A Deep Learning Based Approach for Network Anomaly Detection System in IoT Environments

Lyna Touileb*[1], Kaouthar Zekri[2], Abbas Bradai[3], and Yannis Pousset[1]

[1]XLIM – Mathématiques, Informatique, Matériaux, Mécanique, Energétique de l'Université de Poitiers – France

[2]Sodira-connect – Sodira-connect – France

[3]Laboratoire d'Electronique, Antennes et Télécommunications – University Côte d'Azur – France

Résumé

Keywords: Network anomaly detection, protocols' headers, semi-supervised learning, LSTM, AutoEncoder, IoT.

In the rapidly evolving landscape of the Internet of Things (IoT), ensuring cybersecurity is paramount. This study introduces an innovative approach to anomaly detection in IoT networks using deep learning techniques. Specifically, we propose a hybrid model combining Long Short-Term Memory (LSTM) networks and autoencoders for robust anomaly detection in network traffic. By focusing on the analysis of protocol headers in Packet Capture (PCAP) datasets, our model demonstrates exceptional performance, achieving high F1-scores up to 99% , 80% for CICIDS2017, EdgeIIoT benchmarks datasets and 96% pour notre base de données privée in detecting anomalies. To further validate the efficacy of our model, deployment within our IoT environment is essential while maintaining its performance. To address this, we explore continual federated learning (CFL), enabling the deployment and training of multiple models in a continuous and distributed manner. However, this approach presents certain drawbacks. Thus, to overcome the challenges of continual learning and distributed data in IoT environments, we investigate the application of CFL. While our work on CFL is ongoing, we discuss its advantages, such as continuous adaptation to changing data in the network traffic, as well as potential drawbacks, including catastrophic forgetting (1) and non-IID data distribution (2). Moreover, we will explore the possible solutions to mitigate these challenges, including compression techniques to alleviate catastrophic forgetting and strategies for handling non-IID data. By integrating CFL into our anomaly detection system, we aim to enhance its scalability, adaptability, and privacy preservation capabilities, thereby advancing the security of IoT networks against evolving cyber threats.

(1) J. Peng et al. Nom Overcoming Long-Term Catastrophic Forgetting Through Adversarial Neural Pruning and Synaptic Consolidation Vol. 33 (2022), pp. 4243-4256.
(2) H. Wang, L. Muñoz-González, D. Eklund, S. Raza. Non-IID data re-balancing at IoT edge with peer-to-peer federated learning for anomaly detection. Association for Computing Machinery. In Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks. 153–163.

*Intervenant