# Anomaly Detection Algorithm Using Multi-agents

Asmaa shaker ashoor , prof. Sharad Gore

**Abstract :** A Network intrusion detection system (NIDS) is gaining ever increasing importance in security of the information from network attacks. For better system performance and lesser response time an improved NIDS system is proposed anomaly detection is achieved by using various agents and by implementing adaptive threshold algorithm. Thus utilizing multi agents into the improved NIDS system enhances the system performance and response time, yet achieves higher accuracy and broader spectrum of protection from different types of intrusion attacks. in this work we propose the simple technique of Adaptive Threshold Algorithm that can be used to achieve large improvements in the performance of anomaly agent with using multi agents and less complex structure avoiding dead locks, less bulky operations and faster system response time.

**Keywords:** NIDS, Anomaly detection, Adaptive Threshold Algorithm, Multi-agents, Intrusion, JADE

## 1. INTRODUCTION

As the technology thrives, there are ever increasing number of internet users. Hence the information system security is becoming a growing concern. The rapid increase in connectivity and accessibility of computer systems are becoming increasingly vulnerable to intrusions, misuses, and attacks. There are many sources of threat including software bugs. The unauthorized user (Intruder) can steal valuable and private information belonging to network users. To address this problem intrusions detection systems (IDSs) are designed. The common approach followed in network intrusion detection system is inspection of patterns of user activities within log and usage files. Several intrusion detection systems have been built by manipulating the identified attack and misuse patterns. The intrusion detection systems use different techniques both anomaly and misuse intrusion detection. There are different techniques, to identify anomalies, while some are based on methods of predicting future patterns of behaviour using patterns seen so far, others use statistical approaches to establish anomalous behaviour. In any case, the behaviour that does not correspond with expected behaviour would be an intrusion. In intrusion detection, by inspecting data records observed by processes on the same network, the computer attacks are detected.

The Network attacks are divided into two categories, host-based attacks and network-based attacks. Host based attack detection approach uses system call data from an audit process that tracks all system calls made on behalf of each user on a particular computer. These audit processes usually run on each monitored machine. Network-based attack detection approach uses network traffic data from a network packet sniffer. An improved NIDS system is proposed anomaly detection agent is achieved by using multi-agent with implementing adaptive threshold algorithm. Thus utilizing multi agents into the improved NIDS system enhances the system performance and response time yet achieves higher accuracy and broader spectrum of protection from different types of intrusion attacks.

## 2. AIMS AND OBJECTIVES

The primary objective of proposed research work is development of an improved Network Intrusion Detection System which:

- Achieves anomaly detection agent without compromising on system performance.
- Provides accurate identification unknown attacks.
- 3. Developed using multi agents which will prevent deadlocks and improve system performance.
- Provides a stronger protection to the system from all types of intrusion attacks quickly.

## 3. RELATED WORK

Different approaches are being used globally to detect anomalies, like Rules based approaches, pattern matching, finite state machine, statistical analysis etc. Wang et al. [1] take the difference in the number of SYNs and FINs (RSTs) collected within one sampling period as time series data and use a nonparametric Cumulative Sum (CUSUM) method to detect SYN flooding by detecting the change point of the time series. Thottan and Ji [2] take management information base (MIB) data collected from routers as time series data and use an auto-regressive process to model the process. Network anomalies are detected by inspecting abrupt changes in the statistics of the data. Deri et al [3] show that in every network there are some global variables that can be profitably used for detecting network anomalies, regardless of the type of users and equipment.. Zhang et al [4], describe the use of Change Point monitoring to detect Denial of Service

1 *Asmaa shaker ashoor, Department of Computer Science, Pune University – Pune- India, asmaa_ zaid218@yahoo.com*

2 *prof. Sharad Gore, Department of Statistic, Pune University – Pune- India, sdgore@stats.unipune.ernet.in*

Attacks. The objective of Change-Point Detection is to determine if the observed time series is statistically homogeneous, and if not, to find the point in time when the change happens. Non-parametric CUSUM is again used for the detection of DoS attacks. Barford et al. [5]use wavelet analysis to remove from the traffic the predictable ambient part and then study the variations in the network traffic rate. Network anomalies are detected by applying a threshold to a deviation score computed from the analysis. Zou et al [6], introduce a methodology for fast detection of internet worms called "trend detection". It's based on the fact that a worm, in an early stage, propagates exponentially with a constant, positive exponential rate. The system attempts to detect this trend.

## 4. THE DEFINITION OF SOFTWARE AGENT

Today, the agent technologies becomes a key for the implementation of flexible and scalable solutions for the open services market within the information society. It becomes important technology for designing and developing complex software systems such as security and distributed systems. According to J. Ferber [7], an agent is a real or abstract entity, capable of acting on itself and on the environment. It can have a partial representation of this environment. It can communicate with other agent, finally, its behavior is the result of its observations, its knowledge and its interactions[8]. There are many definitions of agents, agents can be defined by a set of their attributes: active, autonomous, goal-driven, and typically acting on behalf of a user or another agent. Agents are not a new approach, as they have been researched in the area of Distributed Artificial Intelligence for a number of years. The widespread use of computers and their connectivity, particularly the web and the Java object-oriented programming language have provided a new influx in the research, development, and deployment of agents. A particular motivation for the use of agents is the huge amount of information available on the Internet. Agents have a significant potential looking for information, filtering it, and extracting it from the source. The ability to represent and act on behalf of the user represents a crucial capability of agents and provides enormous potential for their deployment. There are at least two communities currently pursuing agent research: the multi-agent system community and the mobile agents' community. The multi-agent and intelligent system community deals mostly with stationary agents distributed on the network, which communicate one another in order to pursue a common goal. The other community deals with mobile agents as approach for widely distributed and heterogeneous systems.

## 5. JAVA AGENT DEVELOPMENT FRAMEWORK (JADE)

It is a software Framework fully implemented in Java language [9]. It simplifies the implementation of multi-agent systems through a middle-ware that complies with the FIPA specifications and through a set of graphical tools that supports the debugging and deployment phases. The agent platform can be distributed across machines (which not even need to share the same OS) and the configuration can be controlled via a remote GUI. The configuration can be even changed at run-time by moving agents from one machine to another one, as and when required. JADE is written in Java language and is made of various Java packages, giving application programmers both ready-made pieces of functionality and abstract interfaces for custom, application dependent tasks. Java was the programming language of choice because of its many attractive features, particularly geared towards object-oriented programming in distributed heterogeneous environments.

## 6. ADAPTIVE THRESHOLD ALGORITHM

Adaptive threshold algorithm is a simple algorithm that detects anomalies based on violations of a threshold that is adaptively set based on recent traffic measurements. Seasonal variations and trends are taken care of by using an adaptive threshold whose value is set based on an estimate of the mean number of the packets under consideration or the rate, either of which are computed from recent traffic measurements. Let s suppose $X_n$ is the number of packets in the nth time interval, and *μ_1* is the mean rate estimated. From measurements prior to *n*, then the alarm condition is then alarm signaled at time *n*.

$$\text{If} \quad x_n \geq (\alpha + 1)\bar{\mu}_{n-1}$$

Where, *α* > 0 is the parameter that indicates the percentage above the mean value which we consider to be an indication of anomalous behaviour. The mean $\mu_n$ can be computed over some past time window or using an exponential weighted moving average (EWMA) of previous measurements: where b is the EWMA factor.

$$\bar{\mu}_n = \beta\bar{\mu}_{n-1} + (1-\beta)x_n$$

Anomaly detection system can detect any type of intrusion that does not match with normal behavior of the system. Anomaly detection system work on the principle of observing run-time deviation from normal behavior, an alarm is raised if the run-time deviation exceeds or falls below a certain threshold. The figure1 shown the principle of operation of anomaly detection is. It can be observed behavior deviates more than a fixed threshold from normal behavior, it is classified as anomalous. [10]

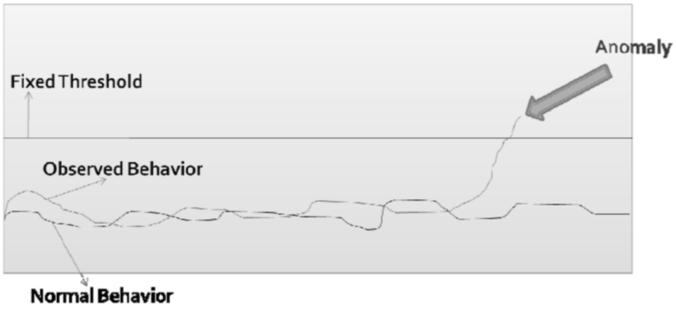

Fig1. Basic principle of operation of Anomaly Detection

## 7. THE PROPOSED SYSTEM ARCHITECTUREWITH MULTIAGENTS

Network Intrusion Detection System (NIDS) [11] investigates each incoming packets received by the computer system and with the implementation of the statistical algorithm and multi-agents, the decision is made whether the received packet is malicious or not, the detection of malicious packets signifies an intrusion with the system. The basic architecture of improved NIDS is shown in Figure3.

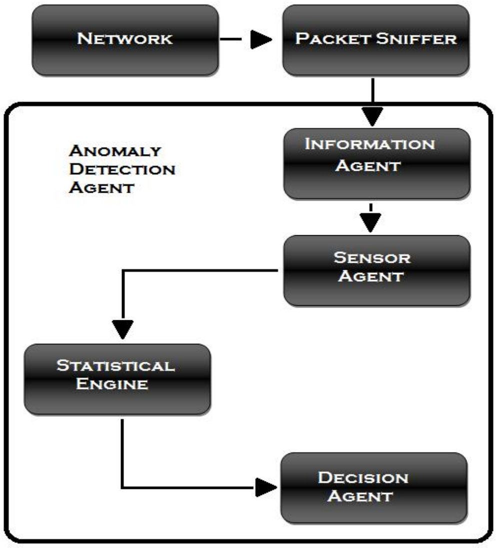

Figure2. illustrates Anomaly Detection Agent

The system architecture, it consists of multiple interacting intelligent agents. Multi-agent systems[12] can be used to solve problems that are difficult for an individual agent or a monolithic system to solve. We are using Java Agent Development framework (JADE)[9] for creating agents. In the proposed system, following agents are considered:

- Anomaly detection agent include:
- Information agent
- Sensor agent
- Decision agent

***Network***: at least two computers interconnected by communication channel so as to share and exchange the information (data) are said to be in a network.

***Packet Sniffer***: A packet sniffer is a program that allows eavesdropping on traffic traveling between networked computers. The packet sniffer will capture data that is addressed to other machines.

***Anomaly Detection Agent***: is a module which observes the system for deviations from normal behaviour. The detection of abnormal behaviour of the system indicates the existence of attack. This agent includes:

***Information agent:*** this agent to collect information from the packet sniffer, it is acting as the unit data repository for anomaly agent.

***Sensor agent:*** this agent sense packet from information agent and, pre-process by reducing irrelevant data, and extract the independent features.

***Statistic engine:*** it is responsible for the process to carry out analysis of data packets by using Adoptive Threshold Algorithm to detection results and it send the information about security status to decision agent.

***Decision agents:*** it is the agent responsible for decision-making, when attacks are detected; they send simple notification messages to the system administrator to take the appropriate decision.

## 8. EVALUATION OF RESULTS

Anomaly detection agent can detect any type of intrusion that does not match with normal behavior of the system. In this work, the system is using techniques based on multi-agent and adaptive threshold algorithm. Anomaly detection agent work on the observing run-time deviation from normal behavior, an alarm is raised if the run-time deviation exceeds or falls below a certain threshold. The primary objective of proposed research work is development of an improved Network Intrusion Detection System which achieves anomaly detection without compromising on system performance and achieves accurate identification unknown attacks. Also improved Network Intrusion Detection System is to achieve less complex structure and faster system response time by implementing Multi-agents.

| Protocol | Normal Packets | Abnormal Packets | Total Packets | Percentage |
|---|---|---|---|---|
| TCP | 8950 | 175 | 9125 | 1.92% |
| UDP | 14560 | 294 | 14854 | 1.98% |
| ICMP | 2486 | 25 | 2511 | 0.99% |

Table1. protocol types for Anomaly detection

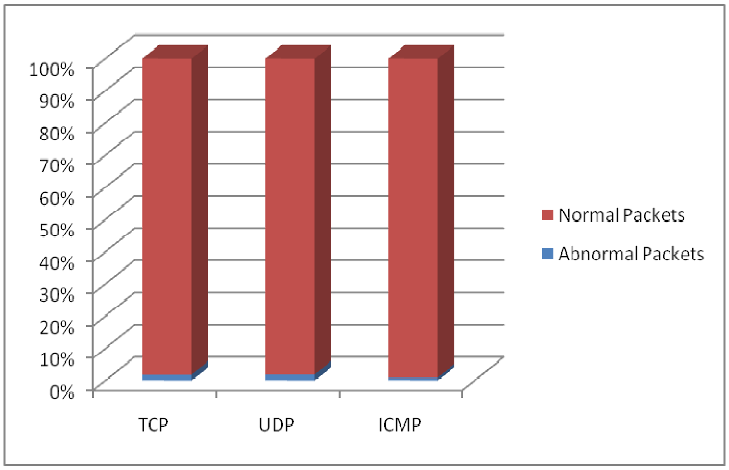

Figure. 3 Illustrates Capture Packet and Anomaly Detection

## 9. CONCLUSION

In this work we description of new NIDS framework using anomaly detection agent, is presented which based on multi agent approach as well as Adoptive Threshold Algorithm, in order to form efficient NIDS system which will deals with anomaly from intruder. So; using multi-agent and Adoptive Threshold Algorithm technology in developing intrusion detection Systems provides many features that improve the performance of these systems. Collaborative multi-agent between them and information sharing may thus improve the overall rate of detecting intrusions. For the anomaly detection system used multiagent and Adoptive Threshold Algorithm is implemented in order to achieve accurate identification unknown attacks. Also improved Network Intrusion Detection System is to achieve less complex structure and faster system response time, and to provide a stronger protection to the system from all types of intrusion attacks with less system processing time.

## REFERENCES

[1] Wang. H., Zhang.D., and Shin.K.G., "Detecting syn flooding attacks" , In Proceedings of IEEE INFOCOM (2002).

[2] Thottan, M, and Ji, C., "Anomaly detection in ip networks", In IEEE Trans. Signal Processing (Aug. 2003), pp. 2191 { 2204.

[3] Deri, L., Suin, S., and Maselli, G., "Design and implementation of an anomaly detection system: An empirical approach", In Proceedings of Terena TNC, 2003 .

[4] Member-Haining Wang and Member-Danlu Zhang and Fellow-Kang G. Shin, "Change-point monitoring for the detection of dos attacks" , IEEE Trans. Depend-able Secur. Comput. 1, 4 (2004), 193{208.

[5] Barford, P, Kline J Plonka D, and A, Ron, "A signal analysis of network traffic anomalies", In Proceedings of ACM SIGCOMM Internet Measurement Work-shop (Marseilles, France, Nov. 2002).

[6] Cliff C. Zou, Member, IEEEWeibo Gong Fellow IEEE Don Towsley Fellow IEEE, and Lixin Gao, Member, IEEE, "The monitoring and early detection of internet worms", IEEE/ACM Transactions on Networking 13, 5 (Oct. 2005).

[7] Gilles Balmisse. Les agents, 2002.

[8] Christophe Pincemaille, Intelligent agent technology, Cork Institute of Technology, 2008.

[9] Fabio Bellifemine1, Agostino Poggi, and Giovanni Rimassa " Developing Multi-agent Systems with JADE",2004, http://www.abdn.ac.uk/~csc232/teaching/CS4027/abdn.only/jade_book.pdf

[10] Muhammad Qasim Ali, Adaptive Thersholding for Anomaly Detection Systems, National University of Sciences and Technology, Pakistan, master thesis, 2009.

[11] Hakan Albag " Network & Agent Based Intrusion Detection Systems" , Istanbul, http://www.model.in.tum.de/um/courses/seminar/worm/WS0405/albag.pdf

[12] M. Benattou, and K. Tamine, " Intelligent Agents for Distributed Intrusion Detection System ",World Academy of Science, Engineering and Technology, 2005 http://www.waset.org/journals/waset/v6/v6-45.pdf

[13] Vasilios A. Siris , Fotini Papagalou "Application of anomaly detection algorithms for detecting SYN flooding attacks", Institute of Computer Science, Hellas,2004. http://www.ist-scampi.org/publications/papers/siris-globecom2004.pdf

[14] Allam Appa Rao, P.Srinivas, B. Chakravarthy, K.Marx, and P. Kiran "A Java Based Network Intrusion Detection System (IDS)", Andhra university college of engineering , India, proceeding of the 2006 IJME-INTERTECH Conference.

[15] Kalle Burbeck, "Adaptive Real-time Anomaly Detection for Safeguarding Critical Networks", Sweden, 2006, http://liu.diva-portal.org/smash/get/diva2:21588/FULLTEXT01

[16] Gaia Maselli , Luca Deri, Stefano Suin "Design and Implementation of an Anomaly Detection System: an Empirical Approach" http://luca.ntop.org/ADS.pdf

[17] Ozgur Depren, Murat Topallar, Emin Anarim, M. Kermal Ciliz, "An intelligent intrusion detection system(IDS) for anomaly and misuse detection in computer networks", expert systems with applications29(2005).[12]