IJCRT Publish Paper record is available at DOI: http://doi.one/10.1727/IJCRT.17179

Two Layer Artificial Immune System for Intrusion Detection System

Akshay U. Mahajan

PG Student, Department of Computer Engineering, SSBT's College Of Engineering and Technology, Bambhori, Jalgaon [M.S], India.

Nitin Y. Suryawanshi

Assistant Professor, Department of Computer Engineering, SSBT's College Of Engineering and Technology, Bambhori, Jalgaon [M.S],

***Abstract* - Artificial immune system (AIS) is an immune-based adaptive computational intelligence method used for detecting and preventing computer network threats in intrusion detection systems (IDS). Distributed control, self-organising and multi-layered detection these are the special features those make AIS efficient for intrusion detection. AIS generate antibodies (self) capable of recognizing antigen (non-self), which is considered as an anomaly technique. Whenever the formation of antibodies and antigens (rule formation) in AIS is implemented at two levels, they are termed as Two Level Artificial Immune Systems (TLAIS). TLAIS uses two different algorithms for self and non-self formation in both levels. The inherent characteristics of the algorithms used in TLAIS limit the efficiency of the TLAIS like premature convergence and overfitting. The proposed TLAIS aims to use two efficient algorithms in terms of time and memory to avoid such limitations.**

***Keywords* – Artificial Immune System, Intrusion Detection System, Adaptive Computational Intelligence, Rule-formation, Antibodies, Antigens, Biological Immune System.**

I. INTRODUCTION

The concept of computer network intrusions and attacks is rapidly evolving with the advent of time and technology. Day by day increasing intrusion actions are becoming a serious threat to security of the system and networks, as they pose a direct threat to integrity, privacy and availability of resources. To tackle the continuous evolving attacks an efficient IDS should evolve and change rapidly. Thus, the importance of Intrusion Detection System (IDS) is increasing in the realm of network security.

Intrusion Detection (ID) is concerned all about monitoring, estimating and reporting unauthorised events, malicious attempts. A good IDS develops resources and robust data security mechanisms. Various techniques are used for implementing IDSs such as artificial neural Network (ANN), support vector machine (SVM), genetic algorithms (GA), artificial immune system (AIS) etc. The purpose behind using so many techniques is to find an intelligent defence system with self maintenance, self-learning and adaptability. Depending on nature of monitoring the activities IDS can be classified into three major classes.

I) Network-based Intrusion Detection System (NIDS), analyse all communication traffic on a particular segment of a network.
II) Host-based Intrusion Detection System (HIDS), analyse communication traffic on a particular host.
III) Third class is hybrid of NIDS and HIDS, which combines data of the agent, with data from NIDS and HIDS [12], [13].

Different approaches are used to detect and prevent intrusion attempts for computer networks. One of these approaches is the artificial immune system (AIS). Computer network threats can be detected and prevented with the help of AIS which is an adaptive computational intelligence method. AIS is inspired by the biological immune system (BIS) used to solve real-world problems. BIS: In general, living organisms try to protect against pathogens using different mechanisms to repel or kill the invaders. More advanced organisms (vertebrates) have developed an efficient defence mechanism called the immune system. Substances that can stimulate specific responses of the immune system are commonly referred to as antigens. Once the immune system gets stimulated it generates a number of antibodies which respond to the foreign antigens. To be effective the immune system should be able to distinguish between the self (molecule that belongs to or is produced by the body) and non-self (antigens). The immune system can be seen as a multilayer system with defence mechanisms in several layers. Biological immune systems show great resilience in harsh environments and demonstrate the ability to cope with large amounts of sensory data as well as the unpredictability of the natural world.

The immune system is complex but very powerful; it can detect many types of pathogens, even unknown one, and it has a strong interaction between all the different actors of the immune system it helps to destroy the pathogens. As the immune

system has some very interesting features, a new artificial intelligence paradigm called the artificial immune system is created from it. Computer security, especially the antivirus and IDS fields, is of course an area that would be benefited by applying AIS. AIS abstract the structure of immune systems to incorporate memory, fault detection and adaptive learning. AIS have the abilities of self-organizing, memory efficient, recognition, adaptability, ability of learning and platform and software independence. AIS is applied to a large range of domains that can broadly be classified as adaptive learning, anomaly detection, fault detection and optimization problems.

Immune based algorithms are used for rule formation where Antibodies (entities those belong to system or are self) are generated which are capable of recognizing Antigen (foreign entity or something that does not belong to the system). Sets of detectors are generated with the help of AIS algorithms which are trained on a dataset having desired features, after got trained the detectors can be placed to detect antigens.
Basically four major AIS algorithms have been widely referred and gained popularity:

1. Negative selection algorithms (NSA).
2. Artificial immune networks (aiNET).
3. Clonal selection algorithms (CLONALG).
4. The Danger Theory and Dendritic cell algorithms (DCA).

Each algorithm among these above listed algorithms follows a particular phenomenon of BIS. Those help immune based algorithms to become self-contained, self-healing and fault-tolerant systems.

To improve the efficiency and accuracy of system AISs are implemented in two levels, each level is using different algorithm for rule formation. Often these algorithms show inherent characteristics like premature convergence (Generic Algorithms) and overfitting (C4.5 decision tree algorithms) etc. These inherent characteristics hammer the efficiency of AIS in terms of time and memory, they induce higher false positive rate as well. This motivates to build a system having algorithms that are more efficient than existing algorithms in terms of memory, time and those help to increase detection rate while reducing false positive rate.

The remaining part of the paper is organized as follows. Section II explains about intrusion detection system research works, Section III presents proposed solution based on detailed survey. Finally, conclusion is given in section IV.

II. RELATED WORK

The artificial immune system introduced as a machine learning algorithm in 1986 by Farmer and was firstly applied to IDS by Hofmayr and Forrest. Special features that make AIS efficient for intrusion detection are distributed control, self-organized, light-weighted and multi-layered detection.

Aziz et al. [1] propose a multi-agent artificial immune system for network intrusion detection and classification. The algorithm applied as an artificial immune system technique is Negative Selection Approach, using Genetic Algorithm. As an intelligent system, data mining is applied throughout the process for best results. Two classifiers are used for anomalies classification, Naive Bayes and Best-First Tree (BFT) classifiers. Naive Bayes classifier is used for attacks that have low representation in the training data set. The BFTree classifier is used for the remaining attacks classification. The main agent is installed on server while detector agents are installed on host machines. Each agent detects and classifies anomalies commencing on it. They found that detection rate is high without any overload on a central gateway. They found that system has achieved high detection rate and attack classification performance. Classification results are low.

Hu et al. [2] use kernel fisher discriminant analysis theory and svm classifier in this work. Openness of deployment area and broadcast nature makes Wireless Sensor Network (WSN) vulnerable to attacks. Hence, the authors discuss how detection techniques can be applied to WSN. The WSN dataset is used. MATLAB is used for simulation. The authors discuss about lifetime and energy consumption of the nodes. They have found that system shows timeliness and lower energy consumption. The system shows lower accuracy and higher false positive rate.

Chen et al. [3] proposed a non-linear system identification scheme based on non-linear autoregressive moving average model with exogenous inputs (NARX) immune network. They have integrated AIS and ANN into a real estate evaluation model. AIS is used to transform the original disorderly raw data into a dimensionless series and the back-propagation algorithm of ANN is used for data training, testing and prediction. They found that the prediction values and the actual values are almost similar and the prediction accuracy of the model is good.

Elhaj et al. [4] proposed a system based on the architecture of the immune system. The system considers the innate immune subsystem as a first layer of defence, which can deal with about 70%of suspicious traffic, using the 1999 DARPA dataset. The innate layer is deployed as a fuzzy expert system that is capable of making decisions, even when under unknown, inconsistent data. The whole detection base is put on a fuzzy knowledge base that is built according to the expert's knowledge and daily general observations of network traffic. Without using any of the immune system principles, the authors proposed the implementation of an adaptive immune layer as future work, which could analyze traffic handled by the innate layer.

Gupta et al. [5] propose the NIDS approach using Linear Regression and K-Means Clustering. The approach uses NSL-KDD data set. The approach pre-processes the data by normalization and transformation. The system uses different data mining techniques to examine the traffic in NIDS. The system aims to protect the confidentiality and integrity of the data. The problem with this approach is the accuracy rate is less (68%).

Manjari jha and Raj Acharya [6] proposed an immune based real time IDS using unsupervised clustering using a probabilistic model based T-cell algorithm and a decision tree based B-cell model. The T-cell unit is built using a Hidden Markov Model (HMM) and trained using unlabelled data; it learns mapping which is used to train B-cells. B-cells combine inputs from T-cells with broader-level feature information to weed out false alarms. The detection rate of the proposed algorithm is around 65% only. Problem with this approach is that it can handle only known attacks and false alarm rate increases if any novel attack commence on it.

Igbe et al. [7] propose a genetic algorithm based unsupervised machine learning approach to detect the attacks for distributed NIDS. In this approach central control is not needed. The system uses NSL-KDD data set. Authors created a network and trained it to differentiate normal traffic (self) from the suspicious one (non-self). The authors evaluated the detection rate and false alarm rate for the system. The problem with this system is it takes more time for training the IDS to recognise inside and outside data when it is deployed in distributed environment.

Brown et al. [8] employed a multiple detector set AIS, to classify intrusion based on features of application layer. Training is done by Negative Selection method. Proportion based classification and interval matching rule are applied to check whether a detector matches a network instance. They found that the system performs identical to the Standard AIS for IDS on the dataset used. The detection rate of the systems is low.

Fang et al. [9] propose genetic clonal selection and negative selection algorithm based approach to implement NIDS. The genetic algorithm is improved by integrating with vaccine autonomous obtaining algorithm. New generating individuals are modified with the help of vaccine library to guide maturation process to maintain diversity and to accelerate affinity maturation process. Less information about vaccine library is known, which directly impacts the accuracy of the system. The efficiency improving parameters like proliferation speed are only working for best samples. The proposed system does not show significant improvements in TP and FP rates.

Al-Douri et al. [10] proposed a two layer AIS to detect and prevent computer network threats using generic algorithm and decision tree algorithm C4.5. Clustered training data is fed to both rule generation phases, to create two antibodies each. Antibodies from first algorithm are fed to decision maker-one along with clustered testing data, it classifies testing data entities into normal or antigen, if decision maker classified testing data as unknown then it is fed to decision maker-two with antibodies generated by second algorithm, it classifies data into normal or antigen. They found that in combination the classifying algorithms are producing higher detection rate than classical algorithms, the system shows higher false positive rate.

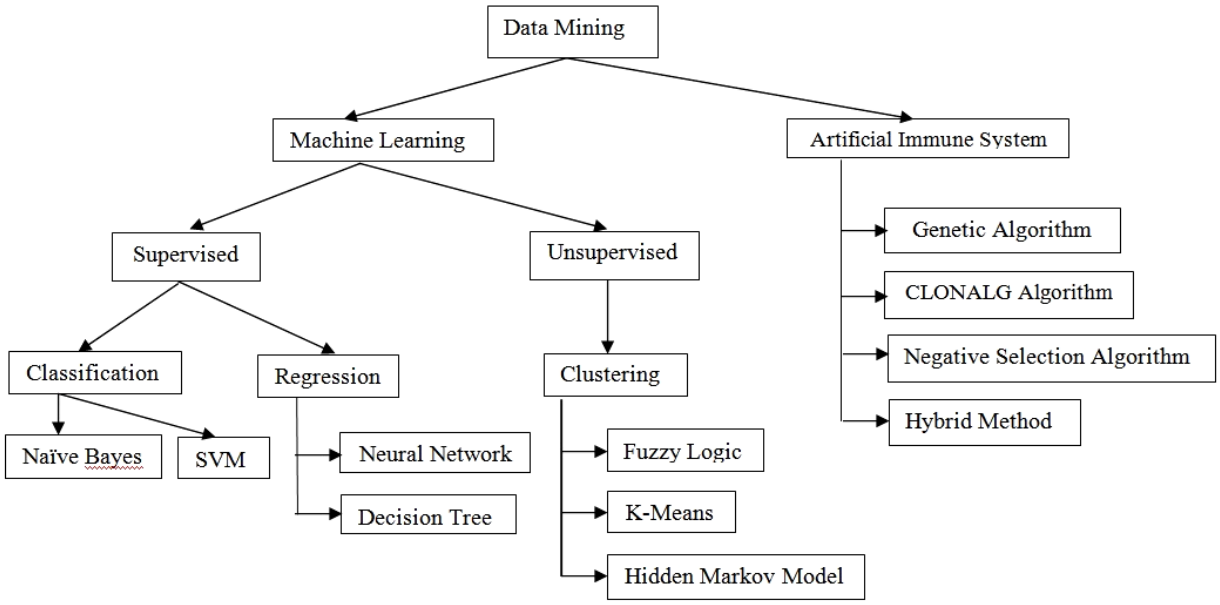

Fig.1 Structure of Literature Survey

III. PROPOSED APPROACH

The Proposed approach follows the hybrid approach; it is a combination of immune based algorithm and clustering algorithms (Two classifier algorithms) two classifiers will add an extra line of security and will help to increase the accuracy of the system. The proposed system is implemented at two levels namely, rule formation level-I and rule formation level-II. The approach used to develop a Two Layer AIS is to generate two efficient algorithms for rule formation. These algorithms will be capable to overcome the limitations of existing systems. The clustered features will be applied to algorithms generating decision antibodies (rules), to differentiate normal access record from attack records (antigens). The NSL-KDD cup dataset contains the collection of records of network traffic. The continuous features of dataset are at first, clustered using a clustering algorithm. Both levels are trained using features of NSL-KDD cup dataset. The clustered data is divided into two sets, majority of the records are used for training purpose while remaining are used for testing purpose. The antibodies generated by both the algorithms are used to discriminate normal access record from attack records from testing data.

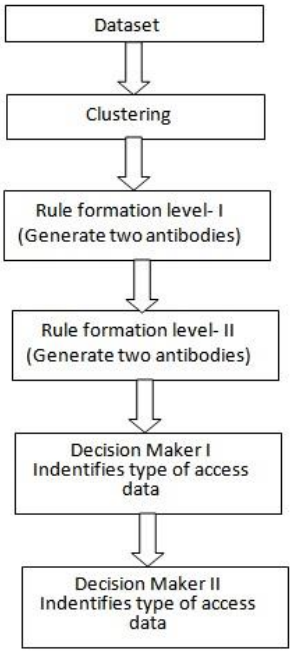

Figure: Architecture of proposed system

Algorithm for Experimental Model:
Input: Dataset having set of features of access records
Output: Classified output

Step 1: if Dataset has more features then
Step 2: Apply the feature selection technique as pre-processing technique.
Step 3: Apply parallelism.
Step 4: Evaluate the entropy value and information gain ratio of all three entropies (Shannon, havrda and Charvats entropy and quadratic entropy).
Step 5: Construct the models separately using second classifier algorithm based on various entropies.

Step 6: Find the accuracy and execution time of each model and store the value in array
Step 7: Find a model that has maximum Accuracy.
Step 8: if two have maximum accuracy
Step9: Find a minimum execution time of the model that has maximum accuracy
Step10: Classify by that model which has minimum execution time
Step11: Else Classification done by the model which has maximum accuracy.

IV. CONCLUSION

This paper provides a detailed literature survey on artificial immune system based intrusion detection systems. The proposed work aims to improve the efficiency of the current AIS based IDS systems. The proposed system will be developed using two levels of efficient algorithms. The proposed system aims to build efficient algorithms those will overcome the limitations of current systems. The proposed system is under process hence, conclusion is yet to come.

REFERENCES

[1] A. S. A. Aziz, S. E.-O. Hanafi, and A. E. Hassanien, "Multi-agent artificial immune system for network intrusion detection and classification," in International Joint Conference SOCO14-CISIS14-ICEUTE14. Springer, 2014, pp. 145-154.

[2] Z. Hu, J. Zhang, and X. A. Wang, "Intrusion detection for wsn based on kernel fisher discriminant and svm," in International Conference on P2P, Parallel, Grid, Cloud and Internet Computing. Springer, 2016, pp. 197-208.

[3] P.-C. Chen, K.-J. Zhu, and Y.-T. Chang, "A study of integrating artificial immune system and artificial neural network in real estate evaluation," in Circuits, Communications and System (PACCS), 2010 Second Pacific-Asia Conference on, vol. 1. IEEE, 2010, pp. 374-378.

[4] M. M. Elhaj, H. Hamrawi, and M. M. Suliman, "A multi-layer network defence system using artificial immune system," in Computing, Electrical and Electronics Engineering (ICCEEE), 2013 International Conference on. IEEE, 2013, pp. 232-236.

[5] D. Gupta, S. Singhal, S. Malik, and A. Singh, "Network intrusion detection system using various data mining techniques," in 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS), May 2016, pp. 1-6.

[6] M. Jha and R. Acharya, "An immune inspired unsupervised intrusion detection system for detection of novel attacks," in Intelligence and Security Informatics (ISI), 2016 IEEE Conference on. IEEE, 2016, pp. 292-297.

[7] J. Brown, M. Anwar, and G. Dozier, "Intrusion detection using a multiple-detector set artificial immune system," in Information Reuse and Integration (IRI), 2016 IEEE 17th International Conference on. IEEE, 2016, pp. 283-286.

[8] O. Igbe, I. Darwish, and T. Saadawi, "Distributed network intrusion detection systems: An artificial immune system approach," in Connected Health: Applications, Systems and Engineering Technologies (CHASE), 2016 IEEE First International Conference on. IEEE, 2016, pp. 101-106.

[9] J. Brown, M. Anwar, and G. Dozier, "Intrusion detection using a multiple-detector set artificial immune system," in Information Reuse and Integration (IRI), 2016 IEEE 17th International Conference on. IEEE, 2016, pp. 283-286.

[10] X. Fang and L. Li, "An improved artificial immune approach to network intrusion detection," in Advanced Computer Control (ICACC), 2010 2nd International Conference on, vol. 2. IEEE, 2010, pp. 39-44.

[11] Y. K. Al-Douri, V. Pangracious, and M. Al-Doori, "Artificial immune system using genetic algorithm and decision tree," in Bio-engineering for Smart Technologies (BioSMART), 2016 International Conference on. IEEE, 2016, pp. 1-4.

[12] C. Endorf, E. Schultz, and J. Mellander, Intrusion Detection & Prevention, ser. Security Series. McGraw-Hill/Osborne, 2004. [Online]. Available: https: //books.google.co.in/books?id=4PwPVag2zFUC

[13] L. Vokorokos, A. Kleinova, and O. Latka, "Network security on the intrusion detection system level," in 2006 International Conference on Intelligent Engineering Systems, 2006, pp. 270-275.