Hardware Security Analyses in Advanced Manufacturing Industry

Qiaoyan Yu
Department of Electrical and Computer Engineering
University of New Hampshire
• Advanced manufacturing is the use of innovative technology to improve products or processes, with the relevant technology being described as **advanced, innovative, and cutting edge**
Hardware Security Threats from Supply Chain of Advanced Manufacturing Industry (AMI)

Supply Collection
- Raw materials
- Unfinished components
- Replacement parts

Setup Assembly
- Initial machine setup
- Obsolete device replacement
- Machine upgrade

Customized Configuration
- Special manufacturing request
- Configuration setting revision

Operation Maintenance
- Operation condition sensing
- Behavioral anomaly detection
- Yield rate prediction

Hardware Attacks:
- Untrusted 4th/5th parties
- Backdoor in discrete components
- Inequivalent replacement
- Mismatch interface
- Imperfect communication protocols
- System design bugs
- Configuration setting spoofing
- Configuration setting tampering
- Hijacking reconfiguration
- Tamper with real-time sensing readings
- Mute anomaly alerts
- Sabotage system feedback loops
Hardware Security in LoRa-based Monitoring System

- **LoRa Gateway**
  - LoRa Node
  - LoRa Node
  - LoRa Node
  - Malicious LoRa Node

- **LoRaWAN Server**

- **Physical attacks on LoRa node devices**

- **Jamming, replay attack**

- **Sensor & LoRa transmitter**

- **LoRa packet tracking system**

- **LoRa receiver**

- **Control console for Ford RAFFT Machine**

- **RAK7244**

- **SparkFun ICM-20948**

- **Arduino MKR Wan 1300**

- **SPI channel**
Hardware Trojan in LoRa Nodes

- Hardware Trojan changes the LoRa transmission
  - Cause packet drop by re-sending the previous value
  - Inject dummy data to jam the transmission link

M. Monuir and Q. Yu, GLSVLSI’22
Security Vulnerability of Hardware Components in AMI
• As more network connectivity is enabled in advanced manufacturing, the security of hardware deployed to manufacturing should be re-examined.
• More demonstration of practical attack cases will be helpful to refine the AMI-specific attack models.
• We suggest new investigation to study the impact of environmental noise in advanced manufacturing on the efficiency of existing attack detection and mitigation methods.
Thank you!
Q&A