International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Artificial Intelligence based Techniques for Intrusion Detection System : A Review

Mitava Shah
M.Tech, Raksha Shakti University, Ahmedabad, Gujarat, India

ABSTRACT

Intrusion Detection systems (IDSs) have previously been built by hand. These systems have adversity successfully classifying intruders, and require a handsome amount of computational overhead making it difficult to create robust real-time IDS systems. Artificial Intelligence techniques (AI) can reduce the human effort required to build these systems and can improve their performance. Network intrusion detection is a serviceable part of an information security system. The rapid increase in the number of different types of attacks has increased the complexity involved in designing an intrusion detection system. In this paper, several AI based techniques used for the development of IDS have been reviewed.

Keywords : Artificial Intelligence, Intrusion Detection, Feature Selection.

I. INTRODUCTION

Traditional protection techniques such as user authentication, data encryption, avoiding programming errors and firewalls are used as the defence for computer security. With the coming of Internet age, computer security has become more essential. Intrusion detection systems, or IDSs, have become a crucial component in the Security Officer's toolbox. IDSs do exactly as it name suggests: they detect feasible intrusions. More specifically, IDS tools designed to detect computer attacks and/or computer misuse, and to alert the proper individuals upon detection.

Intrusion detection systems serve three crucial security functions: they monitor, detect, and respond to illegetimate activity by company insiders and outsider intrusion. Intrusion detection systems use protocols to define certain events that, if detected will issue an alert. In other words, if a particular event is considered to well advised a security incident, an alert will be issued if that event is detected. There are two fundamental types of IDSs: online IDSs and offline IDSs. The offline IDSs analyse connection data from the logs after the connections have happened. The online IDSs, if possible, analyse data before connection is allowed.

IDS come in a various types and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. A *network-based* IDS usually consists of a network tools with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface. The IDS is placed along a network section or boundary and monitors all traffic on that section. A *host-based* IDS requires small programs to be installed on specific systems to be monitored. The agents monitor the operating system and create log files and/or trigger alarms. A host-based IDS can only monitor the specific host systems on which the agents are installed; it doesn't monitor the entire network.

Artificial Intelligence could make the use of Intrusion Detection Systems a lot easier than it is today. They could learn the preferences of the security officers and show the kind of alerts first that the officer has previously been most interested. As always, the hardest thing with learning AIs, is to make them learn the right things. AIs could learn the same things as a rule-based system by watching a security officer work. AIs could also link together events that, by themselves, are insignificant but when combined may indicate that an attack is underway.

II. METHODS AND MATERIAL

Intrusion Detection Techniques

Statistical based Technique

Statistical modelling is among the earliest methods used for detecting intrusions in electronic information systems. It is assumed that an intruder's behaviour is noticeably different from that of a normal user, and statistical models are used to aggregate the user's behaviour and distinguish an attacker from a normal user. The techniques are applicable to other cases, such as user groups and programs.

Anomaly based Technique

An anomaly detection based IDS detects intrusions by searching for abnormal network traffic. It can detect unknown attacks, but the false positive rate is high.

Knowledge based Techniques

A Knowledge based Intrusion Detection technique applies the knowledge garnered regarding specific attacks and system loopholes. In it, the behaviors have being collected from attribute database. If the attack behaviors are same as in the database then it can safeguard it before the attacker destroys our system.

Artificial Intelligence Based Techniques

Data Mining Techniques

Data mining is the non-trivial process of identifying valid, novel, potentially useful, and ultimately understandable patterns in data. Grossmann defines data mining as a field that deals with uncovering patterns, changes, associations, anomalies as well as statistically significantly structures and events in data.

Lee, et al has a framework which consists of programs for learning classifiers and meta-classification, association rules for link analysis and frequent episodes for sequence analysis. The accomplished rules replace the manually encoded intrusion patterns and profiles. There are the major data mining techniques: Genetic Algorithm Based Techniques and Fuzzy Logic Based Techniques.

Balaji, et al. have used a genetic based intrusion detection model to learn individual user behaviour and detect abnormal user activities. The intrusion detector module computes the probability of the current command sample being intrusive from the deviations in the user behaviour.

Bobor has defined a genetic algorithm as a programming technique, which mimics biological evolution as a problem solving approach. Song, et al. have used a hierarchical algorithm called RSS-DSS for dynamically filtering large datasets based on the concept of training pattern age and difficulty. This provides the data set of about half a million patterns in about fifteen minutes.

Chittur developed a model in which the genetic algorithm was given training data from which an empirical model of malicious computer behaviour was generated.

Luo has used fuzzy logic rules integrated with association rules and frequency episodes to classify the data. A normalization step has been added to the procedure for mining fuzzy association rules developed by Kuok, et al. in order to prevent one data instance from contributing more than others.

Decision Tree Based Techniques

A Decision Tree is a tree-like graph consisting of internal nodes which represent a search on an attribute and branches which denote the outcome of the search and leaf nodes which signify a class label. The classification rules are build by the path selected from the root node to the leaf. To divide each input data, first the root node is chosen as it is the most extended attribute to separate the data. The tree is constructed by identifying attributes and their associated values which will be used to analyse the input data at each intermediate node of the tree. After the tree is formed, it can fore show newly coming data by traversing, starting from a root node to the leaf node visiting all the internal nodes in the path depending upon the test conditions of the attributes at each node.

Levin uses the approach of a Kernel miner. It constructs the set of locally optimal decision trees from which it selects the optimal subset of trees used for predicting unknown cases. This modelling technique reduces individual prediction results received from individual classification trees.

Neural Network

Dr. Robert Hecht-Nielsen defines Neural Network as *"A computing system made up of a number of simple, highly interconnected processing elements, which process information by their dynamic state response to external inputs.*"

Lei, et al. use the Improved Competitive Learning Network (ICLN) algorithm. In this algorithm, only the winning weight vector gets its weight vector changed, following every iteration. The other weight vectors remain unchanged. Mukhopadhyay, et al. use the back propagation neural network approach in which the error is propagated backwards, from the output layer to the hidden layer and then to the input layer.

Han, et al. use a technique known as evolutionary neural network (ENN) which takes lesser time than regular neural networks since they discover the structures and weights of the network simultaneously.

Support Vector Machine

Support Vector Machines are based on the concept of decision planes that define decision boundaries. A decision plane is one that separates between a set of objects having different class memberships. A SVM views a classification problem as a quadratic optimization problem. It avoids the "curse of dimensionality" by placing an upper bound on the margin between the different classes. This makes it easy to handle large and dynamic data sets. A SVM classifies data with the help of support vectors.

Li, et al. use a feature reduction method to select critical features in IDS to reduce the training time and prediction time in the IDS classifier with minimal loss of accuracy. Chang, et al. use a parallel SVM (PSVM) algorithm to reduce memory use and to parallelize both data loading and computation. Zhang, et al. use a feature selection technology based on the Fisher score.

Clustering Techniques

Clustering is a process of grouping objects into set of clusters according to a given similarity or distance measure. The main methods for distance measurement are Euclidean distance and Mahalanobis distance.

Guan, et al. present a clustering heuristic for intrusion detection called Y-means. This heuristic is based on the K-means algorithm. K-means clustering is a method of cluster analysis whose aim is to partition n observations into k clusters. Every observation belongs to a cluster with the nearest mean.

Kayacik, et al. use the technique of a hierarchy of Self-Organizing Feature maps. A Self Organizing Map belongs to a class of artificial neural networks which is trained using severally learning. This produces a discrete, low-dimensional representation of the input space applied to the training samples, which is called a map. Self organizing maps are different from other artificial neural networks in the sense that they use a neighbourhood function to preserve the topological properties of the input space.

III. RESULTS AND DISCUSSION

Comparison of Different Techniques

A comparative study of the detection rate of different methods for different classes of attack is as following.

Table 1- Detection rate of different methods for different classes of attacks

Method	DoS	U2R	R2L
Decision trees (Levin)	97.5	11.8	7.32
Neural network (Mukkamala et al.)	99.6	34.3	99.3
SVM (Mukkamala et al.)	99.25	99.87	99.78
Hierarchical SOM (Kayacik et al.)	64.3	10	9.9

Advantages of AI Applications to IDSs

Table 2- Advantages that some AI techniques bring to Intrusion Detection

Technology	Advantages
Artificial Neural Networks	Parallelism in information processing; Learning by example;

	Non-linearity – handling complex non linear functions; Superiority over complex and perplexing differential equations; Resilience to noise and incomplete data; Versatility and flexibility with learning models;
Intelligent Agents	Mobility; Helpfulness – they always attempt to accomplish their tasks having contradictory objectives; Rationality – in achieving their objectives; Adaptability – to the environment and user preferences;
Artificial Immune Systems	Dynamic structure; Parallelism and distributed learning – using data network communications and parallelism in detection and elimination tasks; Self-adaptability and self-organizing – updating intrusion marks without human involvement; Robustness; Selective response – removing malicious activity by the best means available; Diversity – each detector node generates a statistically unique set of non-self detectors; Resource optimization;
Genetic Algorithms	Robustness; Adaptability to the environment; Optimization – providing optimal solutions even for complex computing problems; Parallelism – allowing evaluation of multiple schemas at once; Flexible and robust global search

IV.CONCLUSION

Several studies of AI based techniques in intrusion detection systems are compared on the basis of the key concept used, their advantages and disadvantages and the data set used. The R2L and U2R attack classes have low detection rates since there are less number of training instances. A computationally efficient technique is required for handling large volume of data over a network.

V. REFERENCES

[1]. Tarapore N.Z., Kulkarni D.B. AND Kamakshi P.V. Journal of Artificial Intelligence Volume 3, Issue 3, 2012, pp.-111-116.

[2]. Selma Dilek, Huseyin Çakır and Mustafa Aydın International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, No. 1, January 2015.

[3]. Kajal Rai, M. Syamala Devi and Ajay Guleria Int. J. Advanced Networking and Applications Volume: 07 Issue: 04 Pages: 2828-2834 (2016).

[4]. K.P.Kaliyamurthie, D.Parameswari and DR. R.M. Suresh IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, March 2012.

[5]. Jeremy Frank , Nsa Urp Mda--c In Proceedings of the 17th National Computer Security Conference.

[6]. Citeseer.ist.psu.edu.

[7]. Areej Yassin, Donald Berndt and Monica Chiarini Proceedings Americas Conference on Information Systems(AMCIS) December 2006.

[8]. David Iclanzan, Fabio Daolio and Marco Tomassini Evolutionary Computation in Combinatorial Optimisation pp 157-169.

[9]. José Helano Matos Nogueira The International Journal of FORENSIC COMPUTER SCIENCE IJoFCS (2006) 1, 28-32.