An Enhanced Multi-Agent based Network Intrusion Detection System using Shadow Log

Namita Singh
Department of CSE,
AIET, Lucknow,

Siddharth Krishan
Department of CSE,
AITM, Lucknow,

Uday Kumar Singh
Department of CSE,
AIET, Lucknow,

ABSTRACT
The capability of agent and its distributed problem solving nature makes it useful and powerful; such that it can be utilized in various fields. Various research [1][2][3][4][5][6] has been done and currently in progress based on the utilization of the capability of the agents. Here our focus is on utilization of agent capability for identifying intrusion in network. Some agent based model and framework has been also produced for network intrusion detection system (NIDS)[5][6]. This paper includes a study on theory research an enhanced model based on shadow log.

General Terms
MAS, NIDS, IDS, LOG etc

Keywords
MAS (Multi Agent based System), NIDS (Network Intrusion Detection System), Shadow Log.

1. INTRODUCTION
Agent environment can be arranged according to different factors such as accessibility, determinism (if an action performed in the environment causes a certain effect), dynamic (how many entities influence the environment at this time), discrete (if the number of possible actions in the environment is finite), frequency (if the actions of the agent in certain periods of time affect other periods) and dimensionality (if spatial characteristics are important factors in the environment and the agent considers the space in its decision)[1][2][3].
The agents in a multi-agent system have several important characteristics:

- Autonomy: agents are at least partially independent
- Local views: no agent has a complete overview of the system, or the system is too complex for an agent to make practical use of this knowledge
- Decentralization: there is no agent designated control (or the system is effectively reduced to a monolithic system).
- The self-organization and self-control, multi-agent systems can manifest self-organization and self-management and other control paradigms and complex behaviors related, even if individual strategies all their agents are simple.

When agents can share knowledge using any agreed within the communication protocol of the system language, the approach can lead to a common improvement. Query languages such knowledge Manipulation Language (KQML) and Agent Communication Language FIPA (ACL).
Thus agent system can be considered as a network of agents that coordinate with each other to address complex or say big problem that can be solved by a single agent, without a global surveillance system. MAS (Multi-Agent System) are increasingly an area of growing research that uses the ability of the agent to the problem solving approach distributed. It is a technique of "Distributed Problem Solving"[1][2] in the multi-agent in which agents discuss some aspects of the system as follows:

- How to divide a complex problem into sub-problems?
- How to distribute these sub-problems between them?
- How to share knowledge with each other to resolve dependencies between sub solutions?
- How to combine sub solution to provide an overall solution to the problem?

It is in a multi-agent system (MAS) [5] [6] which contains an environment, objects and agents (the agents being the only act), the relationships between all entities, a set of operations that can be performed by entities and changes in the world of time and because of these actions. From the point of view of distributed problem solving MAS can be defined as a loosely coupled network of problem solving that work together to resolve problems that are beyond the individual capabilities or knowledge of each problem solver.
IDS requirement can be given: -

- Continuous monitoring / reporting intrusions.
- The lowest amount of false alarms.
- Auto-control system for repair in case of failure of any attack.
- IDS should be adaptive nature of the network topology.
- Must be familiar with configuration changes.
- Immediate notification of detection to reduce the harm network.
- Intrusion detection system must be scalable.
- Provide the minimum load network.

It requirements may be treated as short coming of IDS for distributed network environment that can be easily solved by using MAS-based IDS for the network.

IDS most common deficiencies are:

- The high number of false positives
- Lack of efficacy
- Vulnerability to attacks several IDS have hierarchical structures. This fact gives attackers the possibility of

harm to the IDS by cutting a branch control or even turning on the root command.

2. PREVIOUS AGENT BASED APPROACHES

DARPA in the 90 defined under common intrusion detection (FDIC) as a general framework for IDS. The open infrastructure [9] includes a general framework for agent-based identity that is consistent FDIC.

This framework defines a hierarchy of agent layers, including the following types of agents: decision-response agents (responsible for responding to intrusions), agents Recognition (gathering information), agents of (analysis of information collected), and Directory / agents key management and storage agents. Both provide later support functions to other officers.

AAFID (Autonomous Agents for Intrusion Detection) [10] is a distributed network IDS architecture employing autonomous agents, being those defined as "software agents that perform a certain security monitoring function at a host". This architecture defines following main components:

Agents: monitor certain aspects of hosts and report them to the appropriate transceiver.
Filters: intended to be the data selection and abstraction layer for agents.
Transceivers: external communications interfaces of hosts.
Monitors: the highest-level entities that control entities that are running in several different hosts.
User interface: interact with a monitor to request information and to provide instructions.

In Identification distributed architecture, complemented by a data warehouse and mobile and stationary agent is proposed in [8]. MAS is combined with an algorithm for generating rules, genetic algorithms, and techniques of data warehouse to facilitate the design, monitoring and analysis of global views, spatio-temporal intrusions on large distributed systems. The system calls executed by privileged processes are classified after being represented as feature vectors. To do this, different agents are defined:

Data pollutants: the process data of the stationary agents obtained from newspapers monitors network protocol files and monitors system activity in homogeneous formats.

Low-level agents: these mobile agents form the first level of ID. They move each of their pollutants associated data, collect recent information, and classify data to determine whether a suspicious activity is in progress. These agents work together to define their level of suspicion to determine whether a suspect cooperative action is more interesting in the presence of other suspicious activities.

High-level officials: they maintain the data warehouse by combining knowledge and data workers low. The high-level officials apply data mining algorithms to discover patterns and associations.

Agent interface: it directs the operation of agents in the system maintains the status reported by the mobile agents, and provides access to functionality of the data warehouse.

However, IDS using mobile agents are new class of intrusion detection system. Mobile agents can be defined as "independent and autonomous computer programs identified, provided with their code, data and execution state that can move in a heterogeneous network of computer systems. They can suspend their execution on an arbitrary point and transport it to another computer system. Mobile agents have special characteristics that can help intrusion detection in several ways. The use of mobile code and mobile computing agents paradigms have been proposed in several studies. Benefits include: overcoming network latency, reducing network load, asynchronous and autonomous execution, and dynamic adaptation, operating in heterogeneous environments, and having a robust and fault tolerant behavior. In addition, the implementation of mobile agents in languages such as Java provides mobile agents with the system and independence and security features considerable. An early study in this context was JAM (Java Agents for Meta-learning). [11] this work combines intelligent agents and data mining techniques. When applied to the identification problem, algorithm-association rules determine the relationships between different areas of audit trails, while a meta-learning classifier learns the attack signatures. Characteristics of these two techniques of data mining are extracted and used to calculate the models of intrusion behavior.

The requirements set out in the previous section can be easily reached by multi-agents [12] based model for IDS. We know that the lack of centralized IDS causes the idea of IDS agent base. [13] IDS of the agent on the basis not of the central management station. So there is no single point of failure. Requirements mentioned in article above do not meet with centralized IDS while multi-agent [12] network based IDS easily meet these requirements. It has capabilities such as adaptability, reconfiguration at the time of execution, scalability, openness, etc. We know that the agent is autonomous, reactive, proactive, independent and sociable in nature.

The dynamic nature of the agent and to enhance be reconfigured at runtime. This model uses a set of agents to facilitate IDS network. It is an identity that works at the outermost, whenever a case presents itself as an intrusion or suspected to validate one hand and verify that the event facilitator agent, then save the monitor recording intrusion newspaper. This process is based on the different cognitive parameters are predefined for it. Coordinator agent ID that works as a manager. It introduces various identity detectors agents. It works as a mediator between the host and agent detector. We know that the agent is the one who is himself or making others work to work. Various sensor identification officers are also connected to a network system and hosts. These agents are controlled by the coordinator agent ID mentioned above. Using the Agent to different level, to avoid failure of the system and also to minimize the network traffic load. ID sensor agents are connected with network systems and host system. Whenever he gets suspicious cases, it will report to the coordinator agent ID. ID Coordinator Officer Report to moderator agents that maintain identity intrusion detection recording log events and suspicious intrusions. Facilitator ID agent who works as analysts, whenever 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 using the agent communication protocol (ACP). All agents will work in coordination and follow- up work or provides supervision will be allocated to

them based on their feasibility. Balanced distribution of the monitoring process within the network as well as an effective placement intervention processes intrusion must be decided and reconfigured on-site interaction in a peer-to-peer communication between network components. This is true because there is a desire to limit centralized decision-making and centralized collection of data in the network.

The distribution of tasks distributed is a typical problem that is fixed in its different variations in the communities of multi-agent research for years. The distributed task allocation algorithms are based on different approaches to the auction each having different properties in different environments.
.

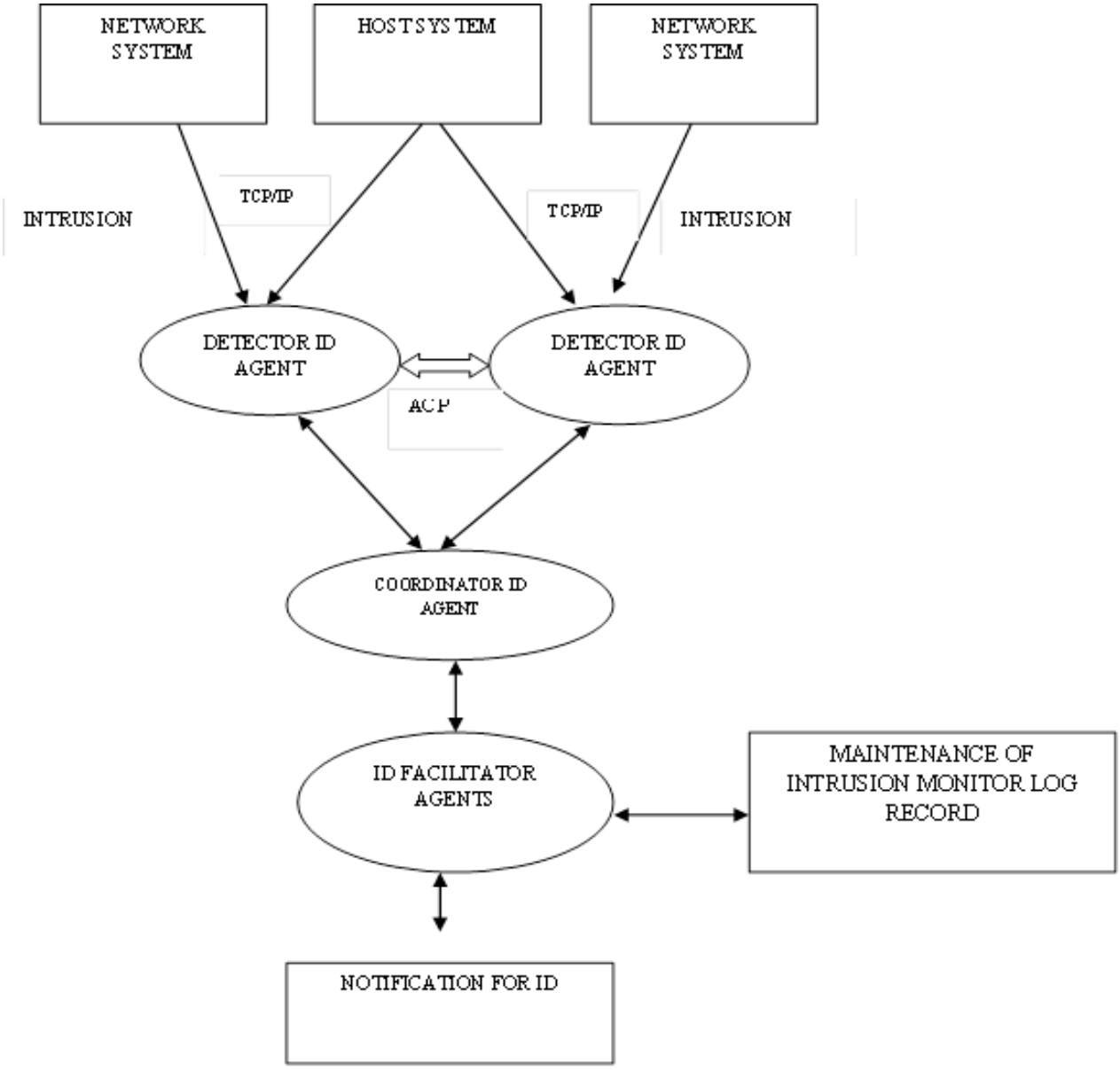

Fig 1: Typical Multi-Agent Based Model for Network ID

Figure 1 shows the typical view of multi agent based intrusion detection model [6]. 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.

3. PROPOSED MODEL

The proposed MAS based model used two shadow logs which is identical copy of original log record as mentioned in model presented in [5]. Various basic agents are used depending upon the size of network. These agents checks activities in network and in case they got subspecies activities they notify this to supervisor agent.

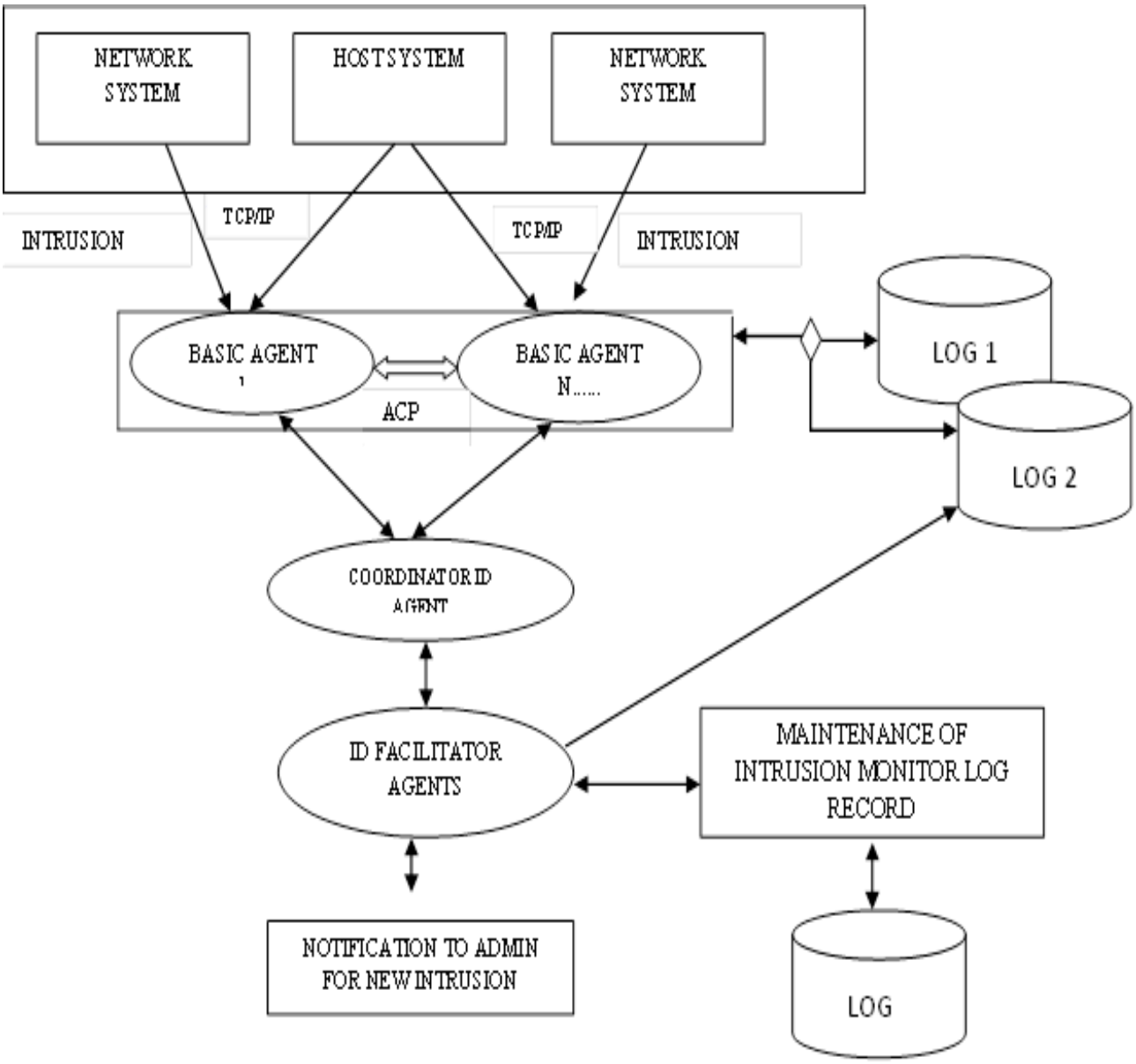

Fig 2: Extension of Agent Based Model for Network ID using Shadow Log (LOG 1, LOG 2)

The functioning of agent based intrusion detection is based on two aspects first one is type of agent here three type of agent is used as shown in figure 2 first one is basin agent, second one is coordinator agent and last one is facilitator agent.

As it is seen that basic requirement of IDS is to maximize CPU utilization, make system robust and batter fault tolerance.

The working algorithm for proposed MAS based model is as following:

F (A, L) that is the functioning of NIDS depends on set of agents (A) and log records (L).

MAS-NIDS (AGENTS, LOG, LOG1, LOG2)

I. First phase is BASIC AGENT which monitors the network.
II. Whenever a suspicions activities is detected is notify is to coordinator agent, otherwise passes it. For this basic agent matches each activity with LOG 1. LOG 1 is identical copy of main LOG record.
III. All BASIC AGENT uses data LOG 1 at its primary level and in case the identify intrusion notify it to coordinator agent, and then it passes it to facilitator agent for verification and validation.
IV. If facilitator agent also agreed that the event is suspicious then the main LOG record is updated.
V. Then the second shadow LOG 2 is then updated i.e. it will be made identical to main LOG record.
VI. If BASIC AGENT will find that LOG 1 !=LOG 2. It switches on LOG 2 for matching events (activities). LOG 1 is then made identical to main LOG record.
VII. If LOG 1 ==LOG 2 then again BASIC AGENT working switches on LOG 1.
VIII. GOTO step II.

4. CONCLUSION

In the above proposed model shadow Logs are used for matching activities to identify suspicious events. As the log data based is always updated to there is no point for interruption which will be beneficial for following –

- Better CPU utilization.
- Less network load.
- Reduced false alarm.
- Continuous monitoring.
- Auto fault tolerance.

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 TW200EX, United Kingdom 2005.

[5] Chandrabhan Singh, Sanjay Sachan and Mohit Gangwar. Article: MAS based Selection and Composition Process of SWS's for Medical Health Care Planning System. International Journal of Computer Applications 60(16):40-44, December 2012. Published by Foundation of Computer Science, New York, USA.

[6] Munish Gupta, Manish Saxena, Vijay Kumar Mishra, Chandrabhan Singh "MAS BASED FRAMEWORK FOR NETWORK INTRUSION DETECTION SYSTEM", International Journal of Computer science & Communication Network (IJCSCN), volume 2 (6), 677-680, ISSN: 2249-5789.

[7] Alankar Srivastava, Shruti Saxena and Chandrabhan Singh. Article: Ontological Description and MAS based Composition Process of SWS's for Recruitment Domain. International Journal of Computer Applications 64(19):42-47, February 2013. Published by Foundation of Computer Science, New York, USA.

[8] Helmer, G., Wong, J.S.K., Honavar, V.G., Miller, L.: Automated Discovery of Concise Predictive Rules for Intrusion Detection. Journal of Systems and Software 60(3), 165–175 (2002).

[9] Reilly, M., Stillman, M.: Open Infrastructure for Scalable Intrusion Detection. In: IEEE Information Technology Conference, pp. 129–133 (1998).

[10] Spafford, E.H., Zamboni, D.: Intrusion Detection Using Autonomous Agents. Computer Networks: The International Journal of Computer and Telecommunications Networking 34(4), 547–570 (2000).

[11] Stolfo, S., Prodromidis, A.L., Tselepis, S., Lee, W., Fan, D.W., Chan, P.K.: JAM: Java Agents for Meta-Learning over Distributed Databases. In: Third International Conference on Knowledge Discovery and Data Mining, pp. 74–81 (1997).

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

[13] 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.