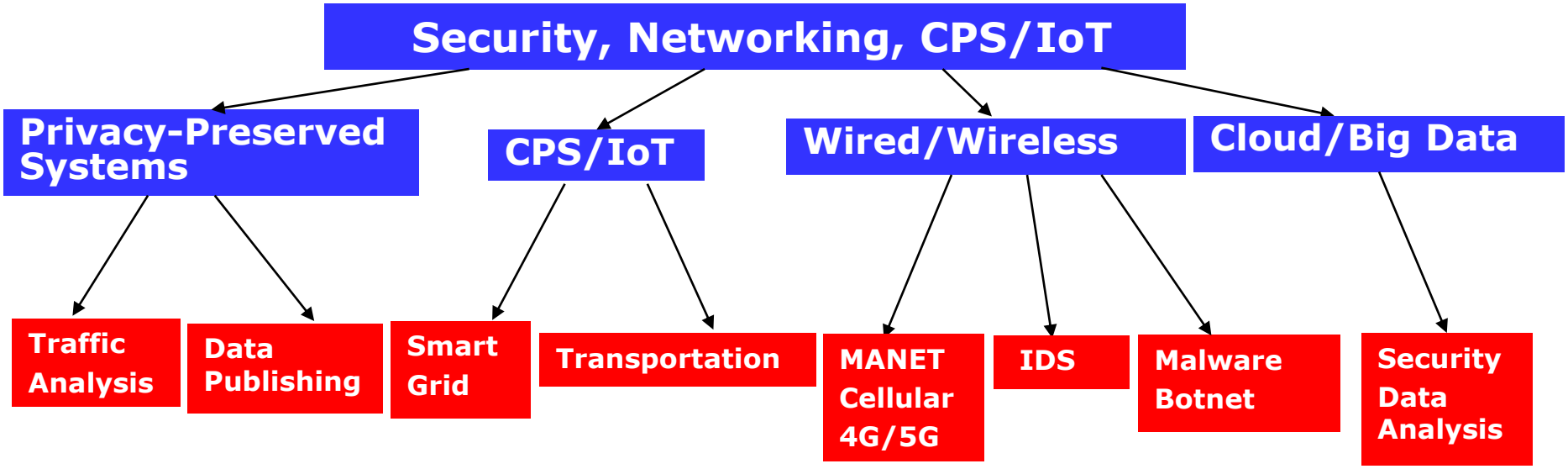
Research Overview

Dr. Wei Yu
Associate Professor
Dept. of Computer and Information Sciences
Towson University
Email: wyu@towson.edu

Research Roadmap

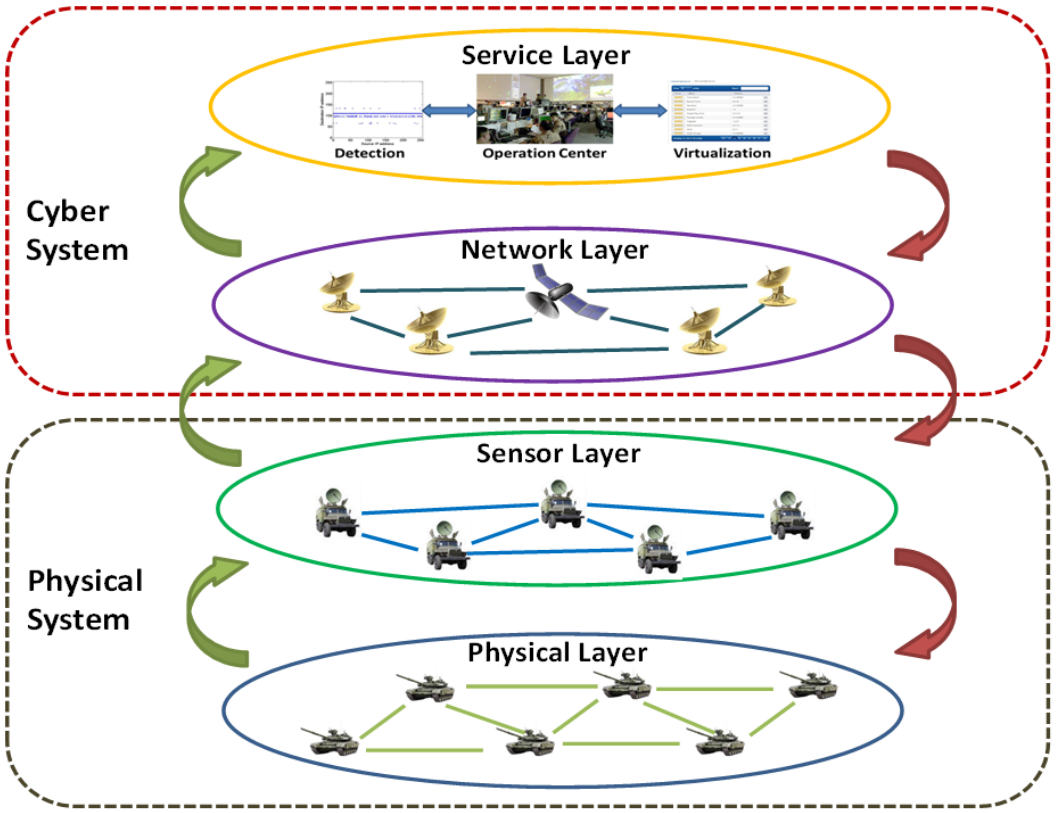


Research Projects

- **CPS/IoT/Next Generation Wireless Networks**
- **Mobile and MANET Security**
- **Network Threat Monitoring and Detection**
- **Privacy and Anonymized Systems**

CPS/IoT Systems

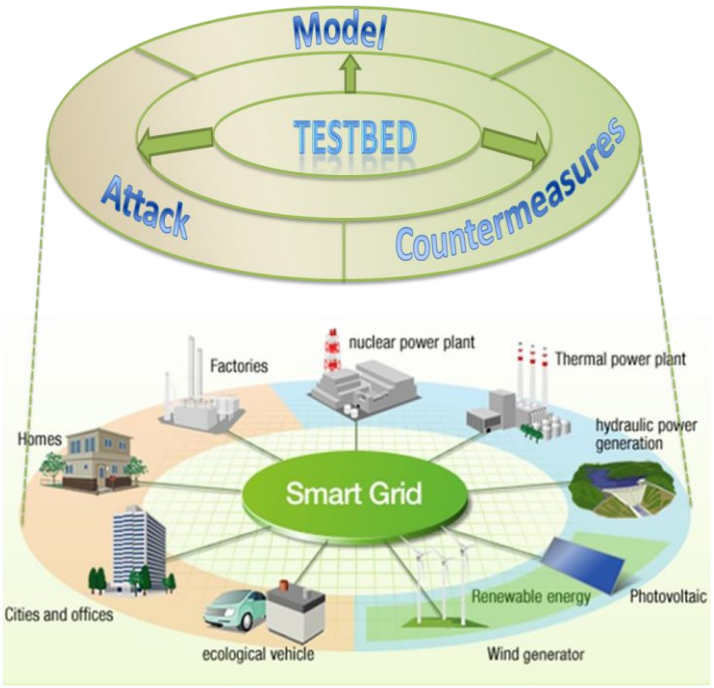
- Integrates modern information and communication technologies
- Efficient, reliable, secure, and resilient



CPS/IoT System Layer Structure

Research Focus

- **Goal**
  - Establish a theoretical and empirical basis for securing energy-based infrastructure
- **Contributions**
  - Develop modeling and co-simulation frameworks for designing efficient energy CPS/IoT systems
  - Conduct a systematical study of exploring attack space and countermeasures
  - Develop toolset for CPS/IoT research and development

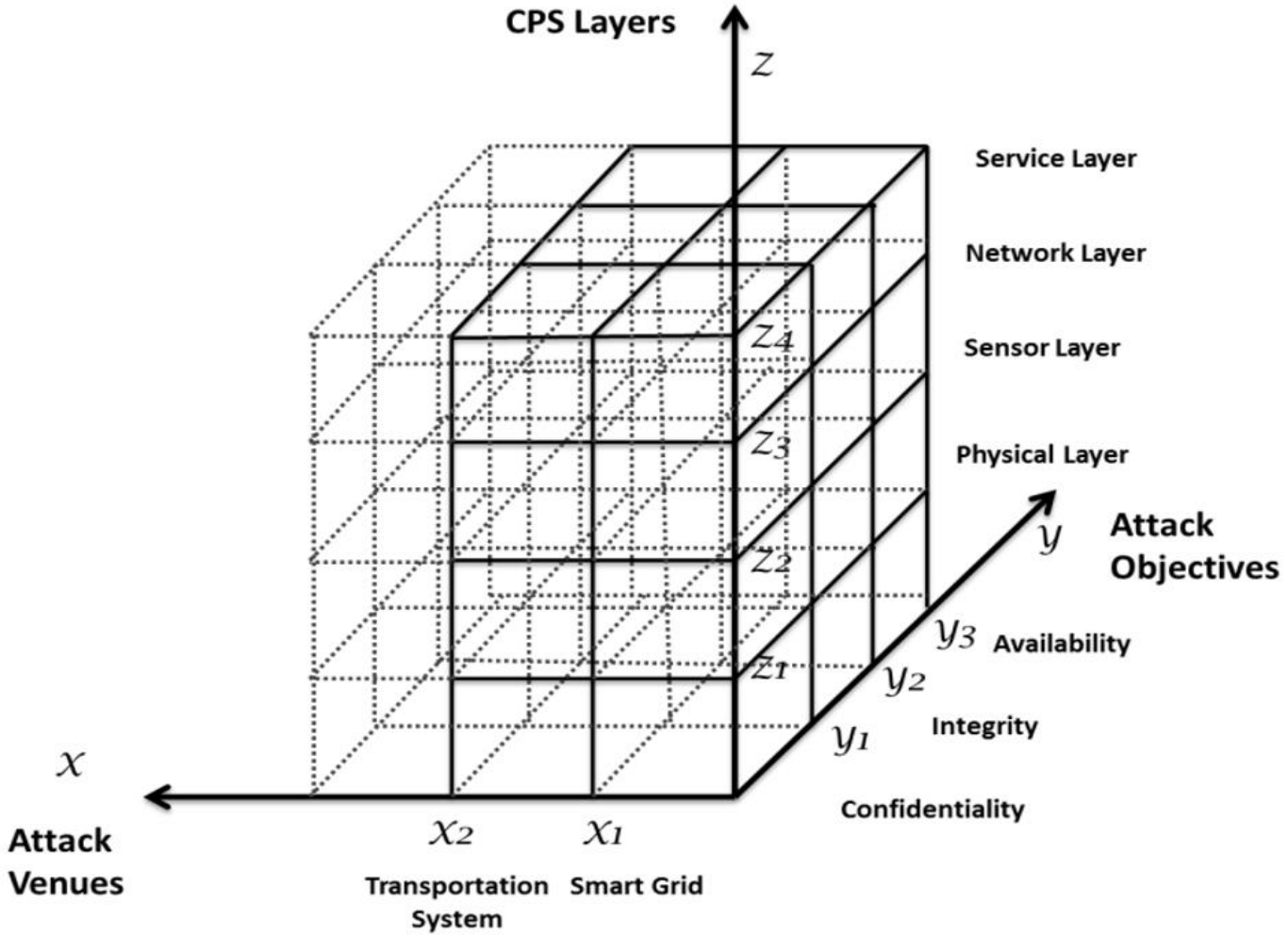


Methodology

Example: Cyber Attacks on Energy-Based CPS/IoT Systems

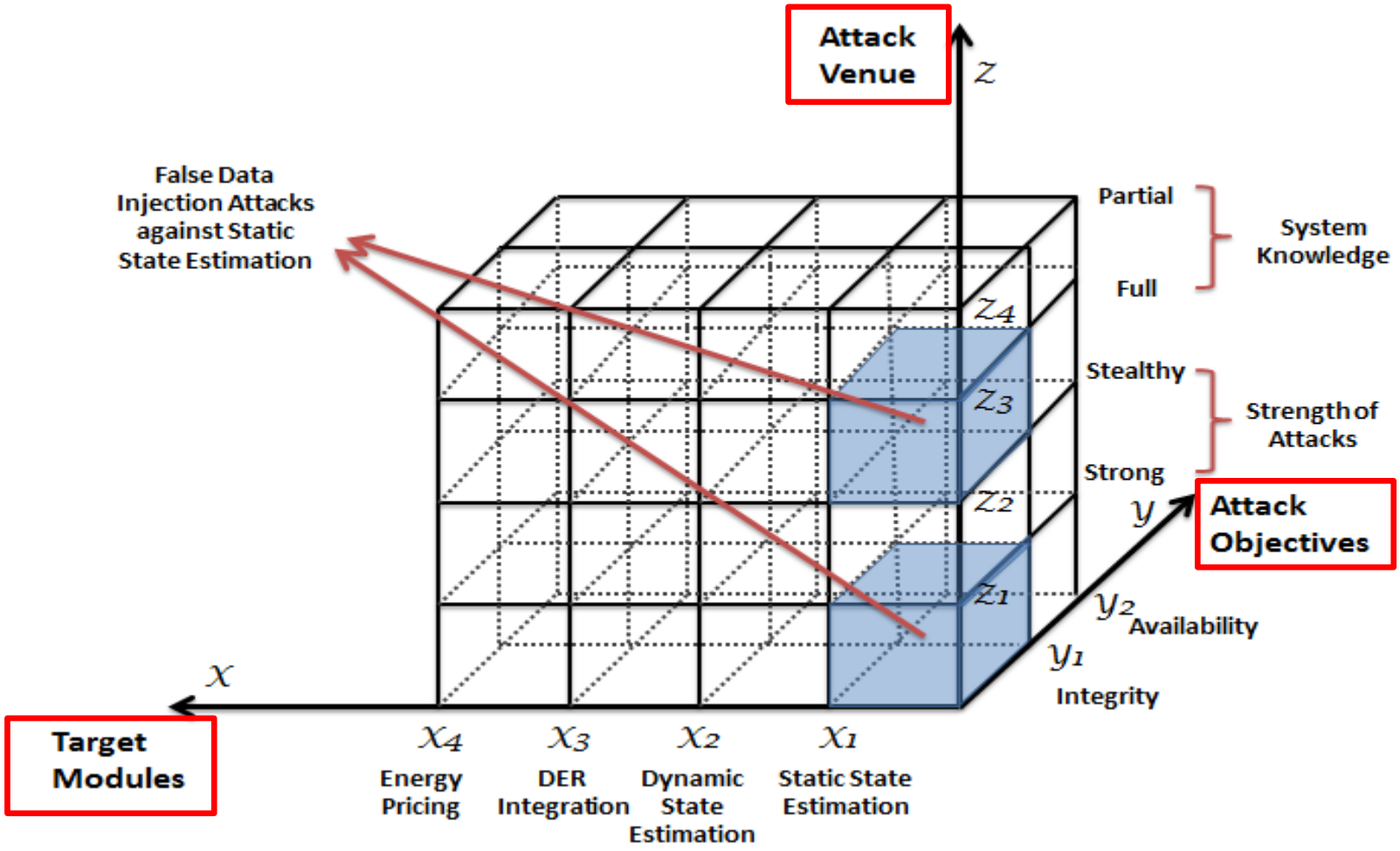
- **Real World Examples**
  - In 2008, *computer intrusions* in European power utilities
  - In 2010, *Stuxnet* worm provides a blueprint for aggressive attacks on control systems
  - In 2011, malware *BlackEnergy* disrupts processes controlled HMIs products from vendors, e.g., General Electric, Siemens, Advantech
  - In 2014, a remote access Trojan program called *Havex* was used to hack into the websites of industrial control system and SCADA manufacturers and poisoning legitimate software downloads
  - In 2014, TrustedSec discovered *Spy malware* in the software that a major U.S. energy provider uses to operate dozens of turbines, controllers and other industrial equipment
  - In 2013 and 2014, there were **224** hacking incidents at energy companies investigated by the Computer Emergency Readiness Team, a division of the Department of Homeland Security (DHS)
  - Between April 2013 and 2014, hackers managed to break into **37%** of energy companies, according to a survey by ThreatTrack Security
  - …

A Framework for Exploring Threats in CPS/IoT Systems



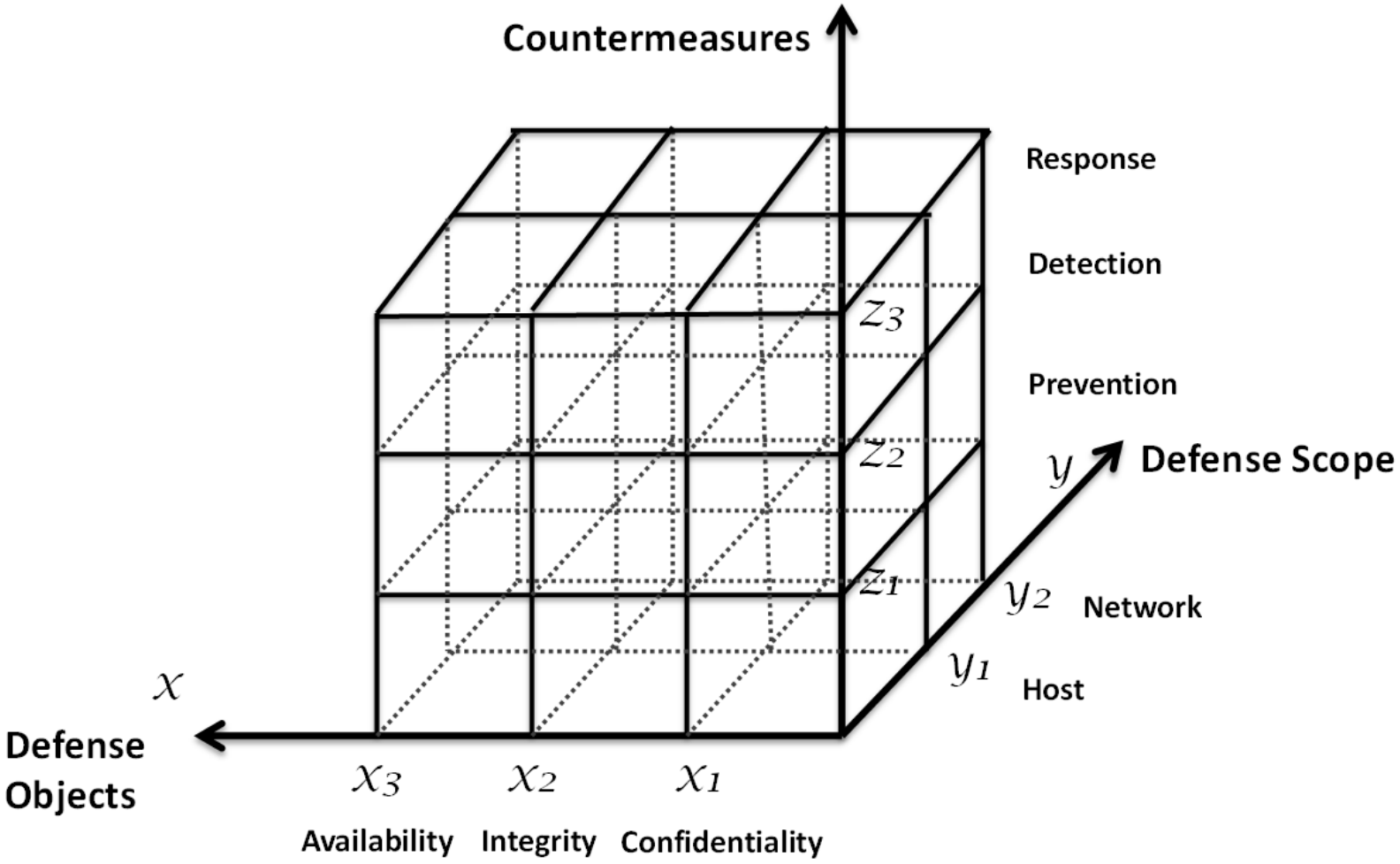
Framework for Exploring Threats

Example: Exploring Threats in Energy CPS/IoT Systems



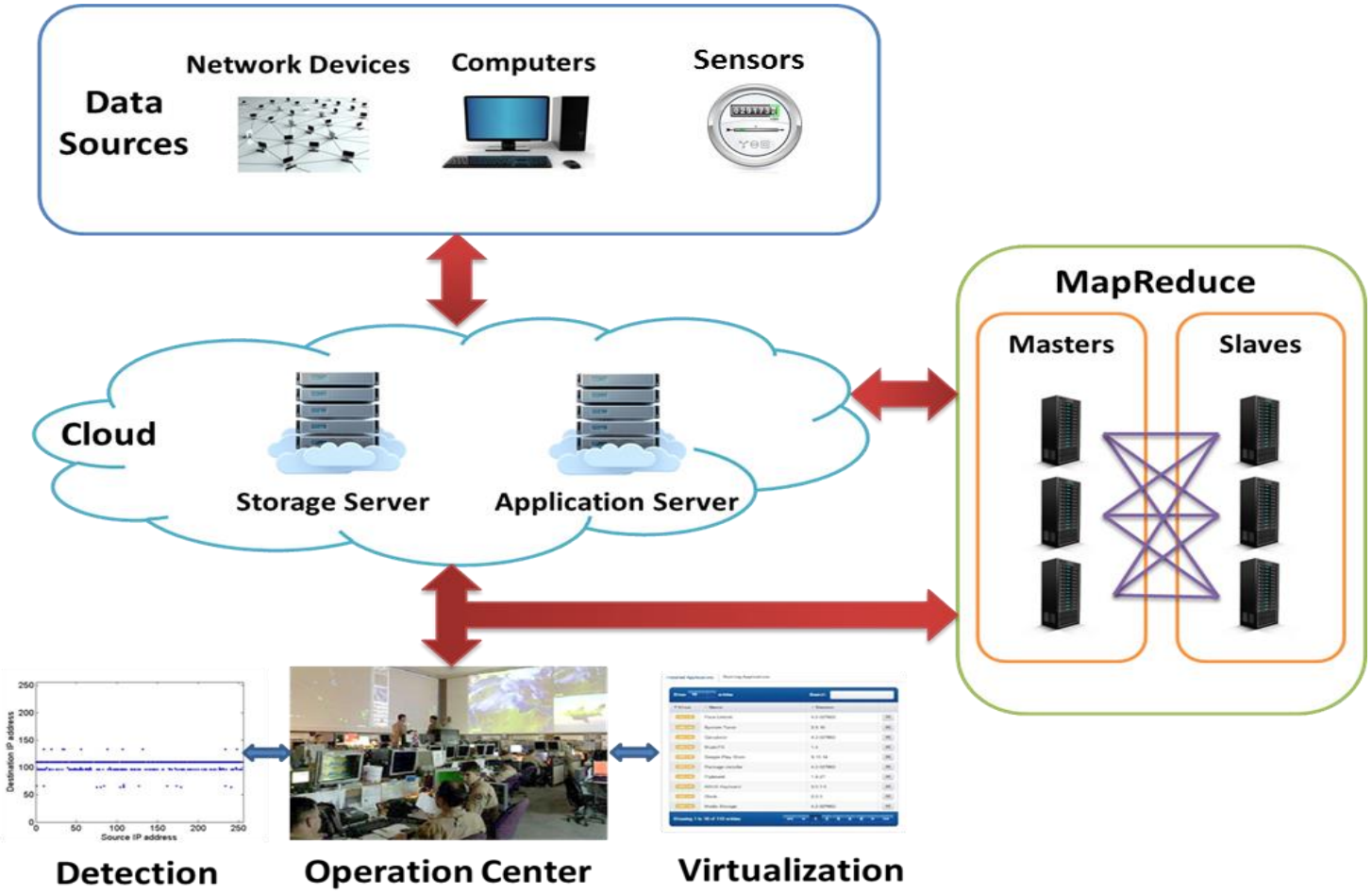
Exploring Threat Space

A Framework for Designing Countermeasures in CPS/IoT Systems



Defense Framework

CPS/IoT System Management and Security Management



System Management and Security Management

Research Projects

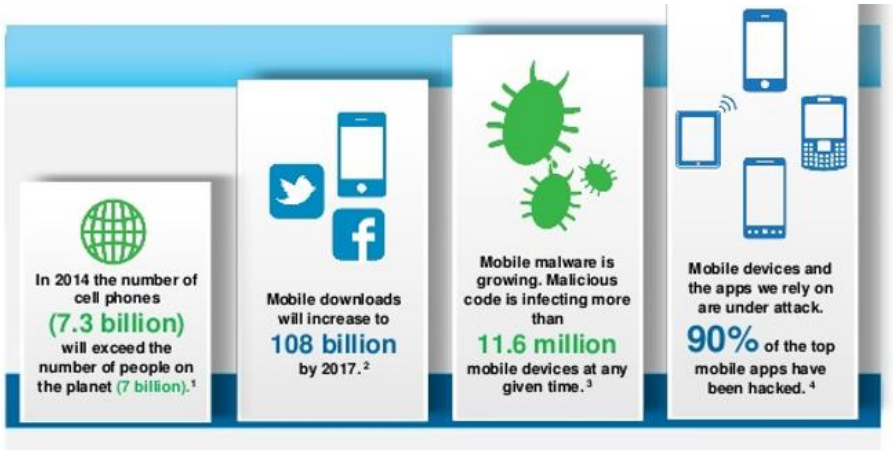
- CPS/IoT/Next Generation Wireless Networks
- **Mobile and MANET Security**
- Network Threat Monitoring and Detection
- Privacy and Anonymized Systems

Issues

- With the increasing popularity, smart mobile devices have become a burgeoning target for cyber adversaries
- Resources in mobile networks are much limited
  - We shall transmit a large amount of suspicious information over MANET in real time
- Big data issues
  - Applications such as network monitoring, network analysis, network fraud and intrusion detection systems are characterized by very high volume data streams

Overview

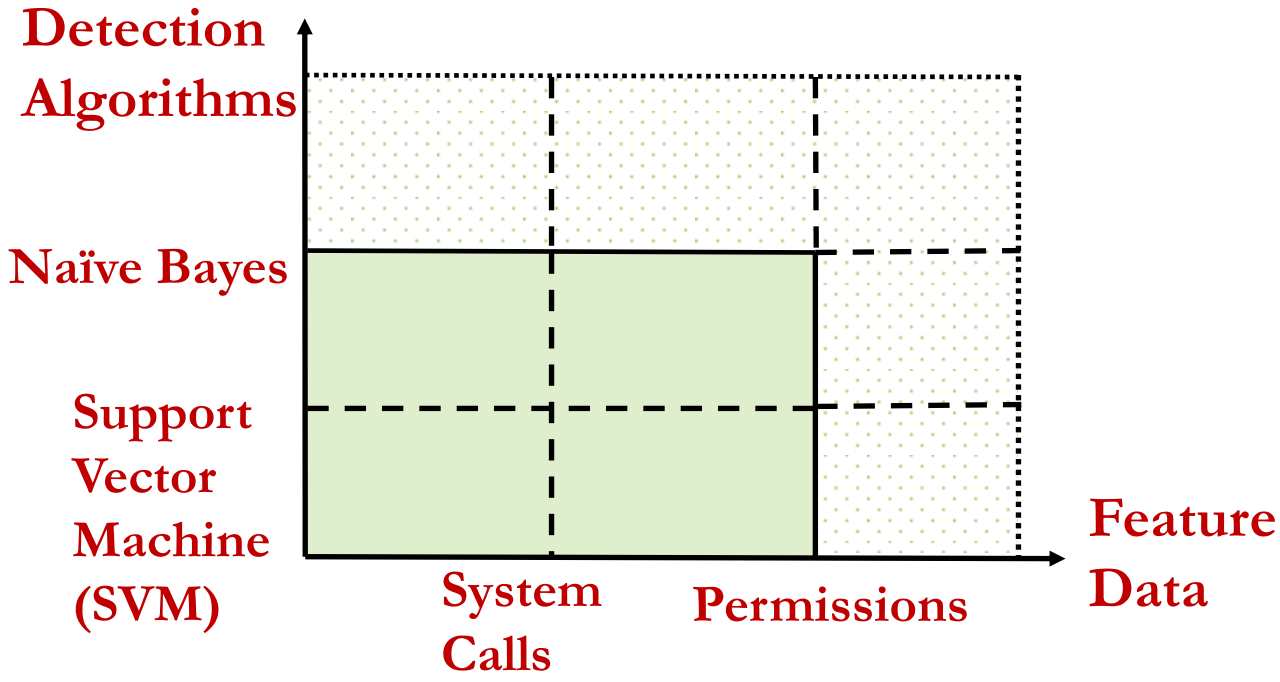
- Smart mobile devices have become a burgeoning target for cyber adversaries
- Resources in mobile networks are much limited (large amount detect data needs to be transmitted)
- The development of effective threat monitor and detect system in MANET is critical



Mobile Threats
(https://www.comscore.com/)

Detection Techniques

- **Permission Analysis**
  - Extract security configurations & check them against configured security policy rules after installing an application
- **Dynamic Analysis**
  - Collect runtime system logs (e.g., system calls) to monitor dynamic behaviors

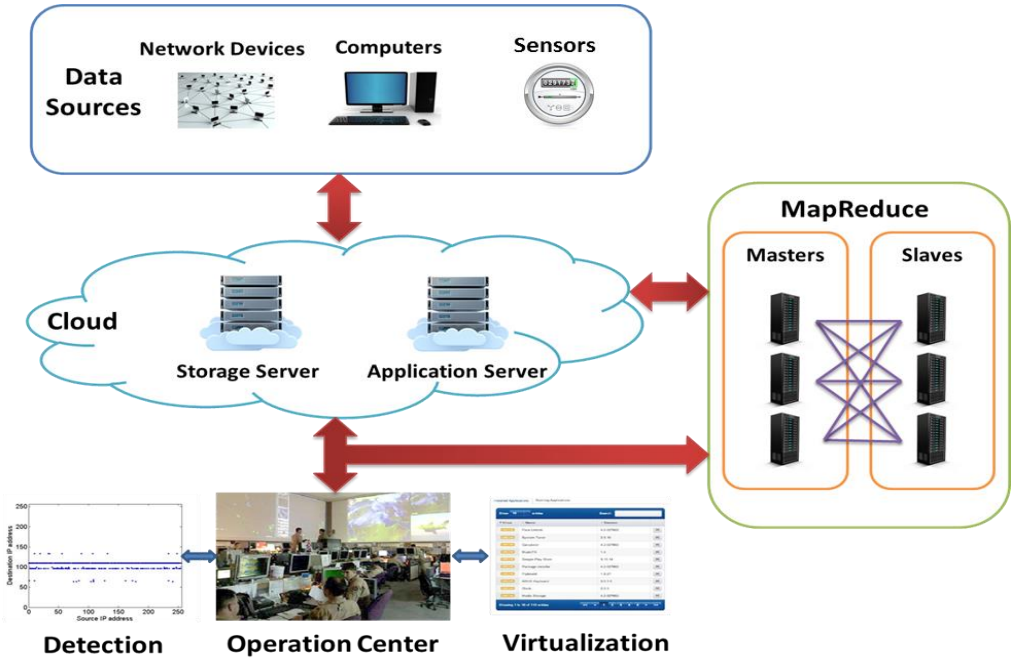


Detection Efficiency & Scalability

- **To enable cyber attack monitoring and detection, a large amount of suspicious information needs be transmitted over MANET with limited resources**
- ***How can we develop the techniques to transmit intrusion data with minimal impact on the MANET while achieving a good detection accuracy?***
  - **Sampling:** simple random sampling and stratified random sampling to select data to be transmitted
  - **Aggregation:** Lossless and lossy aggregation techniques to reduce the energy cost in information transmission and bandwidth overhead, while preserving good detection accuracy

Big Data in Network Security

- Large and complex threat monitoring systems
- Large scale of networks
- A large amount of data collected from hosts and network devices
  - Real-time processing requirement
  - High computation power requirement



Research Projects

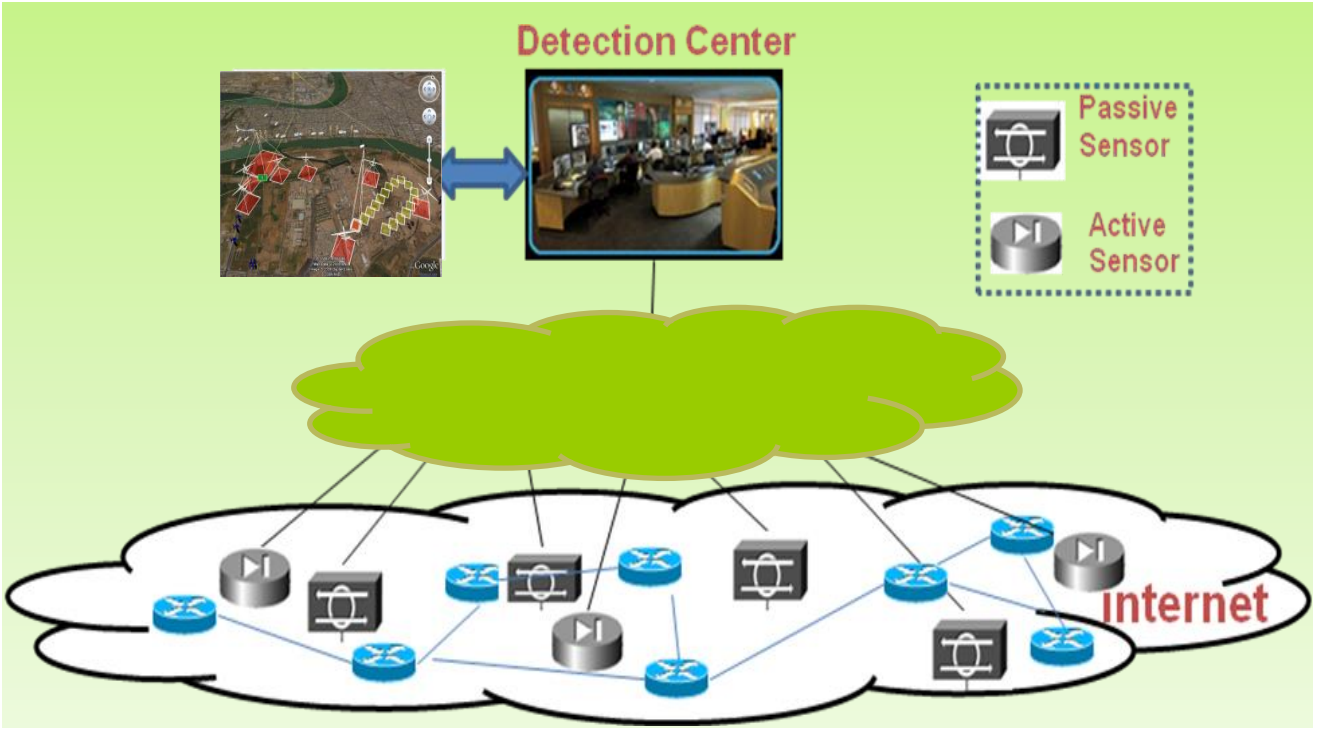
- CPS/IoT/Next Generation Wireless Networks
- Mobile and MANET Security
- **Network Threat Monitoring and Detection**
- Privacy and Anonymized Systems

Problems and Challenges

- **Network data and alerts**
  - Uncertain, ambiguous, and even incorrect
  - Often come from sensors of different modalities
- **Network attacks**
  - Evolve over time (from distributed locations)
  - Determined by attack model's dynamics
- **Conventional pattern recognition techniques**
  - High false positives, passive manner by only using the available alerts instead of actively seeking the most useful alerts to use
  - Difficulty in detecting highly complex attacks
  - Inability to adapt for detecting new types of attacks
  - Inability to provide the effective mitigation of a network threat
- **How to conduct network Situation Awareness in a selective and active manner**
  - To identify the most informative alerts to use
  - To detect the network attacks quickly and accurately
- **How to identify the optimal mitigation strategy**

Our Proposed Framework

- Generalized framework with the aim of handling simultaneously network security awareness, mitigation, and prediction



Key Features

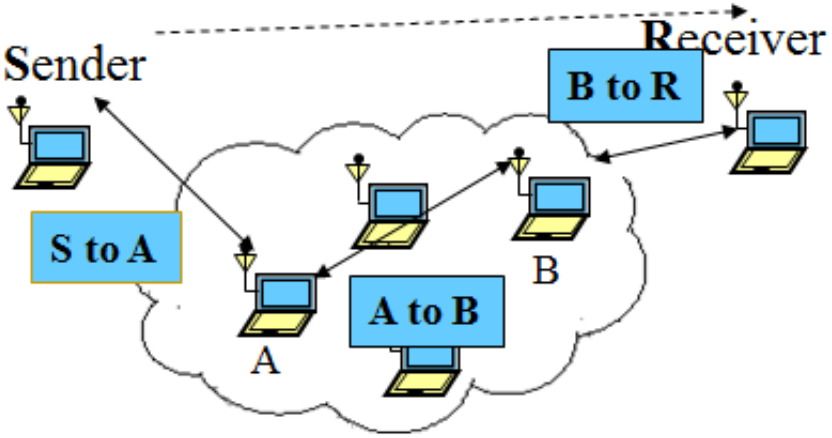
- Enable the capacity of detecting stealthy attacks and tracing attack origins
  - Passive and active network sensors
- Provision various detection algorithms, traceback algorithms, and visualization tools
  - Detect the sophisticated stealthy and anonymous attacks over cyber space to be displayed on a world map
- A network-based feedback loop control cyber-defense system

Research Projects

- CPS/IoT/Next Generation Wireless Networks
- Mobile and MANET Security
- Network Threat Monitoring and Detection
- **Privacy and Anonymized Systems**

Traffic Analysis Techniques on Anonymous Traffic Flows

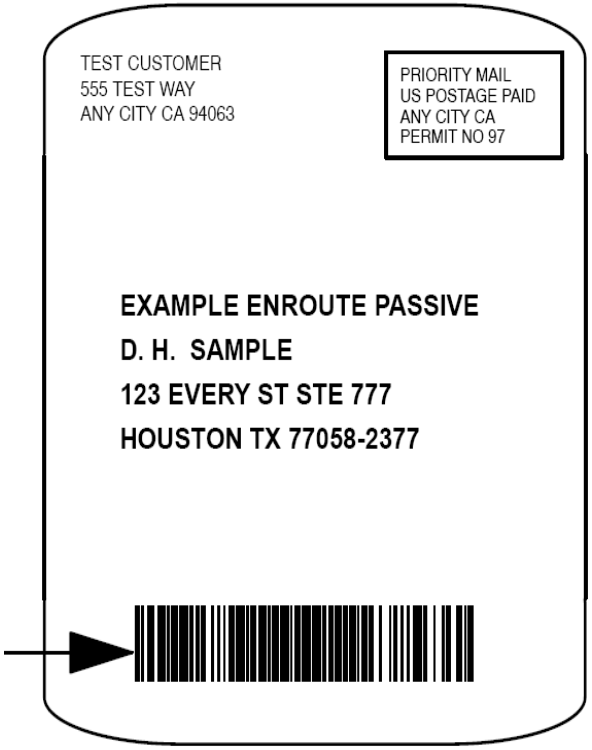
- Criminals may leverage various resources, i.e., varied anonymous communication venues (Tor, Anonymizer) to conduct malicious activities



Anonymous Communication

Traceback in the Real World

Animal traceback



Mail traceback

Problem Statement

Network Model

- When a suspect sender sends data through an encrypted and anonymous channel, how can Investigator link and confirm who is the receiver in a secret, accurate, and efficient manner?
  - We adopt the traffic analysis approach!

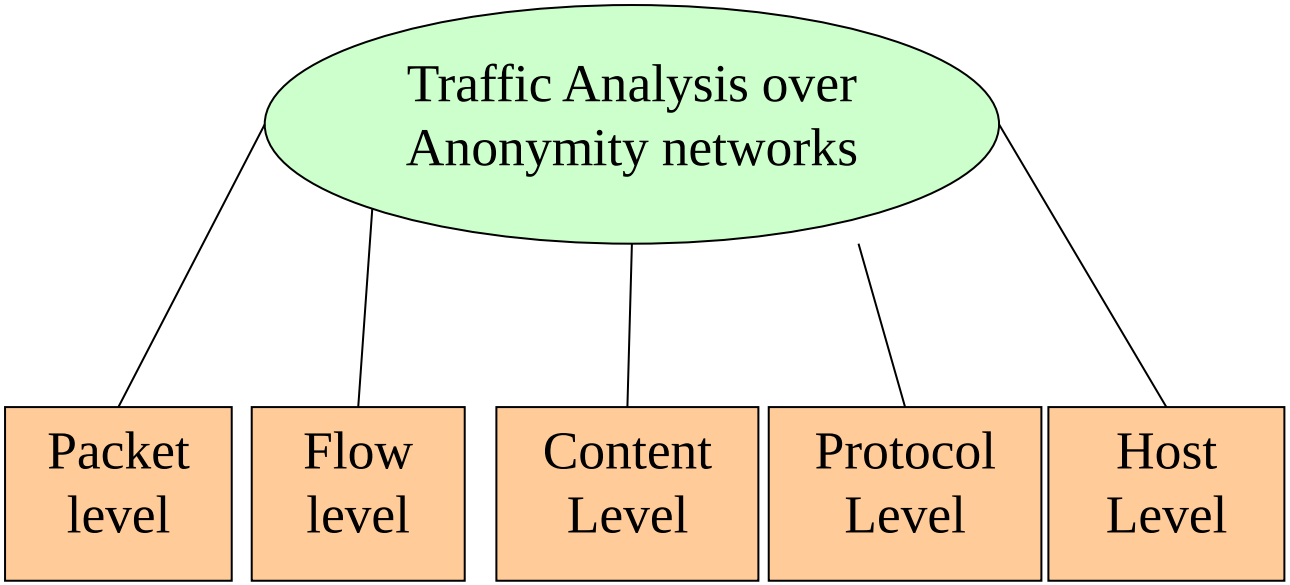
Traffic Marking Solution

- **Our Idea**
  - Changing traffic characteristics, e.g., flow rates, packet size,
  - Traffic characteristics changes represent a "mark", i.e., a special secret code

Flow-level Traffic Marking

Roadmap for Traffic Analysis on Anonymous Traffic Flows

- **Various coding/decoding mechanisms**
- **Different anonymous systems**
- **Various marking schemes**
  - Featuring from all levels of communication



Roadmap for Different Techniques

Developing Your Project and Story!!!

Potential Project Topics

- Security and Privacy Issues in Cyber Physical Systems (CPS)/Internet-of-Things
- Security and Privacy Issues in Wireless Heterogeneous Networks (UAV + Ground Base Station, etc.)
- Security Issues in 5G Wireless Networks (Ultra-Dense Networks, Millimeter Wave, Massive MIMO)
- Security Issues in Public Safety Communication Networks
- Security Issues in Cognitive Radio Networks
- Security Issues in Software Defined Networks
- Security Issues in Device-to-Device Communication and Networking
- Security Issues in Machine-to-Machine Communication and Networking
- Security Issues in Cloud Computing and/or Fog/Edge Computing
- Mobile Security and Privacy
- Security and Privacy Issues in Big Data

Others (please discuss with instructor in person….)