Design and implementation of a machine learning-based IDS model for detecting denial of service attacks on LAN infrastructure

Le Quang Hieu

Abstract: The research focuses on building a specialized Intrusion Detection System (IDS) to counter DDoS attacks in an internal network environment. The author experimented with machine learning algorithms such as Random Forest, SVM, and XGBoost on a real network traffic dataset to identify the model with the highest accuracy and the lowest false alarm rate. The system is capable of real-time traffic monitoring and automatically issuing alerts when detecting abnormal behaviors characteristic of DoS attacks.

Keywords: IDS, Machine Learning, DDoS, LAN

References

[1] L. Breiman, "Random Forests," Mach. Learn., vol. 45, no. 1, pp. 5–32, 2001.

[2] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," in Proc. 22nd ACM SIGKDD, 2016.

[3] M. Tavallaee et al., "A detailed analysis of the NSL-KDD data set," in Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl., 2009.

[4] V. Paxson, "Bro: A System for Detecting Network Intruders in Real-Time," Comput. Networks, 1999.