ENHANCED POWER-AWARE HYBRID INTRUSION DETECTION ARCHITECTURE IN AN AD-HOC NETWORK USING MOBILE AGENTS

Jyoti Attri, Suman Kumari

1IT Department, International Institute of Information Technology (I²IT), Hinjawadi, Pune, Maharashtra
2IT Department, DY Patil College of Engineering, Pune, Maharashtra

ABSTRACT

Enhanced Power-Aware Hybrid Intrusion Detection Architecture in an Ad-Hoc Network Using Mobile Agents describes design and implementation of an energy conscious anomaly based co-operative intrusion detection system. This paper addresses the above stated issue by (1) Applying mobile agent technology to minimize the network load, conserving bandwidth and to improve reactivity, (2) Minimize energy consumption of network monitoring nodes by using Back-Propogation Algorithm. This paper presents a new approach to the architecture of IDS in an Ad-Hoc Network using Mobile Agents. By using this architecture, we are able to determine which network events have to be monitored and where they can be monitored.

Keywords: Introduction, Security, Characteristics, Routing Protocols, Networks.

I. INTRODUCTION

Wireless ad hoc networks are autonomous nodes that communicate with each other in a decentralized manner through multi hop radio network. Wireless nodes form a dynamic network topology and communicate with each other directly without wireless access point. Wireless networks are particularly vulnerable to intrusions, as they operate in open medium, and use cooperative strategies for network communication. Wireless transmissions are subject to eavesdropping and signal jamming. Physical security of each node is important to maintain integral security of the entire network. Intrusion detection is one of the key techniques behind protecting a network against intruders. An intrusion detection system tries to detect and alert on attempted intrusions into a system or network, where an intrusion is considered to be any unauthorized or unwanted activity on that system or network. An IDS is a defense system that detects hostile activities in a network and then tries to possibly prevent such activities that may compromise system security. IDS may work on a
host level and network level to detect intrusions. An intrusion detection system (IDS) is the software and hardware installed to allow intrusion detection. The IDS are described through three fundamental components. Information source: It represents the source of information and events to be analyzed by the IDS to look for eventual intrusion[3]. It can be either the network traffic or the system logs. Analysis method: It defines the method used to analyze the events produced by the information source and to decide whether there is intrusion or not. There are basically two approaches:

1. **Misuse detection**: Response to intrusions: this component indicates whether the IDS takes actions gains intrusions (active IDS) or remains passive, it just report the intrusion (passive IDS).

2. **Anomaly detection**: Detection is performed by looking for anomalous behavior and use of the computer system. Anomaly detection assumes that intrusive activity is a subset of anomalous activity; therefore by detecting the latter it is possible to detect the former[3].

![Diagram of intrusion detection and response](image)

**Fig 1: BASIC ARCHITECTURE**

In this scheme every node is participates in intrusion detection and response. Every node is responsible for detecting signs of intrusion locally and independently by monitoring activities such as user and system activities and the communication activities within the radio range. This activity normally occurs at the following two locations:

1. Host – Host based IDS
2. Network – Network based IDS

Finally, many intrusion detection systems incorporate multiple features into a single system. These systems are known as hybrid systems. These hybrid intrusion detection systems having their architecture based on agents which travel throughout the network, provide a comprehensive solution.
A. Host based intrusion detection

Host based intrusion detection system take care of local intrusion detection attempts on each node. The host monitoring module includes user level and system level monitoring modules[4].

B. Network-based intrusion detection

Network based intrusion detection system detects intrusion attempts at network level. The cluster head has packet monitoring agent, decision making agent and action agent to perform network monitoring of packets within the communication range. The modules of the network based intrusion detection system[4].

II. SECURITY

Ad-hoc networks are a new paradigm of wireless communication for mobile hosts. No fixed infrastructure such as base stations as mobile switching. Nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other nodes to relay messages. Node mobility causes frequent changes in topology.

2.1 Security Goals

1) Availability: Ensures survivability despite Denial Of Service (DOS) attacks. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g.: key management service.

2) Confidentiality: Ensures certain information is never disclosed to unauthorized entities.

3) Integrity: Message being transmitted is never corrupted.

4) Authentication: Enables a node to ensure the identity of the peer node it is communicating with. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

5) Non-repudiation Ensures that the origin of a message cannot deny having sent the message.

2.2 Lack of Centralized Management Facility

Ad hoc networks do not have a centralized piece of management machinery such as a name server, which lead to some vulnerable problems. Now let us discuss this problem in a more detailed manner.

First of all, the absence of centralized management machinery makes the detection of attacks a very difficult problem because it is not easy to monitor the traffic in a highly dynamic and large scale ad hoc network. It is rather common in the ad hoc network that benign failures, such as path breakages, transmission impairments and packet dropping, happen frequently. Therefore, malicious failures will be more difficult to detect, especially when adversaries change their attack pattern and their attack target in different periods of time. For each of the victims, because it can only observe the failure that occurs in itself, this short-time.

2.3 Restricted Power Supply

As we all know, due to the mobility of nodes in the ad hoc network, it is common that the 5 nodes in the ad hoc network will reply on battery as their power supply method. While nodes in the
wired network do not need to consider the power supply problem because they can get electric power supply from the outlets, which generally mean that their power supply should be approximately infinite; the nodes in the mobile ad hoc network need to consider the restricted battery power, which will cause several problems. The first problem that may be caused by the restricted power supply is denial of service attacks. Since the adversary knows that the target node is battery restricted, either it can continuously send additional packets to the target and ask it routing those additional packets, or it can induce the target to be trapped in some kind of time-consuming computations. In this way, the battery power of the target node will be exhausted by these meaningless tasks, and thus the target node will be out of service to all the benign service requests since it has run out of power.

2.4 Scalability

Finally, we need to address the scalability problem when we discuss the vulnerabilities in the mobile ad hoc network. Unlike the traditional wired network in that its scale is generally predefined when it is designed and will not change much during the use, the scale of the ad hoc network keeps changing all the time: because of the mobility of the nodes in the mobile ad hoc network, you can hardly predict how many nodes there will be in the network in the future. As a result, the protocols and services that are applied to the ad hoc network such as routing protocol and key management service should be compatible to the continuously changing scale of the ad hoc network, which may range from decades of nodes to hundreds of nodes, or even thousands of nodes. In other words, these protocols and services need to scale.

III. ROUTING PROTOCOLS

Routing protocols are classified into two types based on their Properties.

- Proactive Routing Protocols
- Reactive Routing protocols

3.1 Table Driven Routing Protocols (Proactive)

In proactive or table-driven routing protocols, each node continuously maintains up-to-date routes to every other node in the network. Routing information is periodically transmitted throughout the network in order to maintain routing table consistency. The areas in which they differ are the number of necessary routing-related tables and the methods by which changes in network structure are broadcast. The proactive IJCA Special Issue on “Mobile Ad-hoc Networks” MANETs, 2010 125 protocols are not suitable for larger networks, as they need to maintain node entries for each and every node in the routing table of every node[6].

3.2 On-Demand routing Protocols (Reactive)

With on-demand protocols, if a source node requires a route to the destination for which it does not have route information, it initiates a route discovery process which goes from one node to the other until it reaches to the destination or an intermediate node has a route to the destination. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery usually occurs by flooding the route request packets throughout the network[6].
IV. PROBLEM

Power-Aware Hybrid Intrusion Detection in Wireless Adhoc Networks using Mobile Agents describes design and implementation of an energy conscious anomaly based cooperative intrusion detection system for wireless ad hoc networks using mobile agent technology. The developed system has two subsystems, host based and network based intrusion detection system. IBM’s Aglet is used as the base agent architecture to create mobile agents for intrusion detection task. Three major agent categories used are namely monitoring agent, decision making agent and action agent. Host based intrusion detection system take care of local intrusion detection on each node. The host monitoring agent monitors user level and system level activities for anomaly detection. Network based intrusion detection system takes care of cooperative intrusion detection at network level. The cluster heads are identified by two techniques based on i) connectivity index ii) power aware selection algorithm. The first method considers number of reachable nodes is the basis for cluster head selection. The node with highest connectivity is selected as cluster head. In second method power level of the nodes is considered for cluster head selection in order to minimize energy consumption.

The mobile agents are used to detect attacks on the network level. The mobile agent itself is the target of the attackers.

V. SOLUTION

As the problem showing that mobile agents are also the target of the attackers. This problem is only solved by using one of the best learning algorithm (BACK PROPAGATION) to detect and prevent multiple attacks.
VI. PROPOSED WORK

A. Proposed Architecture
B. Characteristics

Our proposed IDS architecture has several key properties distinguishing it from other IDS architectures:

1) Seamless Security Level Adjustment

In general, various application environments have different security requirements for their underlying communication networks. MANETs, for example, are required to be protected with higher security level when they are deployed in hostile and harsh environment (i.e. military applications) where network’s availability and security are the first things to consider. On the other hand, the requirement of communication security in civilian applications is comparatively low. In some cases, it is desirable that security level of MANETs provided by IDSs should be adjusted elastically and seamlessly corresponding to application scenario transformation. For instance, one military group is carrying out a rescue operation in the rear area of battlefield that is a comparatively non-hostile environment. In this case, MANET is protected by IDS only with ordinary security level. At this moment, if this group is dispatched to the battlefront for an emergency mission, the IDS should be configured to provide higher security level.

2) Attack tolerance

In addition to protecting communication networks, IDS should defend itself against attacks. However, current IDSs in MANETs do not address this issue effectively: hierarchical IDS architectures possess the SPF security flaw, and flat IDS architectures address this problem at the cost of complex cooperative mechanisms leading to depletion of resources. Our proposed architecture solves this problem from a new aspect: rangers keep roaming in the network, and their non-predictive mobility will cloak them from attackers’ sniffing or orientation. Therefore, it is reasonable to believe that rangers could avoid attacks since it is difficult for attackers to capture (or find) them. Furthermore, rangers are designed in a flexible and modular manner so that each individual ranger might use different ID algorithms when it was dispatched. This is helpful to avoid the following situation: in a uniform IDS agent configuration environment where all IDS agents perform the same ID algorithms, an adversary who is able to find a way to avoid detection at one agent, will exist in the network without being detected by other agents. Hence, in our architecture, even if one ranger is compromised, other surviving rangers will inform each other to isolate the compromised ranger and exclude it. More importantly, the remaining rangers will likely detect the intruder and gather knowledge of the detection schemes which have been compromised.

VII. CONCLUSION

In this paper we have proposed a new architecture that use the concept of Power-Aware Hybrid Intrusion Detection Architecture and learning algorithm to provide better detection and prevent the MOBILE AGENTS from the the attacks of Attackers. They learn from their experiences and provide better detection.

VIII. FUTURE WORK

Some Other learning algorithms can also be used for better performance of an architecture in combination with Power-Aware Hybrid Intrusion Detection Architecture that provides better result.
IX. REFERENCES


3. Ranger, a Novel Intrusion Detection System Architecture for Mobile Ad Hoc Networks, Yinhua Guo Institute for Telecommunications Research University of South Australia Adelaide, Australia Yinhua.Guo@postgrads.unisa.edu.au, Steven Gordon Institute for Telecommunications Research University of South Australia Adelaide, Australia Steven.Gordon@unisa.edu.au

4. Power-Aware Hybrid Intrusion Detection in Wireless Adhoc Networks using Mobile Agents Praveen Kumar Madala PG Scholar, Dept of CSE Saveetha Engineering College, Chennai, Tamil Nadu, India


8. Security Issues in Mobile Ad Hoc Networks - A Survey Wenjia Li and Anupam Joshi Department of Computer Science and Electrical Engineering University of Maryland, Baltimore County.


