A Survey of Various Intrusion Detection Systems

Nitin Namdev[1] Prof. Ravindra Kumar Gupta[2] Dr. Shailendra Singh[3]
[1,2,3]SSSIST Sehore

Abstract— In this paper, we present an overview of existing intrusion detection techniques. All these algorithms are described more or less on their own. Intrusion detection system is a very popular and computationally expensive task. We also explain the fundamentals of intrusion detection system. We describe today's approaches for intrusion detection system. From the broad variety of efficient techniques that have been developed we will compare the most important ones. We will systematize the techniques and analyze their performance based on both their run time performance and theoretical considerations. Their strengths and weaknesses are also investigated. It turns out that the behavior of the algorithms is much more similar as to be expected.

I. INTRODUCTION

In today's scenario, everyone is using Internet to communicate with each other. Internet is not only limited to the web mail and chat but also extended to the field of education, business, media and many more. Day by day, we are becoming more and more dependent to the Internet, which makes our life easier. It is changing our way of communication, business mode and even everyday life. Now question is, whether it is safe to deal each and everything using Internet, whether it is secure enough. The answer is 'no' as we are not fully safe using Internet. This is because, as Internet grows, number of attacks also increases. Intrusion detection concept was introduced by James Anderson in 1980[5] defined an intrusion attempt or threat to be potential possibility of a deliberate unauthorized attempt to access information, manipulate or render a system unreliable or unusable. Sights moved for using data mining in content of NIDS in the late of 1990's. Researchers suddenly recognized the need for existence of standardized dataset to train IDS tool. Minnesota Intrusion Detection System (MINDS) combines signature based tool with data mining techniques. Signature based tool (Snort) are used for misuse detection & data mining for anomaly detection.

II. LITERATURE SURVEY

In [6] Jake Ryan et al applied neural networks to detect intrusions. Neural network can be used to learn a print (user behavior) & identify each user. If it does not match then the system administrator can be alerted. A back propagation neural network called NNID was trained for this process.

Denning D.E et al [7] has developed a model for monitoring audit record for abnormal activities in the system. Sequential rules are used to capture a user's behavior [8] over time. A rule base is used to store patterns of user's activities deviates significantly from those specified in the rules. High quality sequential patterns are automatically generated using inductive generalization & lower quality patterns are eliminated. An automated strategy for generation of fuzzy rules obtained from definite rules using frequent items. The developed system [9] achieved higher precision in identifying whether the records are normal or attack one.

Dewan M et al [10] presents an alert classification to reduce false positives in IDS using improved self-adaptive Bayesian algorithm (ISABA). It is applied to the security domain of anomaly based network intrusion detection.

S.Sathyabama et al [11] used clustering techniques to group user's behavior together depending on their similarity & to detect different behaviors and specified as outliers.

Amir Azimi Alasti et al [12] formalized SOM to classify IDS alerts to reduce false positive alerts. Alert filtering & cluster merging algorithms are used to improve the accuracy of the system. SOM is used to find correlations between alerts.

Alan Bivens et al [13] has developed NIDS using classifying self-organizing maps for data clustering. MLP neural network is an efficient way of creating uniform, grouped input for detection when a dynamic number of inputs are present.

An ensemble approach [14] helps to indirectly combine the synergistic & complementary features of the different learning paradigms without any complex hybridization. The ensemble approach outperforms both SVMs MARs & ANNs. SVMs outperform MARs & ANN in respect of Scalability, training time, running time & prediction accuracy. This paper [15] focuses on the dimensionality reduction using feature selection. The Rough set support vector machine (RSSVM) approach deploy Johnson's & genetic algorithm of rough set theory to find the reduct sets & sent to SVM to identify any type of new behavior either normal or attack one.

Aly Ei-Senary et al [16] has used data miner to integrate Apriori & Kuok's algorithms to produce fuzzy logic rules that captures features of interest in network traffic.

Taeshik Shon et al [17] proposed an enhanced SVM approach framework for detecting & classifying the novel attacks in network traffic. The overall framework consist of an enhanced SVM- based anomaly detection engine & its supplement components such as packet profiling using SOFM, packet filtering using PTF, field selection using Genetic Algorithm & packet flow-based data preprocessing. SOFM clustering was used for normal profiling. The SVM approach provides false positive rate similar to that of real NIDSs. In this paper [18] genetic algorithm can be effectively used for formulation of

decision rules in intrusion detection through the attacks which are more common can be detected more accurately.
Oswais.S et al [18] proposed genetic algorithm to tune the membership function which has been used by IDS. A survey was performed using approaches based on IDS, and on implementing of Gas on IDS.

Norouzian M.R et al [19] defined Multi- Layer Perceptron (MLP) for implementing & designing the system to detect the attacks & classifying them in six groups with two hidden layers of neurons in the neural networks. Host based intrusion detection is used to trace system calls. This system does not exactly need to know the program codes of each process. Normal & intrusive behavior are collected through system call & analysis is done through data mining & fuzzy technique. The clustering and genetic optimizing steps [20] were used to detect the intrude action with high detection rate & low false alarm rate.

III. CONCLUSION

In this paper, we surveyed the list of existing intrusion detection system techniques. Their merits and demerits are also discussed. In a forthcoming paper, we pursue the development of a novel classification based algorithm for intrusion detection system. Our proposed algorithm will be efficient in comparison to existing algorithms.

REFERENCES

[1] Litty Lionel, "Hypervisor-based Intrusion Detectio", Master of Science Graduate department of computer Science University of Torronto, 2005.
[2] Mark Crosbie and gene Spafford, "Active defence of a computer system using anonymous agents", Technical report 95-008,COAST Group, Department of Computer Science, Purdue University, West Lafayette, Indiana, February 1995.
[3] Litty, Intrusion Detection, Http://www.cs.torronto.edu/~litty/papers/MS.pdf.
[4] Network Security by Christos Douligeris, Dimitrios Nikolaou Serpanos page 93.
[5] Anderson.J.P, "Computer Security Threat Monitoring & Surveilance", Technical Report, James P Anderson co., Fort Washington, Pennsylvania, 1980.
[6] Jake Ryan, Meng - Jang Lin, Risto Miikkulainen, "Intrusion Detection With Neural Networks", Advances in Neural Information Processing System 10, Cambridge, MA:MIT Press,1998,DOI:10.1.1.31.3570.
[7] Denning .D.E, "An Intrusion Detection Model", Transactions on Software Engineering, IEEE Communication Magazine, 1987,SE-13, PP-222-232,DOI:10.1109/TSE.1987.232894.
[8] Teng.H.S, Chen.K and Lu.S.C, "Adaptive Real-Time Anomaly Detection using Inductively Generated Sequential Patterns, in the Proceedings of Symposium on research in Computer Security & Privacy, IEEE Communication Magazine,1990, pp-278-284.
[9] Sekeh.M.A,Bin Maarof.M.A, "Fuzzy Intrusion Detection System Via Data Mining with Sequence of System Calls", in the Proceedings of International Conference on Information Assurance & security (IAS)2009,IEEE Communication Magazine, pp- 154-158,ISBN:978-0-7695-3744-3,DOI:10.1109/IAS.2009.32.
[10] Dewan Md, Farid, Mohammed Zahidur Rahman, "Anomaly Network Intrusion Detection Based on Improved Self Adaptive Bayesian Algorithm", Journal of Computers, Vol 5, pp-23-31, Jan 2010, DOI:10.4.304/jcp 5.1.
[11] Sathyabama.S, Irfan Ahmed.M.S, Saravanan.A,"Network Intrusion Detection Using Clustering: A Data Mining Approach", International Journal of Computer Application (0975-8887), Sep-2011, Vol: 30, No: 4, ISBN: 978-93-80864-87-5, DOI: 10.5120/3670-5071.
[12] Amir Azimi, Alasti, Ahrabi, Ahmad Habibizad Navin, Hadi Bahrbegi, "A New System for Clustering & Classification of Intrusion Detection System Alerts Using SOM", International Journal of Computer Science & Security, Vol: 4, Issue: 6, pp-589-597, 2011.
[13] Alan Bivens, Chandrika Palagiri, Rasheda Smith, Boleslaw Szymanski, "Network-Based Intrusion Detection Using Neural Networks", in Proceedings of the Intelligent Engineering Systems Through Artificial Neural Networks, St.Louis, ANNIE-2002, and Vol: 12, pp- 579-584, ASME Press, New York.
[14] Srinivas Mukkamala, Andrew H. Sung, Ajith Abraham, "Intrusion Detection Using an Ensemble of Intelligent Paradigms",Journal of Network & Computer Applications ,pp-1-15, 2004.
[15] Shilendra Kumar, Shrivastava ,Preeti Jain, "Effective Anomaly Based Intrusion Detection Using Rough Set Theory & Support Vector Machine(0975-8887), Vol:18,No:3, March 2011,DOI: 10.5120/2261-2906.
[16] Aly Ei-Semary, Janica Edmonds, Jesus Gonzalez-Pino, Mauricio Papa, "Applying Data Mining of Fuzzy Association Rules to Network Intrusion Detection", in the Proceedings of Workshop on Information Assurance United States Military Academy 2006, IEEE Communication Magazine, West Point, NY,DOI:10.1109/IAW.2006/652083.
[17] Taeshik Shon, Jong Sub Moon, "A Hybrid Machine Learning Approach to Network Anomaly Detection", Information Sciences 2007, Vol: 177, Issue: 18, Publisher: USENIX Association, pp- 3799-3821, ISSN:00200255,DOI:10.1016/j.ins-2007.03.025.
[18] Sadiq Ali Khan, "Rule-Based Network Intrusion Detection Using Genetic Algorithm", International Journal of Computer Applications, No: 8, Article: 6, 2011, DOI: 10.5120/2303-2914.
[19] Norouzian.M.R, Merati.S, "Classifying Attacks in a Network Intrusion Detection System Based on Artificial Neural Networks", in the Proceedings of 13th International Conference on Advanced Communication Technology(ICACT), 2011,ISBN:978-1-4244-8830-8,pp-868-873.
[20] Jin-Ling Zhao, Jiu-fen Zhao ,Jian-Jun Li, "Intrusion Detection Based on Clustering Genetic Algorithm", in Proceedings of International Conference on Machine Learning & Cybernetics (ICML),2005, IEEE Communication Magazine,ISBN:0-7803-9091-1,DOI: 10.1109/ICML.2005.1527621.

