A Novel Architecture for Intrusion Detection in Mobile Ad hoc Network

Atul Patel
Charotar University of Science & Technology
Changa, India

Ruchi Kansara
Charotar University of Science & Technology
Changa, India

Dr. Paresh Virparia
Sardar Patel University
Vallabh Vidyanagar,
India.

***Abstract*— Today's wireless networks are vulnerable in many ways including illegal use, unauthorized access, denial of service attacks, eavesdropping so called war chalking. These problems are one of the main issues for wider uses of wireless network. On wired network intruder can access by wire but in wireless it has possibilities to access the computer anywhere in neighborhood. However, securing MANETs is highly challenging issue due to their inherent characteristics. Intrusion detection is an important security mechanism, but little effort has been directed towards efficient and effective architectures for Intrusion Detection System in the context of MANETs. We investigate existing Intrusion Detection Architecture design Issues, challenges and proposed a novel architecture based on a conceptual model for an IDS agent that lead to a secure collaboration environment integrating mobile ad hoc network and the wired backbone. In wireless/mobile ad hoc network, the limited power, weak computation capabilities of mobile nodes, and restricted bandwidth of the open media impede the establishment of a secure collaborative environment.**

Keywords- Ad hoc network; Intrusion Detection System; Mobile Network.

I. Introduction

Mobile ad hoc networks are complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organise into arbitrary and temporary, ‘‘adhoc’’ network topologies. They allow people and devices to seamlessly internetwork with no pre-existing communication infrastructure and central administration [1].

Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. The military tactical and other security-sensitive operations are still the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. One main challenge in design of these networks is their vulnerability to security attacks. The goal is to investigate the development of a suite of protocols and algorithm that enables to securely collaborate over mobile ad hoc networks as well as the wired backbone. Collaboration requires secure information sharing and communication among a large number of academic, governmental, and military sites. A series of experiments in key management, malicious intruder identification, and detection of denial of service attacks will be conducted to provide the secure networking.

Ubiquitous access to information anywhere, anyplace, and anytime, will characterize whole new kinds of information systems in the 21st Century. These are being enabled by rapidly emerging wireless communication systems, based on radio and infrared transmission mechanisms, and utilizing such technologies as cellular telephony, personal communication systems, wireless PBXs, and wireless local area networks. These systems have the potential to dramatically change society as workers become “untethered” from their information sources and communication mechanisms. While there is a rich body of knowledge associated with radio system engineering, the needed expertise must build upon this to encompass network management, integration of wireless and wire line networks, system support for mobility, computing system architectures for wireless nodes/base stations/servers. User interface appropriate for small handheld portable devices, and new application that can exploit mobility and location information.

Enormous amounts of data are collected from the network for network based intrusion detection. This poses a great challenge. Raw network traffic needs to be summarized into higher-level events, described by some features, such as connection records before feeding the data to a machine learning algorithm. Selecting relevant features is a crucial activity and requires extensive domain knowledge.

In this paper, we propose the novel conceptual architecture for IDS agent for detecting Intrusions effectively. Section 2 gives the general information regarding Intrusion Detection Systems, Section 3 gives the problems with the current Intrusion Detection Techniques, Section 4 gives the novel conceptual model for intrusion agent and finally we conclude in section 5 and give future directions for this work.

II. Intrusion Detection

The concept behind intrusion detection is a surprisingly simple one: Inspect all network activity (both inbound and outbound) and identify suspicious patterns that could be evidence of a network or system attack. Nowadays, network based computer plays an important role in society. There are many advantages of network: one can easily connect anyone on the network, one can share and use the files, folders, and data, they can also call their loved once on the net. At the same time, there are many disadvantages of it too. One welcomes one's enemy, hackers, criminals. There may be chance of misuse of the data. When an intrusion (defined as "any set of actions that attempt to compromise the integrality, confidentially, or availability of a resource [2]) takes place, intrusion prevention technique, such as encryption and authentication (e.g., using passwords or biometrics), are usually the first line of defense[3]. An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

A. Wireless Vs Wired Intrusion

Wired – Physically attached: Intruder/attacker needs to plug directly into the network

Wireless – Intruder can stay anywhere and intrude unseen

No exact "border" between internal and external network-losing exact classification to insider and outsider attacks

Sometimes people assume that host based systems prevent insider attacks where as network based system invites outsider attacks. We may not agree with this practice, but as soon as you add a Wi-Fi signal, the border of defense becomes unclear and not sharply defined.

The primary assumptions of intrusion detection are: user and program activities are observable, for example via system auditing mechanism; and more importantly, normal and intrusion detection activities have distinct behavior. In the network based IDS, normally, it runs on the gateway of a network packets that go through the network hardware interface.

In misuse detection, the IDS analyze the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS looks for a specific attack that has already been documented. Like a virus detection system, misuse detection software is only as good as the database of attack signatures that it uses to compare packets against. In anomaly detection, the system administrator defines the baseline, or normal, state of the network traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies [4].

III. PROBLEMS OF CURRENT IDS TECHNIQUES

There are two different types of networks - wireless and wired network. There has always been having problem of security, collaboration, management and integration. Thus there is a need of intrusion detection system as there may be chances of misusing of data while communicating between these two. There is a big problem to fix IDS between Wired and Wireless network as the wireless network perhaps may not have fix infrastructure.

There is a big difference between how the data transfer in Wireless Ad-Hoc network and Wired network. There is always some limitation while communicating through wireless Ad-Hoc network. One may face the problem of bandwidth, data may be loss, high cost, slower links etc. Intrusion detection in MANETs, however, is challenging for a number of reasons [12,13,14].

The major limitations with the current Intrusion Detection Systems are[5]

- Noise can severely limit an Intrusion detection systems effectiveness. Bad packets generated from software bugs, corrupt DNS data, and local packets that escaped can create a significantly high false-alarm rate.
- It is not uncommon for the number of real attacks to be far below the false-alarm rate. Real attacks are often so far below the false-alarm rate that they are often missed and ignored.
- Many attacks are geared for specific versions of software that are usually outdated. A constantly changing library of signatures is needed to mitigate threats. Outdated signature databases can leave the IDS vulnerable to new strategies.

A. NIDS Performance Issues

It is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts. Network intrusion detection systems NIDS [6,7,8] gain access to network traffic by connecting to a network hub, network switch configured for port mirroring, or network tap. In an NIDS (figure 1), sensors are located at choke points in the network to be monitored, often in the demilitarized zone (DMZ) or at network borders. Sensors capture all network traffic and analyze the content of individual packets for malicious traffic[9]. An example of an NIDS is Snort.

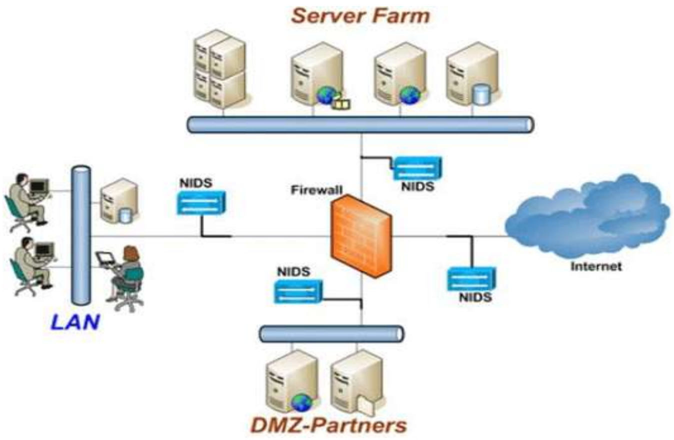

Figure 1. A Network Based IDS

Network Intrusion Detection Systems are usually deployed as a dedicated component on a network segment. There is some debate as to where to place a single NIDS (inside or outside of a firewall), but most agree that multiple NIDS are better. It will then compare captured network data to a file of known malicious signatures. If there is a match, the IDS will log and send an alert according to how it was configured by the network or security administrator[10].

A major difficulty is that true performance statistics are very hard to obtain, especially in a lab. However, a recent test by NSS Labs is probably one of the best[11]. The issue is not how many attacks that an NIDS can detect that is the most important factor (and often the only bench mark used in lab tests), but how effectively the NIDS can pick out one attack in a mass of normal background traffic. It is often not the mass of attacks that an NIDS has problems dealing with, but the proverbial “finding a needle in a haystack”. This becomes especially difficult when SSL (Secure Socket Layer) traffic is involved, because the NIDS cannot read encrypted traffic. It wastes valuable CPU cycles realizing that it can’t do anything with the traffic and then discards it!

A second core performance element to consider is the size of packets. In tests, NIDS vendors usually look at an average packet size of 1024 bytes, however if the packet sizes are smaller, the NIDS will run a lot slower (e.g. consider the negative impact when monitoring a large DNS server).

A third key driver in how fast an NIDS can run is the actual policy that is running on the NIDS. Typically NIDS have hundreds of attack signatures that they are looking for at any given time. The more signatures they are looking for in a stream of data, the longer it will take to look at the next stream. This is more critical for pattern matching based systems than those that utilize protocol analysis.

The nature of mobile computing environment makes it very vulnerable to an adversary's malicious attacks. First of all, the use of wireless links renders the network susceptible to attacks ranging from passive eavesdropping to active interfering. 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 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.

IV. NEW ARCHITECTURE

Though many IDS architecture have been designed for infrastructure-based networks, they are not applicable in Mobile Environment. Motivated by this consideration, we propose the modified architecture based on a conceptual model for an IDS agent proposed by Yongguang Zang and Wenke Lee[3]. The model is extended by introducing two novel ideas, the Data collection is divided in two parts and one Global Data Collection Module is introduced as the outer most layer of the model.

IDS should be both cooperative and distributed to satisfy the need of the wireless Ad-Hoc network. In the proposed architecture, every node in the wireless Ad-Hoc network participate in intrusion detection and response. Each of these nodes is responsible for signaling the intrusion locally and independently. Also this IDS model identifies the black list and white list requests.

The internal of an IDS agent can be fairly complex, but conceptually it can be structured in eight pieces (Figure 2). The data collection module is responsible for gathering local audit trace and activity logs. Next the Identifier will use this data to identify the detection; Notification will take the appropriate action if the intrusion occurs. The Global Data Collection will store all the calls which have been occurred.

A. Data Collection Module

This has been further divided into black list and white list. It gathers all the necessary streams of the data that has been arrive at a time of request. The black list Module stores all the details of the source that may lead to misuse. That is there may be chance of intrusion. Whereas the white list module will store all the details of the most frequently calls and which are authentic. Depending on the intrusion detection algorithms, these useful data streams can include system and user activity within the mobile node. Multiple data collection modules cab consist in one IDS agent to provide multiple audit streams for a multi-layer integrated intrusion detection method.

B. Identifiers

Identifiers can be a local Identifier or Group detection. The local Identifier uses the data from the Data Collection module and identifies whether the intrusion is occurred or not. If yes, then, it sends the signal to the Notification module where it will be proceed. As the days going, there will always been created a newer attacks for the system and to secure a system is not an easy task even more and more devices become wireless so security must be increased accordingly. To establish a new and best security for the mobile Ad-Hoc network is not so easy. So IDS model should be used different statistical and mathematical model to solve the problems.

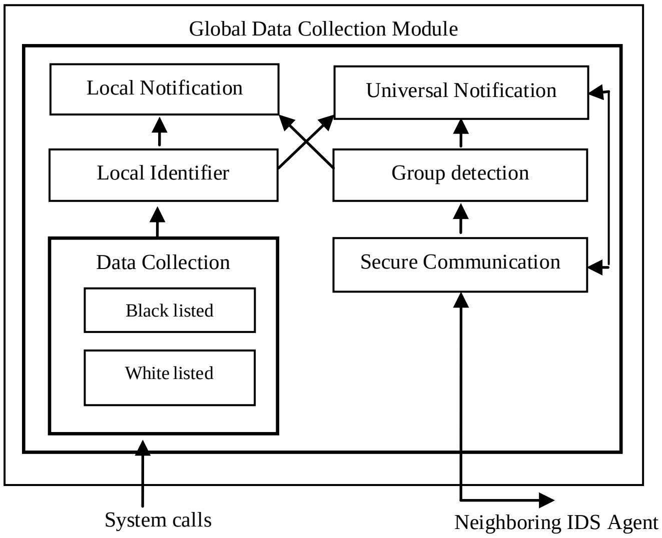

Figure 2. A Conceptual model for IDS Agent

C. Notification

Notification can be local notification or universal notification. According to the type of network the notification has been made to the system. When the system is in the network at that time it will notified universally i.e. it will broadcast the message to its neighbor alongwith the details of the intrusion description and the address of that particular system which initiates the intrusion. In this case, all the system updates their data collection module and put this description in the black list of that module. Also they can refer it in the future to identify the intrusion.

In the Local Notification, it will notify itself that the intrusion has occur then it will terminate the connection with that particular system and update the black list data collection module.

When an intrusion occurs, at that time, it will send the intrusion state information to its neighboring node. Then each node can update the Data Collection module and can initiate appropriate action against that Intruder.

D. Global Data Collection Module

The core and the heart of the new Intrusion detection system as it is centralized and stores all the streams and actions carried out by the system in the network. When any system initiates, the request, at that time, first it will store in this module which can be further used to identify the intrusion by the Data collection module. This module also implements the Cache concepts as it is updated at every interval by itself. The cross checking will be done for every instance of the node to secure the Ad-hoc network and to identify the unauthorized user.

V. CONCLUSION

Here the argument is that any system on the network may find intrusion and their privacy may be exploited. This is especially true for wireless Ad-hoc network. Intrusion detection can help intrusion prevention technique to improve intrusion technique. So that new technique must be developed to solve this problem.

By the continuous investigation, it is shown that how a new model can be developed and how a Global Data Collection module will help IDS Agent to identify the occurrences of the intrusion. Firstly when any system initiates the request, it will be checked in the Global Data Collection Module if it will not found in that it will be put in the Black list and the broad cast of the message is made thus all the neighboring node can know the intrusion point, and can take appropriate action.

At present time, the investigation of the architecture issues is still going on to solve it, implementing it practically and studying its performance issues. In short we are focuses more on the issues that raises in the IDS and try to identify the best solution among all.

In future, the algorithm which supports the model will be developed to identify the Intrusion in cost effective way.

REFERENCES

[1] I.Chlamtac, M. Conti, Jennifer J.-N. Liu., Mobile ad hoc networking: imperatives and challenges, Ad Hoc Networks, 1 (2003), 13-64.

[2] 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.

[3] Wenke Lee and Yongguang Zhan, Intrusion Detection in wireless Ad-Hoc Networks, Technical report, Department of Computer Science, North Carolina State University, Raleigh, NC 27695.

[4] Web site of the Webopedia http://www.webopedia.com/term/i/intrusion_detection_system.html

[5] Anderson, Ross (2001). "Security Engineering: A Guide to Building Dependable Distributed Systems". New York: John Wiley & Sons. pp. 387–388. ISBN 9780471389224.

[6] T. Heberlein, et al. A Network Security Monitor, In Proc. IEEE Symp. Research in Security and Privacy, pp. 296-304, 1990.

[7] B. Mukherjee, L T. Heberlein, and K. N. Levitt, Network Intrusion Detection. IEEE Network, 8(3): 26–41, May/June 1994.

[8] S. R. Snapp, et al, The DIDS (Distributed Intrusion Detection System) prototype. In Proc. Summer USENIX Conference, pp. 227-233, San Antonio, Texas, 8-12 June 1992.

[9] Web site of the Wikipedia – The free encyclopedia : http://en.wikipedia.org/wiki/Intrusion_detection_system

[10] Northcutt, Stephen and Novak, Judy Network Intrusion Detection An Analyst's Handbook Second Edition New Riders 2001. P203-213

[11] Web site of NSS lab : http://www.nss.co.uk/ids/index.htm

[12] P. Brutch and C. Ko, "Challenges in Intrusion Detection for Ad Hoc Networks," IEEE Workshop on Security and Assurance in Ad hoc Networks, Orlando, FL, January 28, 2003.

[13] Konrad Wrona, "Distributed Security: Ad Hoc Networks & Beyond," PAMPAS Workshop, Sept. 16/17 2002, London

[14] Vesa Karpijoki, "Security in Ad Hoc Networks,"

http://citeseer.nj.nec.com/karpijoki01security.html

AUTHORS PROFILE

Atul Patel received Bachelors degree in Science (Electronics), M.C.A. degree from Gujarat University, India. M.Phil. (Computer Science) Degree from Madurai Kamraj University, India. Now he is an Associate Professor and Head, Charotar Institute of Computer Applications – Changa, India. He is pursuing Ph.D. in wireless networks. His main research areas are wireless communication and Network Security.

Ruchi Kansara received B.Sc. Degree from Sardar Patel University, V. V. Nagar. Now she is pursuing MCA programme at Charotar University of Science & Technology, Changa. Her area of research is Wireless networks.

Dr. Paresh Virparia received B.Sc. (Maths), M.C.A. and Ph. D. Degree from Sardar Patel University, V. V. Nagar, India. Now he is a Associate Professor at G. H. Patel PG Department of Computer Science and Technology, Sardar Patel University, India His main research areas are Computer Simulation & Modeling and Networks.