IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

Anomaly Detection in Network Traffic

Prof. Swathi N[1], Prof. Narendra N[2], Medha A[3]
Department of CSE, Nagarjuna College of Engineering & Technology, Bangalore, India[1,3]
Department of CSE, R. L. Jalappa Institute of Technology, Doddaballapur, Bangalore, India[2]

Abstract: *This abstract presents an anomaly detection system designed to address the growth of business networks and the optimization of cyberthreats. With the continuous development of the network infrastructure, has become the most important for ensuring the security and functioning of the computer network. The proposed system uses advanced machine learning techniques, including supervised and unsupervised learning algorithms, to accurately identify anomalies in the network in real time. The system analyzes various parameters such as packet size, protocol type, location and address , and time, using labeled data to form a basis for distinguishing network behavior. The unsupervised learning process was able to detect new and previously undetected anomaly, allowing the system to continually improve its detection capabilities over time. Additionally, the integration of anomaly detection with network monitoring tools provides real-time monitoring of network connectivity. When a suspicious anomaly is detected, the system immediately generates reports and sends a alert to network administrators, making it easier to detect and respond to threats. Detailed information from the system and images facilitate post-mortem analysis and network optimization. Evaluating the performance of an anomaly detection algorithm using large datasets of network traffic containing both normal and abnormal patterns. A comparison with existing methods for invisible detection shows the system's superiority in sensitivity, precision, reversibility, and anomaly. As a result, the vulnerability assessment method helps improve network security by providing effective and reliable solutions to identify and mitigate computer network security threats, and does a total of good jobs*

Keywords: Anomaly Detection, Network Traffic, Network Security, Machine Learning, Supervised Learning, Unsupervised Learning, Packet Size, Protocol Types Source and Destination Ad- dresses, Timestamps, Clustering, Analysis, Reporting, Real-Time Monitoring, Default Models, Performance Analysis

REFERENCES

[1] Patcha, A., Park, J. (2007). An overview of anomaly de- tection techniques: Existing solutions and latest technological trends. Computer Networks, 51(12), 3448-3470.
[2] Chandola, V., Banerjee, A., Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 15.
[3] Alazab, M., Venkatraman, S. (2017). Anomaly detection in network traffic: A behavioral approach. IEEE Communica- tions Surveys Tutorials, 19(2), 1322-1345.
[4] Mahoney, M. V., Chan, P. K. (2011). An analysis of the 1999 DARPA/Lincoln Laboratory evaluation data for network anomaly detection. ACM Transactions on Information and System Security (TISSEC), 14(4), 23.
[5] Ahmed, M., Mahmood, A. N., Hu, W., Yau, D. K. Y. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31.
[6] Goldberger, A. L., Amaral, L. A. N., Glass, L., Haus- dorff, J. M., Ivanov, P. C., Mark, R. G., ... Stanley, H. E. (2000). PhysioBank, PhysioToolkit, and PhysioNet: Compo- nents of a new research resource for complex physiologic signals. Circulation, 101(23), e215-e220.
[7] Buczak, A. L., Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys Tutorials, 18(2), 1153-1176.
[8] Hodge, V. J., Austin, J. (2004). A survey of outlier detection methodologies. Artificial Intelligence Review, 22(2), 85-126.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

[9] Wressnegger, C., Bay, S. D., Backes, M. (2018). Adversarial examples for generative models. arXiv preprint arXiv:1806.00035.
[10] Eskin, E. (2000). Anomaly detection over noisy data using learned probability distributions. In Proceedings of the SIAM International Conference on Data Mining (SDM), 2000, 1-15.