

Artificial Intelligence Based Intrusion Detection Techniques - A Review



Gulshan Kumar* Krishan Kumar** Monika Sachdeva**

© Institute of Management Studies, Noida
Online access at www.publishingindia.com

Abstract

The Internet connects hundreds of millions of computers across the world running on multiple hardware and software platforms providing communication and commercial services. However, this interconnectivity among computers also enables malicious users to misuse resources and mount Internet attacks. Continuously developing Internet attacks poses a severe challenge to develop a flexible, adaptive security oriented methods. Now a day most of commercially available intrusion detection systems are signature based. These systems perform well in detecting known attacks whose signature resides in the database. Such systems require frequent rule-base updates and signature updates, and are not capable of detecting unknown attacks. For detection of known and zero day unknown attacks, anomaly based network intrusion detection systems are best approaches. Anomaly based techniques are conceptually very attractive but many problems remains to be solved before being adapted widely. Problems including false alarm rate, detection accuracy and failure to scale high speed etc. still need to be solved. In this text, we review Artificial Intelligence based intrusion detection techniques.

Keywords : Network security, intrusion, intrusion detection system

1. Introduction

Information access through Internet provides intruders various ways of attacking a computer system. More and more organizations have become vulnerable due to intrusion of cyber attackers which compromise the security objectives of their network. There are five security objectives: first security objective is the Availability—it protects the system against intentional or accidental attempts to deny legitimate users access to information or systems. Second security objective is the Integrity of Data or Systems—it ensures the un-alteration of data in any unauthorized manner. Third objective is Confidentiality of Data or Systems—it ensures the protection of information against unauthorized access or use. Fourth objective is Accountability—it ensures the necessary control to trace actions to their source. Accountability directly supports non-repudiation, deterrence, intrusion prevention, security monitoring, recovery, and legal admissibility of records. Last security objective is the Assurance—it ensures the confidence that technical and operational security measures work as intended. Assurance highlights the notion that secure systems provide the intended functionality while preventing undesired actions [1].

An intrusion or computer attack can be defined as "any set of actions that attempt to compromise the security objectives".

*Dept of Computer Application, Malout Institute of Management & Information Technology, Malout, Punjab, India

**Dept of Computer Science & Engg., SBS College of Engineering & Technology, Ferozepur, Punjab, India

There are various types of attack that can compromise the security objectives. DARPA has divided these attacks into four different classes: first class is **Probe** : here an attacker scans a network to gather information in order to find known vulnerabilities. This type attack affects the confidentiality and accountability security objectives. Second type of attack is **Denial of Service (DoS) attack** : here an attacker makes some computing or memory resource too busy or too full to handle legitimate requests, denying legitimate users access to a machine. This attack directly affects the availability, accountability and assurance security objectives. Third type of attack is **User to Root (U2R) attack** : here an attacker starts with access to a normal user account on the system by gaining root access. This attack affects confidentiality and integrity objectives. Last and fourth type of attack is **Remote to Local (R2L) attack** : here an attacker sends packets to a machine over a network that exploits the machine's vulnerability to gain local access as a user illegally. This attack may leads to affect of confidentiality and integrity objectives. These security objectives are inter-dependent. Any type of computer attack affecting one of security objective also affects the others in some way. With the vulnerability of present-day software and protocols combined with the increasing sophistication of attacks, it comes as no surprise that network-based attacks are on the rise. The Computer Emergency Response Team/Coordination Center (CERT/CC) has reported that the number of computer attacks has increased exponentially in the past few years from 1990 to 2003 as shown in figure 1 [2]. The statistical attacks reported by the Malaysian Computer Emergency Response Team (MyCERT) shows in the fourth quarter of 2008 (Q4), a total of 33036 incidents, inclusive of spam incidents, were reported to MyCERT representing a 52.51% increase of incidents compared to Q3 in 2008 [3]. There was a tremendous increase in fraud incidents which mainly involving phishing, cheatings, Nigerian scams. CSI/FBI has also reported financial losses in 2007 & 2008 is double than loss in 2006 [4]. To minimize the financial losses, various security mechanisms are applied to network. About 86 percent of the organization used firewalls but firewalls by themselves are not sufficient to provide adequate protection. These insecure security mechanisms has introduced ever evolving field of intrusion detection and prevention. An intrusion detection system gathers and analyzes information from different areas of computer or network to identify possible attempts to compromise the security objectives of a system/network.

The main aim of this text is to present a brief survey of various types of intrusion detection system; Artificial Intelligence (AI) based techniques used for intrusion detection and to adopt the multi classifier approach for detecting intrusions efficiently.

The rest of text is organized as follows. Section 2 describes the intrusion detection, architecture and classification of IDS. The section also highlights the various existing IDS. Section 3 highlights various techniques used for intrusion detection. Section 4 gives the details of AI based intrusion detection techniques. Finally section 5 summarizes and concludes the text.

2. Intrusion Detection System (IDS)

An intrusion detection system (IDS) defined as "an

effective security technology, which can detect, prevent and possibly react to the computer attack" is one of the standard components in security infrastructures. It monitors target sources of activities, such as audit and network traffic data in computer or network systems and deploys various techniques in order to provide security services. The main objective of IDS is to detect all intrusions in an efficient manner. The implementation of IDS allows network administrators to detect security objective violations. These security objective violations range from external attackers trying to gain unauthorized access network security infrastructure or making resources unavailable to insiders abusing their access of the system resources.

With passage of time and growth of computer attacks, several IDSs architecture has been proposed. Axelsson [5] proposed a common architecture for IDS as depicted in figure 2. According to Axelsson the common components for IDS are consists of followings:

Network to monitor - it is the identity to be monitored for intrusions. This can be a single host or a network; **Data collection & storage unit** - this unit is responsible for collecting the data of various events and converts them in proper format and store to disk; **Data analysis & processing unit**: this unit is the brain of IDS. It contains the whole functionality to find the suspicious behavior of attack traffic. On detecting attack, a signal is generated. Based on the type of IDS, action can be raised by the system itself to alleviate the problem or signal is passed to network administrator to take appropriate the action; **Signal** : This part of the system handles all output from the intrusion detection system. The output may be either an automated response to an intrusion or alert of malicious activity for a network security administrator.

Based upon the different modules, IDS can be categorized into various classes. Based upon data collection & storage unit, IDS can be divided into two classes :

- **Host based IDS** : Host based IDS collects the data from a host to be protected. They collect the data generally from system calls, operating system log files, NT events log file, CPU utilization, application log files etc. Advantage of Host based IDS is that they are operating system dependent & are very efficient to detect attacks like buffer overflow. These systems become inefficient in case of encrypted data and switched network. The available host based IDS are IDIES [6], MIDAS [7], Haystack [8].
- **Network based IDS** : Network based IDS collects the data from network directly in form of packets. These IDS are operating system independent and easy to deploy to various systems. The available network based IDS are NSM [9], Bro [10].

Depending upon criteria adapted for data analysis & processing unit, IDS can be divided into two classes :

- **Misuse or signature based IDS** : Misuse or signature based IDS maintain a database of known attack signatures. The detection of attack involves comparison of data from data collection unit and data stored in database. If the match occurs then attack signal get generated. Difficult and challenging task is to keep the database of signatures up to date. Signature based IDS perform well for attack whose signatures are in database but they are inefficient to

detect zero day attacks. They also have very low false alarm rate. Most of commercially available IDS belong to this category. The available signatures based are ASAX [11], USTAT [12], IDIOT [13].

- **Anomaly based IDS** : Anomaly based IDS reacts to anomalous behavior as defined by some history of monitored systems previous behavior or some previously defined profile of that system. The system matches the current profile with previous profile, if there is any significant deviation, then that activity is notified as an attack. These systems are capable of detecting zero day attack. The available anomaly based IDS are IDIES [6], W & S [14], Comp Watch [15].

Depending upon criteria adapted for generating the response, IDS can be divided into two classes :

- **Passive IDS** : Passive IDS responds to attacks by notified the proper authority. They do not themselves try to mitigate the damage done, or actively seek to harm or hamper the attacker. The available IDS in this class are IDIES [6], GrIDS [16], NIDES [17].
- **Active IDS** : Active IDS responds to attacks by initiating certain action. The action can be against two entities, which further classifies Active IDS into sub classes. Those entities can be:

Attacking system : In this class, the IDS try to control the attacking system. They try to attack the attacker system to remove his platform of operation.

Attacked system : in this class, the IDS try to control the attacked system. They modified the state of attacked system to mitigate the attack. They can terminate the network connections, increase the security logging or kill the concerned processes etc.

The available active IDS are EMERLARD [18], Janus [19]. The discussion can be summarized in figure 3 and table 1.

3. Intrusion Detection Techniques

In the past, different types of techniques from various disciplines have been applied to detect the intrusions. The techniques are

- Statistical Techniques
- Knowledge-based Techniques
- Artificial Intelligence (AI) based Techniques

In the statistical-based IDS, the behavior of the system is represented from a random viewpoint. On the other hand, knowledge-based IDS techniques try to capture the claimed behavior from available system data (protocol specifications, network traffic instances, etc.). Finally, AI based IDS schemes are based on the establishment of an explicit or implicit model that allows the patterns analyzed to be categorized [48].

4. Artificial Intelligence Based Techniques

Mario Castro Ponce has listed many advantages of AI based new patterns); Fast computing (faster than humans, actually) and Learning abilities.

Many authors [20, 21, 46] have divided AI based detection

approaches into different classes. The major classes include followings :

4.1 Decision Tree Based Approach

Decision trees are powerful and popular tools for classification and prediction. A decision tree is a tree that has three main components: nodes, arcs and leaves. Each node is labeled with a feature attribute which is most informative among the attributes not yet considered in the path from the root, each arc out of a node is labeled with a feature value for the node's feature and each leaf is labeled with a category or class. A decision tree can then be used to classify a data point by starting at the root of the tree and moving through it until a leaf node is reached. The leaf node would then provide the classification of the data point. Levin created a set of locally optimal decision trees from which optimal subset of trees is selected for predicting new cases [22]. 10% of KDD Cups database is used for training and testing. Data is randomly sampled from the entire training data set. Multi-class detection approach is used to detect different attack categories in the KDD data set. Just like Agarwal and Joshi [23], Levin tries to classify the data into five different classes: Normal, Probing, DOS, U2R, and R2L. The final trees give very high detection rates for all classes including the R2L in the entire training data set. The result of experiment is shown in table 2.

ID3 and C4.5 developed by Quinlan [41] are the most popular implementations of the Decision Tree.

4.2 Parzen Window Based Approach

Yeung and Chow propose a novelty detection approach using non-parametric density estimation based on Parzen window estimators with Gaussian kernels [24]. KDD data set was used to train & test system. The total traffic was classified into four classes. The result is shown in table 3

4.3 Rule Based Approach

Rule based approach typically involve the application of a set of association rules and frequent episode patterns to classify the audit data. In this context, if a rule states that "if event X occurs, then event Y is likely to occur", then events X and Y can be described as sets of (variable, value)-pairs where the aim is to find the sets X and Y such that X "implies" Y. In the domain of classification, we fix Y and attempt to find sets of X which are good predictors for the right classification. The advantage of using rules is that they tend to be simple and intuitive, unstructured and less rigid. As the drawbacks they are difficult to maintain, and in some cases, are inadequate to represent many types of information. A number of inductive rule generation algorithms have been proposed in literature. Some of them first construct a decision tree and then extract a set of classification rules from the decision tree. Other algorithms directly induce rules from the data by employing a divide and conquer approach.

Agarwal and Joshi propose a two-stage general-to-specific framework for learning a rule-based model (PNrule) to learn classifier models on a data set that has widely different class distributions in the training data [23]. They utilized KDD Cups database for training and testing their system. The system was classifying the traffic into five different classes. The results are as shown in table 4.

4.4 Data Mining Approach

4.4.1 Fuzzy Logic Techniques

Fuzzy logic techniques have been in use in the area of computer and network security especially in intrusion detection for two main reasons. Firstly, several quantitative parameters that are used in the context of intrusion detection, e.g., CPU usage time, connection interval etc., can potentially be viewed as fuzzy variables. Secondly, the concept of security itself is fuzzy. In other words, the concept of fuzziness helps to smooth out the abrupt separation of normal behavior from abnormal behavior. That is, a given data point falling outside/inside a defined "normal interval", will be considered anomalous/normal to the same degree regardless of its distance from/within the interval.

Dickerson et al in [25] has applied the fuzzy logic and data mining techniques to detect the intrusion in network. They proposed FIRE (Fuzzy Intrusion Recognition Engine) that uses fuzzy logic to assess whether malicious activity is taking place on a network. They use simple data mining techniques to process the network input data and generate fuzzy sets for every observed feature. The fuzzy sets are then used to define fuzzy rules to detect individual attacks. The limitation here is that Fuzzy rules are formed with the help of experts so it is very labor intensive. Norbik Bashah Idris et al in [26] proposed a modified FIRE system. They proposed a mechanism to automate the fuzzy rules generation process and reduce the human intervention by using AI techniques. But the proposed model is in very infant stage. No experimental results are produced.

4.4.2 Genetic Algorithm

Genetic algorithms, a search technique used to find approximate solutions to optimization and search problems, have also been extensively employed in the domain of intrusion detection to differentiate normal network traffic from anomalous one. The major advantage of genetic algorithms is their flexibility and robustness as a global search method. In addition, a genetic algorithm search converges to a solution from multiple directions and is based on probabilistic rules instead of deterministic ones. The disadvantage of genetic algorithm is the high resource consumption. In the domain of network intrusion detection, genetic algorithms have been used in a number of ways.

Some researcher have used genetic algorithms directly to derive classification rules, while others use genetic algorithms to select appropriate features or determine optimal parameters of related functions, while different data mining techniques are then used to acquire the rules.

4.5 Machine Learning Approach

4.5.1 Neural Network Approach

In the neural network approach to intrusion detection, the neural network learns to predict the behavior of the various users and daemons in the system. If properly designed and implemented, neural networks have the potential to address many of the problems encountered by rule-based approaches. The main advantage of neural networks is their tolerance to imprecise data and uncertain information and their ability to

infer solutions from data without having prior knowledge of the regularities in the data. This in combination with their ability to generalize from learned data has shown made them an appropriate approach to intrusion detection. In order to apply this approach to Intrusion Detection, we would have to introduce data representing attacks and non-attacks to the Neural Network to adjust automatically coefficients of this Network during the training phase. Neural networks can be used in following ways:

- **Unsupervised model** : Lippmann et al of MIT Lincoln Laboratory conducted a number of tests employing Neural Networks to misuse detection [27, 28]. The system was searching for attack-specific keywords in the network traffic. A Multi Layer Perceptron had been used for detection UNIX host attacks, and attacks to obtain root-privilege on a server. The system was trying to detect the presence of an attack by classifying the inputs into 2 (two) outputs (normal and attack). The system was able to detect 80% of attacks – 17 out of 20 attacks were identified. The main achievement of this system was its ability to detect old as well as new attacks not included in the training data. They used DARPA intrusion detection evaluation dataset.
- **Supervised model** : Self-Organizing Maps (SOM) has been proved to be effective in novelty detection, automated clustering, and visual organization [29].

Alan Bivens et al in [30] detected the intrusions based on network user behavior. He analyzed the user behavior based on time window using neural networks. After supervised learning of neural network, the network data is classified and clustered by using Self Organizing Map (SOM) neural network in different time intervals. These clusters are used to detect the attack in network. The approach used DRAPA TCP dump data for training of neural network.

Kayacik et al utilize KDD Cups data set for the experiments. They create three layer of employment [31]: First, individual SOM are associated with each basic TCP feature. This provides a concise summary of the interesting properties of each basic feature, as derived over a suitable temporal horizon. Second, integrates the views provided by the first level SOM into a single view of the problem. At this point, they use the training set labels associated with each pattern to label the respective best matching unit in the second layer. Third, the final layer is built for those neurons, which win for both attack and normal behaviors. These results in third layer SOMs being associated with specific neurons in the second layer. Moreover, the hierarchical nature of the architecture means that the first layer may be trained in parallel and the third layer SOMs are only trained over a small fraction of the data set.

- **Hybrid neural network model** : Many researchers have tried to combine the MLP and SOM for intrusion detection. They attempted to create an Intrusion Detection System using Multi-Layer Perceptron model and Self-Organizing Map for misuse detection [21]. They have used a feed-forward network with back-propagation learning, which contained 4 fully connected layers, 9 input nodes and 2 output nodes (normal and attack). The network has been trained for a certain number of attacks. The network has succeeded in identifying attacks it was trained for.

4.5.2 Bayesian Network

A Bayesian network is a model that encodes probabilistic relationships among variables of interest. This technique is generally used for intrusion detection in combination with statistical schemes, a procedure that yields several advantages [47], including the capability of encoding interdependencies between variables and of predicting events, as well as the ability to incorporate both prior knowledge and data. But a major disadvantage is that the results are comparable to statistical techniques but it requires extra computation efforts.

4.5.3 Principal Components Analysis

PCA is a technique that is used to reduce the complexity of a dataset not a detection technique. A given data collection (or dataset), obtained by means of the different sensors in the target environment, becomes more and more extensive and complex as the number of different services and speed of the networks grow. To simplify the dataset, PCA makes a translation on a basis by which n correlated variables are represented in order to reduce the number of variables to $d < n$, which will be both uncorrelated and linear combinations of the original ones. This makes it possible to express the data in a reduced form, thus facilitating the detection process.

4.5.4 Markov Model

There are two types of approaches in this class:

- Markov chains : A Markov chain is a set of states that are interconnected through certain transition probabilities, which determine the topology and the capabilities of the model. During a first training phase, the probabilities associated to the transitions are estimated from the normal behavior of the target system. The detection of anomalies is then carried out by comparing the anomaly score (associated probability) obtained for the observed sequences with a fixed threshold.
- Hidden Markov models : In the case of a hidden Markov model, the system of interest is assumed to be a Markov process in which states and transitions are hidden. Only the so-called productions are observable.

In literature several methods have been presented that address the problem of detecting anomalies in the usage of network protocols by inspecting packet headers. The common denominator of all of them is the systematic application of learning techniques to automatically obtain profiles of normal behavior for protocols at different layers. Mahoney et al. experimented with anomaly detection over the DARPA network data by range matching network packet header fields.

There exist many systems that use markov model. The examples include PHAD (Packet Header Anomaly Detector) [32], LERAD (LEarning Rules for Anomaly Detection) [33] and ALAD (Application Layer Anomaly Detector) [34].

4.5.5 Support Vector Machine

SVM is a technique for solving a variety of learning, classification and prediction problems. SVM originated as an implementation of Vapnik's [35] structural risk minimization (SRM) principle, which minimizes the generalization error, i.e., true error on unseen examples. The basic SVM deals with two-class problems—in which the data are separated by a hyper plane defined by a number of support vectors. Support vectors

are a subset of training data used to define the boundary between the two classes. In situations where SVM cannot separate two classes, it solves this problem by mapping input data into high-dimensional feature spaces using a kernel function. In high-dimensional space it is possible to create a hyper plane that allows linear separation (which corresponds to a curved surface in the lower-dimensional input space). Accordingly, the kernel function plays an important role in SVM. In practice, various kernel functions can be used, such as linear, polynomial or Gaussian. One remarkable property of SVM is its ability to learn can be independent of the feature space dimensionality. This means that SVM can generalize well in the presence of many features. Srinivas Mukkanmalla et al. [36] had proved many advantage of SVM over other techniques. SVMs outperform ANNs in the important respects of scalability, training time and running time and prediction accuracy. Srinivas Mukkanmala et al [37] have also applied SVM for extracting the features for intrusion detection of KDD dataset. They empirically proved that features selected with help of SVM leads to similar results as use of full feature set. This reduction in no of features reduces the computational effort which is requirement of any IDS. Wun-Hwa Chen et al [38] has also proved that SVM is superior to ANN. The superior performance of SVMs over ANNs is due to the following three reasons:

- SVMs implement the structural risk minimization principle which minimizes an upper bound for the generalization error rather than minimizing the training error. However, ANNs implement the empirical risk minimization principle, which might lead to worse generalization than SVM.
- An ANN may not converge to global solutions due to its inherent algorithm design. In contrast, finding solutions in SVMs is equivalent to solving a linearly constrained quadratic programming problem, which leads to a global optimal solution.
- In choosing parameters, SVMs are less complex than ANNs. The parameters that must be determined in SVMs are the kernel bandwidth and the margin C . However, in ANNs, the number of hidden layers, number of hidden nodes, transfer functions and so on must be determined. Improper parameter selection might cause the over-fitting problem.

They used detection rate and false positive rate as performance metrics. DARPA dataset is used for evaluation of models.

4.6 Clustering Based Approach

Clustering techniques work by grouping the observed data into clusters, according to a given similarity or distance measure. The candidates methods are distance measurement are Euclidean distance and Mahalanobis distance. Similarity can be measured by using cosine formula, binary weighted cosine formula proposed by Sanjay Rawat [30] and many more. The procedure most commonly used for this consists in selecting a representative point for each cluster. Then, each new data point is classified as belonging to a given cluster according to the proximity to the corresponding representative point. There exist at least two approaches to clustering based anomaly detection. In the first approach, the anomaly detection model is trained using unlabelled data that consists of both normal as well as attack traffic. In the second approach,

the model is trained using only normal data and a profile of normal activity is created. The idea behind the first approach is that anomalous or attack data forms a small percentage of the total data. If this assumption holds, anomalies and attacks can be detected based on cluster sizes—large clusters correspond to normal data, and the rest of the data points, which are outliers, correspond to attacks.

Minnesota Intrusion Detection System (MINDS) is network-based anomaly detection approach that utilizes data mining techniques & clustering techniques.

4.7 Multi Classifier Approach

Multi classifier approach has been advocated by many researchers in literature [36, 40, 42, 43]. They proved that no single classifier is capable enough to detect all classes of attacks to acceptable false alarm rate and detection accuracy. Srinivas Mukkanmalla et al. [36] studied the SVM, ANN, LGP (linear genetic programs) and MARS (multivariate adaptive regression splines) for classification of KDD data into five classes. They used detection accuracy, attack severity, training & testing time (scalability) as evaluation metrics & used DARPA intrusion detection dataset. They proved that none of single classifier performs well in all attack classes. LGPs outperform MARS, SVMs and ANNs in terms of detection accuracy at the expense of time. MARS is superior to SVMs in respect to classifying the most important classes (U2Su and R2L) in terms of the attack severity. SVMs outperform ANNs in the important respects of scalability (SVMs can train with a larger number of patterns, while ANNs take a long time to train or fail to converge at all when the number of patterns gets large); training time and running time (SVMs run an order of magnitude faster); and prediction accuracy. The results are summarized in table 5.

Mukesh Sabhnani et al [40] also conducted a number of experiments with hybrid systems that contained different approaches for attack classification at University of Toledo. They evaluated a set of pattern recognition and machine learning algorithms. KDD Cups data is chosen for the experiments. The attacks are classified into five main classes, as was done by the researchers discussed above. They highlight that most researchers employ a single algorithm to detect multiple attack categories with dismal performance in some cases. So, they propose to use a specific detection algorithm that is associated with an attack category for which it is the most promising. They experimented with nine different classifiers and suggested following classifier for each attack category. They used probability of detection and false alarm rate as performance metric for different classifiers. Best classifiers along with their probability of detection and false alarm rate are shown in table 6.

Farnaz Gharibian et al [42] compared the supervised probabilistic and predictive machine learning techniques for intrusion detection. Two probabilistic techniques Naive Bayes and Gaussian and two predictive techniques Decision Tree and Random Forests are employed. They used KDD dataset and detection accuracy as performance metric. The best results are summarized in table 7. They proposed best techniques for each class of attack as shown in table 8.

Mrutyunjaya Panda et al [43] has also advocated that there is no single best algorithm to out perform others in all situations. They demonstrated the performance of three well known data mining classifier algorithms namely, ID3, J48 and Naïve Bayes evaluated based on the 10-fold cross validation test of KDD dataset using WEKA. The performance metrics include time to build the model, error rate, confusion matrix, ROC, recall rate vs. precision rate and kappa statistics. The results are summarized table 9.

4.8 Hybrid Systems

Many researcher has suggested [6, 17, 18, 44, 45] that the monitoring capability of current intrusion detection systems can be improved by taking a hybrid approach that consists of both anomaly as well as signature detection techniques. The anomaly detection technique aids in the detection of new or unknown zero day attacks while the signature detection technique detects known attacks.

Tsong Song Hwang et al [44] has proposed a 3 tier hybrid approach to detect intrusions. 1st tier of system is signature based approach to filter the known attacks using black list concept. 2nd tier of system is anomaly detector that uses the white list concept to distinguish the normal and attacks traffic that has by passed 1st tier. 3rd tier component of system uses the SVM to classify the unknown attack traffic into five classes i.e. normal, probing, DoS, U2R and R2L. KDD dataset was used to train and test the system. The results are summarized in table 10.

The same concept is also implemented by Carolina Fortuna et al. [45] using files and KDD dataset. They used different algorithms of SVM i.e. 1-v-1, 1-v-all and 1-v-all 3 category. The best results for 1-v-all 3 category are summarized in table 11. The available hybrid systems are EMERALD, NIDES, and Common Intrusion Detection Framework (CIDF) etc.

The details can be summarized in table 12

5. Summary and Conclusion

Though briefly, we present in general the security objectives and possible attack violating the security objectives of any organization and classification of IDS based on various processing components. Details of various AI based techniques applied in intrusion detection are presented. Finally, a multi classifier approach is discussed that results into detection of known and unknown attacks with high accuracy and low false alarm rate. All these techniques discussed above either train single detector to detect different of classes of attacks or reduce the number of features to make the approach computationally efficient. This compromises detection accuracy and false alarm rate. There is acute need to identify various features to detect different classes of attacks and efficient AI based techniques that can protect the systems. More research on efficient & accurate AI based classification techniques remains to be done so that flexible and adaptable security system can be developed to cope with ever growing number of severe Internet attacks.

6. References

1. Underlying Models for IT Security, NIST, SP800-33, p. 2.
2. CERT, www.cert.org
3. Malaysian Computer Emergency Response Team (MyCERT), <http://www.mycert.org.my/en/services/advisories/mycert/2009/main/detail/641/index.html> [last visited on 9th July 2009]
4. FBI/CSI Computer Crime and Security Survey 2008 Computer Crime Research Center, Available at: i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2008.pdf (last accessed 30th July 2009)
5. Axelsson S (1999), "Research in Intrusion Detection Systems: A Survey". Technical Report No. 98-17, Dept. of Computer Engineering, Chalmers University of Technology, Gteborg, Sweden.
6. Teresa F. Lunt, R. Jagannathan, Rosanna Lee, Sherry Listgarten, David L. Edwards, Peter G. Neumann, Harold S. Javitz, AI Valdes: "IDES: The Enhanced Prototype - A Real-Time Intrusion-Detection Expert System (1988)" USA Oct 1988.
7. Sebring, M. M.; Sellhouse, E.; Hanna, M. E.; Whitehurst, R. A.: Expert system in intrusion detection: A case study, in Proc. of the 11th National Computer Security Conference, Baltimore, MD, Oct. 1988, 74-81
8. Smaha, Stephen E., "Haystack: An Intrusion Detection System," The Fourth Aerospace Computer Security Applications Conference, Orlando, FL, December, 1988.
9. Heberlein, L. Todd, Dias, Gihan V., Levitt, Karl N., Mukherjee, Biswanath, Wood, Jeff, and Wolber, David, "A Network Security Monitor," 1990 Symposium on Research in Security and Privacy, Oakland, CA, pages 296-304
10. Paxson, Vern, "Bro: A System for Detecting Network Intruders in Real-Time," Proceedings of The 7th USENIX Security Symposium, San Antonio, TX, 1998.
11. Jani habra, B le Charlier, A mounji, I Mathieu: ASAX: software architecture and rule based language for universal audit trail analysis, computer security, proc. Of ESORICS 92, vol 648 of LNCS pages 435-40, Toulouse, 1992.
12. Koral Ilgun, Richard A. Kemmerer, Phillip A. Porras : State Transition Analysis: A Rule-Based Intrusion Detection, IEEE transaction on software engineering 21 (3):181 1999 march 1995.
13. Sandeep Kumar, Eugene H. Spafford , A Pattern Matching Model for Misuse Intrusion Detection (1994), Proceedings of the 17th National Computer Security Conference, pages 11-21, Baltimore MD, USA.
14. H. S. Vaccaro, G. E. Liepins, Detection of anomalous computer session activity, Proceedings., 1989 IEEE Symposium on Security and Privacy, 1989. pp. 280-289.
15. Dowell, Cheri, and Ramstedt, Paul, "The Computer Watch Data Reduction Tool," Proceedings of the 13th National Computer Security Conference, Washington, D.C., 1990
16. S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip and D. Zerkle, GrIDS - a graph-based intrusion detection system for large networks, in: The 19th National Information Systems Security Conference
17. D Anderson, T Lunt, H Javitz, Ann T and A Valdes: Next Generation intrusion detection expert system (NIDES), technical report, SRI International USA 1995.
18. Philip A porras, Perter G Neumann, EMERLAD: proc. of 20th national information systems security conf. page 353-365, USA 1997.
19. Lan Goldberg, D wagner, R thomans "A Secure Environment for Untrusted Helper Applications: Confining the Willy Hacker," Sixth USENIX Security Symposium, Jul. 22-25, 1996,
20. Mario Castro Ponce, "Intrusion Detection System with Artificial Intelligence" FIST Conference - June 2004 edition-1/28 Universidad Pontificia Comillas de Madrid.
21. Dima Novikov, Roman V. Yampolskiy, Leon Reznik "ARTIFICIAL INTELLIGENCE APPROACHES FOR INTRUSION DETECTION" Systems, Applications and Technology Conference, 2006. LISAT 2006. IEEE Long Island Volume, Issue, 5-5 May 2006 Page(s):1-8
22. I. Levin, KDD-99 Classifier Learning Contest LLSOFT's Results Overview, SIGKDD Explorations, vol. 1 (2000).
23. R. Agarwal and M. Joshi, PNRULE: A New Framework for Learning Classifier Models in Data Mining, Technical Report TR 00-015 (2000).
24. D. Y. Yeung and C. Chow, Parzen-window Network Intrusion Detectors, Sixteenth International Conference on Pattern Recognition (2002).
25. John E. Dickerson and Julie A. Dickerson : Fuzzy Network Profiling for Intrusion Detection- Proceedings of NAFIPS 19th International Conference of the North American Fuzzy Information Processing Society, Atlanta 2000.
26. Norbik Bashah Idris, Bharanidharan Shanmugam: Artificial Intelligence Techniques Applied to Intrusion Detection, IEEE Indicon 2005 Conference, Chennai, India, 11-13 Dec. 2005 pp 52-55.
27. R. Cunningham and R. Lippmann, Detecting Computer Attackers: recognizing patterns of malicious stealthy behavior, MIT Lincoln Laboratory - Presentation to CERIAS (2000).
28. R. Cunningham and R. Lippmann, Improving Intrusion Detection performance using Keyword selection and Neural Networks, MIT Lincoln University (1998).
29. A. Ypma and R. Duin, Novelty Detection using Self-Organizing Maps, Progress in Connectionist-Based Information Systems, vol. 2 (1998).
30. Alan Bivens, Chandrika Palagiri, Rasheda Smith, Boleslawszymanski: Network-Based Intrusion Detection Using Neural Networks, Proc. ANNIE 2002 Conference 2002, pages 10-13, ASME Press.
31. G. Kayacik, N. Zincir-Heywood and M. Heywood, On the Capability of an SOM based Intrusion Detection System, IEEE 0-7803-7898-9 (2003).
32. M. V. Mahoney and P. K. Chan, "PHAD: Packet Header Anomaly Detection for Identifying Hostile Network Traffic " Department of Computer Sciences, Florida Institute of Technology, Melbourne, FL, USA, Technical Report CS-2001-4, April 2001.
33. M. V. Mahoney and P. K. Chan, "Learning Models of Network Traffic for Detecting Novel Attacks " Computer Science Department, Florida Institute of Technology CS-2002-8, August 2002.
34. M. V. Mahoney and P. K. Chan, "Learning Nonstationary Models of Normal Network Traffic for Detecting Novel Attacks," in Eighth ACM SIGKDD international conference on Knowledge discovery and data mining, Edmonton, Canada, 2002, pp. 376-385.
35. Vapnik. N. Vladimir, "The Nature of Statistical Learning Theory", Springer, 1995.
36. Srinivas Mulkamala and Andrew H. Sung, "A Comparative Study of Techniques for Intrusion Detection " Proceedings of the 15th IEEE International Conference on Tools with Artificial

Intelligence (ICTAI'03) 2003

37. H. Sung, S. Mukkamala (2003) Feature Selection for Intrusion Detection Using Neural Networks and Support Vector Machines. 82nd Annual Meeting of the Transportation Research Board (of the National Academies). (Washington D.C., USA)
38. Wun-Hwa Chen, Sheng-Hsun Hsu, Hwang-Pin Shen "Application of SVM and ANN for intrusion detection" Computers & Operations Research 32 (2005) 2617–2634
39. Sanjay Rawat, "Efficient Data Mining Algorithms for Intrusion Detection" PhD thesis, University of Hyderabad, Hyderabad, June 2005
40. Mukesh Sabhnani and G. Serpen, Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context, EECS, University of Toledo (2003).
41. J. R. Quinlan. C4.5, Programs for machine learning. Morgan Kaufmann San Mateo Ca, 1993.
42. Farnaz Gharibian and Ali A. Ghorbani, "Comparative Study of Supervised Machine Learning Techniques for Intrusion Detection" Fifth Annual Conference on Communication Networks and Services Research (CNSR'07) 2007
43. Mrutyunjaya Panda, Manas Ranjan Patra "A Comparative Study Of Data Mining Algorithms For Network Intrusion Detection" First International Conference on Emerging Trends in Engineering and Technology, IEEE computer society 2008
44. Tsong Song Hwang, Tsung-Ju Lee and Yuh-Jye Lee: A Three-tier IDS via Data Mining Approach, Workshop on Mining Network Data (MineNet) 2007
45. Carolina Fortuna, Blaz Fortuna, Mihael Mohorcic: Anomaly Detection In Computer Networks Using Linear SVMs, SiKDD 2007, October 8 -12, 2007, Ljubljana, Slovenia
46. S. Mukkamala, A. H. Sung (2003) Artificial Intelligent Techniques for Intrusion Detection. IEEE International Conference Systems, Man, and Cybernetics. (Washington D.C., USA).
47. Heckerman D. A tutorial on learning with Bayesian networks. Microsoft Research; 1995. Technical Report MSRTR-95-06.
48. P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, E. Vazquez: "Anomaly-based network intrusion detection: Techniques, systems and challenges", computers & security 28 (2009) 18–28.

7. List Of Figures

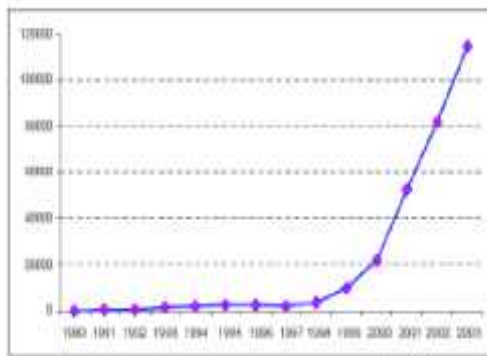


Fig 1 : Growth rate of Internet Attacks

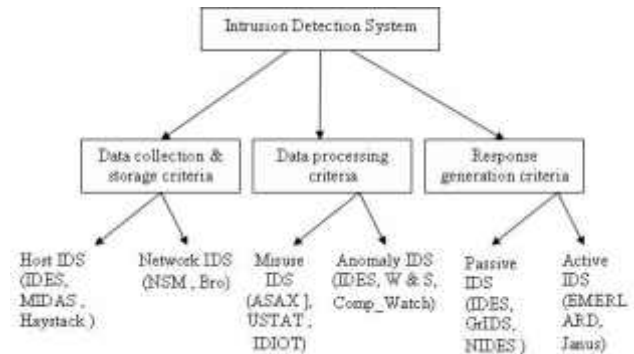


Figure 3 : Classification of IDS

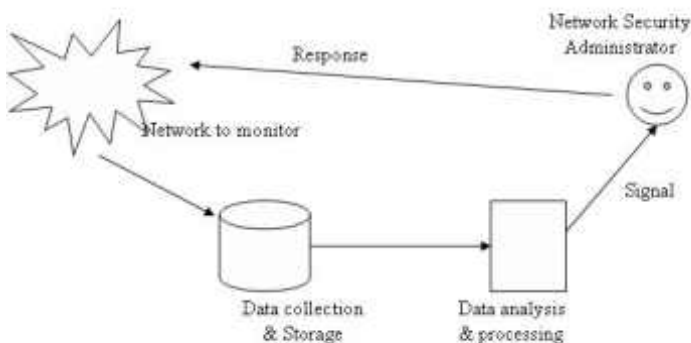


Figure 2 : Architecture of IDS

List Of Tables

Name of system	Detection principle	Data collection source	Type of response
NSM	Hybrid	Network	Passive
Bro	Signature based	Network	Passive
MIDAS	Hybrid	Host	Passive
Haystack	Hybrid	Host	Passive
IDES	Anomaly based	Host	Passive
W & S	Anomaly based	Host	Passive
Comp Watch	Anomaly based	Host	Passive
ASAX	Signature based	Host	Passive
USTAT	Signature based	Host	Passive
IDIOT	Signature based	Host	Passive
GrIDS	Hybrid	Both	Passive
NIDES	Hybrid	Host	Passive
EMERLARD	Hybrid	Both	Active
Janus	Signature based	Host	Active

Table 1

	Normal	Probe	DoS	U2R	R2L
Detection accuracy	99.42 %	84.52 %	97.5%	11.8%	7.32%
False positive rate	-	21.6%	73.1%	36.4%	1.7%

Table 2

	Probe	DoS	U2R	R2L
Detection accuracy	99.2%	96.7%	93.6%	31.2%
False positive rate	No data available			

Table 3

	Normal	Probing	DoS	U2R	R2L
Detection accuracy	99.5%	73.2	96.9%	6.6%	10.7
False positive rate	27%	7.5%	0.05%	89.5%	12%

Table 4

	Normal	Probe	DoS	U2R	R2L
LGP	99.64	99.86	99.90	64	99.47
SVM	98.42	98.57	99.11	64	97.33
MARS	99.71	56.57	99.60	28	98.93
NN (RBP)	99.57	92.71	97.47	48	95.02

Table 5

Attack class	Best classifier	Probability of detection	False alarm rate
Probing	MLP	88.7%	0.4%
DoS	K-Means clustering	97.3%	0.4%
U2R	K-Means clustering	29.8%	0.4%
R2L	Gaussian classifier	9.6%	0.1%

Table 6

	Probing	DoS	U2R	R2L
Gaussian	87.3	96.70	48.6	13.6
Naive Bayes	81.6	79.10	84.3	12.5
Decision Tree	73.6	97.20	28.6	9.3
Random Forest	74.5	97.2	25.7	5.5

Table 7

Technique	Attack class
Gaussian	R2L,Probe
Naive Bayes	U2R,Probe
Decision Tree	DoS
Random Forest	DoS

Table 8

		Probe	DoS	U2R	R2L
Naive Bayes	Precision rate	96%	99 %	90.47%	90%
	False positive rate	0.0014	0.26	0.000163	0.00025
J48	Precision rate	93.16	92.41	40	75
	False positive rate	0.0008	0.0458	0.0004	0.00026
ID3	Precision rate	94.75	92.41	41.86	77.94
	False positive rate	0.0006	0.0458	0.00038	0.000229

Table 9

Class/detection accuracy	Old attacks	New attack	Total detection
Probing	99.92%	98.16%	99.16%
DoS	99.99%	18.03%	97.65%
U2R	20.57%	87.83%	76.32%
R2L	79.84%	26.94%	46.53%

Table 10

	Normal	Probing	DoS	U2R	R2L
Detection accuracy	98.3%	74.8%	96.7%	7.1%	0.8%
True positives	71.1%	82.8%	99.6%	29.4%	55.6%

Table 11

AI Technique		Anomaly/ misuse based	AN N	SV M	Decisi on tree	clusteri ng	G A	Other	Datase t used	Available system	Descript ion
Decision tree based	Levin et al	Misuse			✓				KDD	ID3, C4.5	
	Agarwal et al	Misuse			✓				KDD		
Parzen window based	Yeung et al	Anomaly						✓	KDD		
Rule based	Agarwal et al	Misuse						✓ (PNrule)	KDD	EMERALD at SRI	
Data mining	Dickerson et al							✓ (fuzzy logic)		Data Mining for Network Intrusion Detection at MITRE corporation, Intelligent Intrusion Detection (IIDS) at Mississippi State University	FIRE
	Norbik et al							✓ (fuzzy logic)			Modified FIRE
Machine learning	Lippermann et al	Anomaly	✓						DARPA	Genetic Art For Intrusion Detection (GA-IDS) at Northwestern University, Minnesota Intrusion Detection System (MINDS) at University of Minnesota, NFIDS at Tehran University	
	Biven et al	Anomaly	✓						DARPA		
	Kayrik et al		✓						KDD		
	Canndey	Misuse	✓								
	Mahoney							✓ (Markkov model)	DARPA		
	Mukkanmala et al	Anomaly		✓					DARPA		
	Wun-Hwa et al	Anomaly		✓					DARPA		
Multi classifier	Mukkanmala et al	Anomaly	✓	✓			✓	MARS	DARPA		
	Subhnani et al	Anomaly	✓		✓	✓		GAU, IRBF, LEA, HYP, ART,	KDD		
	Farnaz et al	Misuse			✓			Naive Bayes, Gaussian, Random Forests	KDD		
	Panda et al	Misuse			✓			Naive Bayes	KDD		
Hybrid system	Tsong Song et al	Both		✓					KDD		
	Carofida	Both		✓					KDD		

Table 12