International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 6, December 2019, pp. 4951~4960
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i6.pp4951-4960

An adaptive distributed intrusion detection system architecture using multi agents

Riyad A. M.[1], M. S. Irfan Ahmed[2], R. L. Raheemaa Khan[3]
[1]Department of Computer Science, EMEA College of Arts and Science, India
[2,3]Department of Computer Applications, Nehru Institute of Engineering and Technology, India

Article Info

Article history:

Received Jun 29, 2018
Revised May 10, 2019
Accepted Jun 26, 2019

Keywords:

Data mining
Distributed agents
Intrusion detection system
JADE
Network security

ABSTRACT

Intrusion detection systems are used for monitoring the network data, analyze them and find the intrusions if any. The major issues with these systems are the time taken for analysis, transfer of bulk data from one part of the network to another, high false positives and adaptability to the future threats. These issues are addressed here by devising a framework for intrusion detection. Here, various types of co-operating agents are distributed in the network for monitoring, analyzing, detecting and reporting. Analysis and detection agents are the mobile agents which are the primary detection modules for detecting intrusions. Their mobility eliminates the transfer of bulk data for processing. An algorithm named territory is proposed to avoid interference of one analysis agent with another one. A communication layout of the analysis and detection module with other modules is depicted. The inter-agent communication reduces the false positives significantly. It also facilitates the identification of distributed types of attacks. The co-ordinator agents log various events and summarize the activities in its network. It also communicates with co-ordinator agents of other networks. The system is highly scalable by increasing the number of various agents if needed. Centralized processing is avoided here to evade single point of failure. We created a prototype and the experiments done gave very promising results showing the effectiveness of the system.

Corresponding Author:

Riyad A. M.,
Department of Computer Science,
EMEA College of Arts and Science,
Kumminiparamaba (PO), Kondotty, Malappuram District, Kerala, 673638-India.
Email: amriyad@yahoo.com

1. INTRODUCTION

The threats through the network raise big concerns to the day to day activities in the computer network. It has been a very challenging task for the security analysts and administrators for a very long time. Various hardware and software systems are being deployed for eliminating intrusions. A system is said to be secure if the confidentiality, integrity and availability is maintained [1]. Intrusion detection systems are believed to be the last line of defense in the network security. These are the systems which monitors, analyze and find abnormal patterns. The patterns may resemble a previously known signature or it may be a new attack. It is the intelligence of an intrusion detection system (IDS) to identify whether it is an attack or not. Failing in this can increase the false positives and false negatives.

Here, we address the serious problems prevailing with respect to the current intrusion detection systems. The IDS are usually centralized in nature at least with respect to processing of data. This leads to single point of failure. Moreover, it usually fails miserably in distributed types of attacks like distributed denial of service. Learning the entire network and acting accordingly is a very tedious task for a centralized system and even for the distributed ones without a proper framework. It usually needs to move bulk amount

of data from one place to another for analysis which inturn increase the network load. It doesn't have the support of other similar entities to know any previously learnt information in the network. This can increase false positives. Since the detection components are less in most of the IDSs, the time taken for analysis is also higher. Adaptability to the new scenarios is also difficult due to the absence of a proper framework with components that can communicate seamlessly.

All the issues identified above confirm the necessity for proposing a proper distributed intrusion detection system architecture with various components that can solve the existing concerns [2]. In order to develop such an intrusion detection system, we used the support of mobile agents [3, 4]. Even IDS with mobile agents could be a failure if they are not deployed in a planned manner. A well planned framework with various mobile agents and well supported coordinator agent can resolve the current issues in intrusion detection systems. A mobile agent is a program with its data which is capable of migrating from one host to another and continues its execution in an autonomous fashion. This is the striking feature of an agent which can be utilized in IDS for moving the process to the data rather than moving data to the process for analysis that increases the network traffic load. Since the agents are autonomous in nature no user intervention is needed for its functioning. They are also pro-active in nature and can take necessary preventive actions on the events that can lead to intrusions. The interaction capability with other agents helps in fast analysis and decision making. As the number of agents can easily be increased with the increasing load of the network, the system is easily scalable. Moreover, there is no single point of failure. Fault tolerance is high since one agent can substitute another if needed. Parallel analysis of the events can be achieved using multiple agents which reduce the time taken for analysis significantly. Handling of duplicate alerts from same event can be discarded by proper coordinaton between the agents. This extensively reduces false positive alarms [5, 6]. Moreover, an unidentified novel attack due to the spacial limitations of a detection component can be discovered by the coordinated effort of various components in the detection framework [7, 8]. A novel architecture is proposed here that can resolve the current issues of the existing IDS. We use JADE environment for deploying multiple agents for intrusion detection.

The rest of the paper is organized as follows. Section 2 details the related literatures done on agent based distributed intrusion detection, Section 3 describes the proposed architecture in which the IDS works, Section 4 explains the communication model of analysis and detection agent through which the agent interacts with other entities, section 5 discusses on the implementation and the results obtained and Section 6 concludes the paper.

2. RELATED WORKS

Network security is all about assuring availability, integrity and confidentiality for critical information. The concept of intrusion detection was introduced by James P Anderson. In 1980 he published a technical report on intrusion detection systems. Here, he discussed about host based audit data and logs [9]. Intrusion detection can be anomaly based, misuse based or combinational approach [10]. Misuse detection is conducted with the help of previously available signatures of known attacks. On the other hand, anomaly detection is done by noticing the deviations from normal behaviors.

In conventional approach for intrusion detection, a central IDS monitors the entire network for detecting intrusion. This leads to various drawbacks which gave way to more versatile distributed intrusion detection systems [11]. The hierarchical arrangement of various entities of IDS is also a drawback because a compromised node up in the hierarchy can bring down the entire security system. Hence, in a couple of decades it have been identified that, the single IDS scenario needs to be replaced with distributed IDS. The present IDS should be capable of detecting distributed attacks. Some of them are coordinated ones [12]. Thus the current circumstances demands distributed IDS supporting heterogeneous environments and which can seamlessly communicate with its components and scale according to the requirements of the network [13].

A distributes IDS framework known as EMERALD was introduced by Philip A Porras and Peter G Neumom [14]. It provides a highly distributed architecture by deploying surveillance and response monitors in various abstract layers in a network. A Java agent for meta-learning (JAM) is a multi agent technique finding intrusions using data mining approach. Association rules and frequent episodes mining are used on audit data and a meta-classifier is used to learn signatures [15]. Lin Jianxiao and Li Lijuan introduced an agent based IDS [16]. There are no control servers in this system and claims realistic distributed detection. Each components of the system is independent to each other and also eliminates single point of failure. AAFID is another distributed IDS architecture developed by Eugene H Spafford and Diego Zamboni at CERIUS, Purdue University [17]. It uses agents for collecting the data which resides in the bottom of agent's hierarchy. Upper levels constitutes with the agents for coordination and aggregation.

The latest distributed intrusion detection systems uses mobile agent technologies which reduces network load, collaborative detection and decision making, independent and automated processing, adaptable to future threats and provides excellent fault tolerance mechanism [18, 19].In a multi agent IDS developed by Hancock D L and Lamont G B, flow based IDS is introduced in which reputation is used to select nodes that is most capable of identifying threats. El Ajjouri M, Benhadou S and Medromi H introduced an architecture in which learning features are added where novel attacks are found [20] It provides high adaptability to future unknown threats.

3. THE SYSEM ARCHITECUTRE

We propose a decentralized system in which various agents in collaboration will collect the network data, analyze and identifies the intrusions. The appropriate actions are taken according to the response plan. The events are reported to the administrators as well.

According to this intrusion detection strategy, all the data to the network passes through a co-ordinator agent of the network. The deployment of the co-ordinator agents strategically on each network will facilitate the exchange of valuable information among networks. There are various sniffer agents distributed in the network for collecting network data and send them to the filtering agents nearby. After the preprocessing activities done by the filtering agent, analysis agents collects the preprocessed data stored by the filtering agents for analysis and detection of various kinds of threats. Synchronization with the co-ordinator agent and with other analysis agents in the network is achieved for obtaining better results.

Alerts are generated for the occurrence of attacks and necessary response measures are taken according to the pre-defined response plans to various categories of attacks. An admin log is maintained by the co-ordinator for the verification of critical events happened in the network. Figure 1 depicts the system architecture.

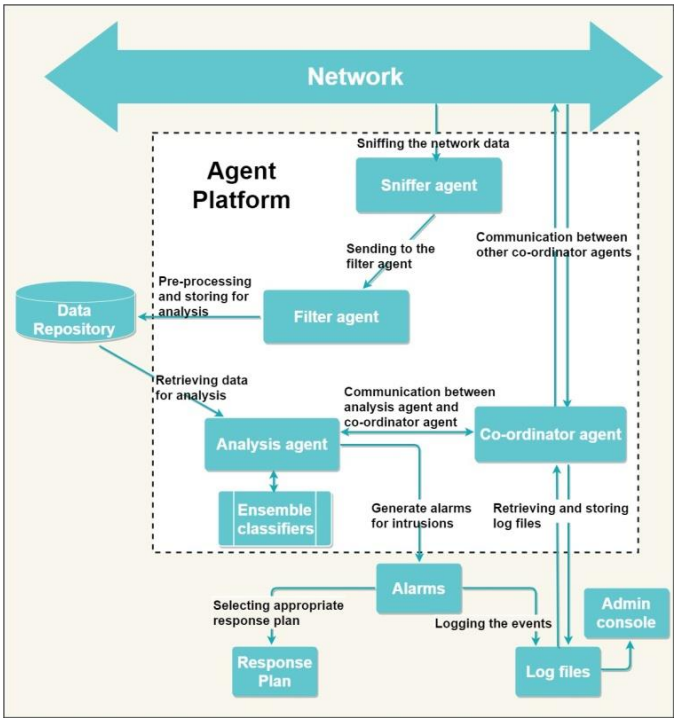

Figure 1. The proposed system architecture

3.1. Co-ordinator agent

The co-ordinator agent in the network passes information among the agents in the same network and the co-ordinators of other networks. The co-ordinator has log files regarding the security threats encountered by the network that can be collected by other co-ordinators agents of other networks. The co-ordinator agent of the network receives similar security information from the co-ordinator agents of other networks which is very useful to find the distributed type of attacks. A feed back from various analysis and detection agents helps the co-ordinator agent for providing valuable recommendations for reducing false positives.

3.2. Sniffer agent

At the initial stage, various sniffer agents are created and deployed in the network for monitoring the network. These sniffers are placed near almost every host in the network. The network data obtained by the sniffers are send to the filtering agents which is available in all hosts for preprocessing and arranging the data for the analysis purpose.

3.3. Filtering agent

The network data obtained from the sniffer agent is filtered by removing unwanted data and necessary preprocessing is done by selecting the relevant features by the filter agents. PCA algorithm is used for this purpose [21]. Eventually, these data repositories are used by the analysis agent for further analysis and detection of attacks.

3.4. Analysis and detection agent

Analysis and detection agents are the core agents of the architecture where the actual detection of the threats are carried out. For this purpose, analysis and detection agents are created and dispatched to various parts of the network with the help of the JADE platform. An analysis and detection agent can traverse through various hosts containing data repositories generated by the filter agents. These repositories are utilized by analysis and detection agents for intrusion detection. The agents are capable of collecting the data from various repositories one by one for improving the accuracy in analysis to reach a final conclusion. For the analysis purpose, an ensemble classification approach is deployed in the analysis and detection agent. The ensemble classification approaches have outperformed the individual classification approaches in terms of detection rate, accuracy and false positive reduction rate. The classifiers used in our ensemble classification technique are Support vector machine (SVM), artificial neural network (ANN) and Random forest (RF) classifiers. This is a very strong ensemble classification approach for detecting intrusions and false positives are very minimum [22-24]. The final results obtained are shared among various agents in the form of agent's knowledge interaction for increasing the accuracy of the results. The findings are forwarded to the immediate response modules of the agent for taking necessary actions if needed and administrator log files. Immediate response against the real time attacks are achieved by the virtue of response plans prepared for each type of attacks.

A number of analysis agents are created in the JADE platform considering the topology of the network. A single analysis and detection agent is employed for a group of workstations in the network. The groups are discovered on the basis of network equipments such as routers and switches by considering the collision domain. An agent is capable of moving from host to host in its territory for analysis and detection. In order to make sure an analysis agent never interfere with another one and is confined to its territory, an algorithm is proposed which is given below.

Algorithm TERRITORY

1. Set Route to NULL
2. Label the home workstation as x and add it to the own territory OT. Label x as "occupied".
3. If there is undiscovered edge e for the node x, Label the link L_x(e) as "OT-Link" and move to next node y.
4. If flag of the node y is set as "occupied" then
   Go back to x and label the link L_x(e) as "Non-OT-Link".
   Else
   Set flag of the node y as "occupied". Include link L_y(e) to Route, include edge e and node y to OT
5. Repeat 3 till all edges are discovered.
6. When no undiscovered edge is left,
   If Route not NULL then
   Move to the last link in the Route and delete the last link entry from Route and repeat 3.
   Else
   Return OT

Algorithm 1. Territory algorithm to avoid interference of one analysis agent with another agent

4. ANALYSIS AND DETECTION AGENT COMMUNICATION MODEL

The Figure 2 depicts the communication layout of the analysis and detection agent with other modules. Analysis and detection agents are true mobile agents which reside in the various parts of the network. These are the primary detection modules of the network. These agents interact with other agents in the same network for determining the accuracy of the detection as well as for identifying the distributed

attacks. Each agent is capable of communicating with the co-ordinator agent of the network for exchanging the findings.

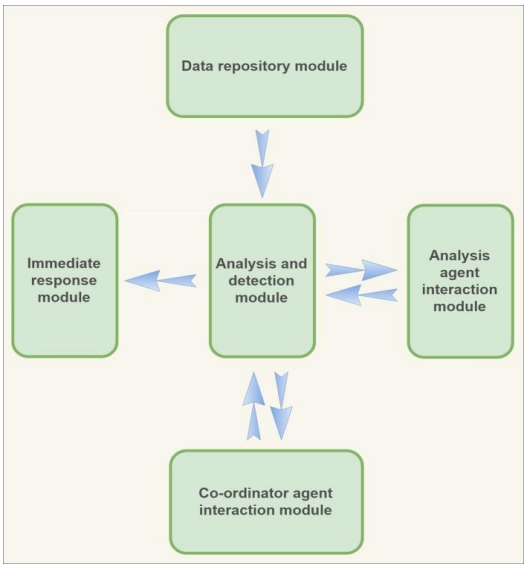

Figure 2. Communication between the analysis and detection module with other modules

4.1. Analysis and detection module

This is the main part of the distributed intrusion detection architecture where the data is classified to either normal or intrusion by the help of ensemble classification approach. Here, SVM, ANN and RF classifiers individually classify the data. But, the final decision is done by the ensemble approach in which each classifiers is given a weight from 0 to 1 with respect to accuracy. If the classifiers agree each other, the classification is done accordingly and if they disagree to each other, the decision of the classifier with the highest weight is taken in to consideration. The final findings are used for the response purpose and also shared between other analysis and detection agents and co-ordinator agent.

4.2. Distributed data repository module

These are repositories where the filtered and pr-processed data is stored for the analysis. The data provided by the sniffer agent is pre-processed by the filtering agents and set for the analysis and detection agent. Analysis and detection agent arrives in the host in which the data repositories are prepared by the filter agents for analysis and detection. This is a huge advantage of this architecture since no massive data is transferred between agents for analysis. Only the findings are communicated between various agents in a secured manner.

4.3. Analysis agent interaction module

The module facilitates the communication between various agents in the same network for gaining confidence of their findings as well as passing the information about the attacks on various hosts. It also helps to find distributed attacks otherwise impossible. The JADE platform is effectively utilized for the communication passing mechanisms [25].

4.4. Co-ordinator agent interaction module

The overall events on various nodes of the network is monitored and logged by the co-ordinator agent with the support of various other agents in the system. The co-ordinator interaction module of the analysis agent sends the critical security information obtained from the analysis to the co-ordinator agent if needed. Co-odinator agent communicates with the analysis agent for providing various suggessions regarding false positives generated by detection agent and it also provides information on distributed types of attacks. This is the feature of this architecture where more accuracy in the detection can be achieved by reducing the false positives by the virtue of other agents in the network.

The findings made by individual analysis agents are compared and unified for collective decision making for administrators with respect to various events.

$$\text{Normal} = \bigcup_{j=1}^{n} Normal(\text{Analysis agent}_j) \quad (1)$$

$$\text{Attack} = \bigcup_{j=1}^{n} Attack(\text{Analysis agent}_j) \quad (2)$$

5. EXPERIMENTAL SETUP AND RESULTS

For implementing and evaluating the system, we have used KDD cup dataset. Usually cross validations like 10-fold cross validation is used for the evaluation purpose. In these validations, same class of training data is used without adding any new class during testing. This may increase the performance with respect to detection accuracy and detection rate. But, as we concentrate on the capability of IDS to detect new attacks, we use 10% KDD cup dataset for training purpose and corrected dataset for testing purpose.

JADE (Java agent development framework) is used to implement multi agent systems. JPCAP (Java library for capturing and sending network packets) is used for communication purpose. An agent can discover another agent in runtime and pass massages each other. The framework is built using JDK 1.4.1, JADE 3.7, eclipse and JPCAP 0.7.

5.1. The experimental layout of the system

The layout for conducting the experiment is given below in the Figure 3. As in Figure 3, a network environment is set up in which various workstations were deployed by connecting them with switches. All workstations are configured with core i7 3.4 GHz processor with eight cores and 8 GB RAM. Operating system used was Windows 8.1 with 64 bits. Agents were deployed through JADE platform. The number of agents generated depends according to the number of switches in the network. Co-ordinator agent aids in summarizing and logging the events for future verification by the administrators. All the packets to the outside networks pass through the router and firewall.

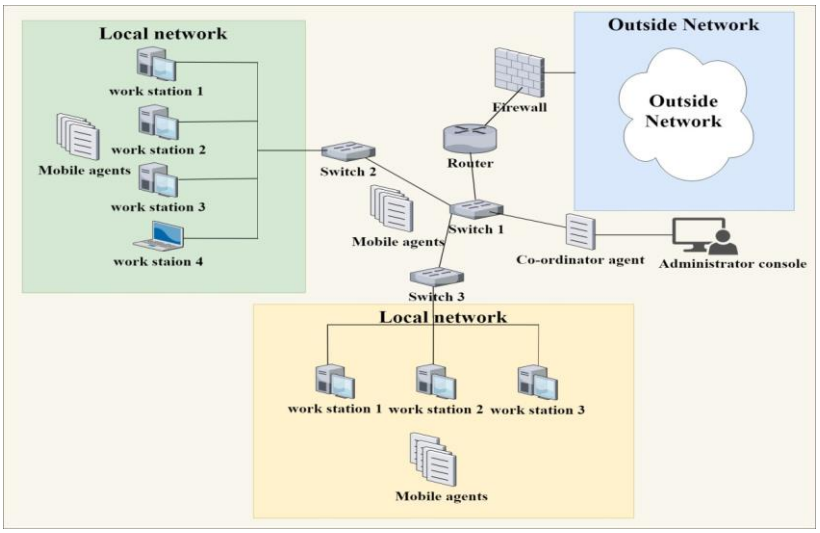

Figure 3. Experimental layout of the system

5.2. Results

In order to verify the performance of our intrusion detection model, comparisons with other techniques are done. We used randomly generated training dataset from 10% of KDD cup dataset. Testing dataset is taken from the corrected KDD dataset. Detailed information on KDD cup dataset can be found from the literatures [26, 27]. Three key measures used for the evaluation purpose are accuracy, detection rate and false alarm rate.

$$\text{Accuracy} = \frac{\text{True positives} + \text{True negatives}}{\text{True positives} + \text{True negatives} + \text{False positives} + \text{False negatives}} \quad (3)$$

$$\text{Detection rate} = \frac{\text{True positives}}{\text{True positives} + \text{False positives}} \quad (4)$$

$$\text{False alarm rate} = \frac{\text{False positives}}{\text{True negatives} + \text{False positives}} \quad (5)$$

The accuracy, detection rate and false alarm rate of our IDS during various testing phases are shown in the Table 1. The consistency of the system with respect to accuracy, detection rate and false alarm rate for different test datasets is given in the Figure 4. The Table 2 compares our results with other techniques [28-30] with respect to normal and four attack types.

Table 1. Accuracy, detection rate and false alarm rate of the proposed IDS during various testing phases

Training dataset	Test dataset	Accuracy	DR	FAR
TrainingSet1	TestSet1	94.21	94.18	0.08
	TestSet2	92.42	96.19	0.09
	TestSet3	94.22	96.89	0.02
	TestSet4	92.65	92.21	0.11
TrainingSet2	TestSet1	93.35	98.62	0.06
	TestSet2	94.66	96.73	0.01
	TestSet3	94.23	95.22	0.19
	TestSet4	95.22	96.99	1.08
TrainingSet3	TestSet1	96.01	90.91	0.05
	TestSet2	93.99	96.23	0.01
	TestSet3	94.76	95.98	0.12
	TestSet4	94.54	99.12	0.03
TrainingSet4	TestSet1	92.12	95.62	0.02
	TestSet2	95.29	96.71	0.01
	TestSet3	93.33	96.01	0.01
	TestSet4	94.71	99.62	0.03

Table 2. Comparison with other techniques with respect to normal and various attack types

Method	Normal	Prob	DoS	U2R	R2L
Our IDS	99.6	92.1	99.9	96.4	91.1
Winner KDD	99.5	83.3	97.1	13.2	8.4
RSS-DSS	96.5	86.8	99.7	76.3	12.4
ESC-IDS	98.2	84.1	99.5	14.1	31.5
Bacon-Perin	99.0	80.0	85.4	94.3	50.0
SVM N-RBF	99.7	98.6	88.7	68.0	24.8

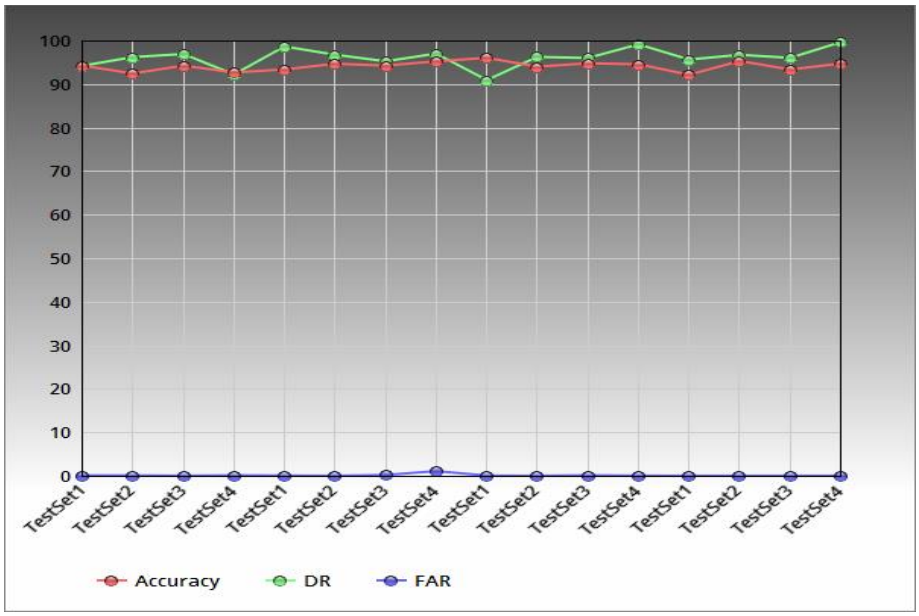

Figure 4. Accuracy, detection rate and false alarm rate for different test datasets

The Table 3 compares our results with other techniques with respect to detection rate and false alarm rate. From the results, it can be found that our IDS is highly promising one. It achieves good results in the detection of various attacks. The false alarms produced are negligible and can be seen from the Figure 5. The Figure 6 depicts the performance comparison of various techniques with respect to normal and other various attack types in the form of bar chart.

Table 3. Comparison with other techniques with respect to detection rate and false alarm rate

Method	DR	FAR
Our IDS	96.1	0.12
Winner KDD	91.8	0.6
RSS-DSS	94.4	3.5
ESC-IDS	95.3	1.9
Bacon-Perin	90.3	99.0
SVM N-RBF	94.9	0.14

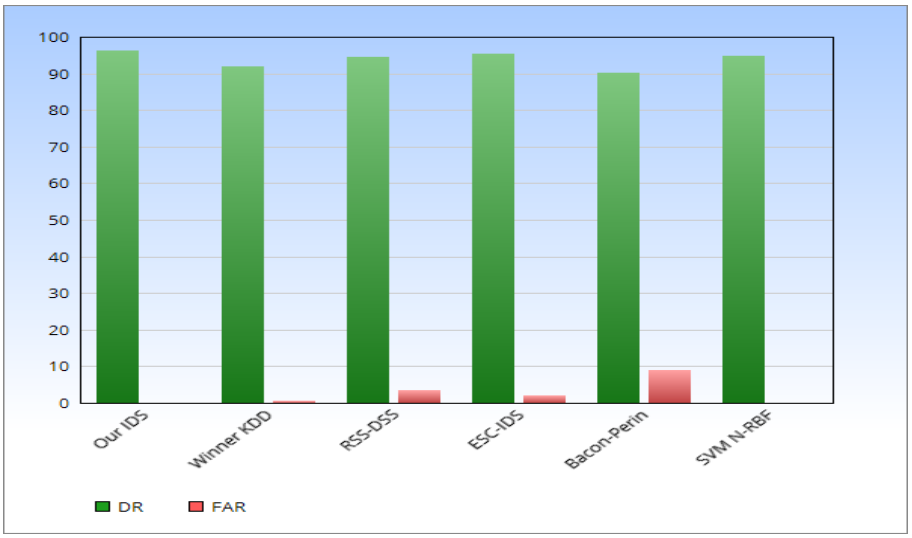

Figure 5. Bar chart showing the detection rate and false alarm rate of various techniques

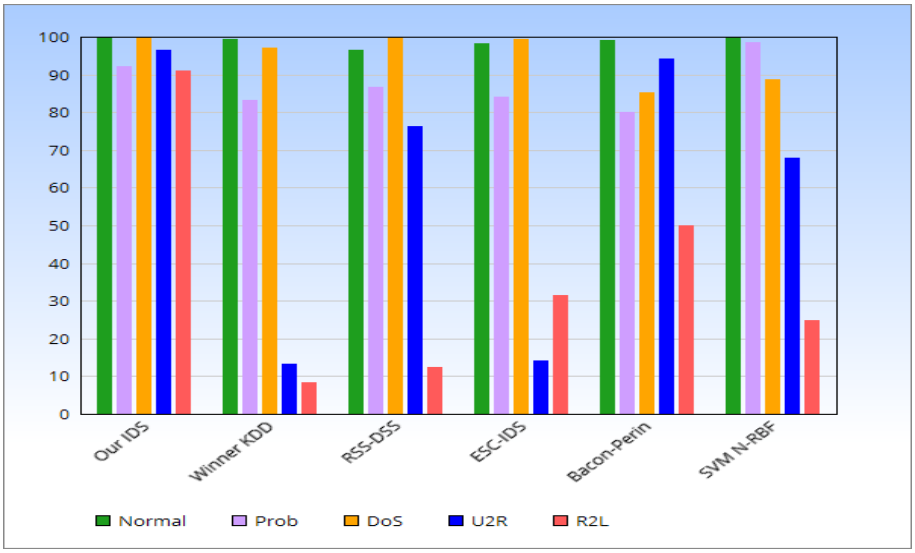

Figure 6. Bar chart showing the normal and four attack types of various techniques

6. CONCLUSION AND FUTURE WORK

In this work, an agent based distributed intrusion detection system architecture is proposed. The system makes use of mobile agents for analysis and detection. This tremendously reduces the network latency since the process moves to the data for analysis. Here, agents analyses and detects in a collaborative fashion facilitating accurate decision making. We used ensemble data mining approach for effective intrusion detection. As agents are distributed throughout the network, the system is capable of finding distributed and collaborated attacks. Moreover, the co-ordinator agent does the summarizing and logging activities of a network. It also has communication facilities with co-ordinator agents of other networks to perceive a higher picture of the threat scenarios. The analysis agent interacts with other analysis agents and co-ordinator agent which reduces false positives significantly. The system is capable of reacting to threats immediately by using the techniques such as packet discard, resetting the connection and alarming to the authorities. The agents logs necessary information for the reference of administrators. The system has the capability of adapting to future novel attacks with the collaborative efforts of various modules in the architecture. As the agents are autonomous in nature, they are easily capable of substituting a malfunctioning agent providing excellent fault tolerance mechanism. The experiments were conducted in JADE platform for mobile agents and results are highly promising. In the future, more security features are to be implemented such as providing secured connections between agent communications and suggest various protection mechanisms for the agent in a hostile environment. Experiments are also to be carried out in a heterogeneous network environment.

REFERENCES

[1] Liao H. J., *et al*., "Intrusion detection system: a comprehensive Review," *Journal of Network and Computer Applications*, 2013.

[2] G. Folino and P. Sabatino, "Ensemble based collaborative and distributed intrusion detection systems: A survey," *J. Network and Computer Applications*, vol. 66, pp. 1-16, 2016.

[3] D. Boukhlouf, *et al*., "Network security: distributed intrusion detection system using mobile agent technology," *International Journal of Communication Networks and Distributed Systems*, 2016.

[4] C. Jain and A. K. Saxena, "General Study of Mobile Agent Based Intrusion Detection System (IDS)," *Journal of Computer and Communications*, pp. 93-98, 2016.

[5] O. Achbarou, *et al*., "A New Distributed Intrusion Detection System Based on Multi-Agent System for Cloud Environment," *International Journal of Communication Networks and Information Security*, vol. 10, 2018.

[6] Ganapathy S., *et al*., "Intelligent agent-based intrusion detection system using enhanced multiclass SVM," *Computational Intelligence and Neuroscience*, 2012.

[7] Z. Ran, "A Model of Collaborative Intrusion Detection System Based on Multi-agents," *International Conference on Computer Science and Service System*, 2012.

[8] Li Y., *et al*., "A New Distributed Intrusion Detection Method Based on Immune Mobile Agent," *Life System Modeling and Intelligent Computing, ICSEE 2010, LSMS 2010. Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, vol. 6328, 2010.

[9] J. P. Anderson, "Computer security threat monitoring and surveillance," Technical report, James P. Anderson Company, Fort Washington, Pennsylvania, 1980.

[10] H. Debar, *et al*., "Towards a Taxonomy of Intrusion-Detection Systems," *International Journal for Computer and Telecommunications Networking*, vol. 31, pp. 805-822, 1999.

[11] R. Gopalakrishna and E. H. Spafford, "A Framework for Distributed Intrusion Detection using Interest Driven Cooperating Agents," *Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection*, Davis, CA, USA, 2001.

[12] W. Jansen and T. Karygiannis, "Mobile Agent Security," NIST Special Publication 800-19. National Institute of Standards and Technology, Computer Security Division, Gaithersburg, MD 20899 Niklas, 1999.

[13] M. Eid, "A New Mobile Agent-Based Intrusion detection System Using distributed Sensors," *Proceeding of FEASC*, 2004.

[14] P. A. Porras and P. G. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," *National Information Systems Security Conference*, 1997.

[15] S. Stolfo, *et al*., "JAM: Java Agents for Meta-Learning over Distributed Databases," *Proceedings of the 3rd International Conference on Knowledge Discovery and Data Mining, Newport Beach, California*, pp. 74-81, 1997.

[16] L. Jianxiao and L. Lijuan, "Research of Distributed Intrusion Detection System Model Based on Mobile Agent," *Proceeding of International Forum on Information Technology and Applicatio*n, pp. 53-57, 2009.

[17] J. S Balasubramaniyan, *et al*., "An Architecture for Intrusion Detection using Autonomous Agents," *Proceedings of the 14th Annual Computer Security Applications Conference, IEEE Computer Society*, pp. 13-24, 1998.

[18] W. A. Jansen, "Intrusion detection with mobile agents," *Computer communication*, vol. 25, pp 1392-1401, 2002.

[19] C. Kruegel and T. Toth, "Applying Mobile Agent Technology to Intrusion Detection," Technical report, University of Vienna, TUV1841-2002-31, 2002.

[20] E. Ajjouri M., *et al*., "Intelligent architecture based on MAS and CBR for intrusion detection," *Proceedings of the 4th Edition of National Security Days* (JNS4), pp 1-4, 2014.

[21] D. Brauckhoff, *et al*., "Applying PCA for traffic anomaly detection: problems and solutions," *INFOCOM* 2009, pp. 2866-2870, 2009.

[22] A. M. Riyad and M. S. I. Ahmed, "An Ensemble Classification Approach for Intrusion Detection," *International Journal of Computer Applications*, vol. 80, pp. 37-42, 2013.
[23] Shrivas A. K. and Dewangan A. K., "An ensemble model for classification of attacks with feature selection based on KDD99 and NSL-KDD data set," *International Journal of Computer Applications*, vol. 99, pp. 8-13, 2014.
[24] G. Folino, *et al*., "An ensemble-based evolutionary framework for coping with distributed intrusion detection," *Genetic Programming and Evolvable Machines*, 2010.
[25] JADE Board, "JADE Security Add-On GUIDE," *Administrator's guide of the Security add-on*, Version 28-February-2005, JADE 3.3, Copyright (C) 2004, TILAB, 2005.
[26] Tavallaee M., *et al*., "A detailed analysis of the KDD CUP 99 data set," *Proceedings of the 2nd IEEE Symposium on Computational Intelligence for Security and Defense Applications*, pp. 1-6, 2009.
[27] E. Charles, "Results of the KDD'99 Classifier Learning," *SIGKDD Explorations, ACM SIGKDD Explorations Newsletter*, vol. 1, pp. 63-64, 2000.
[28] A. N. Toosi and M. Kahani, "A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers," *Computer communications*, 2007.
[29] A. B. Perin, "Ensemble based methods for IDS," *NTNU*, Trandheim, 2012.
[30] F. Kuang, *et al*., "A novel SVM by combining kernel principal component analysis and improved chaotic particle swarm optimization for intrusion detection," *Applied Soft Computing*, 2014.