Abstract

An Intrusion Detection System (IDS) is very important to safeguard computer networks against confidentiality, integrity and availability breaches. Detection effectiveness of an IDS is characterized by high detection accuracy, high detection rate and low false positive rate. Many existing Anomaly-based Intrusion Detection Systems (AIDS) are ineffective and fail to distinguish between normal and abnormal data. This affects the detection accuracy and generates a high false alarm rate. Therefore, this paper has proposed a new AIDS based on Supervised and unsupervised methods that effectively detects attacks with a low false positive rate. The proposed approach consists of ensemble clusters with an efficient clustering technique, and enhancing the capability of the detection classifier by utilizing an efficient method. Experimental results showed an improvement in the detection accuracy which scored 97.0% on the overall accuracy and 0.03 % on the false positive rate for all classes of network traffic. Hence, this validates the proposed GSA-based AIDS.

References
1. Yadav, M. R, and Kumbharkar, P. B, "Intrusion Detection System with Supervised Learning Algorithms ", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Vol. 4(4), (2014), 305–310.

2. Tsai, C. F, and Lin, C.Y, "A triangle Area based Nearest Neighbors Approach to Intrusion Detection. ", Pattern Recognition, 43(1), (2010), 222–229.

3. Gao, H., Zhu, D, and Wang, X. 2010. A parallel clustering ensemble algorithm for intrusion detection system. In The Ninth International Symposium on Distributed Computing and Applications to Business Engineering and Science, DCABES.IEEE, 450–453.

4. Patka, S. (2014). Intrusion detection model based on data mining technique. In International Conference on Advances in Engineering and Technology, ICAET. IOSR-JCE, 34–39.

5. Ghaemi, R., bin Sulaiman, N., Ibrahim, H, and Mustapha, N, " A review: accuracy optimization in clustering ensembles using genetic algorithms", Artificial Intelligence Review, 35(4), (2011), 287–318.

6. Bahri, E., Harbi, N, and Huu, H. N. 2012. A Multiple Classifier System Using an Adaptive Strategy for Intrusion Detection. In International Conference on Intelligent Computational Systems, ICICS. 7–8.

7. Majid, A., Khan, A. and Mirza, A. M, " Combination of support vector machines using genetic programming", International Journal of Hybrid Intelligent Systems, 3(2), (2006), 109–125.

8. Kuang, F., Xu, W, and Zhang, S, "A novel hybrid KPCA and SVM with GA model for intrusion detection ", Applied Soft Computing, 18, (2014), 178–184.

9. Srinivas, M. and, Andrew, H. 2003. Feature selection for intrusion detection using neural networks and support vector machines. Transportation Research Board, winter, 1–11.

10. Tsai, C. F., Hsu, Y. F., Lin, C.Y, and Lin, W.Y, " Intrusion Detection by Machine Learning: A review. Expert Systems with Applications", 36(10), (2009), 11994–12000.

11. Ranaee, V., Ebrahimzadeh, A. and Ghaderi, R, "Application of the PSO– SVM Model for Recognition of Control Chart Patterns", ISA transactions, 49(4), (2010), 577–586.

12. Peddabachigari, S., Abraham, A., Grosan, C, and Thomas, J, "Modeling Intrusion Detection System Using Hybrid Intelligent Systems", Journal of network and computer applications, 30(1), (2007), 114–132.

13. Kausar, N., Samir, B. B, and Hussin,M, " Efficient Intrusion Detection system based on support vector machines using optimized kernel function. ", Journal of Theoretical and Applied Information Technology, 60(1), (2014), 55–63.

14. Wang, J., Li, T, and Ren, R. 2010b. A real Time IDS Based on Artificial Bee Colony-Support Vector Machine Algorithm. In The Third International Workshop on Advanced Computational Intelligence (IWACI). IEEE, 91–96.

15. Govindarajan, M, and Chandrasekaran, R, "Intrusion Detection Using Neural Based Hybrid Classification Methods", Computer networks, 55(8), (2011), 1662–1671.

16. Manekar, V, and Waghmare, K, " Intrusion Detection System using Support Vector Machine (SVM) and Particle Swarm Optimization (PSO ) ", International Journal of Advanced Computer Research, 4(3), (2014), 25–30.

17. Dastanpour, A., Ibrahim, S., Mashinchi, R, and Selamat, A, "Using Gravitational Search Algorithm to Support Artificial Neural Network in Intrusion Detection System", Smart CR, 4(6), 426–434.
Index Terms

Computer Science

Security

Keywords

Network Intrusion Detection, ensemble clusters, unlabeled data.