Optimised Learning Models for Defending Against Cyber Attacks in Cyber-Physical Systems

Waleed Yamany

Supervisors

Dr. Nour Moustafa Assoc/Prof. Benjamin Turnbull

Dr. Marwa Keshk

A thesis submitted in fulfilment of the requirements for

the degree of Doctor of Philosophy

UNSW

AUSTRALIA

School of Engineering and Information

Technology The University of New South Wales

Australia, December 2023

Abstract

This research thesis focuses on the security of Cyber-Physical Systems (CPS) in critical infrastructure. With the increasing use of CPS, security has become a crucial challenge. It is essential to study the vulnerabilities of CPS components under malicious attacks. The main objective of this thesis is to provide a comprehensive understanding of the vulner- abilities of CPS and develop a defence framework using deep learning and optimisation methods to defend against cyber-attacks in CPS, specifically in smart networks such as power systems and transportation systems. This significant challenge is divided into three sub-challenges: identifying coordinating attacks and their behaviours in CPS, investigat- ing the impact of optimising the deep learning-based defence model in adversarial settings, and determining malicious activities in decentralised CPS and optimising the weights of Federated Learning-based defence models.

To address these challenges, this research proposes a novel defence framework using deep learning and optimisation methods to examine and identify the vulnerabilities of CPS, when under cyber-attack. This framework includes three main contributions. The first contribution is the development of an efficient tri-level programming model that deter- mines attacking scenarios, along with the best defensive actions in smart power systems. The second contribution is the design of a new decentralised technique for protecting the confidential information of CPS and defending against malicious observations. This is achieved by using a quantum-behaved particle swarm optimisation technique to automat- ically adjust the hyperparameters of Federated Learning in Autonomous Vehicles. The third contribution is the development of a novel personalised swarm optimisation-based Federated Learning model for achieving the security criteria of heterogeneous decentralised CPS.

To validate the effectiveness of the proposed framework, extensive simulated experiments have been conducted on various data poisoning attacks in various scenarios. The results of these experiments reveal the effectiveness of the proposed framework compared to peer methods.