ISSN: 1304-7981 Number: 2, Year: 2013, Pages: 76-91 http://jnrs.gop.edu.tr

Gaziosmanpasa University

Graduate School of
Natural and Applied Sciences

Journal of New Results in Science

Received: 25.02.2013
Accepted: 22.08.2013

Editors-in-Chief: Naim Çağman
Area Editor: Oktay Muhtaroğlu

Intrusion Detection By Data Mining Algorithms: A Review

Marjan Kuchaki Rafsanjani[a,1] **(kuchaki@uk.ac.ir)**
Zahra Asghari Varzaneh[a] **(asghari_za@yahoo.com)**

[a] *Department of Computer Science, Shahid Bahonar University of Kerman, Kerman, Iran*

Abstract − With the increasing use of network-based services and sensitive information on networks, maintaining information security is essential. Intrusion Detection System is a security tool used to detect unauthorized activities of a computer system or network. Data mining is one of the technologies applied to intrusion detection. This article introduces various data mining techniques used to implement an intrusion detection system. Then reviews some of the related studies focusing on data mining algorithms.

Keywords *-*
Intrusion Detection Systems(IDS), Data mining, Feature selection, Machine learning.

1. Introduction

With the increasing use of network-based services and sensitive information on networks, information security of using the Internet as the media needs to be carefully concerned.
A secure network must provide the following:

• Data confidentiality: The confidentiality property specifies that the only entities authorized to access some particular information are allowed to do so.

• Data integrity: Only authorized entities can alter information within a system. This is the property that keeps information from being changed when it should not be.

[1] ***Corresponding Author***

• Data availability: Availability is the property that the information on a system is obtainable when needed [1].

To prevent these security compromises, layers of defense are used. Preventative measures in the network include proxies, filters, and firewalls. Hosts are also protected through proactive patching, using antivirus and anti-spyware technology, eliminating unnecessary services, and implementing user authentication and access controls [2]. Particularly, intrusion detection systems (IDSs) aid the network to resist external attacks. That is, IDS is a security tool used to detect unauthorized activities of a computer system or network. Data mining is one of the technologies applied to intrusion detection. The remainder of this article is organized as follows. Section 2 provides an overview of IDSs and briefly describes the theme. Section 3 introduces data mining and illustrates how data mining can be applied in IDSs. Section 4 describes the various data mining techniques used to implement IDSs and compares them based on advantages and disadvantages. Section 5 reviews some of the related studies focusing on data mining algorithms to implement IDs.

2. Intrusion Detection Systems (IDS)

Intrusion activities of computer systems are increasing due to the commercialization of the internet & local networks. An IDS, collects the information and analyzing it for uncommon or unexpected events. ID is the process of monitoring and analyzing the events which occurred in a computer system in order to detect signs of security problems [3]. Figure 1 shows a taxonomy of Intrusion Detection Systems. IDS first introduced by James P. Anderson in 1980. [A threat model that classifies intrusions to develop a security monitoring system based on detecting anomalies in user behavior] Later in 1986, Dr. Dorothy Denning proposed several models for IDS based on statistics, Markov chains, time-series, etc. E. Biermann et al. in 2001 select criteria to compare and evaluate the different IDS approaches [5].

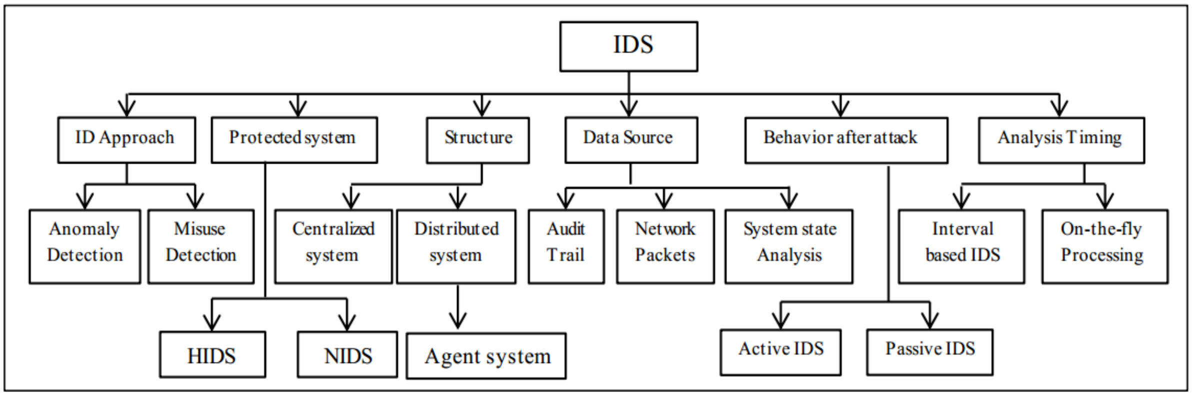

Fig. 1. An Intrusion Detection Systems' taxonomy [4]

2.1. Detection Approaches

Traditionally, intrusion detection techniques are classified into two broad categories:

a) Misuse or signature based IDS

Misuse detection searches for the traces or patterns of well-known attacks which are stored as signatures. These signatures are provided by a human expert based on their extensive knowledge of intrusion techniques. In this process if a pattern matched is found, this signals an event for which an alarm raised [3].

b) Anomaly based IDS

Anomaly detection uses a model of normal user or system behavior and flags significant deviations from this model as potentially malicious. This model of normal user or system behavior is commonly known as the user or system profile [3]. Three broad categories of anomaly detection techniques exist: supervised, semi-supervised and unsupervised anomaly detection techniques [6].

c) Hybrid IDS or compound detection system

It's the combination both misuse and anomaly detection techniques. It makes decisions using a “hybrid model” that is based on both the normal behavior of the system and the intrusive behavior of the intruders.

2.2. Types of IDSs

IDSs are categorized according to the kind of input information they analyze. So this is classified into host-based and network-based intrusion detection system [7, 8, 9].

a) Host-based IDS (HIDS)

Host based intrusion detection system mainly deals with single computer and perform intrusion detection based on the system call, kernel, firewall and system logs.

b) Network-based IDS (NIDS)

Network intrusion detection system works on a large scale. It monitors network traffic and examines the traffic, and based upon the observation it categorizes the traffic into normal or suspicious. Traffic monitoring is done at firewall, hub and switch etc.

As shown in the Table 1, each of the approaches and types of IDS has its own advantages and disadvantages.

Table 1. Advantages and disadvantages types of IDS

Type	Advantages	Disadvantages
HIDS	1. It can judge whether or not the host is intruded more accurately. 2. It can detect attacks under encrypted network environment. 3. It does not need additional hardware.	1. Higher cost. 2. It may affect system efficiency of monitoring hosts.
NIDS	1. Low cost. 2. It can detect attacks that cannot be done by host based IDS, such as: Dos, DDos.	1. The flux is large, and some packets may be lost. 2. In a large-scale network, it requires more rapid CPU and more memory space, to analyze bulk data 3. It cannot deal with encrypted packets.
Anomaly	1. Ability to detect novel attacks or unknown attacks. 2. Low false negative.	1. Slow Timely Notifications. 2. High false alarm rate. 3. Low detection rate (for known attacks).
Misuse	1. High detection rate and low false alarm rate (for known attacks). 2. Fast Timely Notifications.	1. Detection capacity is low for un-known detection methods. 2. Attack database should be renewed on a regular basis.

2.3. Drawbacks of IDSs

Intrusion Detection Systems (IDS) have become a standard component in security infrastructures as they allow network administrators to detect policy violations. These policy violations range from external attackers trying to gain unauthorized access to insiders abusing their access. Current IDS has a number of significant drawbacks [4]:

• False positives: A false positive occurs when normal attack is mistakenly classified as malicious and treated accordingly.

• False negatives: This is the case where an IDS does not generate an alert when an intrusion is actually taking place.

• Data overload: Another aspect which does not relate directly to misuse detection but is extremely important is how much data an analyst can efficiently analyze. That amount of data he needs to look at seems to be growing rapidly.

3. Feature Selection

Feature selection, also known as subset selection or variable selection, is a process commonly used in machine learning, wherein a subset of the features available from the data is selected for the application of a learning algorithm. This has the benefit of generally improving system performance by eliminating irrelevant and redundant features.

4. Data Set

The KDD cup 1999 dataset was used in the 3rd International Knowledge Discovery and Data Mining Tools Competition for building a network intrusion detector, a predictive model capable of distinguishing between intrusions and normal connections. The data set was getting through selecting and arranging the data of DARPA of American Air Force by American Columbia University in MIT Lincoln in 1998, and it was intended to assess the efficiency of intrusion detection algorithm. In KDD99 dataset, each example represents attribute values of a class in the network data flow, and each class is labeled either normal or attack. The classes in KDD99 dataset can be categorized into five main classes (one normal class and four main intrusion classes: probe, DOS, U2R, and R2L) [14].

1. Normal connections: They are generated by simulated daily user behavior such as downloading files, visiting web pages.

2. Denial of Service (DoS): Such attack causes the computing power or memory of a victim machine too busy or too full to handle legitimate requests. DoS attacks are classified based on the services that an attacker renders unavailable to legitimate users like apache2, land, mail bomb, back, etc.

3. Remote to User (R2L): This is an attack that a remote user gains access of a local user/account by sending packets to a machine over a network communication, which include send-mail, and Xlock.

4. User to Root (U2R): In the attack intruder begins with the access of a normal user account and then becomes a root-user by exploiting various vulnerabilities of the system. Most common exploits of U2R attacks are regular buffer-overflows, load-module, Fd-format, and Ffb-config.

5. Probing (Probe): Such attack scans a network to gather information or find known vulnerabilities. An intruder with a map of machines and services that are available on a network can use the information to look for exploits.

Much related work considers these data sets for their experiments. This result shows that these data sets are recognized as standard datasets in intrusion detection.

5. Data mining and IDS

Data mining is also known as knowledge discovery in Databases. It is a process which finds useful patterns from large amounts of data [10]. IDSs use data mining approaches to the following reasons [11]:

- It is very hard to program IDS using ordinary programming languages that require the exploitation and formalization of knowledge.

- The adaptive and dynamic nature of machine-learning makes it a suitable solution for this situation.

- The environment of an IDS and its classification task highly depend on personal preferences. What may seem to be an incident in one environment may be normal in other environments.

Here are a few specific things that data mining might contribute to an intrusion detection project [4]:

- Remove normal activity from alarm data to allow analysts to focus on real attacks

- Identify false alarm generators and "bad" sensor signatures

- Find anomalous activities that uncovers a real attack

- Identify long, ongoing patterns (different IP address, same activity).

6. Data mining techniques in IDS

A number of techniques are available for intrusion detection. Data mining is the one of the efficient techniques available for intrusion detection. Data mining techniques can be classified into 2 categories namely descriptive mining & predictive mining [12]. In this section we present a survey of data mining techniques that have been applied to IDSs by various research groups.

6.1. Statistical techniques

Statistical techniques, also known as "top-down" learning, are employed when we have some idea as to the relationship were looking for and can employ mathematics to aid our search.
Three basic classes of statistical techniques are linear, nonlinear (such as a regression-curve), and decision trees. Statistics also include more complicated techniques, such as Markov models and Bayes estimators.

6.1.1. Hidden Markov Models

A hidden Markov model (HMM) is a statistical model where the system being modeled is assumed to be a Markov process with unknown parameters, and the challenge is to determine the hidden parameters from the observable parameters. The extracted model parameters can then be used to perform further analysis, for example of pattern recognition applications [4].

6.2. Machine Learning

Machine learning techniques are well suited to learning patterns with no a priori knowledge of what those patterns may be, hence they are sometimes referred to as “bottom-up” learning techniques. Here we will look at a variety of machine learning techniques.

6.2.1. Classification techniques

A classification based IDS attempts to classify all traffic as either normal or malicious in some manner. The primary difficulty in this approach is how accurately the system can learn what these patterns are. This ultimately affects the accuracy of the system both in terms of whether a non hostile activity is flagged (false positive) and whether the malicious activity will be missed (false negative). Five general categories of techniques have been tried to perform classification for intrusion detection purposes: inductive rule generation, genetic algorithms, fuzzy logic, neural networks, and immunological based techniques.

6.2.1.1. Inductive rule generation, such as that done by RIPPER has been shown to be a fairly effective and straightforward way to produce a system that classifies traffic into normal or various forms of intrusive patterns. The system is a set of association rules and frequent episode patterns than can be applied to the network traffic to classify it properly.

- Advantages: The rule set generated is easy to understand; hence a security analyst can verify it. Another attractive property is that multiple rule sets may be generated and used with a meta-classifier [13].

6.2.1.2. Genetic algorithms (GA) use the computer to implement the natural selection and evolution. This concept comes from the ‘‘adaptive survival in natural organisms”. The algorithm starts by randomly generating a large population of candidate programs. Some type of fitness measure to evaluate the performance of each individual in a population is used. A large number of iterations are then performed that low performing programs are replaced by genetic recombinations of high performing programs. That is, a program with a low fitness measure is deleted and does not survive for the next computer iteration [14]. Fairly recently, researchers have tried to integrate these algorithms with IDSs. The REGAL System is a concept learning system based on a distributed genetic algorithm [4].

- Advantages: It selects best features for detection and has better efficiency.

- Disadvantages: It is a complex method and Used in specific manner rather than general [15].

  6.2.1.3. Fuzzy logic is derived from fuzzy set theory dealing with reasoning that is approximate rather than precisely deduced from classical predicate logic. It can be thought of as" the application side of fuzzy set theory dealing with well thought out real world expert values for a complex problem" [4]. Luo used the fuzzy association rules mining algorithm with an additional normalization step. He does show a significant reduction in the false positive rate over non-fuzzy methods [13].

- Advantages: Used for quantitative features and Provides better flexibility to some uncertain problems.

- Disadvantages: Detection accuracy is lower than ANN.

6.2.1.4. Artificial Neural network (ANN) encompasses a range of models, including Multi Layer Perceptrons (MLPs) and Self Organizing Maps (SOMs), which are the main models applied to intrusion detection. The majority of the misuse detection applications of ANNs is implemented as feed forward MLPs. Most of the misuse detection applications are network based; whilst host based applications are typically implemented as anomaly detection systems [16, 4 and 17].

- Advantages: Classifies unstructured network packet efficiently, multiple hidden layers in ANN increase efficiency of classification, able to implicitly detect complex nonlinear relationships between dependent and independent variables, high tolerance to noisy data.

- Disadvantages: Requires more time and more sample training phase, has lesser flexibility, "Black box" nature, Greater computational burden.

6.2.1.5. Hofmeyr and Forrest (1999) present an interesting technique based on immunological concepts. They define the set of connections from normal traffic as the "self "and then generate a large number of “non-self” examples: connections that are not part of the normal traffic to a machine. These examples are generated using a byte oriented hash and permutation [13].

6.2.2 Clustering techniques

Clustering is useful in intrusion detection as malicious activity should cluster together, separating itself from non-malicious activity. The clustering algorithms investigated include, k-means, Mixture-Of-Spherical Gaussians, Self-Organizing Map, and Neural-Gas [18].

- Advantages: Clustering is unsupervised learning. Labeling of data is not necessary and natural patterns in the data are extracted. It does not require the use of a labeled data set for training.

6.2.2.1 K-nearest neighbor (k-NN) is one nonparametric technique to classify samples. It computes the approximate distances between different points on the input vectors, and then assigns the unlabeled point to the class of its K-nearest neighbors. During the classification phase, k-NN uses a similarity-based search strategy to determine a locally optimal hypothesis function. Test instances are compared to the stored instances and assign the same class label as the k most similar stored instances [1].

- Advantages: Simple in implementation, Lends itself very easily to parallel implementations, it does not contain the model training stage

- Disadvantage: For large sets of examples, performance can be expensive, Instance based learning can be sensitive to irrelevant attributes and Slow in classifying test tuples.

6.2.2.2 Self-Organizing Map (SOM) is trained by an unsupervised competitive learning algorithm, a process of self organization [14]. It usually consists of an input layer and the Kohonen layer which is designed as the two-dimensional arrangement of neurons that maps n dimensional input to two dimensions.

- Advantages: SOMs are trained using unsupervised learning, i.e. no prior knowledge is available and no assumptions are made about the class membership of data, the SOM algorithm is very efficient in handling large datasets [6].

- Disadvantages: The number of clusters needs to be specified, a user has to either do a manual inspection or apply traditional algorithms, like hierarchical to find the cluster boundaries [6].

6.2.3. Support Vector Machine

Support vector machines (SVMs) are a set of related supervised learning methods used for classification and regression. They belong to a family of generalized linear classifiers. SVMs attempt to separate data into multiple classes (two in the basic case) though the use of a hyper-plane. They are the training samples close to a decision boundary. The SVM also provides a user specified parameter called a penalty factor. It allows users to make a tradeoff between the number of misclassified samples and the width of a decision boundary.

- Advantages: They learn very effectively from high dimensional data, able to model complex nonlinear decision boundaries, less prone to over fitting than other methods; it can correctly classify intrusions, if limited sample data are given and can handle the massive number of features.

- Disadvantage: SVM can only handle binary-class classification whereas intrusion detection requires multi-class classification; the speed both in training and testing is slow, high algorithmic complexity and extensive memory requirements of the required quadratic programming into large-scale tasks [11].

6.2.4. Decision Tree (DT)

A decision tree is a rooted tree with internal nodes corresponding to attributes and leaf nodes corresponding to class labels. Internal nodes have a child node for each value its associated attribute takes. The learning element generates a tree recursively by selecting the attribute that best splits the examples into their proper classes, creating child nodes for each value of the selected attribute, and distributing the examples to these child nodes based on the values of the selected attribute. The algorithm then removes the selected attribute from further consideration and repeats for each child node until producing nodes containing examples of the same class. These methods handle continuous attributes by finding a threshold that best splits the examples into their respective classes [1, 10]. F. Ozturk et al, compared the efficiency of decision tree methods in intrusion detection system [19].

- Advantages: Construction does not require any domain knowledge, Can handle high dimensional data, Representation is easy to understand, Able to process both numerical and categorical data [11].

- Disadvantages: the problem of finding the smallest decision tree consistent with a training data set is NP-complete, Limited to one output attribute, most decision tree construction methods are non-backtracking, Decision tree algorithms are unstable and trees created from numeric datasets can be complex.

6.2.5. Naive Bayes (NB)

Naive Bayes stores as its concept description the prior probability of each class and the conditional probability of each attribute value given the class. The learning element estimates these probabilities from examples by simply counting frequencies of occurrence. The prior probability is the portion of examples from each class. The conditional probability is the frequency that attributes values occur given the class. Given an observation, the performance element operates under the assumption that attributes are conditionally independent and uses Bayes' rule to calculate the posterior probability of each class, returning as the decision the class label with the highest probability [1].

- Advantages: the prior knowledge about the system is simply that some variations might influence others, exhibit high accuracy and speed when applied to large databases.

- Disadvantages: The assumptions made in class conditional independence, lack of available probability data [4].

6.2.6. Random forest

The random forests are an ensemble of unpruned classification or regression trees. Random forest generates many classification trees. Each tree is constructed from a different bootstrap sample from the original data using a tree classification algorithm. After Patterns Network

Traffic Pre- Processors Detector Training Dataset Pattern Builder On-line Off-line Alerts the forest is formed, a new object that needs to be classified is put down each of the trees in the forest for classification [20].

- Advantages: It runs efficiently on large data sets with many features, it can give the estimates of what features are important, it can handle unbalanced data sets.

6.3. Hybrid classifiers and Optimization techniques

The idea behind a hybrid classifier is to combine several techniques so that the system performance can be significantly improved. On the other hand, hybrid classifiers can be based on cascading different classifiers. Optimization techniques are methods typically used to solve search and optimization problems, such as Genetic Algorithms (GAs), Genetic Programming (GP), Particle Swarm Optimization (PSO) and Ant Colony Optimization (ACO) [17]. C. Kolias et al, Survey Swarm intelligence in intrusion detection [21].

- Advantages: It is an efficient approach to classify rules accurately and system performance can be significantly improved.

- Disadvantages: Computational cost is high.

7. A summary of existing data mining algorithms to implement IDS

In Tables 2, we have some work done in the field of network intrusion detection using data mining algorithms with their title, proposition and conclusion that have been mentioned briefly.

Table 2. The related studies focusing on data mining algorithms to implement IDS.

Title	Proposition	Conclusion
A clustering-based method for unsupervised IDs [23]	A novel method is proposed to compute the cluster radius threshold.	The method outperforms the existing methods in terms of accuracy and detecting unknown intrusions.
Network based anomaly IDS uses SVM [24]	A method is proposed for enhancing the training time of SVM, particularly when dealing with large data sets, using hierarchical clustering technique.	It proved to work well and to outperform all other techniques in terms of accuracy, false positive rate, and false negative rate.
Bayesian based IDS [25]	A NB classifier is used to identify possible intrusions.	Improve the accuracy of the R2L attack using Bayesian methods
Using DT to Improve Signature-Based ID [26]	An algorithm generates a decision tree that is used to find malicious events using as few redundant comparisons as possible.	Improve the speed, Optimize the rules-to-input comparison process.

NID using NB [27]	A framework of NIDS based on NB algorithm. It builds the patterns of the network services over data sets labeled.	Improve the false positive rate, cost, and computational time.
NID using Random Forests [20]	A random forests algorithm in NIDSs to improve detection performance.	Reduce the time to build patterns dramatically and increase the detection rate of the minority intrusions.
Y-means: A Clustering Method for ID [30]	A clustering heuristic based on the K-means algorithm and other related clustering algorithms.	It overcomes two shortcomings of K-means: number of clusters dependency and degeneracy.
K-NN classifier for ID [31]	A KNN classifier to categorize each new program behavior into either normal or intrusive class.	The low false positive rate can be achieved; can be easily adapted to intrusion detection.
Detecting Intrusion by using C4.5 algorithm [32]	A new data-mining based approach by combining multiboosting and an ensemble of binary classifiers with feature selection.	High detection rates for U2R and R2L compared to other works performs better than the winning entry of the KDD cup in term of accuracy and cost.
Clustering Approach for Large ID Data [28]	Authors have been used K-Mean evolution clustering method for intrusion detection.	This method decreases the overhead of performing the detection over whole data sets.
Hierarchic Clustering Algorithm used for Anomaly Detecting [33]	Hierarchic Clustering to form normal behavior profile on the audit records and adjust the profile timely as the program behavior changed.	Lower spatio-temporal cost, high detection rate and low false positive rate.
ID Based on Apriori Algorithm [34]	Author applies the rule base generated by the Apriori algorithm to identify a variety of attacks.	Improves the overall performance of the detection system.
SVM with Normalization in ID [35]	Min-Max normalization method in intrusion detection data which SVM is used for classification.	Better performance in speed, accuracy of cross validation and quantity of support vectors than other normalization methods.
A differentiated one-class classification method with to ID [36]	A new one-class classification method (SVDD) with differentiated anomalies to enhance ID performance for harmful attacks.	This method would be beneficial to broader application areas beyond intrusion detection.
Combining NB and DT for adaptive ID [37]	A new hybrid learning algorithm for adaptive NID using NB classifier and ID3 algorithm.	Low false positives, high detection rates.
ID using neural based hybrid classification [9]	It presents two classification methods involving MLP and RBF and an ensemble of MLP and RBF.	Hybrid method shows significantly larger improvement of prediction accuracy than the base classifiers.
Anomaly Detection using a SOM and PSO[6]	A method for anomaly detection, based on a combination of a SOM and PSO.	Low time and space complexity, The algorithm is simple, can be applied to different and variant domains of anomaly detection

Anomaly Detection by K-Means+C4.5 [38]	A method to cascade k-Means and C4.5 methods for classifying anomalous and normal activities.	The algorithm gives impressive detection accuracy in the experimental results.
IDS using NB and HMM [29]	The paper proposes to discuss the IDS model in its elaboration using NB and the HMM approach.	The performance of the model is of high order of classification of normal and intrusion attacks.
IDS using SVM and DT [40]	DT based SVM can be an effective way for solving multi-class problems.	This method can decrease the training and testing time, increasing the efficiency of the system.
Anomaly Detection by K-Means+ID3 [41]	The Author has used k-mean followed by ID3 decision tree for intrusion detection.	Removing the shortcoming of k-mean clustering.
ID using ANN+fuzzy [42]	An approach to ID using ANN and fuzzy clustering.	Removing the shortcomings of ANN, high recall and precision for low frequent attacks (U2R, R2L).
Decision tree based light weight ID [43]	The lightweight IDS have been developed by using a wrapper based feature selection algorithm.	The system can detect the specific attack type; it is suitable for multi-class classification.
IDS based on hierarchical clustering and SVM [44]	An SVM-based network IDS with BIRCH hierarchical clustering for data preprocessing.	Better performance in the detection of DoS and Probe attacks, and the best performance in overall accuracy.
DT for NID with GA-based feature selection [39]	DT+GA are able to focus on relevant features and eliminate unnecessary or distracting features.	Increasing the detection rate and decreasing the false alarm rate.

8. Conclusion

With the increasing use of network-based services and sensitive information on networks, maintaining information security is essential. Intrusion Detection System is a security tool used to detect unauthorized activities of a computer system or network. This paper reviews current studies of intrusion detection by various data mining algorithms. Combining more than one data mining algorithms can give a better performance than any single classifier.

Acknowledgment. The authors would like to express their thanks to the anonymous referees for their comments and suggestions which improved the paper.

References

[1] M.A. Maloof, Machine Learning and Data Mining for Computer Security, Springer-Verlag, 2006.

[2] J.J. Davis and A.J. Clark, Data Preprocessing for Anomaly Based Network Intrusion Detection: A Review, Computers & Security 30 (2011) 353-375.

[3] S.V.Shirbhate, V.M.Thakare and S.S.Sherekar, Data Mining Approaches for Network Intrusion Detection System, International Journal of Computer Technology and Electronics Engineering (2011) 41-44.

[4] T. Lappas and K. Pelechrinis, Data Mining Techniques for (Network) Intrusion Detection Systems, http://atl-svn.assembla.com/svn/odinIDS/Egio/artigos/datamining/dataIDS.pdf

[5] E. Biermann, E. Cloete and L.M. Venter, A comparison of Intrusion Detection systems, Computers & Security 20 (2001) 676-683.

[6] M. L. Shahreza, D. Moazzami, B. Moshiri and M.R. Delavar, Anomaly Detection Using a Self-Organizing Map and Particle Swarm Optimization, Scientia Iranica 18 (2011) 1460-1468

[7] K.K. Bharti, S. Shukla and S. Jain, Intrusion Detection Using Clustering, Proceeding of the Association of Counseling Center Training Agencies (ACCTA), 2010, Volume: 1.

[8] S.Y. Wua and E. Yen**,** Data mining-based intrusion detectors, Expert Systems with Applications 36 (2009) 5605-5612.

[9] M. Govindarajan and R.M. Chandrasekaran, Intrusion Detection Using Neural Based Hybrid Classification Methods, Computer Networks 55 (2011) 1662-1671.

[10] M. Kantardzic, Data Mining: Concepts, Models, Methods, and Algorithms, John Wiley & Sons, 2003.

[11] R. Patel, A. Thakkar and A. Ganatra, A Survey and Comparative Analysis of Data Mining Techniques for Network Intrusion Detection Systems, International Journal of Soft Computing and Engineering 2 (2012).

[12] G.V. Nadiammai, S. Krishnaveni and M. Hemalatha, A Comprehensive Analysis and Study in Intrusion Detection System using Data Mining Techniques, International Journal of Computer Applications 35 (2011).

[13] S.T. BRUGGER, Data Mining Methods for Network Intrusion Detection, University of California, Jun. 2004.

[14] C.F. Tsai, Y.F. Hsu, C. Y. Lin and W.Y. Lin, Intrusion Detection by Machine Learning: A Review, Expert Systems with Applications 36 (2009) 11994–12000.

[15] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel and M. Rajarajan, A survey of Intrusion Detection Techniques in Cloud, Journal of Network and Computer Applications (2012).

[16] V. Jyothsna, V.V. Rama Prasad and K. Munivara Prasad, A Review of Anomaly based Intrusion Detection Systems, International Journal of Computer Applications 28 (2011).

[17] A. Jain, S. Sharma and M.S. Sisodia, Network Intrusion Detection by Using Supervised and Unsupervised Machine Learning Techniques: A Survey, International Journal of Computer Technology and Electronics Engineering 1 (2011).

[18] S. Zhong, T.M. Khoshgoftaar and N. Seliya, Clustering-based Network Intrusion Detection, International Journal of Reliability, Quality and Safety Engineering 14 (2007) 169-187.

[19] F. Ozturk and A. Subasi, Comparison of Decision Tree Methods for Intrusion Detection, Proceeding of the 2nd International Symposium on Sustainable Development, 2010, pp: 401-407.

[20] J. Zhang and M. Zulkernine, Network Intrusion Detection using Random Forests, Proceeding of the Third Annual Conference on Privacy, Security and Trust, 2005.

[21] C. Kolias, G. Kambourakis and M. Maragoudakis, Swarm Intelligence in Intrusion Detection: A Survey, Computers & security 30 (2011), 625-642.

[22] D.Y. Yeung and Y. Ding, Host-based Intrusion Detection Using Dynamic and Static Behavioral Models, Pattern Recognition 36 (2003) 229-243.

[23] S.Y. Jiang, X. Song, H. Wang, J.J. Han and Q.H. Li, A Clustering-based Method for Unsupervised Intrusion Detections, Pattern Recognition Letters 27 (2006) 802-810.

[24] J.A. Renjit and K.L. Shunmuganathan, Network Based Anomaly Intrusion Detection System Using SVM, Indian Journal of Science and Technology 4 (2011) 1105 -1108.

[25] H. Altwaijry and S. Algarny, "Bayesian based intrusion detection system," Journal of King Saud University Computer and Information Sciences 24 (2012) 1-6.

[26] C. Kruegel and T. Toth, Using Decision Trees to Improve Signature-Based Intrusion Detection, Springer-Verlag Berlin Heidelberg (2003) 173–191.

[27] M. Panda and M.R. Patra, Network Intrusion Detection Using Naïve Bayes, International Journal of Computer Science and Network Security 7 (2007).

[28] N. Yasmin, A.S. Nugroho and H. Widiputra, Optimized Sampling with Clustering Approach for Large Intrusion Detection Data, Proceeding of the International Conference on Rural Information and Communication Technology, 2009, pp: 56-60.

[29] N. Devarakonda, S. Pamidi, V. Kumari and G. A, Intrusion Detection System using Bayesian Network and Hidden Markov Model, Procedia Technology, 2012, Volume: 4, pp: 506-514.

[30] Y. Guan, A. Ghorbani and N. Belacel, Y-means: A Clustering Method for Intrusion Detection, Canadian Conference on Electrical and Computer Engineering, 2003.

[31] Y. Liao and V.R. Vemuri, Use of K-Nearest Neighbor classifier for intrusion detection, Computers & Security 21 (2002) 439-448.

[32] R. Naik, V. Kshirsagar and B. S. Sonawane, New Strategy for Detecting Intrusion by Using C4.5 Algorithm, Proceedings of the International Conference on Computational Intellegence Applicaitons (ICCIA), 2012.

[33] Z. Chen and D. Zhu, Hierarchic Clustering Algorithm used for Anomaly Detecting, Procedia Engineering, 2011, Volume: 15, pp: 3401-3405.

[34] L. Hanguang and N. Yu, Intrusion Detection Technology Research Based on Apriori Algorithm, Physics Procedia, 2011, Volume: 24, pp: 1615-1620.

[35] W. li and Z. Liu, A method of SVM with Normalization in Intrusion Detection, Procedia Environmental Sciences, 2011, Volume: 11, pp: 256-262.

[36] I. Kang, M. K. Jeong and D. Kong, A differentiated One-class Classification Method with Applications to Intrusion Detection, Expert Systems with Applications 39 (2012) 3899-3901.

[37] D.M. Farid, N. Harbi and M.Z. Rahman, Combining Naive Bayes and Decision Tree for Adaptive Intrusion Detection, International Journal of Network Security & Its Applications 2 (2010).

[38] A.P. Muniyandi, R. Rajeswari and R. Rajaram, Network Anomaly Detection by Cascading K-Means Clustering and C4.5 Decision Tree Algorithm, Procedia Engineering, 2012, Volume: 30, pp: 174 – 182.

[39] G. Stein, B. Chen, A.S. Wu and K.A. Hua, Decision Tree Classifier for Network Intrusion Detection With GA-based Feature Selection, Proceedings of the 43rd annual Southeast regional conference, 2005, Volume: 2, pp: 136-141.

[40] S.A. Mulay and P.R. Devale and G.V. Garje, Intrusion Detection System USING Support Vector Machine and Decision Tree, International Journal of Computer Applications 3 (2010).

[41] S.R. Gaddam, V.V. Phoha and K.S. Balagani, K-Means+ID3: A Novel Method for Supervised Anomaly Detection by Cascading K-Means Clustering and ID3 Decision Tree Learning Methods, IEEE Transactions on Knowledge and Data Engineering 19 (2007) 345-354.

[42] G. Wang, J. Hao, J. Ma and L. Huang, A New Approach to Intrusion Detection Using Artificial Neural Networks and Fuzzy Clustering, Elsevier (2010) 6225-6232.

[43] S.S. Sivatha Sindhu, S. Geetha and A. Kannan, Decision Tree Based Light Weight Intrusion Detection Using a Wrapper Approach, Expert Systems with Applications 39 (2012) 129-141.

[44] S.J. Horng , M.Y. Su, Y.H. Chen, T.W. Kao, R.J. Chen, J.L. Lai and C.D. Perkasa, A Novel Intrusion Detection System Based on Hierarchical Clustering and Support Vector Machines, Expert Systems with Applications 38 (2011) 306-313.