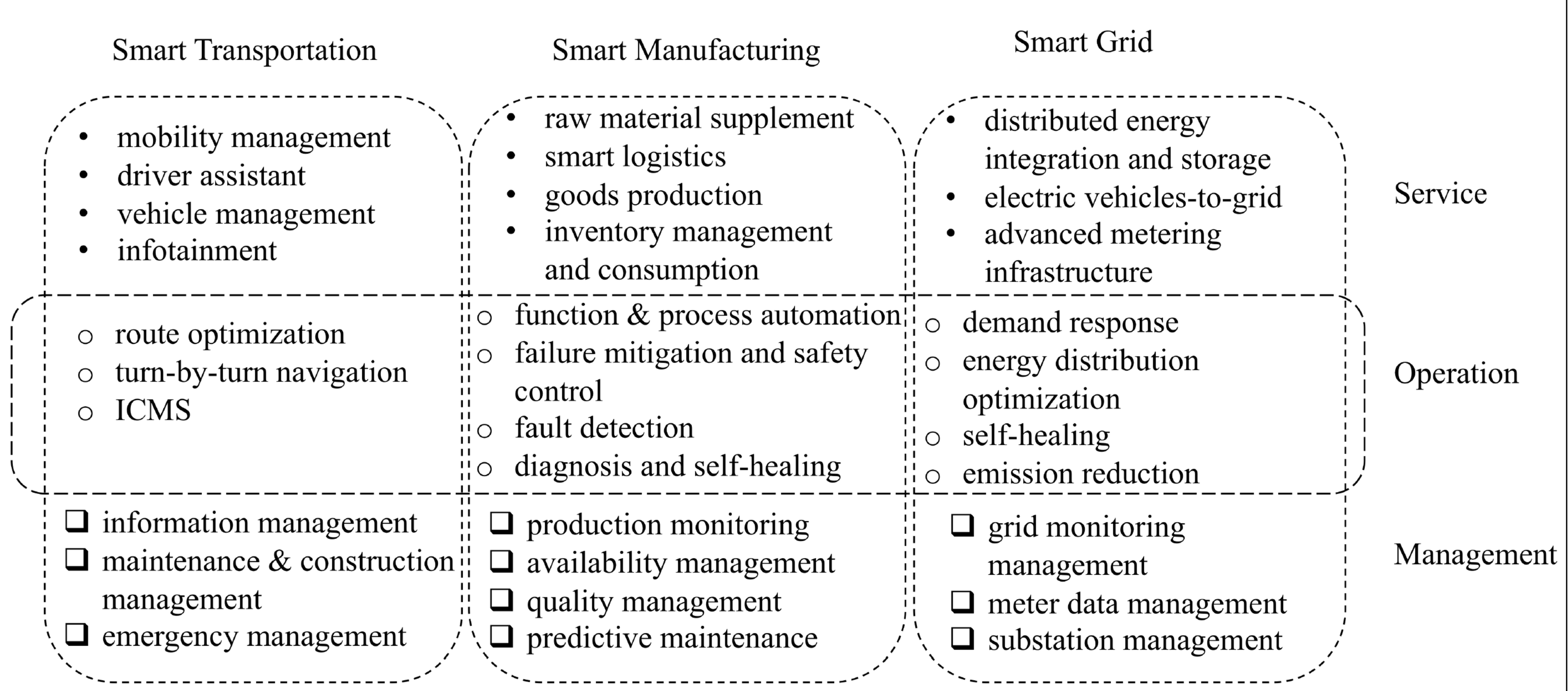
Secure Internet of Things (IoT)-based Smart-World Critical Infrastructures

Xing Liu, Cheng Qian, William Grant Hatcher, Fan Liang, Weixian Liao and Wei Yu
Cyber Physical Networked System and Security Research Laboratory
Department of Computer and Information Sciences, Towson University
Web: http://wp.towson.edu/wyu Email: wyu@towson.edu

Overview

- The number of connected Internet of Things (IoT) devices is increasing significantly
- IoT security and susceptibility to intrusion reach all aspects of society, implicating all domains of cyber-physical systems (CPS) and smart-world systems



Research Focus

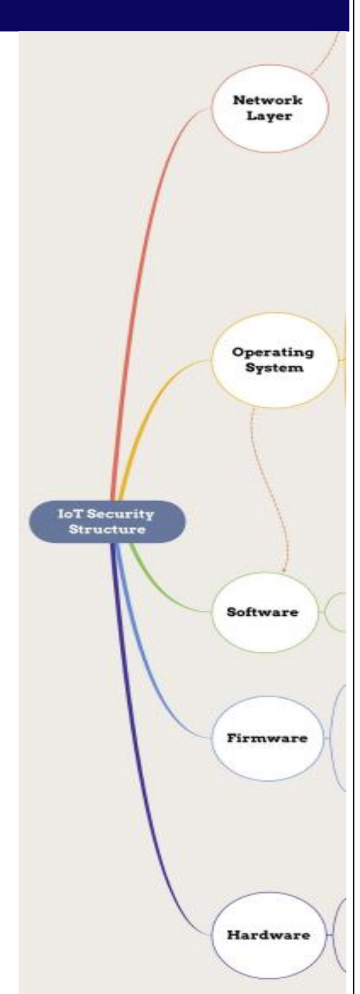
- Systematic exploration of the attack space against IoT systems
- Investigation of the risk of those attacks on critical smart infrastructure systems
- Development of countermeasures for mitigation

Our Contributions

- Investigate vulnerabilities of IoT systems from the perspectives of network layer, operating system, software, firmware, and hardware
- Develop a three-layer architecture to study the key IoT systems, such as smart grid, smart transportation, and smart manufacturing
- Study the impact of both individual small-scale and combinatorial large-scale attacks on disrupting service, operation and management of key IoT system
- Outline countermeasures to protect IoT systems from cyber-attacks via a three-phase framework

Vulnerabilities in IoT

- Network Layer
  - The attack surfaces include networking service, web interface, cloud interface, privacy interface, network traffic, and others
- Operating System (OS)
  - The attack surfaces include the users/administrator interface, system update, and others
- Software
  - The attack surfaces include third-party backend APIs, vendor backend APIs, and others
- Firmware
  - The attack surfaces include update, configuration, firmware package, and others
- Hardware
  - The attack surfaces include the hardware (sensors and actuators), physical interface, and others



A Taxonomy of Cyber-attacks on IoT Systems

- Attacks in management layer: management layer includes massive IoT devices that collect IoT data

Attacks in management layer	IoT systems
Node capture	Compromise perception devices, such as smart meters, sensors, etc.
Malicious code injection	Inject malicious code to IoT devices to perform illegitimate activities
False data injection	Inject false data to perform illegitimate activities
Replay attacks	Grant trust to malicious perception devices
Cryptanalysis and side channel	Leverage side channel information to disrupt authentication functions
Eavesdropping and interference	Eavesdrop on sensitive data and quality disruption
Sleep deprivation attacks	Disrupt the sleep cycle to modify control logics

- Attacks in operation layer: operation layer includes control, computing and networking

Attacks in operation layer	
DoS attacks	Make IoT system resources unavailable to legitimate requests
Spoofing attacks	Adversaries use malicious devices to affect authentication functions
Sinkhole attacks	Adversaries can steal sensitive and valuable data
MITM attacks	Adversaries collect and alter legitimate data via malicious devices
Routing information attacks	Disrupting the timely delivery of data via route loops
Sybil attacks	Malicious devices claim legitimate identities to cause jamming or DoS
Unauthorized access	Adversaries gain unauthorized access to legitimate devices

- Attacks in service layer: service layer includes IoT applications.

Attacks in service layer	IoT systems
Phishing attacks	Adversaries can obtain confidential data from IoT applications
Malicious virus/worms	Infected devices perform illegitimate function to harm IoT systems
Malicious scripts	Adversaries can run malicious scripts in service layer to execute illegitimate functions

Case Study

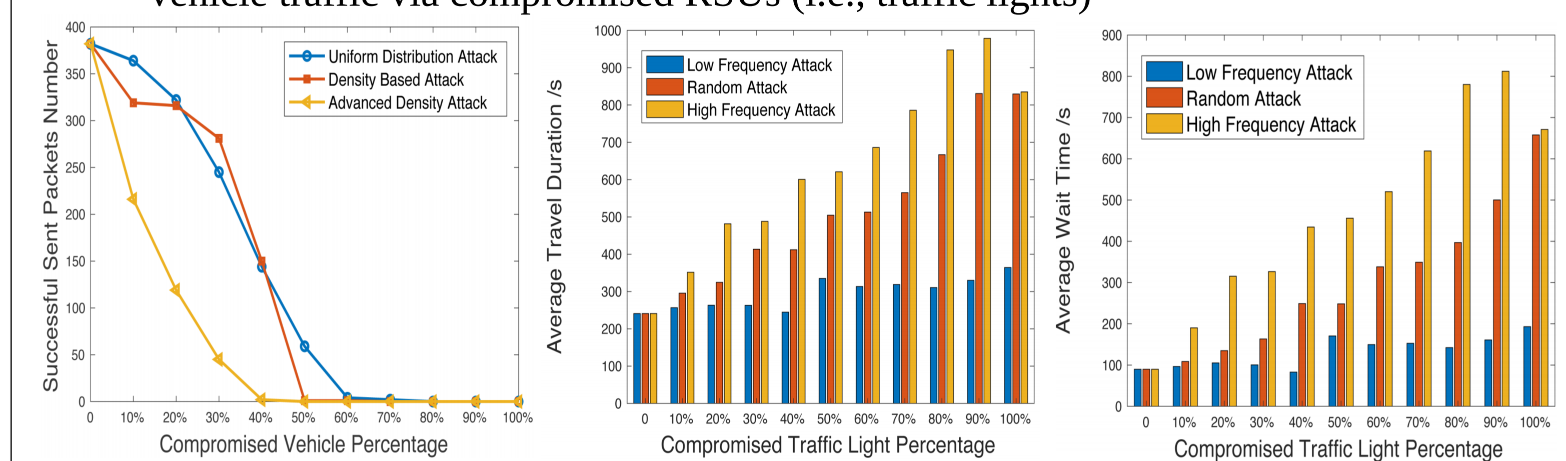
- Investigating cyber-attacks on the smart transportation system
  - Scenarios
    - Attack on the vehicular network in the smart transportation system via compromised OBUs
    - Attack on the vehicle traffic in the smart transportation system via compromised RSUs (i.e., traffic lights)
    - Combined attack on the vehicular network and vehicle traffic in the smart transportation system via compromised OBUs and RSUs

  - Experiment Setup
    - Vehicle motion is generated by SUMO
    - Communication is simulated by OMNET++
    - Real-world road topology is shown in the figure on the top
    - Simulation parameters are shown in the table on the bottom

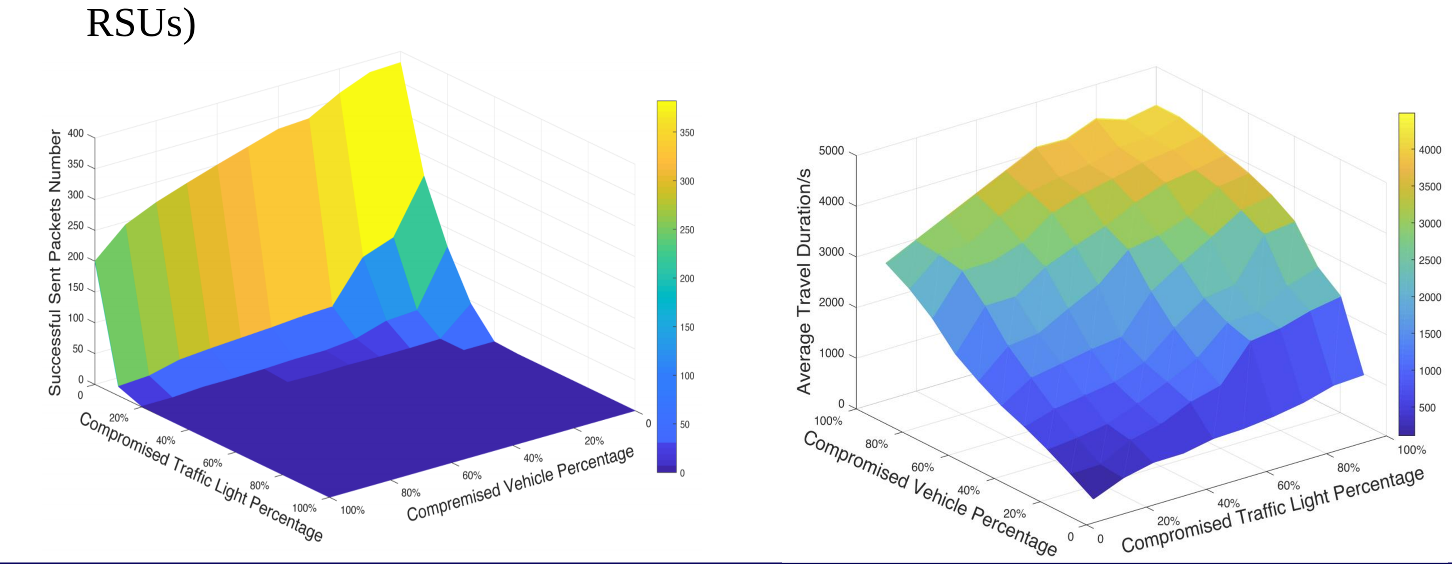
Attacks Targets	Definition
Simulation Area	5000 x 3100 m^2
Simulation Time (Each Trial)	5000 s
Number of Trials	120
Number of Vehicles	200
Network Protocol	802.11p
Number of Traffic Lights	300
Attack Strategies	Low frequency, Random frequency, High frequency
Network Interface	OMNET++
Vehicular Network Simulation Framework	Veins
Traffic Simulator	SUMO
Map	Towson University

Evaluation Results

- Attack on the vehicular network in the smart transportation system via compromised OBUs
  - In the figure on the left, we compare the network performance of three attack strategies (i.e., uniform distribution attack, density-based attack, and advanced density-based attack)
- Attack on the vehicle traffic in the smart transportation system via compromised RSUs
  - In the figure on the middle, we compare the average travel duration during attacks on vehicle traffic via compromised RSUs (i.e., traffic lights)
  - In the figure on the right, we compare the average wait time during attacks on vehicle traffic via compromised RSUs (i.e., traffic lights)



- Attack on the vehicular network and vehicle traffic in the smart transportation system via compromised OBUs and RSUs
  - In the figure on the bottom left, we show the network performance of smart transportation under combined attack strategy (i.e., manipulating both OBUs and RSUs)
  - In the figure on the bottom right, we show the vehicle traffic performance of smart transportation under combined attack strategy (i.e., manipulating both OBUs and RSUs)



Ongoing Research

- Risks of Cyber-attacks
  - Investigate the vulnerabilities (e.g., software vulnerabilities, communication vulnerabilities, side-channel vulnerabilities) of different IoT-based systems
  - Investigate the potential impact of vulnerabilities on functionalities and performance of the IoT-based system
  - Model and analyze the impact of attacks that consider various combinations of factors (attack parameters, strategies, etc.) in time, space, and strength
- Defensive Schemes
  - Defensive schemes include the design of resilient IoT-based systems, the investigation of optimal IoT-based system configurations, the detection of cyber-attacks by identifying key features, and the response to cyber-attacks in a timely manner
- Integrated Evaluation Platforms
  - Develop system-level modeling and simulation tools to study the interactions between physical components (power grid, transportation system, etc.) and cyber components (communication networks and computing infrastructure)

2021 NSF Cyber-Physical Systems Principal Investigators' Meeting June 2-4, 2021
Award ID#: CNS-1350145