INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A SURVEY ON INTELLIGENCE INTRUSION DETECTION SYSTEMS

Hamid Kanani[1-2], Shahram Jamali[3]

[1] *Department of Computer Engineering, Ardabil Science and Research Branch, Islamic Azad University, Ardabil, Iran*
[2] *Department of Computer Engineering, Ardabil Branch, Islamic Azad University, Ardabil, Iran*
[3] *Department of Computer Engineering, University of Mohaghegh Ardabili, Ardabil, Iran*

Abstract: - With the increasing number of users and systems connected to networks, both Internet and individual systems are in danger of intrusion. Various intrusion preventions techniques have been implemented to protect computer systems in the form of authentication and firewalls. However, only the intrusion prevention is not sufficient, as those systems become more complex with the rapid growth and expansion of Internet technology and local network systems. Therefore, Intrusion Detection Systems are designed to keep computer systems security by monitoring Internet and individual systems for suspicious activities. The main intrusion detection techniques have misuse detection and anomaly detection. In recent year use data mining and Machine learning method to design intrusion detection system. In this paper, a survey on intelligent techniques for intrusion detection in networks based on neural networks, genetic algorithms, genetic network programming, fuzzy techniques, and class assassination rule mining has been described. These techniques have been useful for effectively identifying and detecting network intrusions in order to provide security to the networks and to enhance the detection rate.

Keywords*:* Intrusion, Authentication, Misuse detection, Anomaly detection, Data mining.

1. Introduction

Since computer virus was first described by Fred Cohen (F.Cohen), various types of attacks proliferated on computers and Internet. Some of them are produced manually by attackers, which aims at stealing the personal information. Some of them are programmed by hackers, which aim at disrupting the Internet and infecting other systems automatically. On the other hand, the number of users and systems connected to the networks grew dramatically as connecting to networks became more much easier, and the development of e-commerce and e-government dramatically accelerated this process. Many individual persons and organizations prefer using Internet for routine works and business affairs (M.Bishop). Thus, security problems become serious in recent years. Firewalls as a passive defence device is not enough to keep networks secure. Therefore, Different kinds of Intrusion Detection Systems (IDSs) are designed to protect computer networks against various attacks.

Intrusion Detection Systems (IDSs) are software and/or hardware structures that detect malicious behaviours in the systems they protect and produce relevant alerts.

Intrusions can be generally distinguished into known intrusions and unknown intrusions. Both two kinds of intrusions may compromise confidentiality, integrity or availability of the systems or computers (SANS) (Y. a. K.Hwang) (Y. S. K.Hwang) (Z.Yu). Therefore, broadly speaking, there are two kinds of intrusion detection techniques corresponding to known intrusions and unknown intrusions: misuse detection and anomaly detection (B.Mukherjee) (Sundaram.) (R.A.Kemmerer). Misuse detection (B.Mukherjee) (O.Depren) essentially identifies the previously known attacks from normal network connection data. It utilizes the signatures of the known attacks and matches them against the observed activity. If it matches a previously known attack signature, the activity will be detected as an attack. However, if a new attack is produced, the system fails to recognize it. In conclusion, the main advantage of misuse detection is that it focuses on analysing the known attacks and produces few false alarms. The main disadvantage of misuse detection is that it can detect only known attacks which have defined signatures.

Anomaly detection technique (B.Mukherjee) (V. Chandola) (M.Park) establishes the profile of the normal activities of the computer or Internet. It looks for the deviation between the observed activity and normal patterns. Once it does, the observed activity is identified as anomaly intrusion. The main advantage of anomaly detection systems is that they can detect previously unknown attacks. By defining what's normal, they can identify the abnormal whether it is an attack or not. In actual systems, however, it results in a large number of false alarms. Anomaly detection systems are also difficult to be realized in highly dynamic environments.

There are two types of intrusion detection systems that employ one or both of the Intrusion detection techniques introduced above (B.Mukherjee). The principles of the Host-based IDS and Network-based IDS are very similar in that intrusion detection is based on analysing the observed events for patterns, but their operations are quite different (J.Hu).

Host-based systems (Ding) (A.Balaz) (D. Mutz) focus their analysis on user activity or program behaviour at the operating system or application level, while network-based intrusion detection systems obtain data by monitoring the traffic and examining network packets in the network to which the hosts are connected (W. Hu) (S. Chebrolu).

Host-based intrusion detection systems (P.Soto) detect intrusions using audit data which are collected from the target host machine. As the information provided by the audit data can be extremely comprehensive and elaborate, host-based systems can obtain high detection rates and few false alarms. However, there are disadvantages for host based approaches. Firstly, host-based systems cannot easily prevent attacks: when an intrusion is detected, the attack has partially occurred. Secondly, audit data may be altered by attackers, which influence the reliability of audit data.

IDSs can be used to protect a single host or a huge computer network. IDS research has been continuously evolving in order to create robust and effective technologies that will be able to classify activity in a system at an acceptable success rate (G.P. Spathoulas).

Intrusion detection techniques using data mining have attracted more and more interests in recent years. As an important application area of data mining, they aim to meliorate the great burden of analysing huge volumes of data and realizing performance optimization of detection rules. Intelligent IDSs are the ones considered to be intelligent computer programs situated in either a host or a network which analyses the environment and acts flexibly to achieve higher detection accuracy (S.Franklin) (N.Jaisankar).

2. Intelligent intrusion detection system

In recent year many approach to design IDS is described, such as Pattern Matching (E.H.Spafford) (C. Zhou), Statistical Models (C.Manikopoulos) (W. Teng), Information Theoretic measures (Xiang), Data Mining (S. S. W. Lee) (Brugger), Immune System (P. D. Williams) and Machine Learning (P. Laskov) (Paxson). Etc... The

intent of the followings is to give a brief overview of recent intrusion detection approaches on some of these fields.

2.1 Statistical Modelling

Statistical Modelling (C.Manikopoulos) (W. Teng) (N. Ye) (A. Qayyum) is one of the earliest methods used for anomaly detection. It measures the user and system behaviour by a number of variables sampled over time, and builds profiles based on the variables of normal behaviours. The actual variables are then compared against the profiles, and deviations are considered abnormal.

There are many statistical techniques (Hunt). Denning (Denning) proposed a statistics models for intrusion detection. According to audit data, the variables were represented as different metrics. Then, to describe the profiles of variables, a serious of statistical models were built, including mean and standard deviation, multivariate model, Markov process model and time series model. But, these methods construct too simple models leading to worse discrimination. The next generation intrusion detection expert system is the representative IDS based on statistics, which measures the similarity between long term behaviours and short-term behaviours of the systems for intrusion detection (D. Anderson). (J. B. D. Caberera) examined the application of Statistical Traffic Modelling for detecting novel attacks against computer networks. In this method, Kolmogorov-Smirnov statistics was used to model and detect DoS as well as probing attacks. Ye et.al. (Ye) Developed an anomaly detection technique, where the norm profile of temporal behaviours learns the Markov chain model from computer connection data, and detects anomalies based on The Markov chain model of temporal behaviours. However, this method could not provide accurate classification since various features of the connection level are ignored. The multiple linear regression analysis which is one of multivariate statistical analysis methods was used in (Okamoto) to analyze network traffic. But, it is not suitable to express an attack using the linear model since it may be nonlinear.

In short, these approaches in anomaly detection require the construction of a model for normal user behaviour, and any user behaviour that deviates significantly from this normal behaviour is flagged as an intrusion. It can also be difficult to determine the correct anomaly threshold at which behaviour is to be considered an intrusion. Also, to apply statistical techniques, too many assumption conditions are needed, which may contradict the facts.

2.2 Supervised Learning Approaches

Supervised learning is the machine learning task of building a model using labelled Training data.

Naive Bayes classifier (N. B. Amor) is composed of Directed Acyclic Graph (DAG) which is trained as well as Conditional Probability Table (CPT) by the training connection data. Then, it is possible to classify any new data with its attributes values using the Bayes rules based on the quantified network structure. However, Naive Bayes classifier makes a strong independence relation assumption between features when the features are correlated.

S. Mukkamal et.al (S. Mukkamala) implemented Support Vector Machine(SVM) to classify new connection data into normal and intrusion by mapping real valued input feature vectors to a higher dimensional feature space. It has the advantage of dealing with high dimensionality of data. But, the performance of SVM approach lies in the choice of the kernel, which makes it difficult to deal with large scale database.

Neural networks are also used to realize IDS in many researches (A. Rapaka). They are algorithmic techniques (Silva) which are used to first learn the relationship among information and then generalize to obtain new input-output pairs in a reasonable way. Multi-Layer Perceptron (MLP) is a feed forward artificial neural network model that maps the set of input data into the set of appropriate outputs (Cannady). A MLP consists of multiple layers of nodes in a directed graph, with each layer being connected fully to the next layer. In (Chen.),

MLP is the basic unite of the ensemble classifiers. In this way, the different sources of information are integrated with each other, which are called data fusion. Although the neural networks can work effectively with noisy data, they require a large amount of data for the training and it is often hard to select the best architecture for the neural networks. Adaboost is an important method of ensemble learning. It is a stereotype algorithm of boosting, whose basic idea is to select and combine a group of weak classifiers to form a strong classifier (Schapire). But, a group of weak classifiers is required to be designed beforehand. In (W. Hu), weak classifier is constructed by the decision stump which is a decision tree with a root node and two leaf nodes. However, the performance of Adaboost algorithm always relies on the weak classifiers. In addition, it is easily influenced by noises.

2.3 Unsupervised learning Approaches

In machine learning, unsupervised learning refers to the problem of trying to find hidden structure in unlabelled data. Data clustering is a main type of unsupervised methods, such as K-means and fuzzy c-means (L. Portnoy). One of the main drawbacks of the clustering technique is that it is based on calculating the numeric distance between the observations, hence the observations must be numeric. Observations with symbolic features cannot be easily used for clustering, which result in inaccuracy. In addition, the clustering methods consider the features independent and are unable to capture the relationship among different features of a single record, which further degrades the detection accuracy of the attacks.

A self-organizing map (SOM), also known as Kohonen map, is a typical unsupervised neural network based on competitive learning. It can organize and train the structure of neural networks by itself. Except input layer and output layer, it has a competitive layer. Hoglund et al. (A. J. Hoglund) extract features that describe network behaviours from audit data, and they use the SOM to detect intrusions. Kayacik et al. (H. G. Kayacik) propose a hierarchical SOM approach for intrusion detection. Specific attention is given to the hierarchical development of abstractions, which is sufficient to permit direct labeling of SOM nodes with connection type.

2.4 Data Mining Approaches

Data mining approaches generally discover relevant patterns of programs and user behaviours, which are mainly in the form of rules or frequent episodes. Lee et al. (Stolfo) develop a data mining framework MADAM ID (Mining Audit Data for Automated Models for Intrusion Detection) for mining audit data to discover useful frequent patterns and association rules. In this approach, the learned rules replace the manually encoded intrusion patterns and profiles. PIPPER, a rule learning tool, has been used for automatic construction of the detection models in MADAM ID. ADAM (Audit Data Analysis and Mining) (S. J. W. Lee) uses a frequent itemset-based association rule mining algorithm in detection as an online network-based IDS. The framework of ADAM has two phases: training phase and on-line phase. In the training phase, the attack-free training data is fed to a module whose output is a rule-based profile of normal activities. After that, the produced profile is input to another module to perform a dynamic on-line algorithm with association rules.

Some approaches belonging to Soft Computing (SC) are used to find rules from either host audit data or network traffic. Generally speaking, SC is a methodology that provides flexible information processing capability for handling real-life ambiguous situations (Zadeh). Since its features of flexibility and adaptability in new environments and ability of generalizing from training data, it can be widely used in IDS.

Fuzzy set theory is a mathematical technique for dealing with imprecise data and problems with many solutions. It can deal with continuous attributes and handle sharp boundary problems, whose advantages make the rules more comprehensible for humans. (J. E. Dickerson) Proposed Fuzzy Intrusion Recognition Engine (FIRE), which is a network, based intrusion detection system that uses fuzzy system to assess malicious

activity against computer networks. This system uses agent to perform its own fuzzification of input data sources. At the end, all agents communicate with a fuzzy evaluation engine that combines the results of individual agents using fuzzy rules to produce alerts that are true to a degree. A. Tajbakhsh et al. (A. Tajbakhsh) discover fuzzy association rules to build the classifier. In this approach, a set of fuzzy association rules is extracted for each class. In order to determine the label of a new connection data, the similarity of the extracted rules to the new connection data is calculated.

As to Evolutionary Computation, Genetic Algorithm (GA) (Goldberg) is referred firstly. In IDSs, GA can be used to evolve simple rules for either host audit data or network traffic. Besides, GA is a good tool for feature selection (Park) (A. Hofmann) or model selection (D. Kim). In this sense, GA is also used to find the suitable fuzzy membership functions (T. Hong). The final best set of fuzzy membership functions in all populations is gathered to be used for mining fuzzy association rules. However, most of rule mining approaches tend to produce a large number of rules that increase the complexity of the system. In order to solve this problem, many rule pruning methods are proposed. One well known research direction is to remove redundant rules using the concepts of closed item sets (J.M.Zaki) and representative rules (M.Kryszkiewicz). In (J. Li), an algorithm taking advantage of upward closure properties of weak rules is proposed to find a small subset of a class association rule set. And the clustering of association rules has been also used to obtain a reasonable set of rules (B. Lent). But, most of the algorithms need users' information on the complete rule set. Genetic Programming (GP) has been also applied to intrusion detection. GP ensemble (G. Folino) applies cellular GP to create classifiers, which creates some independent decision trees based on different training data and they are finally combined to form the intrusion detection system. On the other hand, Genetic Network Programming (GNP) (K. Hirasawa) has been proposed as an extension of Genetic Algorithm and Genetic Programming (GP). GNP-based data mining has been already applied to intrusion detection systems. The basic framework of IDS using GNP is described in (S. Mabu) where fuzzy class association rule mining is developed and misuse detection and anomaly detection are realized. Then, Fuzzy set theory is induced into GNP to propose the Fuzzy GNP to extract class association rules and misuse detection and anomaly detection are integrated to propose a hybrid intrusion detection system (S. M. N. Lu).

3. Study on IDSs methods

In this section we study about intrusion detection system.

3.1 Class Association Rule Mining and Classification

The proposed hybrid framework generally combines misuse detection and anomaly detection. It can detect misuse intrusions and anomaly intrusions simultaneously. This hybrid intrusion detection system in this chapter contains the two basic components: rule mining and classification. In the rule mining, GNP is used to extract enough class association rules from normal data and misuse intrusion (known intrusion) data. A brand new intrusion should deviate from normal patterns and differentiate from misuse intrusions. Only considering normal patters is not enough to evaluate whether a new connection is anomaly or not. In the classification, the average matching degree is used to project multi-dimensional network connections into a two dimensional space by extracted normal and misuse intrusion rules. Therefore, the combination of misuse detection classifier and anomaly detection classifier is named hybrid classifier/ classification.

3.2 Intrusion Detection System with Rule Pruning using Genetic Network Programming

Class association rule mining is typically known as an important method for data analysis. However, there is a problem in class association rule mining. Even though the goal of the class association rule mining is not to extract a complete set of rules, the number of class association rules extracted is still very large. Therefore, it is

time consuming. Most importantly, the rule pool with a large number of rules usually contains much redundant, irrelevant and obvious information. On the other hand, there are two requirements in intrusion detection. One is the real time, the other is detection ability. This leads to two other issues: we reduce the number of rules in the model.

3.3 Intrusion Detection System using Fuzzy Genetic Network Programming

GNP-based class association rule mining initially deals with the data with discrete attributes. For the data with quantitative attributes, it usually divides them into different ranges by crisp discretization. However, for the values near the border, crisp discretization always results in under or over estimation in mining process, which is called sharp boundary problem. Fuzzy sets theory introduced by Zadeh (A.L.Zadeh) in 1965 can resolve this problem by smoothly transferring between member and non-member in fuzzy membership degrees (values). And fuzzy set theory can also bring solution for imprecision and uncertainty information, because of its simplicity and similarity to human reasoning.
The centric topic of data mining is to extract patterns from transaction data in the form of association rules or class association rules. The previous researches on the rule mining usually deal with the database with those attributes having binary or categorical values. But, for the attributes having quantitative values, it is possible to partition the quantitative values to two or more ranges. However, simple partition leads to losing some important information. In order to reducing the information loss as much as possible, the information gain-based sub-attribute method is utilized to deal with continuous attributes. However, the crisp discretization measure to process continuous attributes results in sharp boundary problem, where the discretization of continuous attributes into intervals would lead to ignore or overemphasize the values that are near boundaries. Fuzzy set theory can help us to overcome this problem by allowing different degrees of memberships. Compared with traditional association rules with crisp sets, the class association rule mining using Fuzzy GNP can provide good linguistic explanation. The features of Fuzzy GNP-based class association rule mining are summarized as follows.

[1] Experienced and expert knowledge on intrusion detection is not required before the training.

[2] Fuzzy GNP can deal with both discrete and continuous attributes in intrusion detection to overtake the sharp boundary problem in sub-attribute method.

[3] Fuzzy GNP can extract diversified class association rules by evolving Fuzzy GNP.

[4] Probabilistic node transition takes place of the traditional node transition in GNP. This change also contributes to extracting diversified rules.

[5] Each continuous attribute has its own initial fuzzy membership function which is different from each other. In addition, the fuzzy membership functions are evolved along with GNP.

3.4 Classification for Intrusion Detection System using Distance Approach

Building an accurate and efficient classifier is one of the essential tasks of data mining and machine learning research. As stated in (s.j.Stolfo), classification generally maps a data into one of several predefined categories. An ideal approach in intrusion detection would be to learn a classifier from gathered normal and intrusion data, then label or predict new unseen data as the normal class or intrusion class. In addition, the two-stage rule pruning method alleviates the overlapping problem by pruning the redundant and irrelevant rules from the rule pool. An efficient classification method is needed to deal with the overlapping part since the rule pruning cannot thoroughly solve this problem. In order to enhance the detection ability of IDS, section 3.2 and section 3.3 will focus on the classification algorithms of intrusion detection systems.

Since efficient classification algorithms are extremely important for intrusion detection, a large number of studies have been conducted. K-Nearest neighbour (KNN) is an extremely simple yet surprisingly effective method for a classification. Its advantages stem from the fact that its decision surface is nonlinear with only a single integer parameter. More importantly, these advantages do not cause the over-fitting (Denning), and it is not restricted to any specific data distribution. The main features of Distance-based classification are summarized as follows.

1. It is a non-parametric approach, where only the number of the closest neighbors should be determined. Whereas, the simulations on different numbers of the closest neighbors indicate that the detection ability is not so sensitive to this number.

2. The nature of anomaly intrusion is taking into account by making full use of the information from normal and misuse intrusion connection data. Therefore, the centroids of different classes are proposed to make the classification.

3.5 Classification for Intrusion Detection System using Gaussian Functions

Anomaly detection is an important problem that has been studied within diverse research areas and application domains, especially for computer security. Finding the hardest-to-detect anomalies is the most critical task in intrusion detection.
In the hybrid framework of the intrusion detection system, it is easy to get good performance when identifying the misuse intrusions from normal data. Whereas, anomaly intrusions are usually difficult to identify because of its no patterns. Traditional detection method of anomaly intrusions relies on normal patterns. However, in reality, the behaviors of normal connection data are too diverse to gather completely. Therefore, if the types of both normal behaviors and misuse intrusion behaviors are considered and the boundary of each type of behaviors is found, then it becomes simple to identify a new connection as normal or intrusion.
It is crucial to adopt an appropriate classification approach for intrusion detection systems. Probabilistic classification proposed in (S. M. N. Lu) assumes that the normal class and misuse intrusion class are independent to estimate the two one dimensional probability density functions which represent the distribution of the data of the normal class and misuse intrusion class, respectively. However, in the field of intrusion detection, the probability density functions of the normal class and misuse intrusion class are usually correlated.
In distance-based classification (S. M. N. Lu), known information of normal and intrusion is used to determine the possible regions of anomaly intrusions. Centroids of anomaly intrusions are defined by normal centroid and intrusion centroid. However, anomaly intrusions are still difficult to distinguish because some of them are close too much to normal or known intrusions. Therefore, it is feasible to identify an anomaly intrusion if the exact boundaries of normal and known intrusions can be found.
This approach is to find such the boundaries of normal and known intrusions. In order to make full use of known information about normal and known intrusions, it is essential to group the similar data into the same cluster, which means they have similar behaviors. Then, the problem becomes finding exact boundary for each cluster. This method intends to solve two points. One is the appropriate number of clusters. The other is the determination of the boundary for each cluster. The advantages of the classification approach are summarized in the following.
1. Both normal and misuse intrusion contain more than one type of behaviors. The clustering is used to gather similar patterns in one cluster automatically.
2. A new clustering method is used by dividing the average matching degree space into many blocks. Each block corresponds to a cluster.
3. Gaussian function is used to decide the boundary of the cluster. Each cluster has its own Gaussian function. All of the Gaussian functions are different with each other.
4. The center of the cluster equals to the center of its Gaussian function. The boundary of the cluster is decided by GA considering its classification performance.

4. Conclusion

Intrusion detection based data mining and intelligence method are currently attracting considerable interest from the research community. Its characteristics, such as adaptation, high detection rate, high speed and error resilience in the face of noisy information, fit the requirement of building a good intrusion detection system.

In this paper, a survey of data mining methods is proposed for building an efficient intrusion detection system. Intrusion detection systems are analyzed from three aspects: class association rule mining, class association rule pruning and classification.

REFERENCES

[1] Hofmann, T. Horeis, and B. Sick. "Feature Selection for Intrusion Detection: An Evolutionary Wrapper Approach." *2004 IEEE International Joint Conference on Neural Networks*. 2004. 1563-1568.

[2] J. Hoglund, K. Hatonen, and A. S. Sorvari. "A Computer Host-based User Anomaly Detection System using the Self-Organizing Map." *Joint Conf. Neural Netw.,*. 2000. 411-416.

[3] Qayyum, M. H. Islam, and M. Jamil. "Taxonomy of Statistical based Anomaly Detection Techniques for Intrusion Detection." *IEEE Symposium on Emerging Technologies*. 2005. 270-276.

[4] Rapaka, A. Novokhodko, and D. Wunsch. "Intrusion Detection using Radial Basis Function Network on Sequences of System Calls." *Joint Conf. Neural Netw.* 2003. 1820-1825.

[5] Tajbakhsh, M. Rahmati, and A. Mirzaei. "Intrusion Detection using Fuzzy Association Rules." *Applied Soft Computing* 9 (2009): 462-469.

[6] A.Balaz, L.Vokorokos. "Host-based Intrusion Detection System." *14th International Conference on Intelligent Engineering Systems (INES)*. 2010. 43-47.

[7] A.L.Zadeh. "Fuzzy Sets." *Information and Control* 18 (1965): 338-353.

[8] Lent, A. Swami, and J. Widom. "Clustering Association Rules." *13th International Conference on Data Engineering*. 1997. 220-231 .

[9] B.Mukherjee, L.T.Heberlein, and K.N.Levitt. "Network intrusion detection." *Network IEEE* 8 (1994): 26-41.

[10] Brugger, S. T. "Data Mining Methods for Network Intrusion Detection." *UC Davis*. 2000.

[11] Zhou, Y. Liu, and H. Zhang. "A Pattern Matching based Network Intrusion Detection System." *9th International Conference on Control, Automation, Robotics and Vision (ICARCV 06)*. 2006. 1-4.

[12] C.Manikopoulos, J.Li and. "Early Statistical Anomaly Intrusion Detection of DOS Attacks using MIB Traffic Parameters." *Information Assurance Workshop Man and Cybernetics Society IEEE Systems* (2003): 53-59.

[13] Cannady, J. "Artificial Neural Networks for Misuse Detection." *National Information Systems Security Conference*. 1998. 443-456.

[14] Chen., D. Parikh and T. "Data Fusion and Cost Minimization for Intrusion Detection." *IEEE Transactions on Information Forensics and Security* (381-389): 2008.

[15] Anderson, T. F. Lunt, H. Javits, A. Tamaru, and A. Valdes. "Detecting Unusual Program Behavior using the Statistics Components." NIDES Technical Report SRI International,. 1995.

[16] Kim, H. Nguyen, and J. Park. "Genetic Algorithm to Improve SVM Based Network Intrusion Detection System." *19th International Conference on Advanced Information Networking and Applications*. 2005. 155-158.

[17] D. Mutz, F. Valeur, G. Vigna, and C. Kruegel. "Anomalous System Call Detection." *ACM Transactions on Information and System Security (TISSEC)* 9 (2006): 61-93.

[18] Denning, D. E. "An Intrusion Detection Model." *IEEE Trans. on Software Engineering* 13 (1987): 222-232.

[19] Ding, D. Y. Yeung and Y. "Host-based Intrusion Detection using Dynamic and Static Behavioral Models." *Pattern Recognition* 36 (2003): 229-243.

[20] E.H.Spafford, S.Kumar and. "Pattern Matching Model for Misuse Intrusion Detection." *17th National Computer Security Conference*. 1994. 11-21.

[21] F.Cohen. "Computer Viruses: Theory and Experiments." *In Proc. of the 7th DOD/NBS Computer Security Conference*. 1984. 240{263.

[22] Folino, C. Pizzuti, and G. Spezzano. "GP Ensemble for Distributed Intrusion Detection Systems." *Pattern Recognition and Data Mining Lecture Notes in Computer Science* 3686 (2995): 54-62.

[23] G.P. Spathoulas, S.K. Katsikas. "Reducing false positives in intrusion detection systems." *computers & security* (2010): 35-44.

[24] Goldberg, D. E. "Genetic Algorithm in Search, Optimization and Machine Learning." *Addison-Wesley* (1989).

[25] G. Kayacik, A. N. Zincir-Heywood, and M. I. Heywood. "On the Capability of An SOM based Intrusion Detection System." *Joint Conf. Neural Netw.* 2003. 1808-1813.

[26] Hunt, T. Verwoerd and R. "Intrusion Detection Techniques and Approaches." *Computer Communications* 25 (2002): 1356-1365.

[27] J. B. D. Caberera, B. Ravichandran, and R. K. Mehra. "Statistical Traffic Modeling for Network Intrusion Detection ." *8th International Symposium on Modeling Analysis and Simulation of Computer and Telecommunication Systems*. 2000. 466-473.

[28] J. E. Dickerson, J. Juslin, O. Koukousoula, and J. A. Dickerson. "Fuzzy Intrusion Detection." *IFSA World Congress and 20th NAFIPS International Conference*. 2001. 1506-1510 .

[29] J. Li, H. Shen, and R. Topor. "Mining the Optimal Class Association Rule Set." *Knowledge-based Systems* (2002): 399-405.

[30] J.Hu, X.Yu, D.Qiu, and H.H.Chen. "A Simple and Efficient Hidden Markov Model Scheme for Host-based Anomaly Intrusion Detection." *Network, IEEE* 23 (2009): 42-47.

[31] J.M.Zaki. "Generating Non-redundant Association Rules." *sixth ACM SIGKDD international conference on Knowledge Discovery and Data Mining*. 2000. 34-43.

[32] K. Hirasawa, M. Okubo, H. Katagiri, J. Hu, and J. Murata. "Comparison Between Genetic Network Programming (GNP) and Genetic Programming(GP)." *Congress on Evolutionary Computation, pages 1276{1282, 2001*. 2001. 1276-1282.

[33] K.Hwang, Y.Chen, and H.Liu. "Defending Distributed Computing Systems from Malicious Intrusions and Network Anomalies." *In Proc. of the 19th IEEE International Parallel and Distributed Processing Symposium*. 2005.

[34] K.Hwang, Y.Kwok, S.Song, M.Cai, Y.Chen, and Y.Chen. "DHT-Based Security Infrastructure for Trusted Internet and Grid Computing." *International Journal Of Critical Infrastructures* 4 (2006): 412-433.

[35] L. Portnoy, E. Eskin, and S. Stolfo. "Intrusion Detection with Unlabeled Data using Clustering." *ACM Workshop Data Mining Applied to Security(DMSA)*. 2001.

[36] M.Bishop. "Computer Security in the Future." *The ISC International Journal of Information* 3 (2011): 3-27.

[37] M.Kryszkiewicz. "Representative Association Rules and Minimum Condition Maximum Consequence Association Rules." *Lecture Notes in Computer Science*. 1998. 361-369.

[38] M.Park, A.Patcha and J. "An Overview of Anomaly Detection Techniques: Existing Scheme for Host-based Anomaly Intrusion Detection." *Network, IEEE* 23 (2009): 42-47.

[39] N. B. Amor, S. Benferhat, and Z. Elouedi. "Naive Bayes vs Decision Tree in Intrusion Detection." *2004 ACM symposium on Applied computing*. 2004.

[40] N. Lu, S. Mabu, and K. Hirasawa. "Integrated Rule Mining based on Fuzzy GNP and Probabilistic Classification for Intrusion Detection." *Journal of Advanced Computational Intelligence and Intelligent Informatics* 15 (2011).

[41] N. Lu, S. Mabu, T. Wang, and K. Hirasawa. "Distance-based Classification using Average Matching Degree and its Application to Intrusion Detection Systems." *IEEJ Transactions on Electronics, Information and Systems* 132 (2012).

[42] N. Ye, S. M. Emran, X. Li, and Q. Chen. "Statistical Process Control for Computer Intrusion Detection." *DARPA Information Survivability Conference and Exposition*. 2001. 3-14.

[43] N.Jaisankar, SGP.Yogesh, A.Kannan And K.Anand, Intelligent. "Agent Based Intrusion Detection System Using Fuzzy Rough Set Based Outlier Detection." *Soft Computing Techniques* (2012): 147-153.

[44] O.Depren, M.Topallar, E.Anarim, and M.K.Ciliz. "An Intelligent Intrusion Detection System (IDS) for Anomaly and Misuse detection in Computer Networks." *Expert Systems with Applications* 29 (2005): 713-722.

[45] Okamoto, A. Kanaoka and E. "Multivariate Statistical Analysis of Network Traffic for Intrusion Detection." *14th International Workshop on Database and Expert Systems Applications*. 2003. 472-476.

[46] P. D. Williams, K. P. Anchor, J. L. Bebo, G. H. Gunsch, and G. D. Lamont. "CDIS:Towards a Computer Immune System for Detecting Network Intrusions." *4th International Symposium on Recent Advances in Intrusion Detection*. 2001. 117-133.

[47] P. Laskov, P. Dssel, C. Schfer, and K. Rieck. "Learning Intrusion Detection: Supervised or Unsupervised?" *Image Analysis and ProcessingICIAP 2005 Lecture Notes in Computer Science*. 2005. 50-57.

[48] P.Soto, D. Wagner and. "Mimicry Attacks on Host-based Intrusion Detection Systems." *In Proc. of the 9th ACM conference on Computer and Communications Security*. 2002. 255-264.

[49] Park, K. Shazzad and J. "Optimization of Intrusion Detection through Fast Hybrid Feature Selection." *Sixth International Conference on Parallel and Distributed Computing Applications and Technologies*. 2005. 264-267.

[50] Paxson, R. Sommer and V. "Outside the Closed World: on using Machine Learning for Network Intrusion Detection." *IEEE Symposium on Security and Privacy (SP)*. 2010. 305-316.

[51] R.A.Kemmerer. "Intrusion Detection: A Brief History and Overview." *Computer* 35 (2002): 27-30.

[52] S. Chebrolu, A. Abraham, and J. P. Thomas. "Feature Deduction and Ensemble Design of Intrusion Detection Systems." *Computer and Security* 24 (2005): 295-307.

[53] S. Mabu, C. Chen, N. Lu, K. Shimada, and K. Hirasawa. "An Intrusion-Detection Model Based on Fuzzy Class-Association-Rule Mining Using Genetic Network Programming." *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews* 41 (2011): 130-139.

[54] S. Mukkamala, G. Janoski, and A. Sung. "Intrusion Detection using Neural Networks and Support Vector Machines." *Joint Conf. Neural Netw*. 2002. 1702-1707.

[55] S.Franklin, A.Graser. "Is it an agent or just a program? in ." *ECAI '96 Proceedings of the Workshop on Intelligent Agents III, Agent Theories, Architectures, and Languages*. London: Springer, 1996.

[56] s.j.Stolfo, W. Lee and. "A Framework for Constructing Features and Models for Intrusion Detection Systems." *ACM Trans. on Information and System Security* 3 (2000): 227-261.

[57] SANS. *SANS Institute-Intrusion Detection FAQ*. 2012. <http://www.sans.org/resources/idfag/>.

[58] Schapire, Y. Freund and R. E. "A Decision-Theoretic Generalization of On-line Learning and An Application to Boosting. Lecture Notes." *Computer Science* (1995): 23-37.

[59] Silva, F. Karray and C. "Soft Computing and Intelligent Systems Design: Theory Tools and Applications." *Addison Wesley Publishing* (2004).

[60] Stolfo, W. Lee and S. J. "A Framework for Constructing Features and Models for Intrusion Detection Systems." *ACM Trans. on Information and System Security* (2000): 227-261.

[61] Sundaram., A. "An Introduction to Intrusion Detection." *Special Issue on Computer Security* 2 (1996): 3-7.

[62] T. Hong, C. Chen, Y. Lee, and Y. Wu. "Genetic-Fuzzy Data Mining with Divide-and-Conquer Strategy." *IEEE Trans. on Evolutionary Computation* 12 (2008): 252-265.

[63] V. Chandola, A. Banerjee, and V. Kumar. "Anomaly Detection: A Survey." *ACM Computing Surveys (CSUR)*. 2009.

[64] W. Hu, W. Hu, and S. Maybank. "AdaBoost-Based Algorithm for Network Intrusion Detection." *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics* 38 (2008): 577-583.

[65] W. Lee, S. J. Stolfo, and K. W. Mok. "Mining Audit Data to Build Intrusion Detection Models." *ACM SIGKDD International Conference on Knowledge Discovery and Data mining*. 1998. 66-72.

[66] W. Lee, S. Stolfo, P. K. Chan, E. Eskin, W. Fan, M. Miller, S. Hershkop, and J. Zhang. "Real Time Data Mining-based Intrusion Detection." *DARPA Information Survivability Conference and Exposition II*. 2001. 85-100.

[67] W. Teng, M. Hsieh, and M. Chen. "A Statistical Framework for Mining Substitution Rules." *Knowledge and Information Systems* 7 (2005): 158-178.

[68] Xiang, W. Lee and D. "Information-Theoretic Measures for Anomaly Detection." *2001 IEEE Symposium on Security and Privacy*. 2001. 130-143.

[69] Ye, N. "A Markov Chain Model of Temporal Behavior for Anomaly Detection." *IEEE SMC Inform. Assurance Security Workshop*. 2000. pages 166-169.

[70] Z.Yu, J. J. P. Tsai, and T.Weigert. "An Automatically Tuning Intrusion Detection system." *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics* 37 (2007): 373-384.

[71] Zadeh, L. A. "Fuzzy Logic, Neural Networks, and Soft Somputing." *Communications of the ACM* 37 (1994): 77-84.