MAD: A Meta-Learning Approach to Detect Advanced Persistent Threats using Provenance Data in Industrial IoT

Bikash Saha
bikash@cse.iitk.ac.in
Dept. of Computer Science and Engineering
Indian Institute of Technology Kanpur, India

***Abstract*—The increasing reliance on Industrial Internet of Things (IIoT) systems in critical infrastructure has made the IIoT environments prime targets for stealthy and prolonged Advanced Persistent Threats (APTs) to perform attacks. The APT attackers are professional to evade traditional security systems. This study introduces our framework named MAD (Meta-learning based APT Detection), which is designed to detect APTs in IIoT environments by leveraging provenance data. This data provides a detailed view of system-level interactions and captures the skillful and persistent malicious behaviors. We evaluate MAD on the CICAPT-IIoT dataset, which simulates real-world APT scenarios with severe class imbalance due to the "low and slow" nature of APT attacks. Our MAD framework includes two variants: MAD v1, and MAD v2. Mad v1 utilizes a multi-layer perception (MLP), and MAD v2 utilizes Model-Agnostic Meta-Learning (MAML) to detect and improve the detection rate of APT-related attacks, respectively. The proposed MAD v1 achieves F1-score of 0.91 and outperforms the existing baselines. Whereas MAD v2 achieves F1-score of 0.95 and surpasses the existing baseline as well as MAD v1. This demonstrates MAD v2's enhanced capability to detect the "low and slow" nature APT activities despite the dominance of benign samples. In this work, we combine provenance-based detection with meta-learning to address class imbalance and enhance APT detection in IIoT which demonstrate MAD's potential in handling the emerging security challenges in IIoT environments.**

***Index Terms*—Advanced Persistent Threat (APT), Industrial Internet of Things (IIoT), Provenance Data, Threat Detection in IIoT, Binary Attack Detection, Cybersecurity in IIoT**

This paper was produced by the IEEE Publication Technology Group. They are in Piscataway, NJ.
Manuscript received April 19, 2021; revised August 16, 2021.