IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Volume-5, Issue-12 E-ISSN: 2347-2693

A Review of Network Intrusion Detection System using Machine Learning Algorithms

Ravinder Kumar

Department of CSE, HMR Institute of Technology and Management (Affiliated with GGSIPU), Delhi, India

*Corresponding Author: ravinder_y@yahoo.com, Tel.: 011 – 27724115

Available online at: www.ijcseonline.org

Received: 20/Nov/2017, Revised: 29/Nov/2017, Accepted: 17/Dec/2017, Published: 31/Dec/2017

Abstract— With the advancement in the communication technology, the probability of external attacks through networks is increasing day by day. Therefore, Intrusion Detection System (IDS) had became very important and an emerging area of research which, attempts to identify and notify the activities of users as normal (or) anomaly. IDS are a nonlinear and complicated problem and deals with network traffic data. Many IDS methods have been proposed and produce different levels of accuracy. That is why the development of effective and robust Intrusion detection system is necessary. This paper presents a state of the art of intrusion detection system (IDS) classification techniques using various machine learning algorithms. Experiments have been conducted to evaluate the performance of various well known machine learning algorithms on NSL-KDD data set.

Keywords— Intrusion Detection System, Attacks, KDD data set, False Acceptance Rate , Detection Rate, Neural Networks

I. Introduction

With the advancement in information and communication technology, threats like intrusions are very likely to occur. The security tools like, access control scheme, firewalls, antivirus software to protect important information from such attacks are highly desirable to enhance the security against these attacks. Intrusion Detection Systems (IDS) have been introduced as a tools designed to enhance security of systems [1]. Various IDS approaches have been proposed in the literature since inceptions, but two of them are proposed by Steniford at al., and Denning are most relevant in this context [2].

Denning's proposal for an intrusion detection system focused on how to develop effective and accurate methods for intrusion detection. During early days of development of such system combination statistical and expert systems based approaches was very popular. Now a day's machine learning based intelligent techniques are most widely accepted and used for developing a training set to detect intrusions. Classification, clustering and rule based techniques are commonly used machine learning techniques.

For intrusion detection system automatically constructing models will work as system has to be trained with latest intrusion behaviour, huge traffic on network, and imbalanced attack class distribution. Under these requirements, Artificial intelligence based machine learning techniques not sufficient alone to achieve high matching / detection accuracy and less computational times. Fortunately, machine learning based techniques has property to adapt and tuned its parameters under varying conditions and can be utilized as techniques for fault detection and fault tolerance, resilience against noisy information and high computational speed to compensate these requirements.

The paper has been written with an objective to introduce various machine learning techniques, those can be employed as a tool to differentiate or classify among external attacked as intrusion or allowed one. This paper also proposed a state of the art comprehensive survey on latest research contributions from various researchers towards development of IDS tools using computational intelligence (CI) methods. This survey only focused on only the basic methods in Machine Learning, using artificial neural networks. The pros and cons of use each method has also been proposed in this paper. Soft computing techniques have been also proposed in the literature to overcome the problems associated with the use of ANN based algorithms in classify the attacks in IDS as tool. Therefore, it becomes necessary and mandatory to introduce a literature review on these techniques here; otherwise this paper cannot be complete in all respects.

The remainder of this work is presented into following sections. Section II introduces IDSs and computation intelligence techniques. In section III various IDS datasets have been presented, Section IV presents the parameters used to evaluate the performance measurement. Section V presents core methods of CI for IDS with the categorization also compares and summarizes these methods. Section VI end with concluding remarks.

II. Background

A. Intrusion Detection System

An intrusion detection system is a tool used for automatic detection and removal of external attack or access to the system and takes a decision to determine whether these attacks constitute a legitimate use of the system or are intrusions [3]. Figure 1 represents the organization of an IDS where solid arrows indicate data/control flow while dotted arrows indicate a response to intrusive activities.

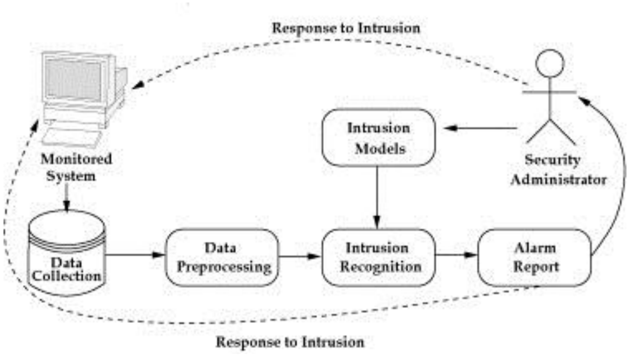

Figure 1. A general organization of a typical intrusion detection system

In general, this paper classifies IDSs on the basis of detection methods they employ into two categories, like (i) misuse detection and (ii) abnormality detection. By matching observed data, misuse detection identifies intrusions with pre-defined descriptions of intrusive behaviour. So prominent intrusions can be detected in an efficient manner utilizing a low false positive rate. Therefore, this technique is widely adopted in the majority of commercial systems. However, the types of new intrusions have evolved every moment and continuously, therefore. Misuse the previous techniques for intrusion detection will fail to detect new unknown intrusions. The only way to get rid over this issue is to learn from all intrusions and get update the data knowledge at every moment. This updating process can either be manual or automatic, the manual process might be very time consuming and also the human intervention is required at every moment of time. This process can work automatically using supervised machine learning techniques. Unfortunately, the preparation of datasets for training the supervised learning algorithms is very difficult and expensive, as this require collection and labeling of each event as normal or an intrusion type. A better anomaly detection approach to get rid over this is proposed by Denning [4].

Anomalies are the undesired activities performed on the network and the detection of such activities is orthogonal to misuse detection. It is presumed that abnormal behaviour is rare and different from normal behaviour. Hence, the models for normal behaviour can detect anomaly in observed data by noticing deviations from these models. Two types of anomaly detection techniques have been proposed in the literature anomaly detection [5]. The static anomaly detection techniques assume that the behaviour of under investigation targets never changes, such as system call sequences of an Apache service; in the second type of anomaly detection is dynamic anomaly detection which extracts patterns from behaviour habits of end users or networks/hosts usage history. Sometimes these patterns are refereed as profiles.

It is concluded here is that for detecting anomaly the system thus designed should have ability of detecting all new types of intrusions, and only requires normal data when building the profiles. However, its major difficulty lies in discovering boundaries between normal and abnormal behavior, due to the deficiency of abnormal samples in the training phase. Another difficulty is to adapt to constantly changing normal behavior, especially for dynamic anomaly detection. In addition to the detection method, there are other characteristics one can use to classify IDSs, as shown in Fig.2. Central Distributed Response to Intrusion Audit Data Source Locus of Detection Detection Method Intrusion Detection System Hosts Networks Passive Active Misuse Anomaly [6].

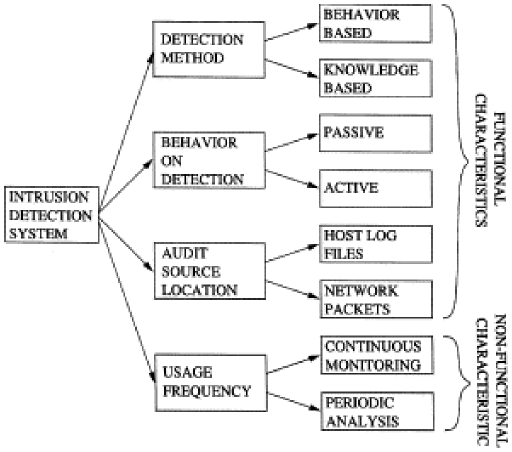

Figure 2. Characteristics of intrusion detection systems

B. Computational Intelligence

Computational Intelligence (CI) is an emerging research field possessing competing definitions. In Computational

Intelligence - A Logical Approach [7], [8], CI is defined as "Computational Intelligence is the study of the design of intelligent agent. An intelligent agent is a system that acts intelligently: What it does is appropriate for its circumstances and its goal, it is flexible to changing environments and changing goals, it learns from experience, and it makes appropriate choices given perceptual limitations and finite computation."

Bezdek et. al. [6] presented CI as "A system is computational intelligent when it: deals with only numerical (low-level) data, has pattern recognition components, does not use knowledge in the artificial intelligence sense; and additionally when it (begins to) exhibit i) computational adaptivity, ii) computational fault tolerance, iii) speed approaching human-like turnaround, and iv) error rates that approximate human performance."

From the above definitions and the combined discussion of Duch [7], and Craenen and Eiben [8], it is summarized that CI systems possess several characteristics such as fault tolerance, computational adaptation, less error prone and high computational speed to noisy information.

CI differs from the field of Artificial Intelligence (AI) as AI handles symbolic representation of knowledge, while CI handles numeric information representation; AI is concerned with cognitive functions of high-level, while AI is concerned with cognitive functions of low-level; AI analyzes the problem structure and constructs an intelligent system on the basis of this structure, therefore operates in a top-down manner, while there is involvement of unordered beginning in CI, therefore operates in bottom-up manner [7, 8].

Although there is no complete definition of computational intelligence, there are huge numbers of accepted views on which different areas belong to CI: evolutionary computation, fuzzy sets, artificial neural networks, swarm intelligence, and artificial immune systems. These approaches, except for fuzzy sets, are capable of the autonomous knowledge acquisition and integration, and are used in either unsupervised or supervised learning mode. These schemes construct data-driven models in a training phase, and performance verification is done in the testing phase.

In the field of intrusion detection, supervised learning basically gives classifiers for misuse detection from class labelled training data. Classifiers are a function mapping data points to their corresponding class labels. Unsupervised learning is distinguished from supervised learning as in this no class-labelled data is available during training phase. Data points are grouped on the basis of their similarities. The hypothesis of anomaly detection is satisfied by unsupervised learning; hence it is used in anomaly detection.

III. DATASETS

The following section summarizes the popular benchmark datasets and evaluates their performance measures in the domain of intrusion detection, to clarify the misuse of these terms that are found during the process of review.

A. Datasets

Since CI approaches build detection models from data, the training datasets quality directly affects the trained models quality. Here we surveyed that the data is in general collected from three sources namely the low-level system information, data packages from networks, command sequences from user input, or system low-level information, such as CPU/memory usage, system call sequences, system error logs, and log files. Several commonly used benchmarks are listed in Table 1. These datasets have been used in either anomaly detection or misuse detection.

The KDD99 dataset and the DARPA-Lincoln datasets In 1998, the first and most comprehensive research project was conducted by MIT's Lincoln laboratory for evaluating the performance of various intrusion detection techniques, under the Air Force Research Laboratory and DARPA ITO sponsorship [9]. This dataset consists of seven weeks training data and two weeks testing data. These include over 300 instances of 38 different attacks that were launched against UNIX hosts. These fall under one of the four categories: U2R (Users to Root), R2L (Remote to Local), Denial of Service (DoS), and Probe. For every week, outside and inside network traffic data, audit data recorded by Basic Security Module (BSM) of the Sun Microsystems's on Solaris hosts, and UNIX hosts file system dumps were collected. In 1999, Lincoln laboratory again evaluated the same. Three weeks and two weeks of training and test data respectively were generated this time. Over 200 instances of 58 different types of attack were launched against UNIX and Windows NT victim hosts and a Cisco router. Also, the host audit data were extended to Window NT systems. Three additional scenario-specific datasets were generated to address Windows NT attacks and distributed DoS in 2009. Even more detailed descriptions of above discussed datasets can be found at http://www.ll.mit.edu/IST/ideval/data/data_index.html.

In 1999, the KDD99 dataset was derived from the DARPA98 network traffic data by a Bro program. These join TCP packets into TCP connections. It was the benchmark dataset used in the Data Mining Tools and International Knowledge

Discovery Competition, and is the most popular dataset to be ever used in the field of intrusion detection. Every TCP connection has 41 features along with a label that specifies the connection status as either being specific attack type [10], [11] or normal. There are 3 symbolic features and 38 numeric features, which can be categorized into the following four categories:

1) *Basic Features:* 9 basic features described each individual TCP connection.

2) *Content Features:* In order to indicate suspicious behavior 13 domain knowledge related features were used in the network traffic.

3) *Time-based Traffic Features:* In order to summarize the connections 9 features were used in the past two seconds that had the same service and the same destination host *as* the current connection.

4) *Host-based Traffic Features:* 10 features were constructed with the help of window of 100 connections to the same host instead of a time window, because slow scan attacks may occupy more than two seconds,4,940,000 data instances constitute the training set which covers 24 attacks and normal network traffic. The test set comprises of 311,029 instances of data along with 38 attacks in total, 14 of these attacks are not part of the training set. 10% of KDD99 training set are frequently used as this dataset is large.

McHugh et. al. [10] proposed an in-depth criticism of the dataset of DARPA, and argued that few methodologies that have been used are questionable and may have led to biased results. For example, attack and normal data possess unrealistic data rates; training datasets are not adequate for anomaly detection; false alarm behaviour of IDSs is not validated and the test shows no significant difference on synthetic and real data. Malhony et. al. [11] confirmed the findings of McHugh's and proposed that numerous attributes had fixed and small simulation ranges, but growing and large real traffic ranges.

Table 1. Most common datasets for Intrusion Detection

Name of dataset	**Source**	**Abv.**
Network Traffic	DARPA 1999 TCPDump Files	DARPA99
	DARPA 1998 TCPDump Files	DARPA98
	10% KDD99	KDD99-10
	KDD99 Dataset	KDD99
	Dataset Internet Exploration Shootout Dataset	IES
Behavior of User	UNIX User	UNIXDS
System Call Sequences	DARPA 1999 BSM Files	BSM99
	DARPA 1998 BSM Files	BSM98

Above limitations can be inherited by KDD99 dataset by sharing the same root with the DARPA dataset. The empirical study conducted by Sabhnani et al. [12] stated that "KDD training and test data subsets represent dissimilar target hypotheses for U2R and R2L attack categories". From their analysis, 4 new U2R attacks have been discovered in test data, which comprise of 80% data of all U2R data in the test dataset. Similarly, they have presented 7 new R2L attacks are there in testing data, and constitute more than 60% of R2L data in the test data. This data has very well explained that why the detection results for U2R and R2L attacks are not satisfactory in most IDSs.

The Internet Exploration Shootout Dataset is another project that tries to evaluate various data exploration techniques. This dataset consists of an attack-free set and 4 sets containing IP spoofing attacks, guessing rlogin or ftp passwords, scanning attacks and network hopping attacks, respectively. The data was captured by TCP Dump in about 16 minutes on the MITRE Corp. network. Only TCP and UDP packets with 13 attributes were collected. For detailed information about the packets and for downloading the dataset, please refer to http: //ivpr.cs.uml.edu/shootout/network.html.

In spite of various problems associated with both the datasets, still KDD99 and the DARPA Lincoln datasets are being used by largest researchers as benchmarks to evaluate their intrusion detection in evaluating machine learning based intrusion or anomaly detection algorithms.

In this proposed survey paper, the problem of IDS along with detailed definitions, proposed solutions, datasets and various machine learning techniques have been proposed.

IV. PERFORMANCE EVALUATION

Various performance measurements have been proposed in the literature. Following are the most popularly used parameters for the evaluation of performance of machine learning based intrusion or anomaly detection algorithms:

A. Confusion Matrix

Effectiveness of different IDS algorithms can be evaluated using their classification accuracy. Not only the higher value of correct matching accuracy is important but also the other values of misclassification is also relevant if access of performance of the algorithms. As the given intrusion can be an attack or a normal intrusion, the matching algorithm may predict as attacks (actual attack) referred true positive (TP), may predict normal (actual attack) referred as False Positive (FP), may predict attack (actual normal) referred as False Negative (FN), and may predict normal (actual normal) referred as True Negative (NP). The combination of all possibilities are shown in the form of table referred as the confusion matrix as shown in Table II. True positives as well as true negatives are corresponding to a proper operation of the IDS; that is, the intrusions are correctly classified as normal and attack, respectively.

Table 2. Confusion Matrix

		Prediction by IDS	
		Normal	**Attack**
Actual	Normal	True Negative (TN)	False positive (FP)
	Attack	False Negative (FN)	True Positive (TP)

The evaluation of various parameters based on the above confusion matrix, are as follows:

– *True Negative Ratio (TNR):* $\frac{T\,N}{T\,N+F\,P}$, also known as Specificity.

– *True Positive Ratio (TPR):* $\frac{T\,P}{T\,P+F\,N}$, also known as Detection Rate (DR) or Sensitivity. In information retrieval theory, this is also called as Recall.

– *False Positive Ratio (FPR)*: $\frac{FP}{T\,N+F\,P}$= 1−*specificity*, also known as False Alarm Rate (FAR).

– *False Negative Rate (FNR):* $\frac{F\,N}{T\,P+\,F\,N}$= 1 − s*ensitivity*.

– *Accuracy:* $\frac{T\,N+FP}{T\,N+TP+FN+F\,P}$

– *Precision:* $\frac{T\,P}{T\,P+F\,P}$, which is another information retrieval term, and often is paired with "Recall".

This evaluation mainly applies as the measurement criteria for the evaluation of performance of IDSs. Among all these parameters detection rate (DR) is the most popularly accepted and practices parameters by the researchers. False Acceptance Rate (FAR) is another parameter used in conjunction with DR to make the complete evaluation system. Attempts have been made to design to have with high value of DR at the same time low FAR. Sensitivity and Specificity, Precision and Recall are the other commonly used combinations used for performance evaluation.

B. Receiver Operating Characteristic

Another popular performance evaluation parameter is the Receiver Operating Characteristic (ROC). ROC was majorly used in Radar signal detection system developed and deployed during 2nd world war. This is used to categorize by the tradeoff between hit rate and false acceptance rate for a noisy channel [13]. This technique is used for the analysis of various detection supervised learning schemes. The optimized value of ROC maximizes the DR and at the same time at a very low value FAR. The graph between DR and FAR is depicted as ROC and the maximized values of this graph is better. The objectives of design of IDS systems is to achieve higher value of DR at a lower value of FAR and are controlled by various parameters of the IDS, like threshold value, size of a sliding window. To plot this ROC curve DR is taken along Y-axis and Far is taken along X-axis for the different values of threshold as shown in Fig. 3.

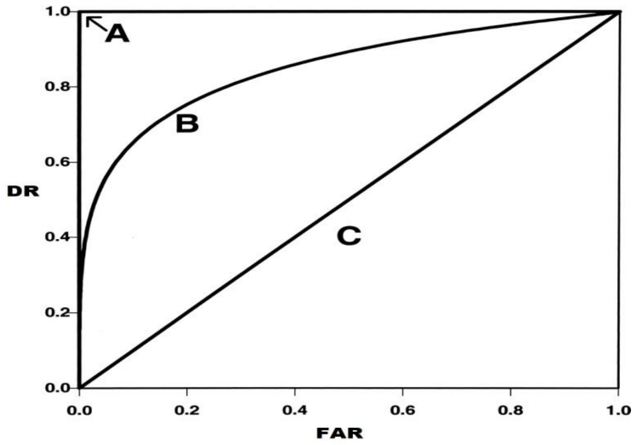

Figure 3. ROC curves showing the average intrusion detection rates

V. ALGORITHMS

This section presents various core computational intelligence approaches proposed so far researched and successfully deployed to solve intrusion detection problems. These techniques include most basic and used artificial neural networks (ANN) and its learning algorithms [14].

A. Artificial Neural Networks

An ANN consists of a collection of interconnected processing units called neurons which are capable of processing information at a very fast rate [15]. These neurons are connected by weighted links and are arranged in various layers. There layers are mandatory among them like input layer, hidden layers, and output layers. The number of nodes at input layer is decided by the size of input vector. The number of nodes at hidden layer is decided by hit and trial basis. At output layer the number of output class decides the number of nodes. ANN can be designed using various topologies varying from application to application. These structures have the ability to learn by examples i.e. values of the weights of the links are calculated [16], [17], [18], [19]. These networks are deployed for three types of application and are categorized in the following subsections:

1) Supervised Learning:

a) Feed Forward Neural Networks: This is one of the most basic and the simplest architecture that has been devised thus far. Feed forward neural networks are the first type of artificial neural networks devised. Normal or intrusive patterns are the two types of FFNN that are used commonly in modeling. Multi-layered Feed Forward (MLFF) Neural Networks makes use of various learning techniques such as back-propagation (MLFF-BP). MLFF-BP networks was primarily used for anomaly detection in the nascent intrusion detection development, in the context of user behavior, e.g. [15] and [16].

b) Radial Basis Function Neural Networks (RBF) It is most widely used feed forward neural networks. RBF perform classification by calculating the distances between centers and the inputs of the hidden RBF neurons, therefore they work faster than several other time consuming back-propagation, and are suitable for large sample size problems [17]. Several research works, employed RBF for learning multiple local clusters for normal events and several well-known attacks [18], [19], [20], [21]. Apart from being a classifier, these were also used to combine results obtained from various classifiers [17]. It outperformed several decision fusion functions, namely Weighted Majority Vote and Dempster-Shafer combination.

c) Recurrent Neural Networks Detection of attack spreads in a time period, such as slow port scanning, is necessary but difficult. For capturing the temporal locality in either anomaly patterns or normal patterns, several authors used similar mechanisms like time windows [, 18, 19, 22, 23], or chaotic neurons [24] in order to provide external memory to the BP networks.

2) Unsupervised Learning

a) Adaptive Resonance Theory and Self-Organizing Maps are two most common unsupervised neural networks. As is the case in statistical clustering algorithms, these also group objects according to the similarity. They are used for several intrusion detection tasks as well, while intrusions and abnormal behavior appear in regions of the sparse pattern space outside the normal clusters.

Self-Organizing Maps: (SOM), also referred to as Kohonen maps, are single-layer FNN with clustered outputs in a low dimensional grid (usually 3D or 2D). It conserves topological relationships between input data based on their similarity. SOM, the most popular neural networks used for tasks of anomaly detection. Fox et al. employed SOMs for virus detection in a multiuser machine [25]. Several other authors [26, 27] employed SOMs for learning normal system activities patterns. SOMs have also been found in the misuse detection, where a SOM functioned as a data pre-processor for clustering input data. Other algorithms, namely feed forward neural networks, was trained using the SOMs output [28, 29, 30]. Also, SOMs map data into one neuron from different classes.

Adaptive Resonance Theory (ART): They embrace several neural network models that perform supervised or unsupervised learning, prediction, and pattern recognition, since its invention by Stephen Grossberg, 1976. Models in unsupervised learning include Fuzzy ART ART-1, ART-2, ART-3, and supervised ones include ARTMAP, Gaussian ARTMAP and Fuzzy ARTMAP. In comparison to SOMs that clusters the data objects on the basis of the absolute distance; ARTs cluster them on the basis of the relative input patterns similarity of the weight vector. Amini et al. analyzed the performance of ART-2 (acceptance of continuous inputs) and ART-1 (acceptance of binary inputs) on KDD99 data [20]. It was proved that ART- 2 has a lower detection rate than ART-1, while ART-1 is 7 to 8 times slower than ART-2. Later, Amini et al. in [31] enhanced self-generated network traffic. They compared the performances of SOMs and ARTs. The results proved that ART nets shows better intrusion detection than SOMs on either online or offline data. Fuzzy ART nets combine adaptive resonance theory and fuzzy set theory. This resulting combination is more stable and faster than ART nets alone. Durgin et al. [33] and Liao et al. [32] proposed two examples using Fuzzy ART for detection of anomalies. Liao et al. proposed Fuzzy ART in an adaptive learning framework making it suitable for dynamic environments. Normal behaviour changes are efficiently accommodated while anomalous activities can still be identified. Durgin et al. investigated the Fuzzy ARTs SOMs and capabilities. Both Fuzzy ARTs and SOMs promised in detecting abnormal network behaviour. The sensitivity of Fuzzy ARTs is much higher as compared to that of SOMs.

VI. Conclusion

This paper present a survey on the problem of IDS along with detailed definitions proposed solutions, datasets and various machine learning techniques have been proposed. Various unsupervised and supervised ANNs were employed in anomaly detection and misuse of tasks. All these works utilized ANNs' ability to generalize from noisy, limited, and incomplete data. Several researchers attempted to address disadvantages of ANNs as well. The results from ANN based attacks classification shows the importance of application of machine learning techniques in IDS.

References

[1] Garcia-Teodoro, Pedro, et al, "*Anomaly-based network intrusion detection: Techniques, systems and challenges*", Computers & Security, Vol. 28, No. 1, pp 18-28. (2009):

[2] D. E. Denning. "*An intrusion detection model*." IEEE Transactions on Software Engineering, Special issue on computer security and privacy, Vol. 13, No. 2, pp 222–232, 1987.

[3] H. Debar, M. Dacier, and A. Wespi. "*Towards a taxonomy of intrusion-detection systems*." Networks, Vol. 31, No. 8, pp 805–822, 1999.

[4] S. Chebrolu, A. Abraham, and J. P. Thomas. *Feature deduction and ensemble design of intrusion detection systems*. Computers & Security, Vol. 24, No. 4, pp 295–307, 2005.

[5] D. Poole, A. Mackworth, R. Goebel. "*Computational Intelligence - A Logical Approach*", Oxford University Press, Oxford, UK, 1998. ISBN-10: 195102703.

[6] J. C. Bezdek, "*What is computational intelligence? Computational Intelligence Imitating Life"*, pp 1–12, 1994. IEEE Press, New York

[7] W. Duch, "*What is computational intelligence and where is it going",* In W. Duch and J. Mańdziuk, editors, Challenges for Computational Intelligence, volume 63 of Studies in

Computational Intelligence, pp 1–13. Springer Berlin / Heidelberg, 2007.

[8] B. Craenen, A. Eiben, "*Computational intelligence. Encyclopedia of Life Support Sciences"*, EOLSS; EOLSS Co. Ltd., 2002.

[9] The *KDD99 Dataset. Retrieved* January 26, 2008, from http://kdd.ics.uci.edu/databases/kddcup99/task.html.

[10] J. McHugh, *Testing intrusion detection systems a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory*. ACM Transactions on Information and System Security, Vol. 3, No. 4, pp 262–294, 2000.

[11] M. V. Mahoney, P. K. Chan, "*An analysis of the 1999 DARPA/Lincoln laboratory evaluation data for network anomaly detection"*. Technical Report TR CS-2003-02, Computer Science Department, Florida Institute of Technology, 2003.

[12] M. Sabhnani and G. Serpen. "*Why machine learning algorithms fail in misuse detection on KDD intrusion detection data set. Intelligent Data Analysis*", Vol. 8, No. 4, pp 403–415, 2004.

[13] J. Balthrop, S. Forrest, M. R. Glickman, "*Revisiting LISYS: Parameters and normal behavior*", In D. B. Fogel, M. A. El-Sharkawi, X. Yao, G. Greenwood, H. Iba, P. Marrow, and M. Shackleton, editors, Proceedings of the IEEE Congress on Evolutionary Computation (CEC '02), volume 2, pp 1045–1050, Honolulu, HI, USA, 12-17 May 2002. IEEE Press.

[14] L. Mé. GASSATA, "*a genetic algorithm as an alternative tool for security audit trails analysis"*. In Proceedings of the 1st International Workshop on the Recent Advances in Intrusion Detection (RAID 98), Louvain-la-Neuve, Belgium, pp 14-16 September 1998.

[15] K. Tan, "*The application of neural networks to unix computer security"*, In Proceedings of IEEE International Conference on Neural Networks, volume 1, pp 476–481, Perth, WA, Australia, Nov/Dec 1995. IEEE Press.

[16] J. Ryan, M. J. Lin, R. Miikkulainen, "*Intrusion detection with neural networks"*, Advances in Neural Information Processing Systems, Vol. 10, pp 943–949, 1998.

[17] A. P. F. Chan, W. W. Y. Ng, D. S. Yeung, and E. C. C. Tsang. "*Comparison of different fusion approaches for network intrusion detection using ensemble of RBFNN*." In Proceedings of 2005 International Conference on Machine Learning and Cybernetics, volume 6, pp. 3846–3851. IEEE Press, 18-21 Aug. 2005.

[18] A. Hofmann, C. Schmitz, and B. Sick. "*Rule extraction from neural networks for intrusion detection in computer networks"*, In IEEE International Conference on Systems, Man and Cybernetics, volume 2, pp 1259–1265. IEEE Press, 5-8 Oct. 2003.

[19] Z. Liu, G. Florez, and S. M. Bridges. "*A comparison of input representations in neural networks: A case study in intrusion detection"*, In Proceedings of the International Joint Conference on Neural Networks (IJCNN '02), volume 2, pages 1708–1713, Honolulu, HI, USA, 12-17 May 2002. IEEE Press.

[20] A. Rapaka, A. Novokhodko, and D. Wunsch. *Intrusion detection using radial basis function network on sequence of system calls*. In Proceedings of the International Joint Conference on Neural Networks (IJCNN '03), volume 3, pages 1820–1825, Portland, OR, USA, 20-24 July 2003. IEEE Press.

[21] C. Zhang, J. Jiang, and M. Kamel. *Comparison of BPL and RBF network in intrusion detection system*. In G. Wang, Q. Liu, Y. Yao, and A. Skowron, editors, Proceedings of the 9th International Conference on Rough Sets, Fuzzy Sets, Data Mining, and Granular Computing (RSFDGrC '03), 26-29 May, Chongqing, China, volume 2639 of Lecture Notes in Computer Science, chapter Proceedings of the 9th International Conference on Rough Sets, Fuzzy Sets, Data Mining, and Granular Computing (RSFDGrC '03), pages 466– 470. Springer Berlin / Heidelberg, 2003.

[22] A. K. Ghosh and A. Schwartzbard. *A study in using neural networks for anomaly and misuse detection*. In Proceedings of the 8th USENIX Security Symposium, volume 8, pages 141–152, Washington, D.C., USA, 23-36 August 1999.

[23] Z. Zhang, J. Li, C. Manikopoulos, J. Jorgenson, J. Ucles, "*HIDE: a hierarchical network intrusion detection system using statistical preprocessing and neural network classification*", In Proceedings of the 2001 IEEE Workshop Information Assurance and Security, pp 85–90, West Point, NY, USA, 2001. IEEE Press.

[24] Y. Yu, F. Gao, Y. Ge, "*Hybrid BP/CNN neural network for intrusion detection*" In Proceedings of the 3rd international conference on Information security, volume 85 of ACM International Conference Proceeding Series, pp 226–228, 2004.

[25] K. Fox, R. Henning, J. Reed, "*A neural network approach toward intrusion detection*" In Proceedings of the 13th National Computer Security Conference, Vol. 1, pp 124–134, Washington, D.C., USA, 1-4 Oct. 1990.

[26] A. J. Hoglund, K. Hatonen, A. S. Sorvari, "*A computer host-based user anomaly detction system using the self-organizing map*", In Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks (IJCNN '00), Vol. 5, pp 411–416, Como, Italy, 24-27 July 2000. IEEE Press.

[27] W. Wang, X. Guan, X. Zhang, L. Yang, "*Profiling program behavior for anomaly intrusion detection based on the transition and frequency property of computer audit data*", Computers & Security, Vol. 25, No. 7, pp. 539–550, 2006.

[28] A. Bivens, C. Palagiri, R. Smith, B. Szymanski, M. Embrechts, "*Network based intrusion detection using neural networks",* Intelligent Engineering Systems through Artificial Neural Networks, Vol. 12, No. 1, pp 579–584, 2002.

[29] J. Cannad, J. Mahaffey, *The application of artificial neural networks to misuse detection: Initial results*", In Proceedings of the 1st International Workshop on Recent Advances in Intrusion Detection (RAID 98), Louvain-la-Neuve, Belgium, ppn14-16 September 1998.

[30] C. Jirapummin, N. Wattanapongsakorn, P. Kanthamanon, "*Hybrid neural networks for intrusion detection system*", In The 2002 International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC '02), Vol 7, pp 928–931, Phuket, Thailand, 2002.

[31] M. Amini, R. Jalili, H. R. Shahriari, "*RT-UNNID: A practical solution to real-time network-based intrusion detection using unsupervised neural networks*", Computers & Security, Vol. 25, No. 6, pp 459–468, 2006.

[32] Y. Liao, V. R. Vemuri, and A. Pasos. "*Adaptive anomaly detection with evolving connectionist systems"*, Journal of Network and Computer Applications, Vol. 30, No. 1, pp 60–80, 2007. Special Issue on Network and Information Security: A Computational Intelligence Approach.

[33] N. A. Durgin, P. Zhang, "*Profile-based adaptive anomaly detection for network security*", Technical report, Sandia National Laboratories, 2005.

Authors Profile

Dr. Ravinder Kumar received Ph. D. in IT from GGSIP University, Delhi in 2013 and M. Tech. degree in Computer Science & Engineering in 1998 from GJ University of Science and Technology, Hisar, India. Since 1999, he has been with the University School of ICT, GGSIP University, Delhi. Currently, he is Professor and Head, Department of CSE with HMR Institute of Technology and Management Delhi, India. His research interest is in the image processing and biometrics. He has 18 years of teaching experience and 8 years of Research Experience.