Machine Learning Approach to IDS: A Comprehensive Review

Kunal
Department of Computer Engineering
NIT, Kurukshetra
Kurukshetra, INDIA
kunalrohilla333@gmail.com

Mohit Dua
Department of Computer Engineering n
NIT, Kurukshetra
Kurukshetra, INDIA
er.mohitdua@nitkkr.ac.in

***Abstract*— Due to the very fast growth of computer networks, Internet emerges as an important tool to obtain the desired information. As the data transferred using networks is rapidly increasing, simultaneously the possibility of security threats have also increased. Hence, there is a need to constantly monitor the network traffic in order to secure private networks. Intrusion occurs when a set of actions trade off the confidentiality, integrity, or availability of a system. Intrusion detection systems (IDS) raise alerts if any unusual network traffic is detected and thus remains critical for network safety. Utilization of machine learning led methodologies in anomaly-based detection has gained popularity in recent years. In this paper, we conduct a thorough survey of studies based on the intrusion detection systems by using machine learning algorithms and present comparison dependent on dataset used, data reduction approaches, type of classifiers used and the outcome achieved by such different algorithms.**

Keywords— Computer Network Security, Intrusion Detection, Machine Learning, Data Mining

I. INTRODUCTION

The sensitive information available on the internet constantly attracts adversary and thus susceptible against intense network invasion. When adversary forwards malicious packets to host systemto steal or change confidential data via a compromised network, which is generally termed as intrusion. It may occur on server or system because of the existing vulnerabilities like mis-configuration or program defects. Assembling different vulnerabilities can also result in a smart attack. A successful intrusion consists of following steps [1]:

- Reconnaissance: Act to explore specially to gain information about the target. It is achieved by executing network commands such as "nslookup", "whois" to get domain name, IP addresses, server details etc.
- Scanning and probing: Includes finding insecure areas in target system to search for valuable information.
- Remote to local attacks (R2L): To gain access by remotely sending malicious network packets so that attacker can run commands on the target system. These attacks are generally performed by taking advantage of system vulnerabilities, using open ports, password prediction, sniffing etc.
- User to root attacks (U2R): These attacks are done for acquisition of administrator access of system for entire control.
- Start attacks: Attacks are instigated after getting root access. For example, stealing or modifying confidential information.

Intrusion detection systems (IDS) are deployed to raise an alarm if any such activity occurs in internal networks. Productive IDS are typically created through the usage of machine learning and data mining strategies because they can incredibly distinguish intrusions. These procedures include a training phase in which model is trained using datasets. Datasets contains labelled samples of both attack and normal class. After training these models with mathematical algorithms, trained model is tested on separate samples of data to check accuracy of prediction.

This paper is divided in 7 sections. After introduction, we explain Architecture of generic IDS in section II, then in section III learning procedures in IDS are explained. After that we discuss data reduction methods in section IV. Performance evaluation metrics are explained in section V, and then, a comparison table of studies based on Machine Learning techniques and their respective precision is done in section VI and lastly, we conclude the paper with in section VII.

II. ARCHITECTURE OF INTRUSION DETECTION

Dorothy E. Denning et al. implemented the first Intrusion Detection System (IDS) in 1986 under research group named SRI International [2]. The double component model was described to have signature detection component which contained attack rule base and anomaly recognition phase by the use of statistical based approach to detect novel attacks. After that IDS became an interesting issue of study in research community. Intrusion identification systems (IDS) are commonly divided into two types: Signature and Anomaly intrusion detection systems. Signature-based intrusion identification rely on comparison with signatures of recognized attacks which are stored in a database, but it cannot detect unknown attacks. However, Anomaly-based IDS use statistical approach to detects activities that deviates from usual limit of resource use and typical conduct parameters. False positives and False negatives rate remain high in case of anomaly-based identification. Figure 1. Illustrates working of these Intrusion Detection Systems.

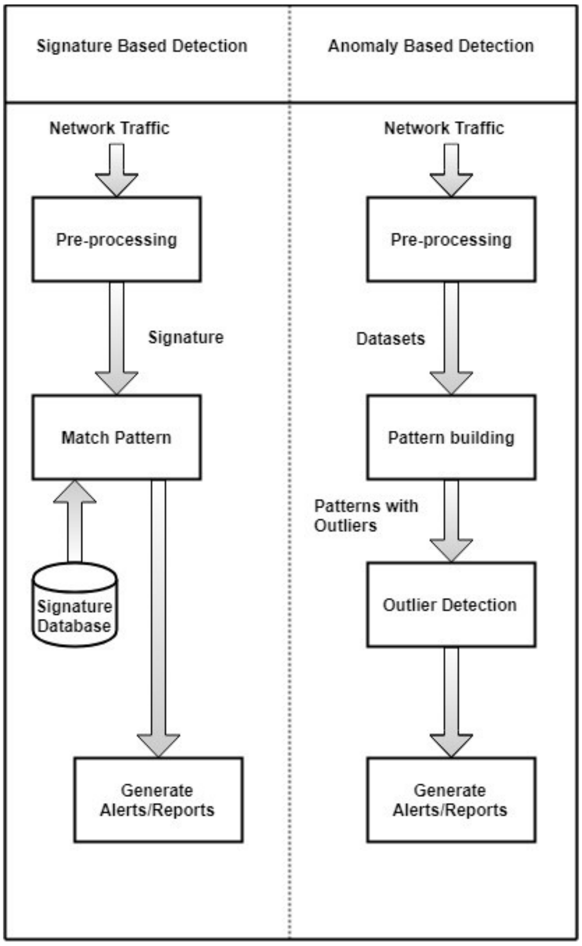

Fig. 1. Signature and Anomaly IDS

Anomaly-based Detection methods should be prepared for detecting irregular behaviors and to accomplish ideal accuracy. Machine learning techniques utilize mathematical algorithms to train the model from datasets. An IDS may even predict zero-day attacks if enough training data is available and well enough algorithms are implemented. Cyber security managers can make use of these techniques to ensure security measures.

III. LEARNING PROCEDURES IN INTRUSION DETECTION SYSTEMS

In Supervised learning, we first train the machine by giving data labelled with correct solutions, while in unsupervised learning no initial training is done, so there are no connections in data and their corresponding solutions. In Semi-supervised learning only a little amount of data is labelled.

A. Supervised learning

Supervised learning is a procedure, where we provide both input and corresponding desired output to a learning model which forms the basis of future data prediction [3]. A well labelled training dataset containing attacks and normal samples is required to build such models. Although supervised learning gives classifiers more information, hypothetically it should produce better results than unsupervised learning, but Supervised learning has some issues.

- There is no guarantee of accurate labelling in dataset.
- Noise and redundancy in dataset produce high false positives and negatives alarm rate.

B. Semi-supervised learning

Semi-supervised learning methods lie somewhat in-between supervised and unsupervised methods. This method benefits real-time anomaly detection implementations as labelled samples of normal class needs to be matched. Currently, this strategy isn't utilized as labels for almost all possible anomalies are already available in training time [4].

C. Unsupervised learning

In this method, Statistical models are used to classify data samples into normal or anomalous with no metadata. Hence labelled data is not needed in light of following suppositions [5].

- Majority of information available is non-attack data and attack data signifies a very little measure of it.
- Statistically, Attack and Non-attack data isn't exactly equivalent to each other.

IV. DATA REDUCTION METHODS USED IN IDS

Majority of Machine learning and data mining approaches couldn't work well with intrusion detection because of gigantic complexity and size of datasets. These techniques take huge computational time to classify attacks which makes implementation more difficult in real time environments. This is because of huge number of features are contained in network data which is to be processed by Intrusion Detection System [6]. For better classification, quantity and quality of features matter and it helps us understand their importance and their co-relation [7]. If features selected are very less, then classification quality will reduce and if they are more than required, it will make loss of generalization. Experimental results show that accuracy and computational cost is improved when we use feature extraction techniques in Intrusion Detection Systems [8]. Thus, dimensionality and feature reduction strategies are being used as a pre-processing step to improve accuracy and to reduce time for attack detection.

A. Feature Selection

Feature selection techniques are used to discover subset of finest features which could improve overall outcome of the procedure and generate few errors. Another goal is to decrease computation time and storage utilization. In IDS, feature selection techniques are utilized to improve accuracy of attack detection. Some of the dominant feature selection methods are Principal component analysis (PCA), Information gain (IG), and genetic algorithm (GA) [9]. Filter and Wrapper are two kind of features selection strategies in which we incorporate different FS methods.

• In Wrapper technique, a classifier is utilized as a black box for evaluating optimal features. Such methods achieve great speculation, yet sometimes endure high dimensionality due to the computational expense of preparing the classifier.

• Filter methods don't utilize any classifier for feature evaluation and are relatively powerful against overfitting, yet it utilizes autonomous estimation techniques, for example, distance measures, consistency measures, and correlation measure.

B. Feature Extraction

In a dataset, rows represent samples and columns represents features, where features are a result of quantitative and subjective findings. Feature extraction is used to reduce the dimensionality of data set by reducing set of features in a way that accuracy of attack detection is not altered and time used in discovery is reduced. Numerous feature extraction methods are available in the field. For example, self-organizing maps, principal component analysis etc.

C. Clustering

In clustering data samples are grouped into sets of data where data samples in each set is similar in one way or the other.

V. PERFORMANCE METRIX

Confusion matrices are used to represent the data associated to predicted and actual classification done by classifiers. Following terms are used while representing a confusion matrix.

- True-Positive (TP): Correctly classify an anomalous sample as attack.
- True-Negative (TN): Correctly classify a non-attack sample as ordinary instance.
- False-Positive (FP): Incorrectly classify an ordinary sample as anomalous instance.
- False-Negative (FN): Incorrectly classify an attack sample as ordinary instance.

Reduction of False negatives and False positives is a major research problem as these have very negative effects on overall security of networks.

Table 1. Confusion Matrix

		Predicted	
		Attack	Normal
Actual	Attack	TP	FN
	Normal	FP	TN

Using above mentioned terms and matrix from table 1, we evaluate Accuracy, Attack Detection Rate, and False Alarm Rate.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$Attack\ Detection\ Rate = \frac{TP}{TP+FN} \quad (2)$$

$$False\ Alarm\ Rate = \frac{FP}{FP+TN} \quad (3)$$

Diagonal elements in matrix signifies correct predictions while remaining elements indicates wrong estimation [10]. Receiver operating characteristics (ROC) curve is a measure to find cost sensitivity of a classifier [1],[11].

VI. COMPARISION OF PREVIOUS METHODS

Table 2. shows a comparison of IDS models which are proposed in recent years.

Table 2. Comparison of recent IDS models.

Author(s)	Year	Database Used	Feature Extraction (Data Reduction) Method Used	Classifier Used	Outcome/Accuracy
S.J. Horng, et al. [12]	2011	kddcup99	BIRCH Hierarchical clustering	Support Vector Machines (SVM)	95.72%
W. li, et al. [13]	2011	kddcup99	NA	SVM	99.93%
Y. Li, et al. [14]	2012	kddcup99	GFR Method (Wrapper based approach)	SVM	98.62%
S. Mukherjee, et al. [15]	2012	NSL KDD	Feature Vitality Based Reduction Method	Naïve Bayes	97.78%

R. M. Elbasiony [16]	2013	KDD Cup 1999	NA	Random Forests + Weighted K-means	98.3%
M. S. Pervez, et al. [17]	2014	NSL-KDD	Self-Proposed Algorithm	SVM	91% using 3 features, 99% using 36 features
E. D. L. Hoz, et al. [18]	2015	KDD Cup 1999	PCA-FDR	PSOM	88%
U. Ravale, et al. [19]	2015	kddcup99	K-Means Clustering	Radial basis function and SVM	NA
R Singh, et al. [20]	2015	NSL KDD, Kyoto University benchmark dataset	Alpha Profiling	Online Sequential Extreme Learning Machine	97.67%, 96.37%
Farnaaz, N., et al. [21]	2016	NSL KDD	Symmetrical uncertainty (SU)	Random Forest	DoS 99.67 Probe 99.67 R2L 99.67 U2R 99.67
Belavagi., et al. [22]	2016	NSL KDD	NA	Multiple (Random Forest, Logistic Regression, Support Vector Machine Gaussian and Naive Bayes)	99% with Random Forest
Al-Yaseen, et al. [23]	2017	kddcup99	Modified K-Means	Multi-Level Hybrid ELM and SVM	95.75
Thaseen, I. S., et al. [24]	2017	NSL KDD	Chi-square	SVM (Multiclass)	98
Jabbar, M. A., et al. [25]	2017	Kyoto data set	NA	Ensemble (RF + AODE)	90.51
S. Aljawarneh, et al. [1]	2017	NSL KDD	Vote algorithm with Information Gain	Hybrid (Naïve Bayes, REP Tree, Random Tree, Meta Pagging, AdaBoostM1, J48, and Decision Stump)	99.81
Belouch, M., et al. [26]	2018	UNSW-NB15 dataset	NA	Random Forests (Best of 4 classifiers)	97.49
Shenfield, A., et al. [27]	2018	Various	NA	ANNs (MLP)	98
Salo, F., et al. [28]	2019	ISCX 2012, Kyoto 2006+ and NSL KDD	Information Gain and Principal Component Analysis	Ensemble (SVM, IBK and MLP)	99.01 (ISCX 2012) 98.24 (NSL-KDD) 98.95 (Kyoto 2006+)

Sara M, et al. [29]	2019	KDD Cup 1999	Linear correlation coefficient algorithm and Cuttlefish algorithm	Decision trees	95.03

VII. CONCLUSION

In present scenario, intrusion detection remains critical for network security and machine learning based applications which have given a major boost in finding novel attacks. Application of Multiple classifiers i.e. hybrid systems and ensemble learning methods in recent years have given a major boost in increasing the accuracy of attack detection techniques. But the rate of false positives and false negatives still needs to be addressed. We urge scientists/researchers to contemplate the likelihood of applying more methods which has a superior precision rate.

REFERENCES

[1] S. Aljawarneh, M. Aldwairi, and M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model", Journal of Computational Science, 25, 152-160, 2018.

[2] D.E. Denning, "An intruison-detection model", IEEE Symposium on Security and Privacy (1986) 118–131, 1986.

[3] A. Oberthur and P. Warnat, "Supervised classification", Encyclopedia of Cancer, pp. 3563–3565, 2012.

[4] A. Daneshpazhouh and A. Sami, "Entropy-based outlier detection using semi-supervised approach with few positive examples," Pattern Recognition Letters, vol. 49, pp. 77–84, 2014.

[5] S. Jiang, X. Song, H. Wang, J. J. Han, and Q. H. Li, "A clustering-based method for unsupervised intrusion detections," Pattern Recognition Letters, vol. 27, no. 7, pp. 802–810, 2006.

[6] C. Guo, Y. J. Zhou, Y. Ping, S. S. Luo, Y. P. Lai, and Z. K. Zhang, "Efficient intrusion detection using representative instances," Computers & Security, vol. 39, pp. 255–267, 2013.

[7] S. Saha, A. S. Sairam, A. Yadav, and A. Ekbal, "Genetic algorithm combined with support vector machine for building an intrusion detection system," in Proceedings of the International Conference on Advances in Computing, Communications and Informatics, ACM, pp. 566–572, 2012.

[8] F. Amiri, M. R. Yousefi, C. Lucas, A. Shakery, and N. Yazdani, "Mutual information-based feature selection for intrusion detection systems," Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1184–1199, 2011.

[9] J. R. Vergara and P. A. Estevez, "A review of feature selection methods based on mutual information,"Neural Computing and Applications, vol. 24, no. 1, pp. 175–186, 2014.

[10] D. H. Deshmukh, T. Ghorpade, and P. Padiya, "Improving classification using preprocessing and machine learning algorithms on NSL-KDD dataset," in Proceedings - 2015 IEEE International Conference on Communication, Information and Computing Technology, ICCICT 2015, 2015.

[11] G. Kumar, "Evaluation Metrics for Intrusion Detection Systems -A Study," Int. J. Comput. Sci. Mob. Appl., vol. 2, no. 11, pp. 11–17, 2014.

[12] 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(1), 306-313, 2011.

[13] Z. Liu, "A method of SVM with normalization in intrusion detection", Procedia Environmental Sciences, 11, 256-262, 2011.

[14] Y. Li, J. Xia, S. Zhang, J. Yan, X. Ai, and K. Dai, "An efficient intrusion detection system based on support vector machines and gradually feature removal method". Expert Systems with Applications, 39(1), 424-430, 2012.

[15] S. Mukherjee and N. Sharma, "Intrusion detection using naive Bayes classifier with feature reduction", Procedia Technology, 4, 119-128, 2012.

[16] R. M. Elbasiony, E. A. Sallam, T. E. Eltobely and M. M. Fahmy "A hybrid network intrusion detection framework based on random forests and weighted k-means", Ain Shams Engineering Journal, 4(4), 753-762, 2013.

[17] M. S. Pervez and D. M. Farid, "Feature selection and intrusion classification in NSL-KDD cup 99 dataset employing SVMs," The 8th International Conference on Software, Knowledge, Information Management and Applications (SKIMA 2014), Dhaka, pp. 1-6, 2014.

[18] E. De la Hoz, E. De La Hoz, A. Ortiz, J. Ortega, and B. Prieto, "PCA filtering and probabilistic SOM for network intrusion detection", Neurocomputing, 164, 71-81, 2015.

[19] U. Ravale, N. Marathe, and P. Padiya, "Feature selection based hybrid anomaly intrusion detection system using K means and RBF kernel function", Procedia Computer Science, 45, 428-435, 2015.

[20] R. Singh, H. Kumar, and R. K. Singla, "An intrusion detection system using network traffic profiling and online sequential extreme learning machine", Expert Systems with Applications, 42(22), 8609-8624, 2015.

[21] N. Farnaaz and M. A. Jabbar, "Random forest modeling for network intrusion detection system", Procedia Computer Science, 89, 213-217, 2016.

[22] M. C. Belavagi, and B. Muniyal, "Performance evaluation of supervised machine learning algorithms for intrusion detection", Procedia Computer Science, 89, 117-123, 2016.

[23] W. L. Al-Yaseen, Z. A. Othman and M. Z. A. Nazri "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system", Expert Systems with Applications, 67, 296-303, 2017.

[24] I. S. Thaseen and C. A. Kumar, "Intrusion detection model using fusion of chi-square feature selection and multi class SVM", Journal of King Saud University-Computer and Information Sciences, 29(4), 462-472, 2017.

[25] M. A. Jabbar, R. Aluvalu, "RFAODE: A novel ensemble intrusion detection system", Procedia computer science, 115, 226-234, 2017.

[26] M. Belouch, S. El Hadaj and M. Idhammad, "Performance evaluation of intrusion detection based on machine learning using Apache Spark", Procedia Computer Science, 127, 1-6, 2018.

[27] A. Shenfield, D. Day and A. Ayesh, "Intelligent intrusion detection systems using artificial neural networks", ICT Express, 4(2), 95-99, 2018.

[28] F. Salo, A. B. Nassif, and A. Essex, "Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection", Computer Networks, 148, 164-175, 2019.

[29] S. Mohammadi, H. Mirvaziri, M. Ghazizadeh-Ahsaee, and H. Karimipour, "Cyber intrusion detection by combined feature selection algorithm", Journal of information security and applications, 44, 80-88, 2019.