IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AN EVALUATION ON CLUSTER BASED HYBRID INTRUSION DETECTION SYSTEM WITH FAULT TOLERANCE

[1]Author Kamal Kishore Prasad- [2]Author Dr. Rajendra Singh Kushwar

[1]Author Research Scholar and [2]Author Professor –Computer Application & Science department of Sri Satya Sai University of Technology & Medical Sciences-Sehore-MP

ABSTRACT

In the distributed intrusion detection method, the agent can travel from one node to an alternate node within a network and perform the errand concurrently and autonomously in various cycles over the distributed system. The proposed architecture is made out of three layers: Layer 1 consists of host agent and net agent. Layer 2 has the mobile agent and Layer 3 contains the decision making and replication agents. The layers in the system are arranged into network and mobile agent layers, and they send messages to the system administrator utilizing a decision making agent. They are further arranged into replication agent and profile database. The decision making agent triggers the 6 messages, for example, REQUEST, REPLY, CANCEL and ACK because of the execution of applications. The replication agent generates the control messages including CALL and REPORT because of the execution of the intrusion detection procedure.

KEYWORDS: Distributed, Intrusion, Detection, Agent, Layer, Replication.

1. INTRODUCTION

In the distributed intrusion detection method, the agent can travel from one node to an alternate node within a network and perform the errand concurrently and autonomously in various cycles over the distributed system. Subsequently, the agent has equivalent measure of information, and bear equivalent responsibility to take an ultimate conclusion. In any case, a solitary server needs to have enough memory space and processing power in the centralized procedure. Subsequently, the centralized procedure is asset concentrated. In addition, the distributed procedure is more dependable than the centralized procedure because of the nonappearance of single purpose of disappointment. Additionally, they are effectively adaptable. The data is gotten from the static agent and the mobile agent to decrease the network bandwidth utilization by moving the data analysis computation to the location of the intrusion data. Nevertheless, regardless of every one of its advantages, the distributed summed up intrusion detection procedure has the accompanying limitations. The distributed procedure has considerably decreased the data forensic abilities and throughout the long term, they trade a greater number of messages than the centralized procedure. Henceforth, the communication cost of distributed procedure is exceptionally high. For example, the most proficient distributed procedure proposed has added the concept of mobile agent with distributed intrusion detection environment. An agent in a node can either be a functioning or a receptive component during network implementation. Connections and nodes are responsive components that respond to approaching packets and apply their conduct

to the packet. Contrasted with them, agents are dynamic components. For example, when transport agents, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) respond to outer remarks for sending data, they may generate the fundamental packets for data transmission or generate connection control packets. Another distributed procedure, Hybrid intrusion detection of cluster based network with fault tolerance to detect anomaly detection and strategy detection. It utilizes mobile agent with fault tolerance procedures to kill the holes in data analysis when the system is offline and it can operate in a heterogeneous environment.

2. LITERATURE REVIEW

Ionita, I. and Ionita, L. (2013) depicted a straightforward system based on multi agents for Intrusion Detection, used to keep running on broadly useful gadgets, for example, web servers, this system with extensive information is competent to identify port outputs and "syn" attacks against a particular port, and it is fit to perform activities to keep the suspicious attack. Additionally, by utilizing its component of mobility which is qualities to mobile agents, the system has capacity to ensure a few hosts in a little time outline, by activating agents which go onto the hosts and answer the insurance activities has done on where the attack was detected at first.

Gutierrez, S.A. and Branch, J.W (2013) proposed a blended approach contingent upon the mobile agents for the detection of intrusion (HAMA-IDS). The outline of the system permits the treatment of information straightforwardly to where it is available by means of the use of mobile agents (aglets). In this manner, the technique is based on the platform Aglets for the creation and appropriation of agents. These last ones can move from one post to other to break down packets gathered by the collector agents. The half breed analysis is guaranteed by the analyzers and redirectors agents, with the goal that conceivable attacks could be detected. The proposed approach has the accompanying hypothesizes: o The application for detection of intrusion by mobile agents for the detection of intrusion permit dispersion of the Intrusion Detection system (IDS) (unmistakable from the concentrated systems) o The utilization of a blended approach make utilization of both kind of intrusion detection (situation and behavioral technique) o The platform Aglets permit of this strategy to be use as an administrator of the mobile agents and for their conveyance.

Djemaa, B. and Okba, K.(2012), intrusion detection model based on multi-agents utilizes four sorts of agents are characterized in this system, which are organized in a specific structure. The fundamental agents in each host or toward the start of subnets are normally in charge of performing the basic detection and some separate coordination agents performs the reaction undertaking; they are additionally in charge of breaking down the suspicious behavior artificially that isn't conceivable by lower level agents. Coordination agents are likewise fit to appoint the undertaking to the lower-level related agents. Based on the hierarchical structure, the general depiction of the model is given. By adaptable conventions and relationship among a few components, this model gives dynamic adaptability to the changing condition and attacks. Aside from this the idea of coordination domain which encourages the administration of collaborative detection is additionally proposed. The model gives a theoretical establishment to making of dynamically adaptive intrusion detection system.

Ran, Z. (2012) It has good adaptive limit and grater reaction and treatment on the network condition and discretionary attack strategies, likewise uses different data mining algorithm with linking detection mechanism to void the new intrusion behavior. The most recent mechanism of govern library adopts LFU for the objective of disposal of pervious principles; productively modify the abuse detection of coordinating pace. In the interim, the wellspring of alert, auxiliary detection can viably maintain a strategic distance from the multiple occasions caution marvel caused by a similar attack, it can likewise diminishment the rate of wrong cautions. At the point when the system is attacked or collapsed, dynamic election algorithm of administration agent with the enhanced algorithm Bully timely recuperation system, make the straightforward task of the system has good against destruction ability and self-restoration ability.

Gopalakrishna and Spafford (2017) have displayed the engineering of an intrusion detection system that is worked with a gathering of distributed, self-ruling and helpful agents. In the intrigue based collaboration and correspondence demonstrate proposed by the creators, the agents ask for and get data exclusively based on their interests. The agents can likewise indicate new interests because of another occasion or alarm. As a noteworthy favorable position, the whole system isn't imperiled if an

agent fizzles. Rather, there is an effortless corruption of system performance.

3. RESEARCH METHODOLOGY

The system consists of 3 layers, where each layer has a one of a kind personality. The cycles convey through a coherent communication channel by message passing. There is no shared memory in the system. The messages are conveyed at the destination in a similar request as sent by the sender, with subjective yet limited deferral. The messages are neither lost nor copied and the whole system is sans fault. The layers in the system are arranged into network and mobile agent layers, and they send messages to the system administrator utilizing a decision making agent. They are further arranged into replication agent and profile database. The decision making agent triggers the 6 messages, for example, REQUEST, REPLY, CANCEL and ACK because of the execution of applications. The replication agent generates the control messages including CALL and REPORT because of the execution of the intrusion detection procedure. The proposed architecture is made out of three layers: Layer 1 consists of host agent and net agent. Layer 2 has the mobile agent and Layer 3 contains the decision making and replication agents.

3.1 Layer 1 Architecture:

Layer1 encases the host agent and net agent. Each host agent and net agent in the network has the overall intrusion detection and response functions, measures the information and based on this processing makes a decision. A host agent or net agent generates an ID (Intrusion Detection) occasion when it detects dubious exercises may or may not be an intrusion. Instances of such exercises are dubious connections, fizzled login endeavors, modification of system delicate document from dubious users. The ID occasions identified with such dubious conduct are sent by the host agent or net agent to the mobile agent in layer 2.

- **Host Agent:**

The imperative objective of a host agent is to distinguish unapproved users before they get access or during the way toward getting access. The errand of the host agent is to secure the systems accessible in its environment host agent intrusion detection system to assess data that begin from application logs and working system occasion logs. These host occasion logs incorporate proof about record gets to and program performances related with special users.

- **Net Agent:**

The job of the net agent is to detect network intrusions and forestall network intruders from outside sources. Generally net agents are introduced at the passage of the network or on the server. The net agent controls the network traffic, records all speculated occasions in a database and responds to intrusions. The manner in which the net agent manages the intrusions is equivalent to host agent. In layer 1, the net agent distinguishes whether the user is approved or unapproved.

3.2 Layer2 Architecture:

Layer 2 consists of mobile agents dispatched by layer 3 for the continuous observation of the host and net agent in layer1. The mobile agent visits all the hosts in the network and gathers the connected attack data information. Then it relates the gathered information with the data it has gotten from the other host agent or net agent that has generated a similar sort of ID occasion. The MA conveys alerts when it detects intrusions. On one hand it informs each host it has visited to take the corresponding response gauges and demonstrate the alerts; on the other hand, it sends this connected information to layer3 and shows them on the user interface.

3.3 Layer3 Architecture:

Layer3 has the Decision-making Agent (DA), Replication Agent (RA) and Profile Database (PRDB).

- **Decision-making Agent (DA):**

Decision-making Agent (DA) is the most noteworthy element and utilizations MA to control and organize with each host agent and net agent in this system. It commands the agent to execute explicit functions, for example, updating document manages dynamically. DA is the core of the whole framework. DA is responsible for the analysis of the information gathered by MAs.

- **Replication Agent (RA):**

Replication Agent (RA) is responsible for replication and recuperation management. In other words, for the organization of the gathering of recreated agents, adding or eliminating an agent from a gathering; for the strategies of replication of each gathering and alteration

is important; for the consistency of the imitations. The replication is straightforward to the agents. Only RA knows the gatherings, the strategies and the number of reproductions in each gathering. RA knows about the localization of the dynamic agents and its reproductions.

- **Profile Database (PRDB):**

PRDB is the database of profiles. It stores the information identified with the standard conduct of every agent on the network. All the approved actions of every agent in the system ought to be enrolled, other than the agents that can send solicitations to agents that are enlisted. DA utilizes this information during the time spent evaluation for the detection of malicious agents.

- **Fault Tolerance:**

Fault tolerance can be a sensible or an actual one. The decision-making agent examinations the data gathered by MA and pass the control to replication agent. In the event that it is a coherent issue the RA amends the network. In the event that it is an actual issue it sends a SMS to the network administrator. At the point when the user signs on the specific system, the user id and system subtleties are imparted to the manager on the server side.

4. DATA ANALYSIS

4.1 Creating a Topology

This construction is established for a wireless network based topology plan where all nodes are placed at a particular distance. The nodes are physically interconnected without using any cables. The construction is appeared in Figure 1. The packet is transmitted and gotten based on wireless gear. The sink is at the focal point of the circular detecting area.

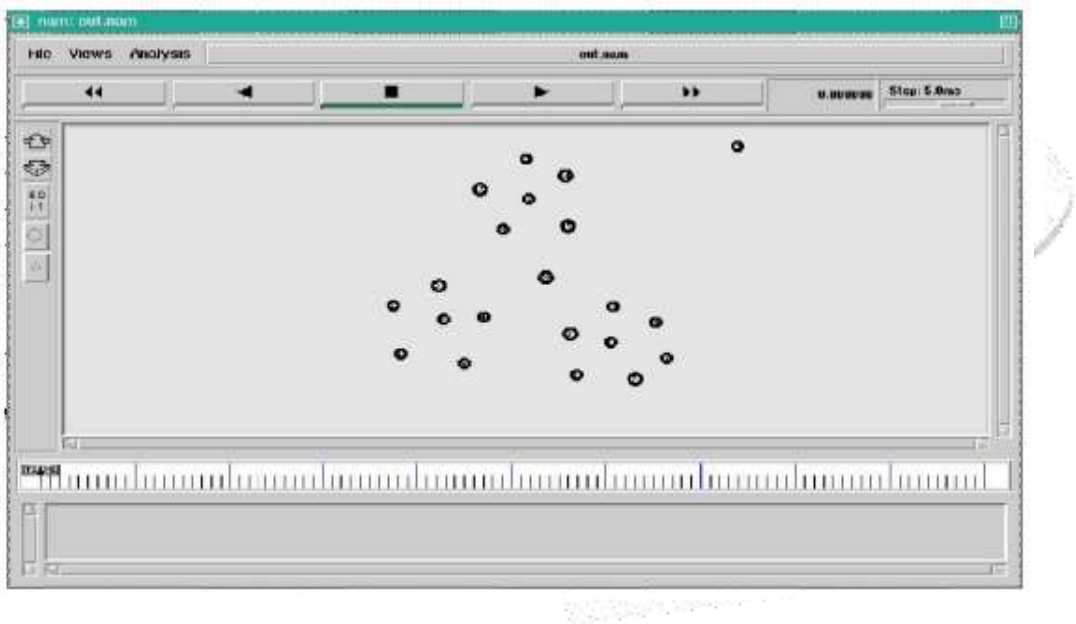

Figure 1: Creation of a Wireless Network Based Topology

4.2 Data Transmission in the Network

This construction is created for node formation where in excess of 10 nodes are situated at a particular distance. Wireless nodes are placed in the intermediate area. Each node knows its location relative to the sink and is programmed with the total number of nodes in the network.

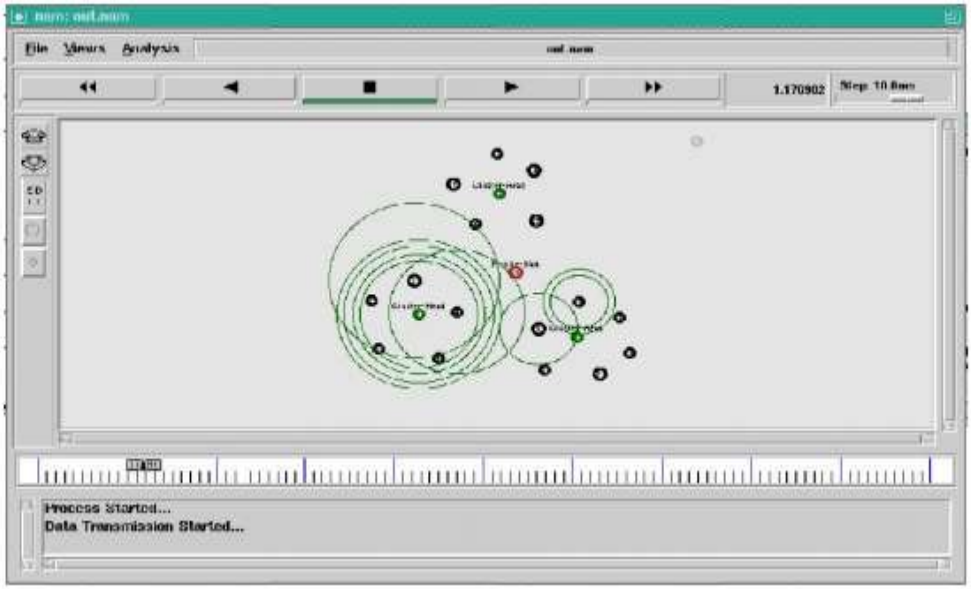

Figure 2: Node Coverage Areas on the Network

The node coverage areas of the network are portrayed in Figure 2. Wireless nodes have a transmitter and recipient. Each node knows its area and transmits the data in their coverage area of the network.

4.3 Cluster Data Transmission

In each clustering unit, a particular sort of node named the head node is chosen to detect development inside the small network. The Cluster Head (CH) performs data separating on the raw data abusing potential data redundancy and forward the sifted information to their BS (Base Station).The concept of data transmission is appeared in Figure 3.

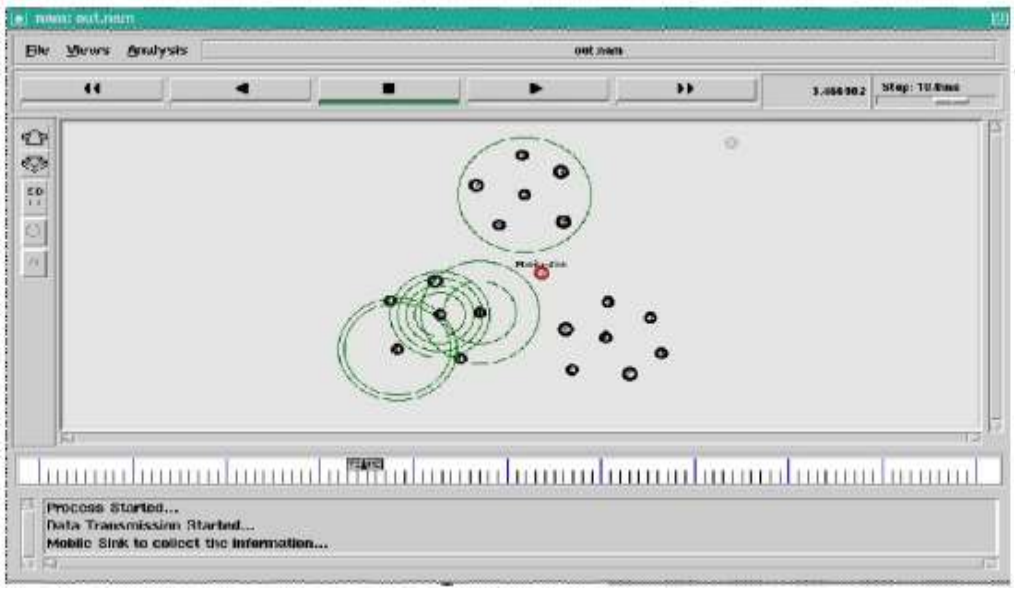

Figure 3: Cluster Node Data Transmission

The performance improvement of cluster head over alternative approaches has been validated by broad simulation tests. The network may contain a large number of nodes; each node visit may take a long time. To save the energy, nodes may turn on their transceivers only when they need to send or relay packets. In the Figure 4, the clusters are picked by the cluster head, yet it changes dynamically in this network. The proposed approaches also have a dynamic cluster model to actualize, for achieving energy efficiency and diminishing packet collisions in this way bringing about improved network throughput under high load.

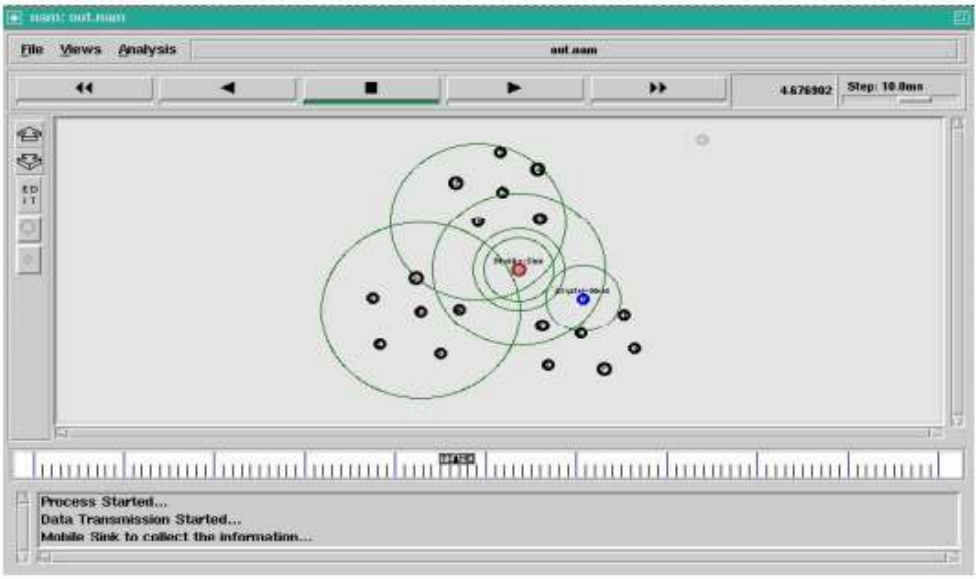

Figure 4: Creating a Dynamic Cluster

4.4 Malicious Nodes on Network

On the off chance that the malicious nodes lead to attacks on the network, then the network performance is diminished and the data could be lost. The attacks can appear from numerous points of view, for example, shrouded data, data misfortune, duplicate packets and data hacked from original data. Figure 5 shows the malicious nodes in red tone.

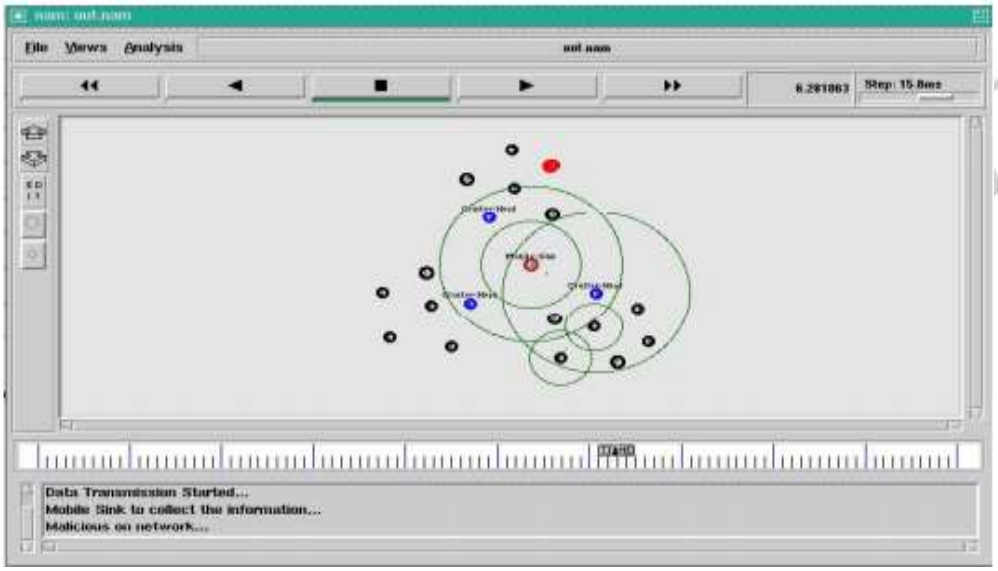

Figure 5: Malicious Nodes on Network

4.5 Removing Attacks Node from the Network

Comparing the current and proposed method, cluster based dynamic IDS eliminates the malicious attacks as well as give proficient transmission on the network. After recognizing the malicious node, the cluster head sends the information to the base station on the network. In the event that a malicious node is recognized, then the node is taken out from the network with the assistance of mobile node. Figure 6 displays the design without malicious node. It gives a more successful outcome which is a helpful cycle on the cluster based network as mobile node based data transmission enables fast access to the data transmitted from source to destination on the system.

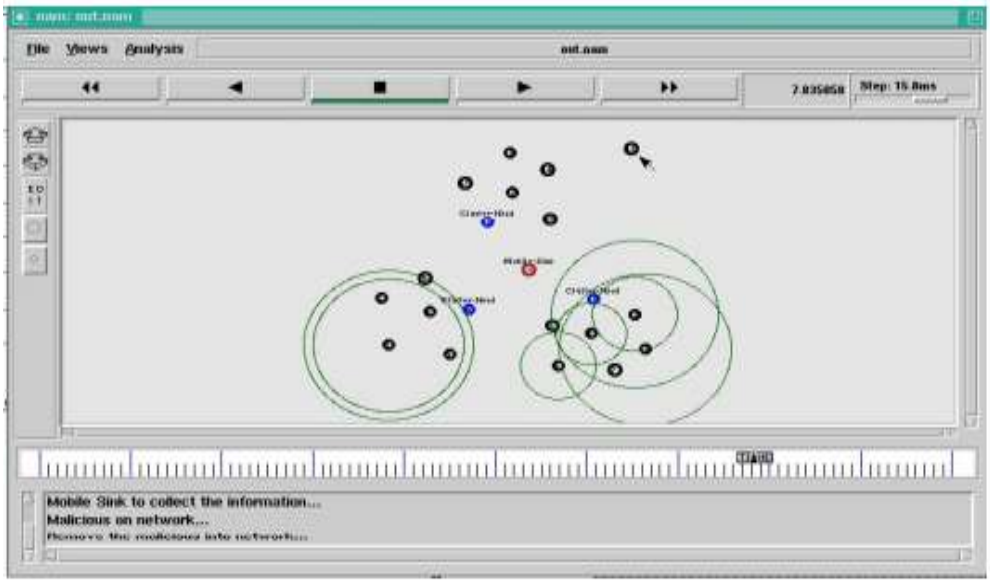

Figure 6: Remove the Malicious Node on Network

5. CONCLUSION

This theory proposes a versatile fault tolerant mobile agent based intrusion detection system. This system has four significant parts in particular group arrangement, mobile agent server, mobile assistance agent and incorporated authoritative server. The bunch arrangement is engaged with getting sorted out a mobile network into various groups. Utilizing a standard political race calculation, the focal point of a bunch is processed dependent on hash esteems and this is assigned as the group head. The Mobile Agent Server (MAS) goes about as the top of the whole network. All nodes in a bunch are associated with the MAS. The MAS is liable for performing host agent and network agent exercises.

REFERENCES

[1]. Ionita, I. and Ionita, L. (2013) An Agent-Based Approach for Building an Intrusion Detection System. RoEduNet International Conference 12th Edition on Networking in Education and Research, Iasi, 26-28 September 2013, 1-6. http://dx.doi.org/10.1109/RoEduNet.2013.6714184

[2]. Gutierrez, S.A. and Branch, J.W. (2013) A Preliminary Application of Mobile Agents to Intrusion Detection. 47th International Carnahan Conference on Security Technology (ICCST), Medellin, 8-11 October 2013, 1-4. http://dx.doi.org/10.1109/ccst.2013.6922045

[3]. Djemaa, B. and Okba, K. (2012) Intrusion Detection System: Hybrid Approach Based Mobile Agent. International Conference on Education and e-Learning Innovations (ICEELI), Sousse, 1-3 July 2012, 1-6. http://dx.doi.org/10.1109/iceeli.2012.6360647

[4]. Ran, Z. (2012) A Model of Collaborative Intrusion Detection System Based on Multi-Agents. International Conference on Computer Science & Service System (CSSS), Nanjing, 11-13 August 2012, 789-792. http://dx.doi.org/10.1109/csss.2012.202

[5]. R. Gopalakrishna and E. Spafford, "A Framework for Distributed Intrusion Detection using Interest Driven Cooperating Agents", in Proceedings of Recent Advances in Intrusion Detection, 4th International Symposium (RAID 2017), October 2017.

[6]. S.R. Snapp, J. Brentano, and G.V. Dias, "DIDS Distributed Intrusion Detection System-Motivation, Architecture and an Early Prototype", in Proceedings of the 14th National Computer Security Conference, July 2018.

[7]. Banik, S.M. and Pena, L. (2015) Deploying Agents in the Network to Detect Intrusions. IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS), Las Vegas, 28 June-1 July 2015, 83-87. http://dx.doi.org/10.1109/ICIS.2015.7166574

[8]. Can, O. (2014) Mobile Agent Based Intrusion Detection System. 22nd Signal Processing and Communications Applications Conference (SIU), Trabzon, 23-25 April 2014, 1363-1366. http://dx.doi.org/10.1109/SIU.2014.6830491

[9]. Abdurrazaq, M.N., Bambang, R.T. and Rahardjo, B. (2014) Distributed Intrusion Detection System Using Cooperative Agent Based on Ant Colony Clustering. International Conference on Electrical Engineering and Computer Science (ICEECS), Kuta, 24-25 November 2014, 109-114. http://dx.doi.org/10.1109/ICEECS.2014.7045229

[10]. Biswas, A., Sharma, M., Poddder, T. and Kar, N. (2014) An Approach towards Multilevel and Multiagent Based Intrusion Detection System. International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), Ramanathapuram, 8-10 May 2014, 1787-1790. http://dx.doi.org/10.1109/icaccct.2014.7019417