MA-NID : a Multi-Agent System for Network Intrusion Detection

Karima Boudaoud, Houda Labiod
[boudaoud, labiod]@eurecom.fr
Institut EURECOM
06904 Sophia-Antipolis Cedex- France
Phone : (33) 4 93 00 26 38
Fax : (33) 4 93 00 26 27

Keywords : Distributed Intelligent Systems, Autonomous Agent, Security Management, Distributed Intrusion Detection, Intelligent Agent Theory, Multi-Agent System Technique.

Abstract: The application of the new technology DAI (Distributed Artificial Intelligence) seems promising for designing efficient secure networks. Intelligent agents features should offer to future networks, the capacity to become autonomous and adaptive to changes in a given environment. In fact, systems vary considerably in time in terms of component number, user access queries and intrusion possibilities. The focus point of our study concerns one critical security issue : intrusion detection. This paper proposes a new approach MA-NID (Multi Agent Network Intrusion Detection) based on intelligent agent technology. It is used to provide a flexible integration of multi-agent technique in a classical network to enhance its protection level against inherent attacks.

I. Introduction

The increasing number of users and machines make computer and network systems more vulnerable to attacks. As these networks are used by a large number of organizations, network security becomes a critical and major issue that must be considered carefully. Securing a network involves protecting it against all possible attacks. However, in practice, it is not possible to have a completely secure network. So, it is important to detect security violations instantaneously in order to execute appropriate actions to repair caused damages. The existing solutions are very complex and costly. What needed is a flexible, adaptable and affordable security solution which provides greater autonomy. Therefore, it is necessary to review the way in which standard intrusion detection is designed and performed in order to identify and to alleviate its weakness. In this context, we propose a new approach based on intelligent agent technique which reveals itself as a suitable candidate to make a balance between security requirements and system flexibility and adaptability in the case of the network intrusion detection (NID).

Actually, intelligent agent technology is viewed as one of the fastest growing areas of research and new application development in telecommunications. The DAI concept [1] consists of a group of individual named agents that have distributed environments. Each agent cooperates and communicates with other agents. Combined knowledge and experience of the agent with the information coming from neighboring agents permits the agent to make the best (optimum in some sense) decision. In this paper, we suggest to improve network security by integrating DAI (Distributed Artificial Intelligence) approach based on multi-agent system technique in Intrusion Detection Systems (IDS). We propose a new approach based on providing the NID hosts with additional functionalities. These entities become more intelligent, capable of making various decisions with autonomy to detect intrusions and to overcome their bad effects. The introduction of multi-agent system (MAS) in a network seems so promising to embed adaptive features thereby enabling network entities to perform adaptive behavior and becoming "intelligent". The term intelligence is used in the sense that network entities provide reasoning capabilities, exhibit behavior autonomy, adaptability, interaction, communication and co-operation in order to reach some goals. Then, we built a new architecture called MA-NID (Multi Agent Network Intrusion Detection). It is used to provide a flexible integration of multi-agent technique in a classical network to enhance its protection level against inherent attacks. Our paper is organized as follows. Section 2 provides a short description of IDS. The agent concept and MAS technique are outlined in section 3. In section 4, a distributed architecture integrating a multi-agent system for NID is briefly presented. Finally, Section 5 provides concluding remarks and perspectives.

II. Intrusion Detection

Intrusion detection is a practical approach for enhancing the security of computer and network systems. The goal of IDS is to detect attacks especially in real-time fashion. There are systems based on host-audit-trail and/or network traffic analysis to detect suspicious activity. These systems use one or both of two approaches of intrusion detection. The first approach is the behavior-based intrusion detection, which discovers intrusive activity by comparing the user or system behavior with a normal behavior profile. The second approach is a knowledge-based intrusion detection approach, which detects intrusions upon a comparison between parameters of the user's session and known pattern attacks stored in a database. The behavior-based intrusion detection approach allows to detect unknown intrusions contrarily to the knowledge-based intrusion detection approach which detects well-known intrusions. We focus our work on network intrusion detection systems and we present below two specific systems DIDS and CSM.

DIDS (Distributed Intrusion Detection System) operates on a local area network (LAN) and its architecture combines distributed monitoring and data reduction with centralized data analysis [2]. A DIDS director, a LAN monitor, and series of host monitor constitute it. The LAN monitor reports to the DIDS director unauthorized or suspicious activities on the network. The host monitor collects audit data for the individual host and perform some simple analysis on the data. The relevant information is then transmitted to the DIDS director. This director is responsible for analyzing all these data and detecting possible attacks. A shortcoming of DIDS is that the centralized nature of DIDS will limit its usefulness in wide area networks where communication with a central director from all hosts may swamp portions of the network.

CSM (Co-operating Security Managers) was designed to perform intrusion detection in a distributed environment [3]. A CSM must be run on each computer connected to a network to facilitate the co-operative detection of network intrusions. It is composed of the following parts: a local intrusion detection component, a security manager, an intruder handling component , a graphical user interface, a command monitor, and a TCP communication module. The security manager co-ordinates the distributed intrusion detection between CSMs.

CSM takes an approach that uses no established centralized director but each of the individual managers assumes this role for its own users when that manager suspects suspicious activity. The most important feature of CSM is that the co-operation among CSMs permits them to handle attacks in a proactive manner (e.g. doorknob rattling attack). In a heterogeneous environment, two CSMs can communicate because communication takes place via messages that relay information that need not be system-specific. However CSM cannot simply be ported from one computer system to another because the action-based intrusion detection module is heavily system-specific.

Looking at these approaches undertaken to counter security attacks, some features of these approaches can be derived as main requirements such as distribution of activities, autonomy, co-operation and mobility.

III. Description of multi-agent technique

Intelligent agent technology is a growing area of research and new application development in telecommunications. Having highlighted the main requirements for security management, the intelligent agent concept seems to be an appropriate approach to fulfill the intrusion detection requirements. Until now, there is no an internationally accepted definition of an intelligent agent concept [4]. Ferber [5] defines an agent as a computational or physical entity situated in an environment (either real or virtual) which is able to: act in the environment, perceive and partially represent its environment, communicate with other agents, driven by internal tendencies (goals, beliefs,..) and has an autonomous behavior which is the consequence of its perception, its representation and its interactions with the environment and with the agents. In fact, this new concept is used in different domains and possesses various meaning depending on the context of its application. However, it can be described by a set of properties including:

-**autonomy**: is the ability of an agent to operate without direct intervention of humans or other agents and to have some kind of control based on its internal and/or external environments.

-**sociableness**: is the capability of an agent to integrate itself in a large environment populated by a society of agents with which the agent has to exchange messages to achieve purposeful actions. This property is satisfied even when systems have to share their knowledge and mental attitudes (beliefs, goals, desires,…) .

-**proactivness:** is a relevant property which occurs in network and system management in order to avoid disastrous effects on global performance. Indeed, proactive agents are capable of exhibiting goal-direct behaviors by taking some initiatives [6][7].

-**reactivity**: this kind of behavior means that the agent reacts in real-time to changes that occur in its environments.

-adaptability: is the ability of an agent to modify its behavior over time to fulfill its problem-solving goals.

-intelligence: the term "Intelligence" means that the agent is able to exhibit a certain level of intelligence priority, ranging from predefined actions (planning) up to self learning (define new actions).

Moreover, multi-agent systems, as a sub-domain of DAI, are viewed as computational systems in which several autonomous and intelligent agents interact and work together in order to perform a set of tasks and to satisfy a set of goals [1][5]. Three kinds of agents are distinguished in DAI [8] according to the "intelligence" level:

1) Cognitive agents: A cognitive agent is able to find a solution for a complex problem while communicating with other agents and interacting with its knowledge base. Its main features include a high reasoning capacity, data processing, perception, learning, control, communication and expertise per activity domain.

2) Reactive agents: A reactive agent reacts quickly for a simple problem that does not require complex reasoning. Thereby, system intelligence emerge from interactions between a great number of this type of agents.

3) Hybrid agents: An hybrid agent, a mixture of reactive and cognitive agents, owns some reflex (reactive evolution) to resolve repeated problems and thinks (a cognitive attitude) about complex system situations.

In our work, the term intelligence is used in the sense that security network entities and especially NID components should provide reasoning capabilities, exhibit behavior autonomy, adaptability, interaction, communication and co-operation in order to reach some intrusion detection goals.

IV. Multi-agent network intrusion detection architecture

We have highlighted in section II, that distribution of detection activities is found mainly in all the approaches. It is very important to distribute the process of intrusion detection among a number of entities that can monitor the network and system behaviors at different points. The CSM and DIDS approaches have shown the necessity to have a certain level of autonomy in the various entities that constitute the system. They differ in the sense that the final decision in the DIDS system is taken by a centralized manager, whereas in the CSM some decisions can be directly taken in the entity. So, we propose to add appropriate functionnalities to make network entities more autonomous by performing local analysis tasks. Moreover, the CSM has shown the necessity of security manager co-operation in order to detect security attacks that can not be detected by individual manager.

The key characteristics of our architecture include autonomy, adaptability, efficiency and distribution to make the network intrusion detection more flexible and less costly in term of maintenance. In our proposed approach, we define a new architecture, called MA-NID which supports NID activities. It is based on a multi-agent system architecture (see Figure 1). It is viewed as a collection of autonomous and intelligent agents located in specific network entities named NID hosts. These agents cooperate and communicate in order to perform intrusion detection tasks efficiently and achieve consequently better performance.

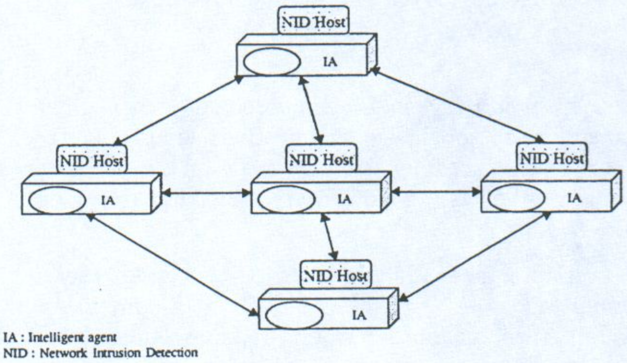

Figure 1 : MA-NID Architecture

In fact, by giving more autonomy to agent in the control of the overall intrusion detection, the task of administration becomes easier. Administrators do not have to concern about all the security problems. They interact with the agent from a high level using security policies. Security policies tell the agents what behavior they should exhibit when attacks occur. Hence, communications between agents permit to collect information. This information permits the agents to identify attacks that can not be detected if it is static. Giving more autonomy to the agent permits the system to react in "real time" to attacks and to take necessary actions to avoid severe consequences of the attack.

In this paper, the hybrid model depicted in Figure 2 applies.

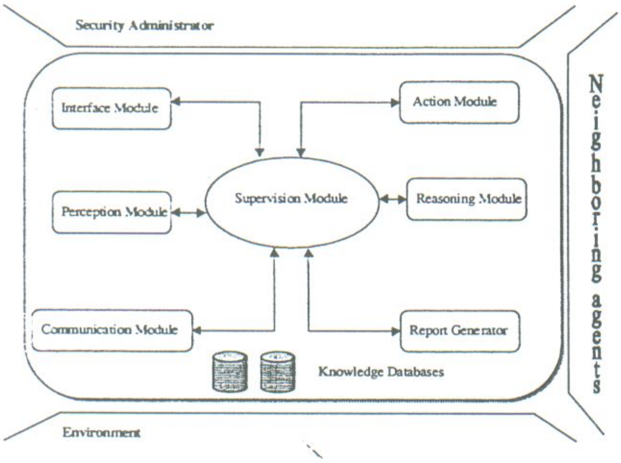

Figure 2 : Hybrid agent functional model.

Our hybrid agent is composed of six modules: perception, reasoning, communication, action, interface, report; each executing a different task. The supervisor entity coordinates tasks of different modules (see Figure 2).

An **interface module** interacts with the security administrator receiving administrator requests/specifications, delivering reports, sending alarms when an attack is detected and asking for additional information or confirmation when necessary. For example, the administrator can ask for the current network security status.

A **perception module**: that gathers all security-relevant events produced in the agent environment.

A **communication module**: that allows agents to communicate their analysis, decisions and knowledge.

An **action module**: its role is to take appropriate actions when an intruder is detected.

A **report generator:** establishes reports on detected attacks to be sent to the administrator.

A **reasoning module**: that enables agent intelligence and autonomy. The cognitive agent should be able to reason and extrapolate by relying on built knowledge and experience in a rational way. Decisions of the agent depend on the security environment status, the neighboring system evolution and its mental attitudes.

A **supervisor module** coordinates interactions between the different modules using a finite state automaton.

V. Conclusion

Intrusion detection seems to be an important issue in network security. Limitations of existing IDS involve the necessity of improvement of their processing. In this context, we propose to use the intelligent agent concept to fulfill intrusion detection requirements. Thus, the introduction of a multi-agent system is described as a means of implementation of adaptive decision making intrusion detection more flexible, customizable and cost-effective. The main goal of distributing intrusion detection function through agents is to provide network with more flexibility, autonomy responding in real-time to different arisen attacks. For further work, we intend to specify more precisely mental attitudes in terms of beliefs, goals and motivations used by the reasoning module of the agent to perform detection of network attacks.

References

[1] L. Glasser, "An overview of DAI", Kluwer Academic Publisher 1996.

[2] L.T. Heberlein, B.Mukherjee, and K.N.Levitt, "Network Intrusion Detection", IEEE Network journal, May/June 1994, pp. 26-41.

[3] Maj.Gregory B. White, Eric A. Fisch, and Udo W. Pooch, "Cooperating Security Managers: A Peer-Based Intrusion Detection System", IEEE Network journal, January/February 1996, pp. 20-23.

[4] H. Nwana and M. Wooldridge. "Software Agent Technologies". BT Tech. Journal, 14(4) :68-78, 1996.

[5] J. Ferber, "Les Systèmes Multi-Agents", InterEditions 1995.

[7] M. Wooldridge and N. R. Jennings. "Intelligent Agents : Theory and Practice". Knowledge Engineering Review, 10(2) :115-152, 1995.

[8] H. Labiod, "Error Control in Wireless ATM networks", Thesis 1998.

[9] Z. Guessoum, "Un Environnement Opérationel de Conception et de Réalisation de Systèmes Multi-Agents", Thesis 1996.