CHAPTER 3

SYSTEM OVERVIEW

3.1 INTRODUCTION

Efficient and reliable intrusion detection system with a fault tolerance method is useful for wired and wireless networks. In addition, a number of researches have been attempted in intrusion detection and fault tolerance techniques, but none of them have dealt completely with a fault tolerant system. The autonomous agent presents many challenging research issues in intrusion detection systems. With the help of agent technology, this work puts forward a robust system for an automatic detecting intrusion detection system. A mobile agent is regarded as an active entity that represents a user in a computer network. When interposed into the network, for applications, it autonomously moves from one node to another to perform a task given by its owner. It promises to offer a unified and scalable framework for such applications in widely distributed heterogeneous open networks particularly intrusion detection.

Cluster head and mobile agent are critical pre-processing activities required for the anomaly intrusion detection system. The cluster head and mobile agent present in every network collect the information from its hosts and using a distributed mobile agent checks the anomalies. If the network is too large, checking the anomalies and detecting misuses leads to high detection rates and an increase in network traffic. As this is a centralized model, there exist issues with respect to storage capacity. This has led to the
development of a new intrusion detection system to tackle the above challenges.

This system encompasses various factors such as cluster head formation, creation of host agent, net agent, mobile agent, replication agent and decision making agent. Hence, this thesis aims at presenting an adaptive fault tolerant mobile agent based intrusion detection system. The thesis also discusses about the cluster head namely the mobile agent server, mobile service agent, decision making agent, fault tolerance problems and presents their solution in the following chapters. In the aspect of intrusion detection system using mobile agents, it is clear that the various issues to be dealt with are dynamic travel plan, hybrid intrusion, fault tolerant node as well as the fault tolerant mobile agent.

This concept motivated the exploration of the research work in this direction. Hence in this research work, a multifaceted mobile agent system that provides an efficient dynamic travel plan, hybrid intrusion and fault tolerance support. This multifaceted mobile agent system to reduce the network bandwidth usage by moving data analysis computation to the location of the intrusion data and maximize the fault tolerance at two levels in the entire architecture is proposed.

This chapter is organized into three sections that describe the three layers of the proposed architecture. Layer1 gives a global view of the proposed system for the formation of various nodes and creation of a small network in the form of a cluster. An overview of cluster formation is presented in the first layer. In distributed intrusion detection procedure, the clusters are created to divide the network into commodious network suitable for conventions. Each node in the entire cluster network connects with the cluster head namely the Mobile Agent Server (MAS). In layer 1, an overview of the host agent and net agent is briefly introduced.
Layer 2 comprises of mobile agents and their services. This section describes the mobile agent that will be helpful to understand the related techniques proposed in the subsequent chapters. Layer 3 comprises of decision-making and replication agents. It discusses the characteristics of the databases used for evaluation and fault tolerance.

### 3.2 INTRUSION DETECTION SYSTEM

Intrusion detection system can be divided into the following subtasks.

- **Cluster Formation:** Clusters are created to split the network into convenient units for a well-organized structure, easy monitoring of nodes and short procedures for the network.

- **Mobile Agent Server:** In the multi-region environment considered for this work, each region is assigned to a dedicated server referred to as the Mobile Agent Server (MAS).

- **Mobile Service Agent:** Multiple mobile agents are created in order to deploy them in parallel if the agents are to be operated in a multi-region environment. The components used by the agent service center in order to perform these functions are task allocator, itinerary planner, monitoring, and...
Cluster Formation

A mobile network can be organized into a number of clusters. Every node must be a member of at least one cluster. To form a cluster, nodes in the network calculate a hash value based on the parameters namely computational power, power level and a random number. The nodes then broadcast these hash values. Based on these hash values, the centre of a
cluster is computed by using standard election algorithm and this is designated as the cluster head. The cluster head is the one with highest value. The nodes whose hash values are closest to that of the clusters head are then assigned to this cluster. The ordering of the nodes in the cluster is done based on the score. This process is repeated until the cluster head does not significantly change.

3.2.2 Mobile Agent Server

Each node in the cluster has to be connected with the mobile agent server. Mobile agent server acts as the head of the entire network. In MAS, the agent can travel from one node to a different node within a network and perform the hybrid intrusion detection system task i.e., host level and network level intrusion detection concurrently and independently in different processes over the distributed systems. Hence, the entire agent has equal amount of information and bear equal responsibility to take the final decision.

The responsibility of the mobile agent server is to perform host agent and network agent activities. The role of the host agent is to observe the individuality of a single host and gather information about its nodes. The role of the net agent is to detect network intrusions. It is installed at the entrance of the network or on the server. If the host agent or net agent detects activities such as suspicious connections, failed login attempts or modification of system sensitive file from suspicious users, then the host agent or net agent sends ID events related to such behavior of the host to the mobile agent server. The misuse detection agent is used to detect the known attacks in the network. The anomaly detection agent is used to detect the new or unknown attacks. If suspicious activities are found, then the mobile agent gives an alert signal to the mobile agent server.
The server maintains a member list which is used for storing information about each node. It not only manages its own cluster, but also communicates with other clusters for cooperative detection and response. It maintains information about every member node and neighboring clusters, which is useful for network-wide communication. The cluster management responsibility is circulated among the capable members of the cluster for load balancing and fault tolerance. It must be fair and secure. The proposed clustering algorithm can be related with the intrusion detection process as partial analysis of the incoming traffic is done at the head node and rest of the analysis is done at the intermediary or destination member nodes.

3.2.3 Mobile Service Agent

Agent based information retrieval is one of the services provided by the mobile service agent. The mobile service agent is responsible for performing the task assigned to it. The components used by the agent service center in order to perform these functions are task allocator, monitoring agent, travel planner and mobile agent dispatcher and collector. Task allocator focuses mainly on efficient coding of the mobile agent. Travel planner makes use of one of the two possible travel plans, namely static and dynamic. For a static travel plan, it is the responsibility of the mobile service agent to identify the nodes from which it tends to retrieve the related information.

This process must be done before the start of migration. In case of a dynamic travel plan, the mobile service agent initially requests the monitoring agent residing at the centralized server for selecting the next optimal node to visit. Every node in the cluster sends its willingness to become the cluster head by participating in the selection procedure. This information is sent to the current cluster head. The cluster head sends this information to the centralized database through the mobile service agent.
3.2.4 Centralized Administrative Server

The centralized server monitors the movement of the mobile agent globally, in the absence of MAS. The services of the common server are centralized to all the nodes in the entire network, whereas that of MAS is distributed to the nodes of a particular region. The foremost services like failure detection and recovery, location update, decision making and information sharing will be done globally. Agent execution environment is the place where the mobile agents are executed. At the time of execution, a mobile agent server may get blocked and result in a state from which it is not able to continue its execution and this state are defined as a mobile agent failure. This failure occurs as a result of link failure, node failure or application failure. In a mobile agent system, the failure is tolerated by replication and decision making agent approaches.

The fault detection and recovery layer contains the Decision-making Agent (DA), Replication Agent (RA) and Profile Database (PRDB). DA is responsible for the analysis of the information collected by MAs and to control and coordinate with every Host Agent and Net Agent in this system. RA is responsible for the organization of the group of replication agents, adding or removing an agent from a group. PRDB is the database of profiles. It stores the information related to the standard behavior of each agent and each node of the network. All the information is sent to the server.

3.3 DATABASES FOR EXPERIMENTS

This thesis is intended to handle various data like detecting number of attacks, number of detected attacks and corrected attacks. The data are collected from various benchmark sources as given below.
✓ Proposed cluster formation with mobile agent

- Data sets have been gathered from the 2011 Research Article Cluster based statistical anomaly intrusion detection for varied attack intensities

- Data sets have been gathered from the 2006 research article Cluster based Intrusion Detection (CBID) Architecture for Mobile AdHoc Networks by AusCERT2006 R&D Stream.

✓ Autonomous and intelligent agent approach

- Data sets have been taken from the Traditional Distributed Intrusion Detection System 2004 (TDIDS).

✓ Distributed mobile agent

- Intrusion detection system using mobile agent approach is taken from Mobile agent Distributed Intrusion Detection System 2008 (MDIDS).

- For this development, data sets have been taken from the Mobile agents based intrusion detection system for mobile Ad-hoc network presented in the International conference on innovative computing and communication 2010.

✓ Fault Tolerance

- For this process, data sets have been gathered from the Fourth IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems and the Second International Workshop on Collaborative Computing Integration and Assurance (SEUS-WCCIA 06), 2006.
3.4 SUMMARY

This chapter provided a global view of the proposed system for intrusion detection. In the first section, an overview of the cluster formation is presented. The optimal node selector is introduced in this section. The second section briefly presented an overview of the proposed mobile agent server whose role is to select the next optimal node dynamically for the efficient migration of the mobile agent server with the help of the specially allocated mobile service agent.

The third section mainly discussed about the mobile service agent and its basic security principles. The mobile agents are used to detect the known and new or unknown attacks exploited the intruders. Thus the attacks are detected by the mobile agents and the attacks are updated in the database and the entire network environment is alerted about the intrusion. The fourth section describes the four functional components namely, i) Profile database, ii) Decision making Agent, iii) Replication Agent and iv) Fault detection and recovery. The fault detection module of the mobile agent centralized server, which is specifically introduced in this architecture, manages the recovery of mobile agent server in the event of its failure.