CHAPTER 5

MOBILE AGENT FRAMEWORK FOR NETWORK INTRUSION DETECTION SYSTEM

5.1 INTRODUCTION

Wireless computing system is a type of parallel and distributed system consisting of a collection of interconnected computers that are dynamically provisioned and presented as one or more unified computing resources based on service level agreements established through negotiation between the service provider and the user. In a wireless environment as the systems are distributed there is a greater chance of exploiting attacks by the intruders. Intruders are those who use the services without any authorization and also misuse the privileges. Intrusion detection is the process of detecting the individual who misuses the privileges assigned to them and also access the data or services of legitimate users without any authorization. The intrusion detection system was designed to detect the intruders trying to exploit attacks in the network. In this proposed intrusion detection system, a mobile agent is used to detect the attacks that are being exploited by the intruders.

An Intrusion Detection System (IDS) monitors network traffic for suspicious activity and alerts the system or network administrator. In some cases, the IDS may also respond to anomalous or malicious traffic by taking actions such as blocking the user or source IP address from accessing the network. The goal of the IDS is to detect suspicious traffic. Several types of IDS are available for performing the detection in different ways. There are
network based (Mell et al 2000) and host based intrusion detection systems.

Network based IDS and host based IDS detects based on specific signatures of known threats similar to the way antivirus software detects and protects against malware. Here network based IDS and host based IDS detect based on comparing traffic patterns against a baseline and looks out for anomalies. Network based IDS and Host based IDS simply monitor and alerts and perform an action or actions in response to a detected threat.

An attack against a wireless computing system can be silent for network-based IDS (Vieira et al 2010) deployed in its environment, because node communication is usually encrypted. Attacks can also be invisible to host-based IDS, because specific attacks don’t necessarily leave traces in the nodes operating system, where the host -based IDS resides. In this way, traditional IDS can’t appropriately identify suspicious attacks in the wireless environment.

The mobile agent is an agent having the capability of moving from one host to another. It interacts with other nodes to collect the data. The advantages of mobile agent technology in a heterogeneous environment are reducing the network overload, overcoming network latency, robustness and fault tolerance. The mobile agent technology (Jansen 2002) has been shown to be very suitable to solve the intrusion detection in a distributed environment. The proposed system employs the mobile agent technology to detect the known and unknown attacks exploited by the attacker.

This chapter presents a new intrusion detection framework using mobile agent, to detect misuse detection and anomaly detection. Moreover, it uses the mobile agent dynamically with alert agent techniques in order to reduce the false positive rate in this mechanism. This chapter is organized as follows. Section 5.2 describes the need of mobile agents. Section 5.3 describes the system architecture of mobile agent framework for IDS. Section
5.4 describes the procedure of intrusion detection mechanism. In Section 5.5, the performance of the proposed procedure is analyzed and compared with the existing distributed procedures. Section 5.6 describes the implementation discussion and results. Finally, Section 5.7 contains the concluding remarks.

5.2 WHY MOBILE AGENT?

The recent expectations of the research community from a mobile agent are more realistic. A decade after the introduction of mobile agents, it is now clear that mobile agent is best suited for remote information retrieval. Considering the nature of mobile computing where computing hosts are away from each other and in such scenarios if we want to know what is happening at the remote host, use of a mobile agent become unavoidable. Therefore detection of the presence of rogue access points in wired, wireless or hybrid (wired and wireless combined) type of network is a suitable case for the use of mobile agent.

Software agents can be treated as a mobile agent (Jansen et al 1999), as they are able to migrate from one computer to another computer. Mobile agents are very powerful programs, which can act even in the absence of the machine that initiated them. After completion of their assigned tasks, the mobile agents return to the host machine to report the result or simply terminate. The advantages (Jansen 2002) of using mobile agents in IDS are listed below:
- Operates in heterogeneous environments
- Robust & Fault tolerant
- Overcomes network latency

5.3 SYSTEM ARCHITECTURE

The Intrusion detection system for this environment is proposed based on the mobile agent, which uses the data mining technique to detect the intrusions in the wireless environment. Figure 5.1 contains various mobile agents for collecting and analyzing the data in the wireless environment. There are different agents used for detecting intrusions namely Collector agent, Misuse detection agent, Anomaly detection agent, Classifier agent and Alert agent. These agents collect and analyze the data gathered from the wireless environment to detect the attacks exploited by the intruders.

5.3.1 Collector Agent

The collector agent is the first agent to work in the system, since it is the one that is connected to the network. It collects the data from the wireless environment and stores it in the centralized database. From this, the collector agent gives the control to the misuse detection agent. The collector agent collects the information related to the users and its processes. The following set of characteristics about the user behavior is collected. i) Number of processes started by user ii) User login host iii) User session time iv) time of start of user session. The agent in this architecture is initiated on a timely basis to record user activity and program operation related information from different hosts in the network. The collector agent in this architecture gathers user and process related information and passes the collected information to the misuse detection agent for further processing.
5.3.2 Misuse Detection Agent

Misuse detection systems try to identify the known bad performance. This means that these systems unlike virus detection systems
can detect many or all known attack patterns. The misuse detection agent analyzes the collected data and detects the known attacks by checking the similarities between the collected data with the data available in the centralized database; if the collected data matches with the data available in the centralized database then it reports the attack as pattern matching attack with the help of alert agent.

### 5.3.3 Anomaly Detection Agent

The anomaly detection agent is used to detect new or unknown attacks by using the classification techniques. The anomaly detection agent collects the data from the misuse detection agent and analyzes it to detect the unknown attacks. If the collected data is not matching with the data available in the centralized database, the misuse detection agent feeds the collected data to the anomaly detection agent. The anomaly detection agent receives the data from the misuse detection agent and analyses the collected data based on the logic defined for the attacks. The logic is defined for the attacks such as Ping of Death, Land, Teardrop, TCP flooding. If the collected data violates or exceeds the constraints defined in the logic then the data is detected as a new or unknown attack and the detected new attack is updated into the centralized database. It feeds the data to the classifier agent to detect the new attack.

In anomaly detection, the attacks such as ping of death, tear drop, and land are detected based on the conditions. Ping of death attack is detected if the packet size exceeds the limit value that is calculated based on the condition defined in the function. The land attack is detected based on the source IP and destination IP. If the source IP and destination IP are equal then the attack is reported to alert agent. The tear drop attack is detected based on the special characters; if the message consists of any special characters then it is reported as the tear drop attack.
5.3.4 Classifier Agent

The classifier agent is used to detect new attacks. It classifies the data based on the dataset available in the centralized database. If the incoming data is detected as an attack, then it reports this to the anomaly detection agent, which in turn reports to the alert agent about the attack. It also updates the detected attack in the centralized database.

5.3.5 Alert Agent

The alert agent is used to alert the system if any intrusion occurs in the network. It alerts the system based on the output of the misuse and anomaly detection agent. An alert agent receives alerts generated from misuse and anomaly detection agent. The alert agent sends these alerts to an IDS console that can be used by the security administrator to view alerts generated from the IDS. The alert agent is also responsible for preventing multiple alerts from being generated. The alert agent also stores the information gathered from a misuse and anomaly detection agent for further analysis.

5.4 PROCEDURE OF INTRUSION DETECTION MECHANISM

JADE (Java Agent Development Framework) is a software framework which is used to implement the mobile agents for the proposed intrusion detection system. The collector agent is assigned a task to collect the data from the wireless environment and stores it as a file. The file is then forwarded to the misuse detection agent, which analyses the data by matching the collected data with the attacks available in the centralized database. If the data is similar to the patterns in the database then it reports to the alert agent. If the data are not matched with the patterns in the database then the classifier agent is used to classify the data based on the dataset and then it reports to the
alert agent and updates the database about the attack. The alert agent alerts the system based on the outcome of the misuse and anomaly detection agents.

5.4.1 Agent Procedure

Step1 : The threshold value is assigned by the user.

Step2 : Based on the threshold value the data received from the misuse detection agent is compared with the dataset available in the centralized database.

Step3 : If the compared value exceeds the threshold value then it is detected as an attack and reports this to the anomaly detection agent.

Step4 : The detected attack is updated in the centralized database.

Step5 : The anomaly detection agent reports to the alert agent.

Step6 : An alert is raised by the alert agent about the attack.

5.4.2 Procedure to Detect Ping of Death Attack

A Ping of Death attack is simply sending an IP datagram. If the size of packet exceeds the standard limit based on condition then the attack report is generated. Figure 5.2 & Figure 5.3 displayed the snap shot of ping of death and ping of death attack report.

Step1 : Get the packet size of the data sent from one system to another system.

Step2 : The temporary value is assigned to the variable named “inc”.

Step3 : The limit value is calculated based on the condition

\[ Lmt = 2^{\text{inc}} \]
Step 4: The packet size is compared with the limit.

Step 5: The stored agent procedure is called if the packet size exceeds the limit.

Step 6: The stored agent procedure then reports this attack as ping of death attack.

Figure 5.2 Snapshot-Ping of Death Attack

Figure 5.3 Ping of Death Attack Intrusion Detection Report
5.4.3 Procedure to Detect Land Attack

A Land attack involves IP packets where the source and destination address are set to address the same device. If the sender IP address and destination IP address are same then the attack is generated. Figure 5.4 & Figure 5.5 displayed the snapshot of land attack and land attack report.

**Step1** : Get the message details such as source IP and destination IP.

**Step2** : Check whether the source IP and destination IP are the same using the condition If (nodeIP.equals (IreceiverP))

**Step3** : The stored procedure is called if the source IP and destination IP is equal.

**Step4** : The stored agent procedure then reports this attack as land attack.

![Figure 5.4 Snapshot- Land Attack](image-url)
5.4.4 Procedure to Detect the Tear Drop Attack

In Tear drop attack the packets are corrupted or overlapped on each other when the packets are sent from one system to another system. The special characters are used in the message to denote the packets are corrupted. Figure 5.6 & Figure 5.7 displayed the snap shot of tear drop attack and tear drop attack report.

**Step 1:** Get the message sent from the source system.

**Step 2:** The special characters are defined in the function.

**Step 3:** Check the message character by character for special characters using the condition if (msg.contains(splchar.get(i).toString()))

**Step 4:** If the condition is true then it calls the stored procedure for the tear drop attack. The stored agent procedure is called if the condition is true.

**Step 5:** The stored procedure then reports this attack as tear drop attack.
5.4.5 Procedure to Detect Known Attack

In this procedure it checks the similarity between the data and dataset available in the database. If the data is similar with the data base then it report as a known attack.
Step 1: Get the message and fetch the details such as source IP and destination IP, number of bytes and packet size.

Step 2: Check the collected data against the data available in the centralized database.

Step 3: The stored agent procedure is called if the collected data matches with the data in the centralized data base.

Step 4: If the result is true the attack is reported as a pattern matching attack.

5.5 PERFORMANCE ANALYSIS

To analyze the strength of the enhanced structure, this chapter designs an experiment to hold back some kinds of attack activities with two different systems. One is the improved intrusion detection system based on agent, and the other is a general Rule-based intrusion detection system. Then, the chapter reaches a conclusion by analyzing and comparing the result with the test result. In this system, agents can communicate with each other using UDP and TCP. Communication between agents is very essential. If the problem occurs in between two agents then the entire IDS is in a sticky situation.

A simple model to evaluate the performance of the TCP is an extension of the packet-loss model. The losses in the internet are supposed to be independent and they are often rushed and correlated (Fayed et al 2010). Therefore, new models are needed to capture the impact of random correlated losses on the TCP performance. TCP detects losses in two ways: (i) Retransmission Time Outs (RTOs) and (ii) triple-duplicate ACKs.
5.5.1 RTT

Transmitting a TCP segment depending upon the modulation and coding schemes used on the radio interface is done using the “stop and wait” protocol. The number of retransmissions required to deliver the TCP segment is a random variable due to varying radio channel conditions (Bellamy 2000). The time needed to transmit an error free TCP segment (Ibraheem et al 2010) is given in equation (5.1),

\[ RTT = \frac{\sum_{i=1}^{n_s} NTTI(i)}{s_N} T_j + RTT_{\text{wired}} = RTT_{\text{wireless}} + RTT_{\text{wired}} \]  \tag{5.1}

where,

\[ N_s = \frac{\sum_{i=1}^{n_s} NTTI(i)}{n_s} \]  \text{is the number of transmissions of a TCP segment;}

\begin{itemize}
  \item \( n_s \) (variable) is the number of TTI needed to transmit a TCP segment when no errors occur on the radio interface;
  \item \( NTTI_{(i)} \) is the number of transmissions of TTI due to HARQ;
  \item \( T_j \) is the transmission time of a segment on the radio interface.
\end{itemize}

5.5.2 Number of Transmissions of Packets

Since in each file, packet call or TCP segment is transmitted over a certain number of Trail Traces Identifier (TTIs), the use of scheduling on a shared channel makes the errors on each TTI independent (the successive TTIs are allocated to various users), and the number of retransmissions of each TTI data independent of the other TTIs (Stallings 2009). A few of the general network parameters that can be monitored are (Zhang & Lee 2000) and (Dahill et al 2001).
5.5.3 Forward Percentage (FP)

FP computes the ratio of actually forwarded packets to the packets that are transmitted from the sender to the intermediate node and that intermediate node should forward. The FP ratio is specified in equation (5.2),

$$\text{FP}_m = \frac{\text{Packets actually forwarded}}{\text{Packets to be forwarded}}$$  \hspace{1cm} (5.2)

FP determines the ratio of actually forwarded packets to the packets that are transmitted from M to m and that m should forward. If the denominator is not zero and $\text{FP}_i = 0$, the attack is detected as unconditional packet dropping and m is identified as the attacker. Throughput performance increases network performance and packet delivery ratio and minimizes packet delay. It is the ratio of data packets delivered to the destination to those generated by the sources. It is calculated by dividing the number of packets received by the destination by the number of packets originated from the source.

Finally, evaluation of the performance of two experiments using Detection Rate (DR), False Positive Rate (FP) and accuracy is done according to the formulae specified in the equation (5.3), (DU and Lin 2005), (Heinzelman et al 1999) and (Heinzelman et al 2000).

$$\text{Detection Rate} = \frac{\text{Number of Detected Attacks}}{\text{Number of Attacks}} \times 100\%$$  \hspace{1cm} (5.3)

5.5.4 Attack Detection Rate (ADR)

It is the ratio of the total number of attacks detected by the system to the total number of attacks present in the dataset. False positive rate is specified in the equation (5.4),
\[
\text{False Positive Rate} = \frac{\text{Number of misclassified connections}}{\text{Number of normal connections}} \times 100\% \quad (5.4)
\]

5.5.5 **False Alarm Rate (FAR)**

It is the ratio of the total number of misclassified instances to the total number of normal instances discussed in the equation (5.5).

\[
\text{Accuracy} = \frac{\text{Number of correct classified connections}}{\text{Number of connections}} \times 100\% \quad (5.5)
\]

To test the validity of the improved system, this study designs an experiment to hold back some kind of attack activities with two different systems. One is the improved intrusion detection system based on Agent and the other is a general Rule-based intrusion detection system. Then, it concludes by analyzing and comparing with the test result.

5.6 **IMPLEMENTATION DISCUSSION AND RESULTS**

The IDS for a wireless computing environment integrated with the mobile agent for detecting known and unknown attacks is proposed. All the mobile agents are configured in order to perform the operation of collecting data from the wireless environment. This data is analyzed by the misuse detection agent. The misuse detection agent detection checks whether the data collected matches with the attack dataset available in the centralized database. If any collected data matches then the misuse detection agent informs the alert agent to alert the system about the intrusion. On the other hand, if the collected data does not match with the dataset, then the collected data is analyzed by the anomaly detection agent, which uses a classifier to detect the unknown or new attacks. The final result is such that all the known and unknown or new attacks are detected by the proposed architecture.
The standard network intrusion dataset involved is commonly used in network security research for training and evaluating IDSs. Attacks in the location of information can be divided into five groups namely Denial of Service (DOS), Remote to User (R2L), User to Root (U2R), Probing (Probe) and Normal (Li et al 2009). DoS attacks are performed on a host by using up its resources so that it will not be able to provide network service to the legitimate users. R2L attacks are conducted by sending packets to a targeted machine in a computer network to gain access as if the intruders own an account in the targeted machine.

R2L attacks can be performed in many forms. It takes advantage of weakly configured security features, perform buffer overflow attacks and guess or capture password of hosts in computer networks. For U2R attacks, a local user may exploit flaws in poorly designed systems so that root level privileges can be obtained. Probing normally precedes an actual access or DoS attack (Srinivasan et al 2005).

**DOS**: (BackSide, Ground, Neptune, Shell, Smurf, Slant Crash, Processor Table, UserDataGram Protocol, Mailbomb, Apache2)

**R2L**: (File-Transfer, Protocol Write, Password Guessing, Image map, Multihop, Email Master, Mails Sending Block Messages, Worm Messages, Send Number of Messages Protocol, Named Data)
U2R : (Buffer Overloading, Load Section, Perl Model, Source Kit, Xname, Protocol Server, Hypertext Transfer Protocol Channel, Structure Query Language Attacking)

PROBING : (Internet Protocol Cleaning, Network Mapping, Port Cleaning, Mscan)

**Intrusion detection attack result**

Figure 5.8 is a snapshot of the comparison between the number of attacks detected among the four main types of attacks namely DOS, R2L, U2R and Probing attack.

![Intrusion Detection Attack Chart](image)

**Figure 5.8 Intrusion Detection Attacks Comparison Chart**

Table 5.1 showed the summary report of various intrusion detection attacks. The client data is analyzed to check for any attack by using the misuse detection agent. If the misuse detection agent finds any match with the attacks defined in the centralized database then the alert agent alerts the system by sending a message.
5.7 SUMMARY

The IDS for wireless computing makes the mobile agent to identify well-known and anonymous attacks. The results produced show that the proposed model professionally classifies the unpredictability profile from the normal profile as opposed by the centralized controller. Additions of new hosts are not a problem for this architecture because the architecture makes the IDS scalable. Communication with the server cannot overload parts of the network because of the use of mobile agent. The proposed IDS does not contain platform components. The IDS for wireless networks is proposed which uses the mobile agent technology to detect known and new or unknown attacks. Due to the distributed nature of wireless networks, it is an easy target for intruders to exploit the attack, hence security is a major issue.
To overcome the security issues in the wireless networks, the intrusion detection system is deployed. Therefore, mobile agents are used to detect the known and new or unknown attacks exploited by the intruders. Thus the attacks are detected by the mobile agents and the attacks are updated in the centralized database and the wireless network environment is alerted about the intrusion. The final result of the proposed architecture is that the known and unknown or new attacks are detected by the mobile agent technology.