ISSN:2249-5789
Munish Gupta al , International Journal of Computer Science & Communication Networks,Vol 2(6), 677-680

MAS BASED FRAMEWORK FOR NETWORK INTRUSION DETECTION SYSTEM

Munish Gupta[1], Manish Saxena[2] Vijay Kumar Mishra[3] and Chandra Bhan Singh[4]

1 Research Scholar, CMJ University, Shillong
hi_munish@yahoo.com

2 Asst. Professor, MCA Department, FGIET, Raebareli, UP, India. Pin - 229001
manish.mohan.saxena@gmail.com, URL : www.manishsaxena.in

3 Assistant Professor, MCA Department, FGIET, Raebareli, UP, India. Pin - 229001
vijaymishra.rbl@gmail.com

3 Lecturer, Sagar Institute of Technology & Management, Barabanki, UP, India. Pin - 225001
chandrabhan98@gmail.com

Abstract

The growing use of internet forces us to work of security aspect also as the security related incident increases. It becomes reason for thinking for organizations to protect their sensitive information with an effective Intrusion detection system (IDS). MAS (Multi-Agent System) are becoming a growing research field which uses agent capability with distributed problem solving approach. Intrusion detection system (IDS) can be treated as a software appliance that monitors network deeds for spiteful actions and generate reports. Here in this paper we are focusing on intrusion detection model based on multi-agent system where the capabilities of autonomous software components can be successfully used to make IDS more efficient, consistent and ingenuousness. Thus the design of distributed network IDS is based on agents which are used as security guard to supervise network and on getting any intrusion it gives alerts and send report also. Multi-agent based IDS has low network traffic load.

Keywords- *Multi-agent system, intrusion, IDS*

1. Introduction

Multi Agent Systems[1] can be viewed as a collection of autonomous, self-contained software components which interact with each other to coordinate, collaborate and communicate their actions with each other. Capabilities such as sociability, reactivity and pro-activity make agent system [2] useful for IDS.

Generally there are two approaches that can be worked to make system protected. First one is by constructing a highly secure network system and the second approach emphasises on detection of attacks. If we talk practically the first approach seems to be impossible, we have to focus on the second one which is based on detection of attacks.

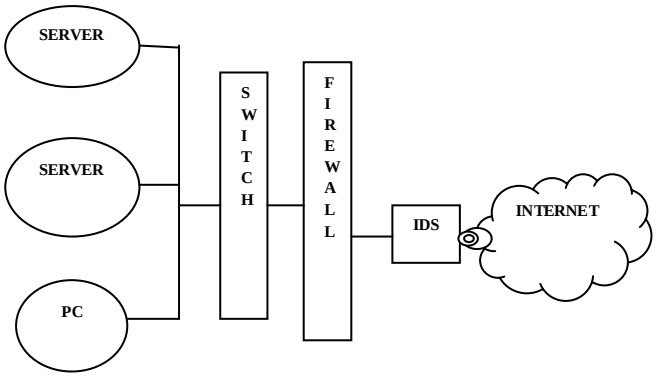

Figure 1. Simple Model for IDS Technique

Figure 1 shows the simple model for intrusion detection system.

Lot of researches [3,4] are done on intrusion detection. In simple IDS method the IDS reports suspected intrusions those are already defined in enabled IDS policies. Whenever an intrusion is detected by IDS it generally report or notify to a message queue and email letter. The IDS contains two types of stacks containing TCP/IP modules.

First one is production stack and second is service stack. Service stack which contains TCP/IP for service and support of system comes first and remain until the next IPL comes.

Production stack which contains TCP/IP for network operation comes after service stack and remains till the end of TCP/IP. Any intrusion detected by service stack first of all registered in record of intrusion monitor.

While figure 2 shows typical view of Detection and monitoring records of IDS. In this network system and hosts are connected to service stack and production stack. Both stacks contains TCP/IP. These stacks play important role in detection and reporting on intrusions and other unauthorised access.

The detected intrusion are reported shortly to log record manager who maintains the record of these intrusions and attacks.

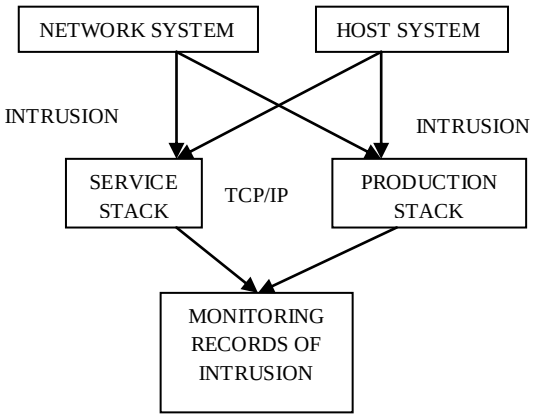

Figure 2. Typical view of Detection and monitoring records of IDS

Agent concept [5] can be used to build up and set up proficient distributed Intrusion Detection System on the computer network. Various methods and approaches are provided for intrusion detection some methods are also base on agent system. But the agent approach[1,2] and IDS is not used much in collaboration as they can be used to construct more efficiently method for IDS. Earlier the attacks littered single system, to immobilize it or to get an illegal right to use to data. But now attacks don't emphasises only on single hosts. The attack domain grows to distributed environment and focuses on network infrastructure using worms and Distributed Denial of Service.

The paper contains four sections section 1 is introduction one which focuses on MAS approach and IDS process individually, section 2 emphasises on requirements of IDS, section 3 gives the collaborative approach of MAS and IDS by solving the short coming discussed in section 3, section 4 contains conclusion.

2. Requirements Of IDS

Intrusion detection systems are an integral and necessary element of a complete information security infrastructure performing as "the logical complement to network firewalls." [7] Simply put, IDS tools allow for complete supervision of networks, regardless of the action being taken, such that information will always exist to determine the nature of the security incident and its source.

Studies show that nearly all large corporations and most medium-sized organizations have installed some form of intrusion detection tool.[8]

As per MITRE research [9], the requirements of IDS are as follows:

1) **Processing Requirements:** The IDS module should have three high-level processing activities: monitoring, an activity of the sensors; assessing, an activity of the analyzers; and managing, an activity of the directors.

2) **Functional Requirements:** The IDS module needs to perform a variety of functions grouped these functions into several categories covering collecting, processing, analyzing, reporting, and storing intrusion and vulnerability data, providing alerts, displaying information, controlling IDS resources, reacting to intrusions and vulnerabilities, and interacting with other modules. These functions provide lower level requirements than the processing requirements of the previous section.

3) **Output Requirements:** In providing the needed functionality and processing, the IDS module must generate several outputs. The outputs identified here are very general in nature—they must be further delineated for specific requirement specification and design. They will contain information from the requirements already defined. The outputs are organized into Attacker Profile, Security Profile, and System Profile.

4) **Technical Requirements:** The technical requirements of IDS should be based on General needs like-Implementation, Performance and Standards; Network requirements based on local environment variables; Security requirements as per ever evolving requirements.

5) **Other Requirements:** Some Other requirements of the IDS includes Architecture issues, Configuration issues, Evolution of IDS issues, issues related to IDS Interfaces, Robustness issues for heavy duty 24x7 operations, IDS application updates issues, User Friendliness issues.

The requirement of proposed IDS can be given as:-

- Continuous monitoring/reporting of intrusions.
- Lowest amount of false alert.
- Self command to repair system in case of failure by any attack.
- IDS should be adaptive in nature for network topology.
- Must familiarize itself with the changes in configuration.
- Immediate reporting of detection in order to reduce network harm.
- Intrusion detection system must be scalable.
- Give minimum network load.

There requirements can be treated as short coming of IDS for distributed network environment which can be easily overcome by using MAS based IDS for network.

3. MAS Based Network IDS Model

The requirements given in above section can be easily achieved by multi-agent[5] based model for network IDS. We know that the shortcoming of centralised IDS causes the idea of agent based IDS[6]. Agent based ids has no central station for management. So it has no single point of failure. The requirements mentioned in above section do not meet with centralised IDS while multi-agent [5] based network IDS easily fulfil these requirements. It has capabilities like adaptability, reconfiguration at run time, scalability, openness etc. We know that agent is self-contained, reactive, pro-active, autonomous and sociable in nature.

The dynamic nature of agent beneficiated it to be reconfigured at run time. This model uses a set of agents to facilitate network IDS.

There is a facilitator ID agent who works at outer most, when ever any event comes to it as intrusion or suspected it firstly validate and verify that event and then record it in the intrusion monitor log record. This process is done on the basis of various cognitive parameters which are predefined to it. Coordinator ID agent which works as manager. It initiates various detectors ID agents. It works as mediator between facilitator and detector agent. We know that agent is one which either work itself or make others to work. Various detector ID agents are also connected to network and hosts system. These agents are controlled by the above mentioned coordinator ID agent. Using agent at different level will avoid system failure and also minimise network traffic load. Activities that will be performed in MAS based network IDS are as following:-

- Coordinator ID agent will monitor overall network.
- Detector ID agents that work as collector spread over the entire network, gather all events which are occurring in that network for which it is related.
- Detector ID agents are connected with network systems and host system. Whenever it gets any suspected event it will report to coordinator ID agent.
- Coordinator ID agent report to facilitator ID agents which maintain intrusion detection log record for suspected events and intrusions.
- Facilitator ID agent who works as analysts, when ever any event comes to it as intrusion or suspected by coordinator ID agent it firstly validate and verify that event and then record it in the intrusion monitor log record.
- The communication between agents is done by using agent communication protocol (ACP).

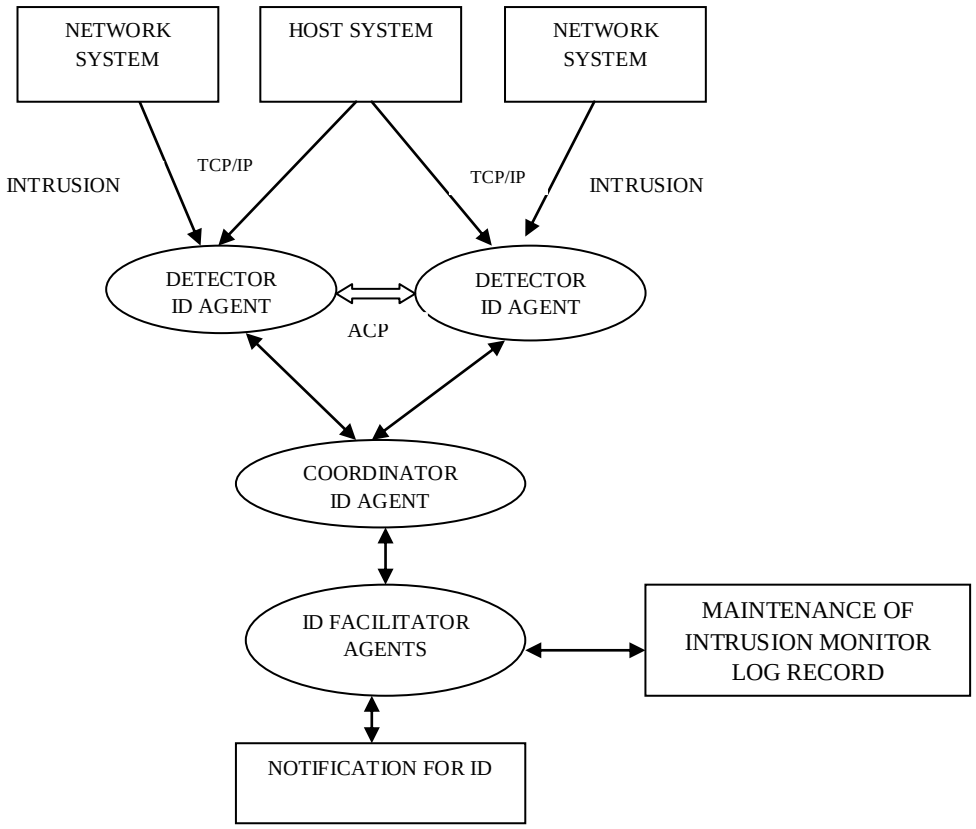

Figure 3. Typical agent Based Model Model for Network ID

Figure 3 shows the typical view of multi agent based intrusion detection model. Here each agent communicates with each other with its sociability properties using agent communication protocol (ACP). Various languages are available to create agents. Java based agents are more effective in nature.

Thus the use of agent increases the network efficiency and reduces the network load as instead of huge data now only little code of agents traverse over network.

4. Conclusion

Thus we have seen that IDS which becomes mandatory for today's network environment and the growing use of internet forces organizations as well as individuals to think about security aspect of their personal information's. We here presented an agent based model collaborated with intrusion detection system to make the system more reliable and effective. The use of agent increases the network efficiency and reduces the network load as instead of huge data now only little code of agents traverses over network. Although the presented framework is efficient, robust, less network load, scalable but the security and performance will be the important area for researches for agent based network intrusion detection system.

5. References

[1] Wooldridge, M. An introduction to Multi agent system. Wiley Ed. (2002).

[2] Jeffrey M. Bradshaw, "An Introduction to Software Agents," In Jeffrey M. Bradshaw, editor, Software Agents, chapter 1. AAAI Press/The MIT Press, 1997.

[3] Jones Anita K, Sielken Robert S.: Computer System Intrusion Detection: A Survey. University of Virginia, USA 19–20.

[4] Andreas Fuchsberger, "Intrusion Detection Systems and Intrusion Prevention Systems"; Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 0EX, United Kingdom 2005.

[5] Walsh, W.E., Wellman, M.P.: A market protocol for distributed task allocation. In: In Third International Conference on Multiagent Systems, Paris (1998)

[6] M. Bernardes, E. Moreira. Implementation of an Intrusion Detection System Based on Mobile Agents. Proceedings of the International Symposium on Software Engineering for Parallel and Distributed Systems, 2000.

[7] Bace, Rebecca, "An Introduction to Intrusion Detection and Assessment: for System and Network Security Management," ICSA White Paper, 1998.

[8] SANS Institute Staff, "Intrusion Detection and Vulnerability Testing Tools: What Works?", 101 Security Solutions E-Alert Newsletters, 2001.

[9] Therese R. Metcalf, Leonard J. LaPadula, "A Capabilities Description in Terms of the Network Monitoring and Assessment Module of CSAP21", September 2000