IJCTA, 9(15), 2016, pp. 7517-7522

A Survey on Intrusion Detection System Using Fuzzy Logic

M. Azhagiri*[*] and A. Rajesh[**]

ABSTRACT

Network security is used to monitor and prevent unauthorized access, exploitation, alteration, or denial of a computer network and network-handy resources. Network security is main issue of computing because many varieties of attacks are growing day by day. Network Security Situational Awareness (NSSA) has been a hot analysis within the network security domain. As a result of the big quantity of Intrusion Detection System (IDS), if clustering is used in KDD Cup 1999 knowledge sets which are grouped into several clusters and the integration of two IDS methods such as C4.5 and ID3 are applied into each clusters as experimental knowledge and comes to a conclusion that our planned methodology is practicable, reliable and economical.

Key Words: Network security, Clusters, C4.5, ID.

1. INTRODUCTION

Network security consists of the provisions and strategy adopted by a network administrator to monitor and prevent unauthorized access, exploitation, alteration, or denial of a computer network and network-accessible resources. Network security is considered to be more important because of inventive property that can be easily obtained through the network. The confidentiality and the integrity are needed to be considered for developing a secure network. It must ensure that the non-authenticated party does not audit the data and also it must guarantee that the data which is received has not been altered. NSSA plays an important role in the field of network security.

NSSA is a rising technique within the field of network security and it helps security analysts to be aware of the particular security scenario of their networks. NSSA has been a hot analysis within the network security domain. Intrusions are the activities that violate the security policy of the system. The general attacks on the network are DoS, U2R, R2L and probe. An IDS is a device, typically another separate computer that monitors the activity to identify these attacks, malicious or suspicious events.IDS monitors the system and user activities. It audits the system configuration vulnerabilities and misconfigurations. It corrects the system configuration errors. ID3 and C4.5 are the two intrusion detection algorithms which were efficiently combined here to avoid intrusion in the clusters. ID3 (Iterative Dichotomize 3) is an algorithm invented by Ross Quinlanused to generate a decision tree from a dataset. ID3 is the forerunner to the C4.5 algorithm, and is used in the machine learning and natural language processing domains. C4.5 is an extension of Quinlan's earlier ID3 algorithm. The decision trees generated by C4.5 can be used for classification, and so C4.5 is often referred to as a statistical classifier. In this paper these two algorithms are integrated to detect the intrusion in cluster set.

This paper is organized as follows. Section I describes the introduction about the network intrusion detection. Section II describes about the related works was carried out regarding the intrusion detection. Section III deals with the discussion about the related work. Research directions are pointed out in section IV. Section V describes the conclusion about the techniques available in literature work

[*] Dept of CSESt. Peter's University, Avadi, Chennai-600054, *Email: azhagiri1687@gmail.com*

[**] Dept of CSEC Abdul Hakeem College of Engineering and Technology, Tamil Nadu 632509, *Email: amrajesh73@gmail.com*

2. RELATED WORK

The intrusion detection system is the system to seek out the intruders in networks. Vivek K. Kshirsagar et al.[1] were mentioned the assorted IDS models and techniques. The author have primarily targeting signature based i.e. misuse detection system. Anomaly based IDS needs to spot new anomalies based on rules stored in IDS whereas misuse IDS will notice solely those attacks whose matching rules are already keep in rule set. The author self-addressed solely numerous IDS techniques out there in networks and therefore the author didn't claim that the precise model to predict intrusion in networks.

Mahdi Zamani and Mahnush Movahedi [2] were reviewed many influential algorithms for intrusion detection supported numerous Machine Learning (ML) techniques. Characteristics of ML techniques makes it potential to style IDS that have high detection rates and low false positive rates whereas the system quickly adapts itself to ever-changing malicious behaviors. The algorithms may be divided into two sorts of ML-based schemes: artificial intelligence (AI) and computational Intelligence (CI). though these 2 classes of algorithms share several similarities, many options of CI-based techniques, like adaptation, fault tolerance, high machine speed and error resilience within the face of noisy data, adjust the need of building economical intrusion detection systems. Eventhough a lot of range of techniques used for locating the intruders which supplies a lot of intrusion rate. If clustering is applied, the proportion of intrusion detection rate is reduced.

Emma ireland [3] used fuzzy genetic algorithmic program had a better detection rate than a decision tree algorithmic program in most cases, and it absolutely was sensible at detecting unknown attacks. The genetic algorithmic program had a high detection rate for denial of service attacks. when compared with the winning entry of the KDD99 Classifier Learning Contest, it was shown to possess a more robust detection rate for each denial of service and user to root attacks. This paper showed that the employment of genetic algorithms and fuzzy genetic algorithms in intrusion detection and it efficiently detecting the attacks. The author did not claim that the clustering approach to seek out the intrusion in networks.

R. Shanmugavadivu and Dr. N. Nagarajan [4] have developed an anomaly primarily based intrusion detection system for detecting the intrusion behaviour within a computer network. A fuzzy decision-making module was designed to build the system a lot of correct for attack detection, using the fuzzy inference approach. an efficient set of fuzzy rules for reasoning approach were known mechanically by creating use of the fuzzy rule learning strategy, that are more practical for detecting intrusion in a very electronic network. At first, the definite rules were generated by mining the one length frequent things from attack knowledge further as traditional knowledge. Then, fuzzy rules were known by fuzzifying the definite rules and these rules got to fuzzy system, that classify the take a look at knowledge. we have used KDD cup 99 dataset for evaluating the performance of the proposed system and experimentation results showed that the projected technique is effective in detecting numerous intrusions in computer networks.

Persi Pamela. I, Gayathri. P and N. Jaisankar [5] were measured the accuracy of the proposed system is found to be sensible for each Cleveland and Switzerland databases when compared to that of the prevailing work. Choice and application of solely the essential attributes greatly influences the performance of the system. With the prediction of coronary cardiovascular disease, early treatment may be given at the correct time that avoids the chance of heart attacks. Since the diagnosing involves straightforward procedures and is simple to get the specified results, the projected system is found to be economical than the opposite existing systems.

However, the performance of the projected work may be increased by as well as few extra attributes and checked for accuracy. This should be done along with detailed survey and doctors' opinion. As for the proposed system, only benchmark databases have been used, in future real-time databases can also be applied and checked for results. The optimization is performed for the fuzzy system, however with other soft computing methodologies like neural networks; this optimization technique could be applied in future.

Prathibha K S , Pankaj Kumar and Shyni T S [6] were used two data mining techniques are used in misuse and anomaly detection. A random forest classification algorithm is utilized in misuse detection part. And weighted kmeans clustering algorithm is used for cluster the data. Random forest is a powerful algorithm for building the patterns automatically instead of coding rules manually. The proposed approaches are evaluated over 10% KDD'99 dataset. In misuse detection framework, intrusion patterns are built in the offline phase.

The main attribute of misuse detection techniques is in comparing network traffic against a predefined intrusion pattern in order to decide whether it is measured an attack. In case of anomaly detection techniques involves any important deviation of a system from normal behavior. Hybrid framework, we used advantages of both abuse and anomaly detection, thus offering speed and accuracy to detect the intrusion. To improve the performance of clustering, we are modifying the clustering algorithm by including a weight of data feature. The result shows that our framework achieves a higher detection rate and low false positive rate, compared to other approaches. In the hybrid framework, in order to improve the performance of the anomaly detection component, misuse detection is applied first to filter out the known intrusions from the datasets. Thus, the number of connections in the anomaly detection component is significantly reduced. The limitation of the hybrid system is to keep the intrusion patterns in the dataset need to be much less than normal data. Another problem associated with our hybrid system, in anomaly detection, some intrusions cannot detect if it has a high degree of similarity. In future, more advanced data mining algorithms could be investigated to overcome the earlier limitations. And try to make all process online. The performance of weighted k means algorithm is strongly depending on the value of k clusters. Try to find the best method for deciding the value of k.

Weiming et. al.,[7] proposed an online Adaboost-based intrusion detection algorithm. In this algorithm decision stumps and online GMMs were used as weak classifiers for the traditional online Adaboost and for the proposed online Adaboost. The results of the algorithm were compared with the results of the algorithm using online GMMs and the proposed online Adaboost. A distributed intrusion detection framework is also proposed. Some of the advantages of the proposed work is online Adaboost based algorithms successfully overcame the difficulties in handling the mixed-attributes of network connection data. The local parameterized detection models were suitable for information sharing: Among nodes only a very small number of data were shared.

Guisong Liu and Xiaobin Wang [8] proposed an integrated scheme for intrusion detection (IIDS). Its function can be splited two parts, outer intrusion detection and inner illegal hosts detection and prevention. To detect intrusions from the Internet a novel methods GNG, a clustering methods PCASOM and adaptive GHA based PCANN are hierarchically integrated. The simulation explains that the IIDS system can obtain obviously better performance than single method.

Zubair Md. Fadlullah et. al., [9] highlighted the importance of designing appropriate intrusion detection systems to combat attacks against cognitive radio networks. And also an effective IDS, which can be easily implemented in the secondary users' cognitive radio software is proposed. The proposed IDS uses a non-parametric cusum algorithm, which offers anomaly detection. In particular, the authors presented an example of a jamming attack against a CRN secondary user, and demonstrated how the proposed IDS is able to detect the attack with low detection latency.

Yun Wang et. al., [10] analyzed the problem of intrusion detection in a Gaussian distributed WSN by characterizing intrusion detection probability with respect to intrusion distance and network deployment parameters. The network deployment parameters are intruder's starting point, deployment point, deployment deviation, number of deployed sensor, and sensing range. Two detection models are considered: single-sensing detection and multiple sensing detection. This work allows to analytically formulate the intrusion detection probability within a certain intrusion distance. The proposed model for intrusion detection allows to analytically formulate the intrusion detection probability within a certain intrusion distance under various network settings.

Omar AI-jarrah et. al., [12] provided the TDDNN neural network to solve the problem of IDS with temporal behavior of network attacks and use the packet capture engine to capture packets to preprocessing stage. The preprocessor saved the features of trapped line of time delay neural network (TDNN). The output of the preprocessor is connected directly to pattern recognition component and detecting attacks using neural networks. DARPA data sets are used to analysis the system in terms of capability and throughput. The output of test will be reduced all the probes in network and provide much better solution for the system.

The overall survey has been taken and as shown in table 1.1

Table 1
survey work related to intrusion detection

Name of the author	*Title of the paper*	*Publications/ year*	*concept*	*Advantages*	*Disadvantages*
Vivek K et. al.,	Intrusion Detection System using Genetic Algorithm and Data Mining: An Overview	IJCSI / 2012	Mainly focuses on genetic algorithm (GA) and data mining based IDS.Mainly concentrated on signature based i.e. misuse detection system.	Genetic algorithm based systems can be re-trained easily. This improves its possibility to add new rules and evolve intrusion detection system.	Misuse IDS can find only those attacks whose matching rules are already stored in rule set.
Mahdi Zamani and Mahnush Movahedi	Machine Learning Techniques for Intrusion Detection	CR 2015	Dividing the schemes into methods based on classical artificial intelligence (AI) and methodsbased on computational intelligence (CI) and the characteristics of CI techniques used to build efficient IDS are explained	Adaptation, fault tolerance, highcomputational speed and error resilience in the face of noisy information,	This workunfortunately does not provide any experimental results making it difficult for the reader to compare the performance of the proposed system with other ML-based IDS.
Emma Ireland	Intrusion Detection with Genetic Algorithms and Fuzzy Logic		Two ways of training an intrusion detection system are described to recognize possible attacks on a system: genetic algorithms and fuzzy logic.	The results Shows that the use of genetic algorithms and fuzzy logic intrusion detection are effective ways of detecting unknown attacks. The genetic algorithm had a high detection rate for denial of service attacks.	The fuzzy genetic algorithmis not the same as the traditional genetic algorithmwith fuzzy logic added to it.
R. Shanmugavadivu and Dr.N.Nagarajan	Network Intrusion Detection System Using Fuzzy Logic	IJCSE / 2015	The proposed fuzzy logic-based system can be able to detect intrusion behaviour of the networks since the rule base contains a better set of rules. Here the automated strategy for generation of fuzzy rules were used.	the proposed system achieved higher precision in identifying whether the records areNormal or attack one. The proposedmethod is effective in detecting various intrusions in computer networks.	Unfamiliar intrusions though constructed as a least alteration of previously known attacks cannot be found.
Persi Pamela.	A Fuzzy Optimization Technique for	IJET/ 2013	A fuzzy system is proposed in this paper along with a data mining	The system'saccuracy was found to be good**.**	However, the performance of the proposed work can be enhanced by including

(*contd...*)

(*Table 1 contd...*)

Name of the author	*Title of the paper*	*Publications/ year*	*concept*	*Advantages*	*Disadvantages*
	the Prediction of Coronary Heart Disease Using Decision Tree		technique forefficient diagnosis of coronary heart disease.		few additionalattributes and checked for accuracy. This should be done along with detailed survey and doctor's opinion.
Prathibha K S	Analysis of Hybrid Intrusion Detection System Based on Data Mining Techniques	IJETT/ 2014	A hybrid intrusiondetection framework based on data mining classification and clustering techniques is proposed.A random forest classificationalgorithm is used in misuse detection part. And weighted kmeans clustering algorithm is used for cluster the data.	In the proposed hybrid framework, The result shows that the proposed framework achieves a higher detection rate and low false positive rate, compared to other approaches	The performance of weighted kmeans algorithm is strongly depending on the value of k clusters.

3. DISCUSSION

There are more number of approaches are available for detecting the intrusion. Even though the rate of detection is high, the time taken to find the intrusion is also high. If clustering approach is used in a particular data set, it finds the intrusion fastly and less time. Clustering is not explored in the past literature and quality of cluster is not addressed.

4. RESEARCH DIRECTIONS

The intrusion detection and evaluation can be done using the following techniques.

1. Selection of data set is an important factor to find the intrusion.
2. If the clustering algorithm is used, easy to find the intrusion
3. If the algorithm is used to find the intrusion in cluster, detection rate will be high.
4. If the quality of the cluster is evaluated by precision, recall, purity , entropy, inter and intra cluster distance yields better performance.

5. CONCLUSION

Network security is considered to be more important because of inventive property that can be easily obtained through the network. The confidentiality and the integrity are needed to be considered for developing a secure network. In this paper, a detailed survey has been taken regarding the intrusion detection technique used in the literature. If clustering is applied in the given data set, the intrusion will be avoided in a high rate. The result of our integrated system will effectively and efficiently notice attacks such as DoS, U2R, R2L when compared to other well known strategies.

REFERENCES

[1] Vivek K. Kshirsagar, Sonali M. Tidke & Swati Vishnu, "Intrusion Detection System using Genetic Algorithm and Data Mining: An Overview" , *International Journal of Computer Science and Informatics*, vol.1, no. 4, pp. 2231 –5292, 2012.

[2] Mahdi Zamani and Mahnush Movahedi, "Machine Learning Techniques for Intrusion Detection", *CR* pp.1-11, 2015.

[3] Emma Ireland, " Intrusion Detection with Genetic Algorithms and Fuzzy Logic", Journal of Intrusion in network", vol.3, no.5, 2014.

[4] R. Shanmugavadivu and Dr.N.Nagarajan, “Network Intrusion Detection System Using Fuzzy Logic”, *Indian Journal of Computer Science and Engineering (IJCSE),* vol. 2, no. 1, pp. 101-111, 2015.

[5] Persi Pamela. I, Gayathri. P and N. Jaisankar, “A Fuzzy Optimization Technique for the Prediction of Coronary Heart Disease Using Decision Tree”, *International Journal of Engineering and Technology (IJET),* vol. 5, no. 3, 2013.

[6] Prathibha K S , Pankaj Kumar and Shyni T S, “Analysis of Hybrid Intrusion Detection System Based on Data Mining Techniques”, *International Journal of Engineering Trends and Technology (IJETT),* vol. 15, no. 9, pp. 447-452, 2014.

[7] Weiming Hu, Jun Gao, Yanguo Wang, Ou Wu, and Stephen Maybank, “Online Adaboost-Based Parameterized Methods for Dynamic Distributed Network Intrusion Detection”, *IEEE Transactions On Cybernetics*, pp.1-17, 2013.

[8] Guisong Liu and Xiaobin Wang, “An Integrated Intrusion Detection System by Using Multiple Neural Networks”, Proceedings of CIS, IEEE, pp.22-27, 2013.

[9] Zubair Md. Fadlullah, Hiroki Nishiyama, and Nei Kato, Mostafa M. Fouda, “Intrusion Detection System (IDS) for Combating Attacks Against Cognitive Radio Networks*”, International Conference on Networks*, pp. 51-56, 2013.

[10] Yun Wang, Weihuang Fu, and Dharma P. Agrawal, “Gaussian versus Uniform Distribution for Intrusion Detection in Wireless Sensor Networks”, *Ieee Transactions On Parallel And Distributed Systems*, vol.24, no.2, pp. 342-355, 2013.

[11] Omar Al-Jarrah, Ahmad Arafat, “Network Intrusion Detection System Using Attack Behavior Classification”, Proceedings of *5th International Conference on Information and Communication Systems (ICICS),* IEEE, pp.1-6, 2014.