IoT が拓く未来　　2022 年度
2021 年度採択研究代表者　　年次報告書

白川 真一

横浜国立大学 大学院環境情報研究院
准教授

IoT セキュリティのための機械学習の自動カスタマイズ技術

研究成果の概要

本研究では、複数の IoT 機器のデータ連携によって、各 IoT 機器で実行される機械学習モデルを効率的に自動カスタマイズする技術を確立し、IoT におけるサイバー攻撃検知システムの検知性能や学習効率を向上させることを目指している。本年度は、マルウェアの悪性通信や IoT 機器の正常通信のデータの収集・整備を進め、悪性通信の検知モデルの構築を行った。特に、異なる環境で収集された IoT 機器の通信データセットを、ターゲットとなる環境での検知モデルの学習に有効に活用する方法を開発した。まず、実用上はターゲット環境のデータに対するラベル（悪性/正常の情報）を得ることが困難であることから、Positive-Unlabeled Learning を利用して、事前に収集できるマルウェアの悪性通信のデータとラベルなしのターゲット環境のデータだけからモデルの学習を行う方法を開発した。

さらに、事前に収集したデータセットの中にはターゲット環境とは性質の異なるデータが存在することに対処するため、ターゲット環境のデータ分布を学習し、利用できる悪性通信データの中からターゲット環境のデータに近いものを選択的に利用する方法を開発した。開発手法を実験的に評価したところ、データを選択的に用いることで、検出性能が向上することを確認した。

また、機械学習モデルの構造を IoT デバイスに合わせてカスタマイズする方式の開発にも着手した。モデルをエッジデバイスとクラウド側に分割配置し推論を行う Split Inference 向けの構造探索手法を開発し、推論時間の制約を満たす分割位置や構造が獲得できることを実験的に示した。これらに加え、モデル構造等の自動化カスタマイズのための最適化手法の効率化に関する研究も推進した。

【代表的な原著論文情報】

1) R. Hamano, S. Saito, M. Nomura, and S. Shirakawa, “CMA-ES with Margin: Lower-Bounding Marginal Probability for Mixed-Integer Black-Box Optimization,” Genetic and Evolutionary Computation Conference (GECCO), pp. 639-647, 2022.
2) Y. Noda, S. Saito, and S. Shirakawa, “Efficient Search of Multiple Neural Architectures with Different Complexities via Importance Sampling,” 31st International Conference on Artificial Neural Networks (ICANN 2022), Part IV, Vol. 13532 of LNCS, pp. 607–619, 2022.
3) T. Yamaguchi, K. Uchida, and S. Shirakawa, “Improvement of sep-CMA-ES for Optimization of High-Dimensional Functions with Low Effective Dimensionality,” 2022 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 1659-1668, 2022.
4) S. Shimizu, T. Nishio, S. Saito, Y. Hirose, C. Yen-Hsiu, and S. Shirakawa, “Neural Architecture Search for Improving Latency-Accuracy Trade-off in Split Computing,” 2022 IEEE Globecom Workshops, Edge Learning over 5G Mobile Networks and Beyond, pp. 1864-1870, 2022.