Collaborative Anomaly Detection for Constrained Devices using Federated Learning

Gregory Blanc and Georgios Bouloukakis

Topics of interest — Federated Learning, Internet of Things, Anomaly Detection

Context

Next-generation networks will be characterized by a huge and increasing number of autonomous nodes with computational, communications and storage capabilities, e.g. Internet of Things (IoT). Furthermore, when sensors and actuators are involved, the IoT becomes an instance of the more general class of cyber-physical systems (CPS). Such systems extend the cyber attack surface into the physical world, with far reaching damages into the society (human casualties included) not only security-wise, but also in terms of safety and privacy. While mission-critical objects such as health devices cannot be halted, attacks against IoT devices usually seek to leverage what little capabilities they have to carry out larger-scale attacks within a botnet. More surreptitious attacks include eavesdropping on the physical environment or the other adjacent devices, and leaking out the collected information [4].

In order to prevent the massive exploitation of vulnerable IoT devices, the owners may deploy intrusion detection probes among other measures. The main advantage is to try to identify compromised devices and isolate them before malware propagates further. But such measure cannot be implemented in devices themselves as they are resource-constrained. IoT gateways could therefore be leveraged to protect a small network of devices. But with modern deep-learning-based anomaly detection approaches [2], this approach may also be costly for IoT gateways. Another issue depends on the dynamics of IoT devices that may often migrate from one network to another. This mobility makes detection model all the more unstable. Probes could then collaborate to circulate detection models for different devices, reducing the rate of false negatives that could lead to alert fatigue.

Federated Learning is such Machine Learning paradigm that has the potential to enable knowledge sharing [5] by aggregating local models from several participants, distributed among the different subnetworks [1]. It offers several other advantages including the ability to choose the clients involved in the aggregation process [3], sparing less resource-constrained devices from excess computing, or the fact that only model weights is exchanged, preventing unnecessary leakage of training data. In this project, we wish to demonstrate these properties for a real domestic IoT network.

Activities

1. State of the art:
    - study aggregation algorithms for Federated Learning,

    - compare aggregation algorithms in terms of knowledge sharing, resource consumption and privacy.

2. Formalization:
    - formalize knowledge sharing for selected aggregation approaches,
    - formalize aggregation requirements with respect to device mobility.

3. Experimentation:
    - design an experimental protocol, including relevant scenarios, for assessing knowledge sharing for IoT device anomaly detection,
    - evaluate the approach on a real testbed.

References

[1] E. M. Campos, P. F. Saura, A. González-Vidal, J. L. Hernández-Ramos, J. B. Bernabe, G. Baldini, and A. Skarmeta. Evaluating federated learning for intrusion detection in internet of things: Review and challenges. *Computer Networks*, 203:108661, 2022.

[2] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki. Network intrusion detection for iot security based on learning techniques. *IEEE Communications Surveys & Tutorials*, 21(3):2671–2701, 2019.

[3] L. Fu, H. Zhang, G. Gao, M. Zhang, and X. Liu. Client selection in federated learning: Principles, challenges, and opportunities. *IEEE Internet of Things Journal*, 2023.

[4] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani. Demystifying iot security: An exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations. *IEEE Communications Surveys & Tutorials*, 21(3):2702–2733, 2019.

[5] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. V. Poor. Federated learning for internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 23(3):1622–1658, 2021.