PETRAS – Sectors – Supply Chains and Control Systems, Infrastructure

Power-SPRINT: Power Grid IoT System Protection and Resilience using Intelligent Edge

Dr. Subhash Lakshminarayana

Prof. Carsten Maple

Dr. Hamidreza Jahangir

University of Warwick

INTRODUCTION

Power-SPRINT investigates the cybersecurity risks posed by the growing integration of IoT- enabled high-wattage smart-home appliances (e.g., WiFi-enabled air-conditoners, electic vehicles, etc.) on power grid operations.

AIM

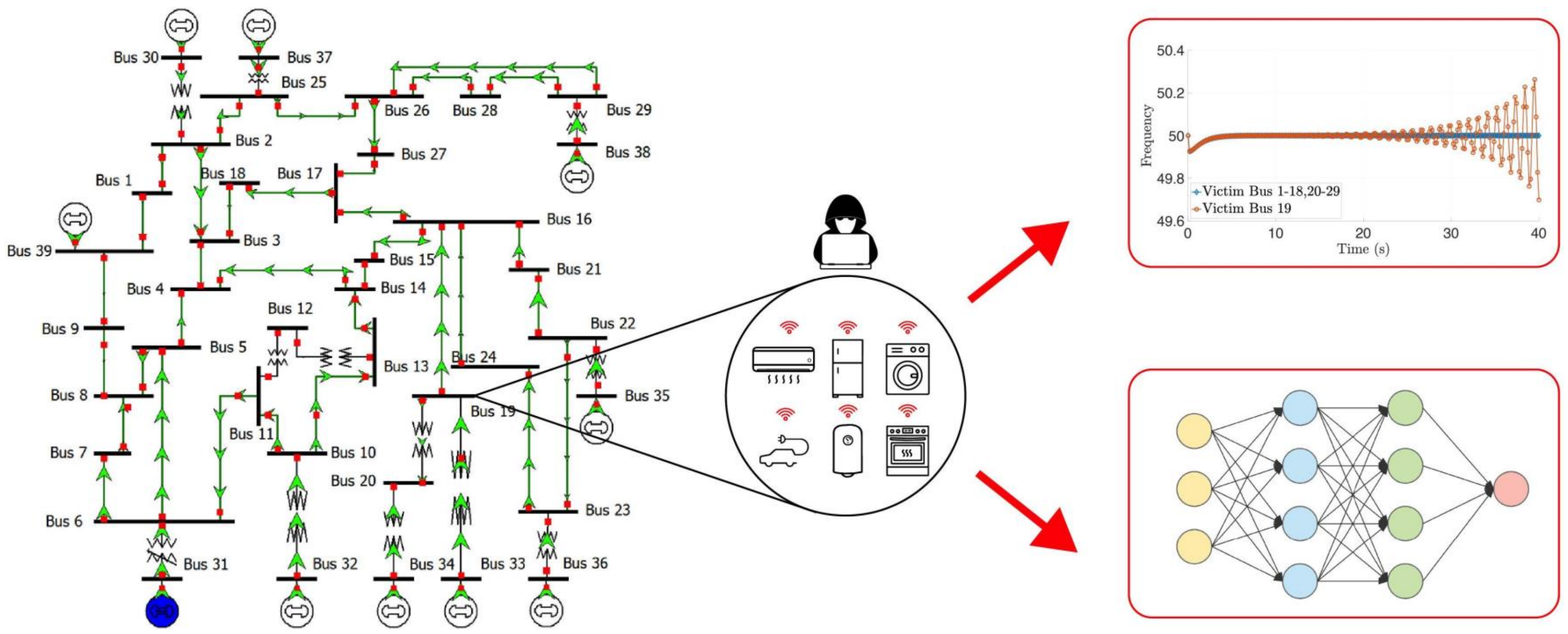
- Perform a systematic risk analysis of large-scale IoT-enabled load altering attacks against power grids
- Develop an intrusion detection system to detect IoT-enabled load altering attacks.

WHY

- IoT-enabled smart-home appliances are often poorly engineered from a security point of view. They may become convenient entry points for malicious parties to gain access to the system and disrupt important grid operations by abruptly changing the demand.
- Unlike utility-side and SCADA assets, these devices cannot be monitored continuously due to their large numbers.

Objectives

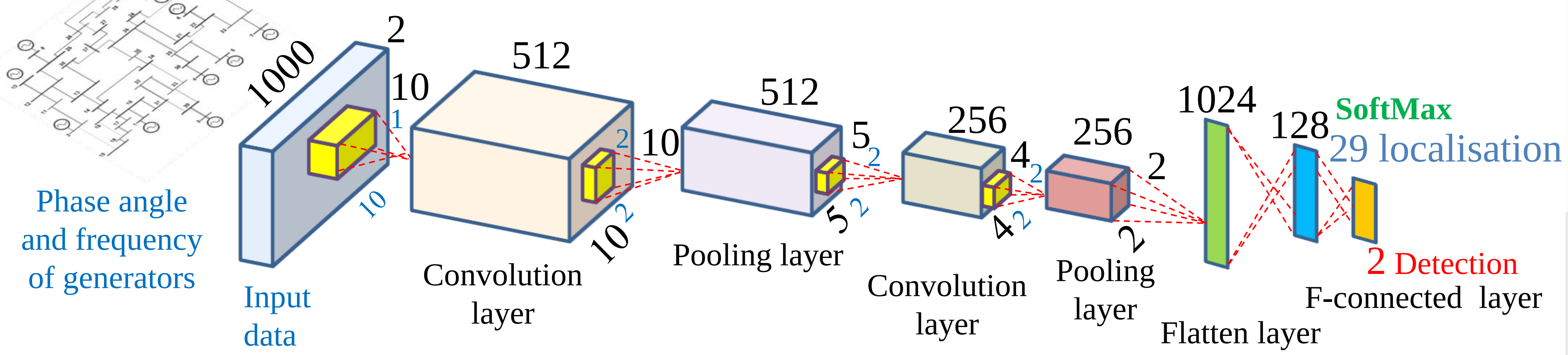
- Conducting a comprehensive risk assessment of large-scale Internet-of-Things-enabled load-switching attacks against power grids
- Designing a data-driven detection system based on artificial intelligence techniques detecting upcoming IoT-enabled load-altering threats.

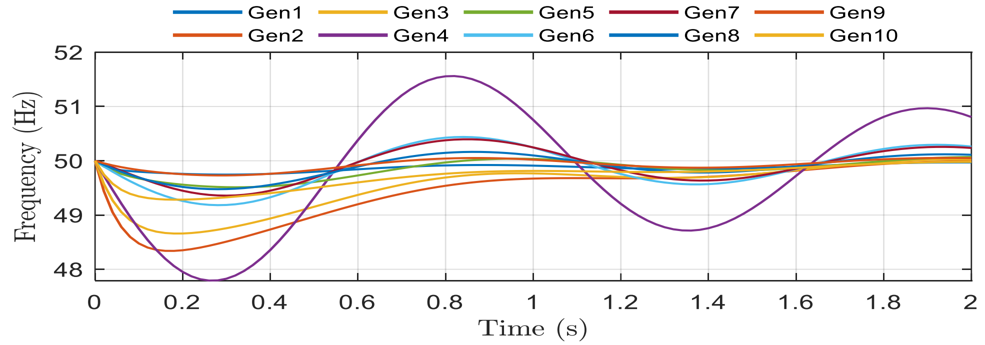


Control-theoretic Impact Analysis

Machine learning based Attack detection and Edge Intelligence

What happens if a large-scale Botnet-type attack targets IoT-enabled high-wattage home appliances?
What impact will it have on the power grid?





HOW /METHODOLOGY

- A cyber-physical approach by analysing the network attack data from IoT-home appliances gathered using a honeypot deployed in the wild and control-theoretic attack impact analysis.
- Real-time analysis of the power grid's physical signals monitored using smart meters (e.g., load consumption, voltage, frequency, etc.).

USER PARTNERS

- Schneider Electric, UK
- Global Cyber Alliance

PUBLICATIONS

- S. Lakshminarayana, S. Adhikari, and C. Maple, "Analysis of IoT-Enabled Load-Altering Attacks Using the Theory of Second-Order Systems," IEEE Transactions on Smart Grid, 2021
- S. Lakshminarayana, S. Sthapit, Hamidreza Jahangir, and C. Maple, "Data-Driven Detection and Identification of IoT-Enabled Load-Altering Attacks in Power Grids", IET Smart Grid Journal, 2022.

REFERENCE

S. Soltan, P. Mittal, and H. V. Poor, “BlackIoT: IoT botnet of highwattage devices can disrupt the power grid,” inProc. USENIX SecuritySymposium, Baltimore, MD, Aug. 2018, pp. 15–32

UK Research and Innovation

WARWICK
THE UNIVERSITY OF WARWICK