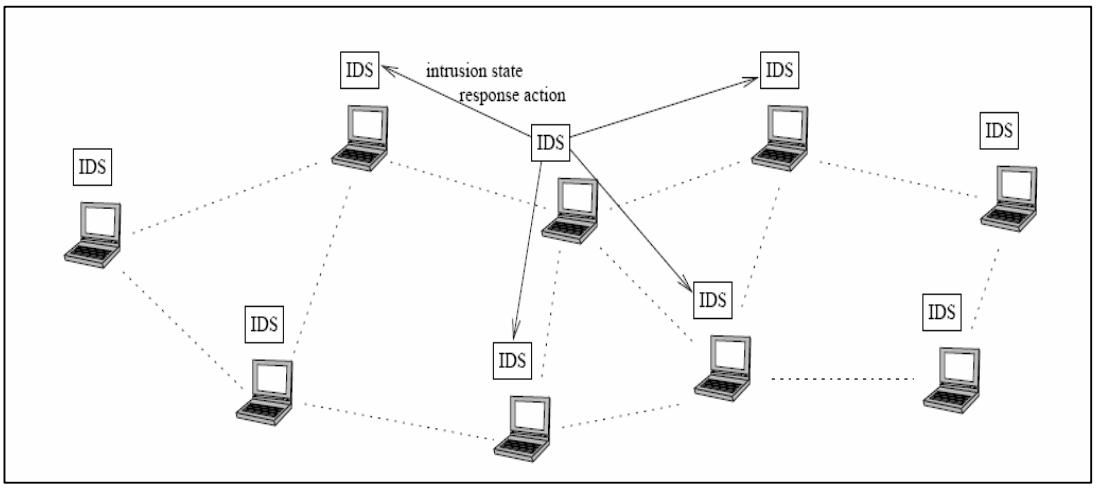

Figure 3 shows the IDS architecture of the wireless mobile network.

LOCAL INTRUSION DETECTION SYSTEMS

According to Albers, P. et al., (2002), they proposed a distributed and collaborative architecture of IDS by making use of mobile agents. This means that a Local Intrusion Detection Systems (LIDS) is mounted on every single node for either local or global concern depending on the type of intrusion detected. While using the LIDS architecture, there are two types of data that are communicated and exchanged amongst the nodes.

- ***Security data*** – this would be capturing highly favorable information for all the combined nodes;
- ***Intrusion alerts data*** – would be to inform all the other nodes of any locally detected intrusion.

Basically, the way the LIDS operates is that all the data that has been collected from what has been deleted from the individual or combined nodes on the network. Since each node might be running different OS or may be using data from various sources which might include system, application, or network activities might make the analysis process of LIDS harder. However, on making use of simple network management protocol (SNMP) all the data located in the management information base (MIB) as a source of data auditing.

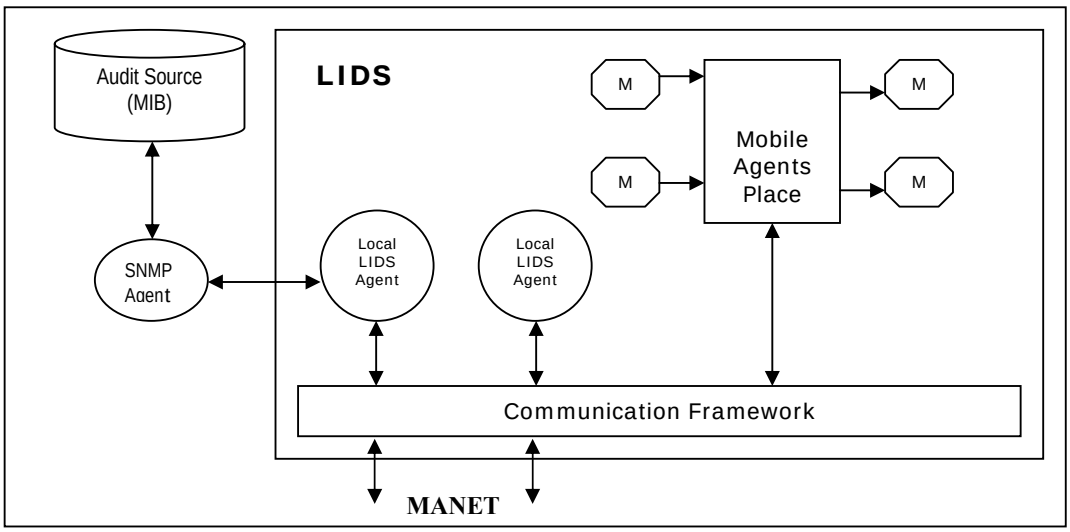

Figure 4 below shows the LIDS architecture in a mobile environment which is further exploded into 3 different sections.

1) Communication Framework: This enables both internal and external communication with LIDS.
2) LIDS Agent: Has the responsibility for locating intrusion detection and local response. It therefore has the capability to react to intrusion alerts from other independent nodes on the network and hence protect itself against that particular intrusion.
3) MIB Agent – This would be a way of gathering MIB variables for either mobile agent of LIDS agent. In another word, local MIB Agent xx as interface with SNMP agent. However, if SNMP is present on a particular node, or within an agent which as been tailored-made therefore retrieval of MIB variables used by intrusion detection.
4) Mobile Agents (MA): Responsible in collecting and processing data on the different nodes.
5) Mobile Agents Place: To enable a better security control to the MAs.

Having gone through the different section of the LIDS, it is noted that it can either use anomaly or misuse detection but a preferred combination of both techniques will definitely offer a better model became as soon as the local intrusion is recorded, the LIDS will initiates a response and thus inform all the other nodes on the mobile network which is turn of receiving that alert, the LIDS can protect itself from that particular intrusion.

DISTRIBUTED INTRUSION DETECTION SYSTEM USING MULTIPLE SENSORS

A multi-sensor intrusion detection system combining a mobile agent technology is proposed by Kachirstu & Guha (2003) which can be further categorized into 3 main areas each representing an MA with some intelligence such as decision making, being capable of initiating a response and performing monitoring.

Decision making Agent

According to Kachirski, O. & Guha, R. (2003), the described the decision making agent on an agent that is posted only on certain nodes of the network and preferably on the same nodes that the performance monitoring agent are run. The decision making agent will therefore gather all the packets within its radio range and will be subject to analysis in order to determine whether the network is being attacked. However, if for any particular reason that the detection agent can not come to a decision due to a lack of evidence, the local detection agent report to this decision agent so that for the investigation be carried out using packet monitoring outcomes that has been collected from network monitoring sensor run locally.

Performance Monitoring Agent

In this category, tow distinct functions are performed involving host monitoring and network monitoring. In the first instance, the host based monitoring agent hosting system level sensor and user-activity is run on every node whereas in network monitoring, sensors are and would be running on selected nodes to monitor the captured packets going through the network.

Initiation Action Agent

This agent is omnipresent on every node onto the network since that every node onto the network host a host based monitoring agent. When corporative evidence is gathered supporting any inconsistencies that have aroused on the network, this initiating action agent can therefore trigger termination of processes or even blocking any particular user from the network.

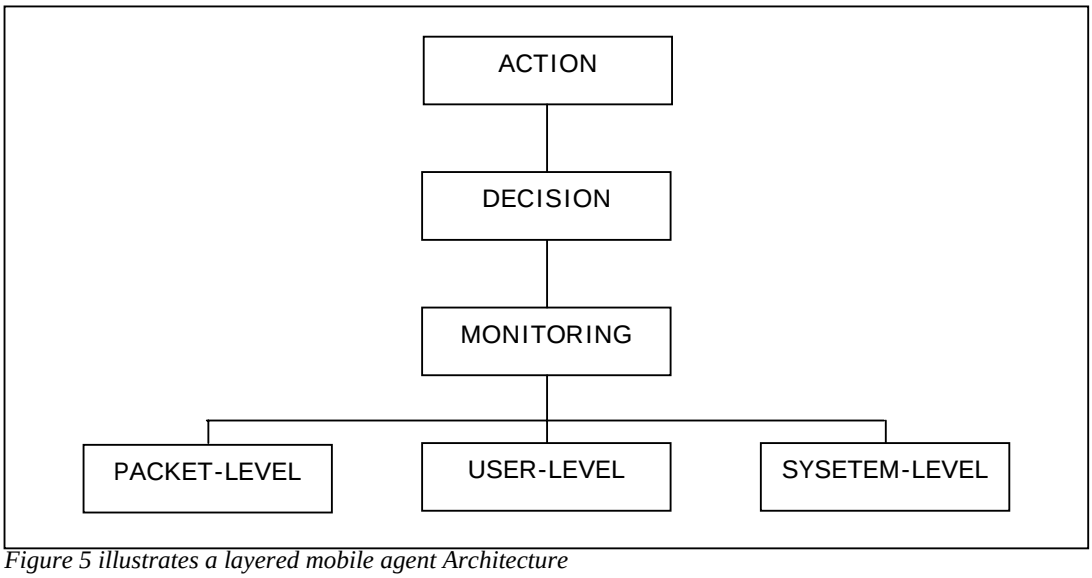

Figure 5 illustrates a layered mobile agent Architecture

DYNAMIC INTRUSION DETECTION HIERARCHICAL ARCHITECTURE (DIDHA)

Sterne, D. et al., (2005), hence came up with a Dynamic intrusion detection hierarchy which is quite capable of spreading onto huge networks by making use of clustering. In figure 6, a dynamic intrusion detection hierarchy is depicted with structures in more that two levels. According to this proposed dynamic intrusion detection hierarchy, all nodes have the responsibilities of performing monitoring (-ie by accumulating counts and statistics), logging, analyzing (packet headers and payloads), reaching to intrusions if there is enough supporting evidence and finally alerting or reporting to cluster heads

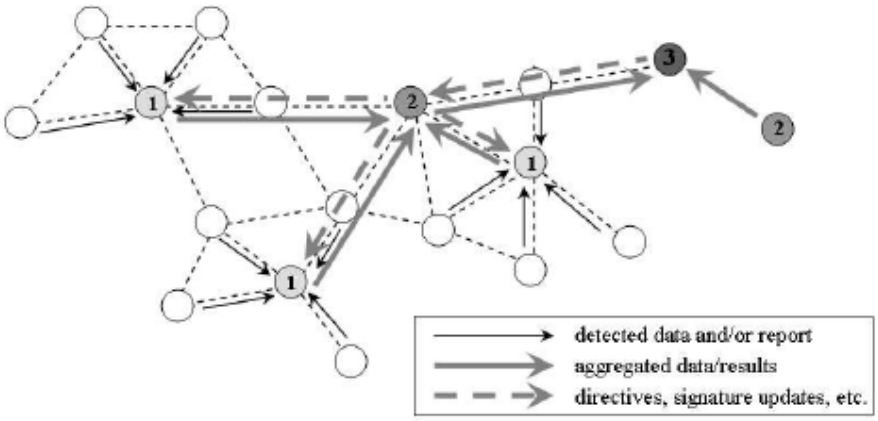

Figure 6 illustrates the Dynamic Intrusion Detection Hierarchy

In addition to report intrusion, cluster heads must be able to carry out

- Integration and data reduction – Hence avoiding conflicting data, fictitious and entered reports.
- Intrusion detection estimations – provided that different attacks will depend upon different sets of detected data, therefore the data held on a single node might not be able identify the attacks.
- Security Administration – According to this DIDHA the apical layers of the hierarchy are responsible for controlling any detection and responding actions of both the clusters and the cluster heads under their supervision.

However, to construct the hierarchy structure, every node uses clustering, which is normally found in Mobile Ad-hoc Networks to build up the trace routes, to then self-implement them into local precincts (known as the first level clusters) and the identify the cluster heads which then make use of clustering to form second-level clusters thus suggesting that the following criteria are respected:

a) Connectivity
b) Proximity
c) Hardening
d) Processing power
e) Storage Capacity
f) Energy remaining and so on

ZONE – BASED INTRUSION DETECTION SYSTEM (ZBIDS)

In a proposal by Sun, B. et al., (2003), an anomaly-based two-level non-overlapping Zone-Based Intrusion Detection System (ZBIDS) can be used by separating the network into non-overlapping, zones. Referring to Figure 7, the nodes can be classified into 2 different groups:

- Intrazone would be independent nodes by a shown in Figure 7 with nodes F, E, I, and J.
- Interzone node would be the nodes that have a physical connection to a different node in a different zone area. Example would be node H, B, C and K as illustrated in Figure 7.

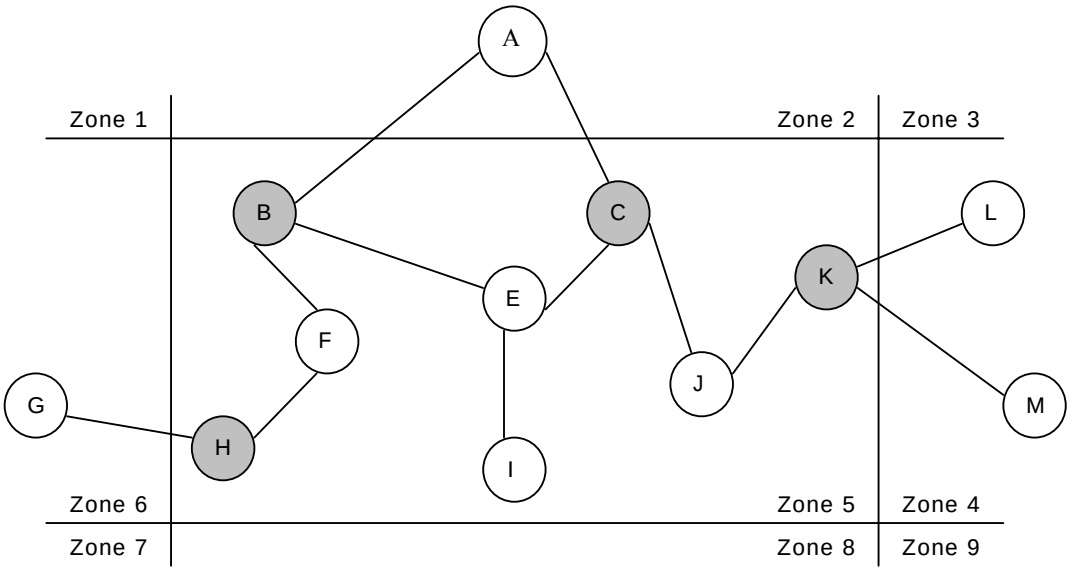

Figure 7 depicting the ZBIDS architecture

Consequently each node has an IDS agent that sits upon and run as illustrated in Figure 8. Same as the IDS agent supported by Zhang and Lee (2003) the data gathering and detection agent are the major agents for collection local data in the instance of system log files and system call activities and then putting the collected data under analysis for any form of intrusion.

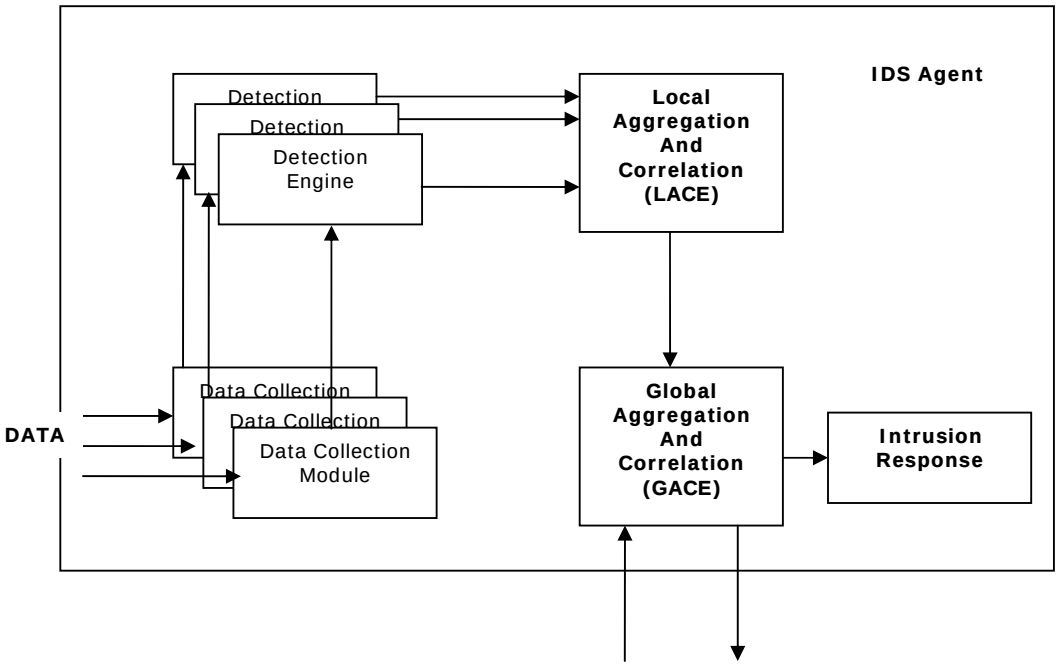

Figure 8 illustrate an IDS agent in ZBIDS

Having had a look at the different intrusion detection system architectures and the way in which they do operate, it has noted that on a wireless mobile network same of the discussed intrusion detection system and response would not stand any chance if implemented future due to the fact that a mobile wireless network is quite exposed due to its features of open medium of communication, corporative algorithms dynamically changing

network topology just to mention a few of them. Therefore at this pointing time, the best IDS, techniques and approach for mobile wireless network would be to adopt the cooperative and distributed IDS referring to figure 2 mentioned earlier.

Having already chosen the architecture for the mobile wireless network, we will now be looking at how it really adapt to the wireless network and how

Data Collection

Referring to figure 2 the first area, the local data collection, would be the area responsible in gathering of real-time data from different sources and on the intrusion detection algorithms these crucial data would include the user's activities as well as the system's activities within the node and also all the communication activities within the range of that node. Yet it is very possible that multiple data collection can be fully operative within one IDS agent in order to contribute to a multi-layer integrated intrusion method discussed later in this report.

Local Detection

The local detection process normally would analyze the collected data from the local data unit to identify or trace out any irregularities on the network knowing that attacks will definitely increase at an alarming rate as more and more network application tends to adopt mobility – i.e. becoming mobile and wireless-hence anomaly detection methods will hence a crucial function which will be looked into further detail later in this report.

Cooperative Detection

With the cooperative detection, any node on the mobile wireless network that identifies on intrusion or an irregularity can therefore individually identify that the mobile network is under intrusion and hence trigger a response to that intrusion. However, if ever happens hat a node indemnify an anomaly on an irregularity of the mobile network with weak evidence, it can hence eventuate a cooperative global intrusion detection guide which normally operate by spreading the intrusion detection status information to the other nodes onto the network. A typical example of distributed intrusion detection would consider the following actions:

Step 1: The node would transmit to the closest nodes on the network an irregularity state request.

Step 2: Then each and every node will then diffuse the state information manifesting an inconsistency to its closest neighbors.

Step 3: Afterwards all the nodes would conclude whether the greater number of received reports identifying this irregularity and of positive, then the outcome would be clear that the network is subject to attacks

Step 4: And finally any node that identifies any inconsistency or irregularity onto the network can hence trigger a response.

So, careful attention should be focused as audit data from different nodes cannot be relied upon because the corrupted nodes can be sending erroneous data. Therefore a wireless mobile network is known to be highly dynamic due to its nature of its nodes which can more in and out of the network. However, since each node is capable of intrusion response and report, it does not build on fixed network topology but simple rely on the preponderance routing codification allowing any particular node to trigger a response.

Intrusion Response

Any intrusion on the mobile network would be treated differently depending obviously on the type of intrusion and also the different network protocols and application in used on the wireless network. An example of this response would be like re-connecting the communication channel between the nodes hence forcing a re-keying to take place or to locate the corrupted nodes and hence re-calculate how to anticipate for the other nodes that have not be compromised. This means that the IDS agent running on the node can inform the end user, who may carry out their own investigation and hence response accordingly with the appropriate actions. The IDS agent can and should normally request every other node to identify themselves to authenticate the nodes as only nodes have been re-validated would be able to reconnect a new communication channel and been identified as being clean and acknowledged leaving the attacked node to be excluded.

IDENTIFYING INCONSISTENCY IN MOBILE WIRELESS NETWORKS

This section of this report will be focusing on how to create an inconsistency model for the mobile wireless network. It is also a fact that the intrusions on different networks layers will differ accordingly with the variety of auditing data in relation to the algorithm model to emphasize and have a better interpretation of this proposal.

Building the Model

The foundation layout for anomaly intrusion detection is based upon the fundamental perceivable features of normal habits that are contrary from that of abnormal actions. According to Corer and Thomas (1991) the use of information – theoretic measures, entropy and conditional entropy, which depicts the behaviors of normal information flows and to use classifications mathematical calculations in cheating that inconsistency model.

On selecting this schematic structure, a few guidelines need to be flowed which are illustrated below;

1) Select or separate audit data so that the normal set of data has really low entropy.
2) Achieve the necessary data transformation according to the entropy measure
3) Calculate classifier using training data
4) Apply that classifier to the test data collected previously
5) Post-process alarms to produce intrusion reports.

Having mentioned the different guidelines for this schematic approach, we now have to consider the attack model which in this report would emphasizes on routing protocols. Following a publication by Venkatraman, L., (2002), attacks performed on the routing protocols normally behave in the 2 following forms:

1) Route logic compromise, this particular attack will normally alter or modify the routing information either externally or internally thus forcing us to analyze different scenarios with misrouting of a pallet to an incorrect node and detecting false message spreading.

2) Traffic pattern distortion: This specific attack would change typical traffic behavior such as pallet dropping, denial-of-service (DOS), pallet having fake source addresses etc.

Given that these attacks are treated and explained briefly separately, they could easily be associated into a single attack or intrusion.

Audit Data

Two local data sources can be baited for inconsistency detection on the wireless network. The first one is making use of the local routing information which enclose cache data entries, traffic statistics and secondly a GPS which will allow us to locate information on the nodes within the locality. It is also assumed that the GPS will not be compromised. However, when collecting and gathering these data, only information gathered locally will be used to avoid using un-trusted data from uses that might have been compromised.

Feature Selection:

An important and crucial milestone in creating a detection model is the feature selection due to the fact that classifiers are being re-adapted as detectors from the available audit data from the nodes. Hence this is carried out initially by, designing a large range of behaviors which is not expected to run on all the nodes. Only a small audit data traces selected from a previously stored audit log would be needed to run on the nodes where a corresponding model is hence built and we note that each different routing protocol come with different scenarios hence making the feature selection to be different.

Classifier

In this report 2 types of classifiers are used. The first one is a decision tree equivalent classifier and the second one being a support vector machine classifier, sum light defined by Joachinis (1999). The decision tree equivalent classifier is a typical conventional classifiers which focuses it search on specific features and the calculate how to classify the data. Whereas the SVM light goes further when it comes to compute the data. It hence represents the data in much higher amplitude, thus allowing the purpose of categorization of data. However the SVM light is much more defined and explicit compared to the decision tree equivalent classifier due to its preferred understanding of the intrinsic composite forms.

Post-Processing:

When it comes to post-processing feature, initially we would have a sensor that will be able capture and analyze each observation. Once this has been implemented, a blue-print of the post-processing can be established to forecast and create intrusion reports. This can be achieved by a set of parameters

1) Choosing a variant "x" and allowing a margin to be "2x+1"
2) Having then mentioned that the zone covered is "2x+1", any inconsistencies going above this defined range will then be classified as being abnormal as the number of inconsistencies in far greater than "x".
3) All the observation should be labeled with high inconsistencies and those without should be clearly identified.
4) The steps 2&3 are to be repeated over the whole zone to be covered
5) Finally do a count of all the zones with high anomalies which can be grouped as in one intrusion report.

We do note that with this detection modes it can lead to deceitful errors and trigger false alarms to start obviously filtering of these alarms would be expected. However, the way that alarms are activated within a short period of time within that window frame, it can hence be grouped in a single intrusion report.

INCONSISTENCIES UPDATE IN ROUTING TABLES

One of the major conditions in intrusion detection system and creating an inconsistency model is low false positive rate according to Zhang & Lee (2003) which is hence computed as the percentage of normal deviations detected as inconsistencies and high true positive rate which devotes the percentage of detected inconsistencies or irregularities which fall beyond the margin zone defined earlier.

The principal task when it comes to mobile ad-hoc network about the routing protocols is to make sure that the corrupted or wrong routing information originating from the compromised node will be propagated to the other nodes on the network.

Typically a routing index would consist of information about the next hop to each destination node together with the amplitude of the next nodes-i.e the number of hops. A logical and appropriate change in the routing index can be caused by nodes being forced to move (physically) onto the network or when network membership is being reassigned to. However for a node the only trustworthy information would be when it comes to its own moment thus altering its own routing appendix. Therefore, we use that information – i.e. both the nodes movement and routing index modification as the substructure of the trace data.

INCONSISTENCIES IN OTHER LAYERS

When it comes to wireless mobile application networks, there are other layers that are to be considered due to its high risk of being compromised is its weak wireless links.

The MAC protocols can hold some indenting characteristics such as total number of nodes requesting the channel, the most requested channels, and average of the requests and can also determine what the least number of requests was. Therefore having a classifier of this trace data would be denoting the normal framework of a request. We can then conclude that an anomaly detection model can be used to calculate from the deviation data. The principle is similar at the mobile application layer and can be used to gather the following aspects: total number of requests, from either a different or same services the nodes that have requested this service.

Numerous attacks breed altered statistical behaviors than normal requests. However, the few enumerated features mentioned above are devised for the statistical study of the gathered requests, therefore it is concluded that the attacks will have large differences that what would expected from normal requests. Such example would be that DOS attacks via resource exhaustion would normally involved huge number of requests in a very short period of time frame and that a DDOS has the enervating reasoning that it comes from numerous nodes.

CONCLUSION

Having explored all the possibilities around we can come to the conclusion that any secure network will be subjected to attacks from outsiders and this will be true in the wireless networks too. Even though that we have mentioned that intrusion detection should work in hand with intrusion prevention techniques to provide more

secure network and that new techniques should be developed and implemented in order to provide more secure wireless network.

Through this report, we have demonstrated that when it comes to wireless mobile networks, the most appropriate intrusion detection to be implemented in a mobile wireless network should be both distributed and cooperative. Since irregularity detection is a crucial aspect in the intrusion detection and response mechanism, trace analysis should be carried out on each node and even though cooperation on the whole network

However, this area is under continuous investigation and striving for a better intrusion detection system and model feasible to securely protect wireless mobile network.

REFERENCES

Albers, P., Camp, O., Percher, O.J., Jouga, B.,and Puttini, M.(2002). *Security in Ad Hoc Networks: A General Intrusion Detection Architecture Enhancing Trust Based Approaches.* Retrieved October 5, 2007, from http://www.rennes.supelec.fr/ren/rd/ssir/publis/wis02_albers_camp_percher_als.pdf

Anantvalee, T. and Wu, J. (2006). *A Survey on Intrusion Detection in Mobile Ad-Hoc Networks*. Retrieved October 2, 2007 from http://www.cse.fau.edu/~jie/research/publications/Publication_files/intrusion06.pdf

Binkley, J. (1996). *Authenticated ad hoc routing at the link layer for mobile systems.* Retrieved September 19, 2007, from http://portal.acm.org/ft_gateway.cfm?id=375455&type=pdf&coll=portal&dl=ACM&CFID=2609539&CFTOKEN=79804387

Brutch, P. and Ko, C. (2003*). Challenges in Intrusion Detection for Wireless Ad-hoc Networks*. Retrieved October 7, 2007, from http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/proceedings/&toc=comp/proceedings/saint-w/2003/1873/00/1873toc.xml&DOI=10.1109/SAINTW.2003.1210188

Cover, T.M. and Thomas, J.A (1991). *Elements of Information Theory*. Wiley, 1991

Huang, Y. and Lee, W. (2003). *A Cooperative Intrusion Detection System for Ad Hoc Networks*. Retrieved October 5, 2007, from http://www.cc.gatech.edu/~wenke/papers/sasn.pdf

Heady, R., Luger, G., Maccabe, A., and Servilla, M.(1990). *Architecture of a network level intrusion detection system.* Retrieved September 10, 2007, from http://www.eurecom.fr/util/publidownload.fr.htm?id=410

Jacobs, S. and Corson, M.S. (1999). *MANET authentication architecture*. Retrieved September 25, 2007, from http://www.sigmobile.org/MC2R/articles/manet_v3n2.pdf

Joachims, T. (1999). *Making large-scale SVM learning practical.* Chapter 11. MIT-Press.

Kachirski, O. and Guha, R. (2003). Effective *Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks.* Retrieved September 22, 2007, from https://www.cs.tcd.ie/publications/tech-reports/reports.05/TCD-CS-2005-49.pdf

Smith, B. R., Murthy, B., and Garcia-Luna-Aceves, J.J. (1997). *Securing distance-vector routing protocols*. Retrieved September 11, 2007, from http://portal.acm.org/citation.cfm?id=523975.830483

Sterne, D., Balasubramanyam, P., Carman, D., Wilson, B., Talpade, R., Ko, C., Balupari, R., Tseng, C.Y., Bowen, T., Levitt, K and Rowe, J. (2005). *A General Cooperative Intrusion Detection Architecture for MANETs.* Retrieved October 1, 2007 from http://seclab.cs.ucdavis.edu/papers/manet_ids.pdf

Sun, B., Wu, K. and Pooch, U.W. (2003). *Alert Aggregation in Mobile Ad Hoc Networks.* Retrieved September 14, 2007, from http://portal.acm.org/ft_gateway.cfm?id=941323&type=pdf&coll=GUIDE&dl=GUIDE&CFID=2659735&CFTOKEN=45841533

Venkatraman, L. (2000). Secured routing protocol for ad-hoc networks. MIT-PRESS.

Zhang, L. and Lee, W. (2003). Intrusion Detection Techniques for Mobile Wireless Networks. Retrieved September 15, 2007, from http://www.cc.gatech.edu/~yian/Zhang_03.pdf

Zhou, L. and Haas, Z.J. (1999). Securing ah hoc networks. Retrieved September 30, 2007, from http://portal.acm.org/ft_gateway.cfm?id=570682&type=pdf&coll=GUIDE&dl=GUIDE,ACM&CFID=38653882&CFTOKEN=62869473

COPYRIGHT

Krishnun Sansurooah ©2006. The author/s assign SCISSEC & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SCISSEC & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.