Transfer Learning for IoT Network Anomaly Detection

Gregory Blanc, Houda Jmila, Mustafizur R. Shahid, Marwan Lazrag

Keywords — Intrusion Detection, Transfer Learning, Energy-efficiency, IoT

Context

IoT devices are expected to pervade every aspect of life and every industry sector, amounting to 75 billions of objects by 2030. However, they are often shipped with many vulnerabilities as time to market must be short to increase market shares. Hopefully, their behavior is often predictable making the detection of anomalous behaviors indicative of a compromission [1], with a high level of confidence. But this only works if the learnt behavior precedes the compromission. With the cooperation of the device vendor, it may be possible to learn the model of expected behavior of a device at the vendor's site and to apply this model at a customer's premise, avoiding any pollution to the model, and saving learning time. *Transfer Learning* [2] aims to extract the knowledge from one or more *source tasks* (resp. *source domains*) and applies the knowledge to a *target task* (resp. *target domain*). In our use case, the vendor's site represents one domain, and the customer's premises another. The task we are training is device identification and anomaly detection [3].

The internship aims at exploring transfer learning in the scope of the above-mentioned use case. Concretely, we have generated data for some IoT devices in different manners, one in a controlled, isolated way, and the other in a more natural way, involving daily interactions. The goal of the internship is to demonstrate the feasibility of learning device identification models (based on deep learning approaches [4]) and transfer them to test against other network settings.

Activities

1. Survey of transfer learning for anomaly detection
2. Design transfer learning protocol w.r.t. IoT use case
3. Implement prototype to process the available datasets
4. Evaluate the approach and its feasibility in terms of precision and recall, time and energy consumption.

Delivrables

- Report
- Prototype

References

[1] Mustafizur R Shahid, Gregory Blanc, Zonghua Zhang et Hervé Debar : Anomalous Communications Detection in IoT Networks Using Sparse Autoencoders. *In 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA)*, pages 1–5. IEEE, 2019.

[2] Sinno Jialin Pan et Qiang Yang : A Survey on Transfer Learning. *IEEE Transactions on Knowledge and Data Engineering*, 22(10):1345–1359, 2009.

[3] Jerone T.A. Andrews, Thomas Tanay, Edward J Morton et Lewis D Griffin : Transfer Representation-Learning for Anomaly Detection. 8, 2016.

[4] Raghavendra Chalapathy et Sanjay Chawla : Deep learning for anomaly detection: A survey. *arXiv preprint arXiv:1901.03407*, 2019.