Seventh Annual
Cyber-Physical Systems Principal Investigators' Meeting
Arlington, VA | October 31 – November 1, 2016

Synergy: Securing the Timing of Cyber-Physical Systems

CNS-1646641, 10/1/2016 – 9/30/2019, University of California, Riverside
Qi Zhu, Matthew Barth, Zhiyun Qian, Fabio Pasqualetti, Nael Abu-Ghazaleh, Eamonn Keogh

Challenges of Timing Attacks

- CPS functionality is affected not only by the data values of operations but also by the time those operations are conducted.
- **Timing-based security attacks:** attackers compromise system functionality by changing the timing of computation or communication operations.
- Broad attack surface across cyber and physical domains.
- Various threat models: a) malicious node outside of the system, b) malicious node participating in the system, c) partially compromised node.
- Timing attacks could be stealthy, and difficult to defend against at real time under limited resources.

Proposed Framework

Thrust A: Identify and Analyze Timing-based Attack Surface and Strategies

A1. Identification and Analysis of Timing-based Attack Surface

- Examples: wireless jamming at physical layer; denial-of-service on TCP/IP, WAVE or similar protocols; compromised nodes on CAN, Ethernet or other buses; partially compromised computation nodes.

A2. Investigate Precise and Stealthy Timing-based Attack Strategies

- Multipronged attacks; Flow-In-the-Middle (FIM) attacks; attacks on clock synchronization algorithms (e.g., NTP).

Thrust B: Cross-Layer Analysis of Timing Attacks on System Properties

B1. Analysis of System Properties under Timing Aberration

- Analyze the impact of timing on various system properties (e.g., safety, stability, performance). Two driving domains: consensus-based applications for multi-agent robotic system; safety and mobility applications for vehicular networks.

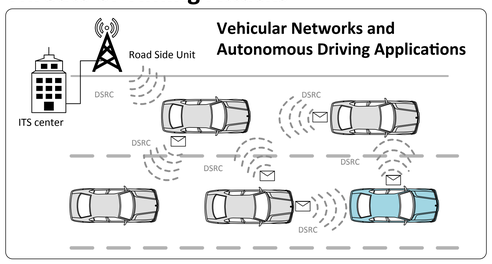
B2. Cross-Layer Timing Analysis for Timing Attacks

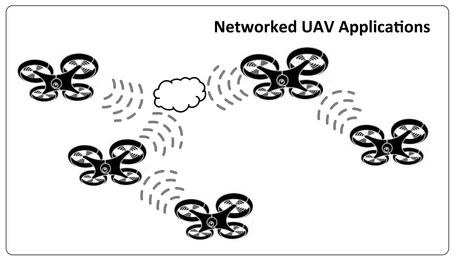
- Correlate system-level timing changes with local timing changes at attack point.

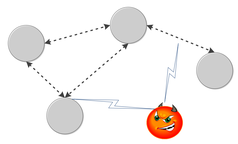
Thrust C: Control-based & Cybersecurity Defense for Timing Attacks

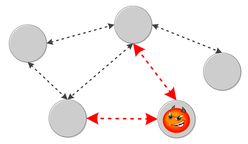
- System level control-based detection mechanisms.
- System interconnection adaptation for improving resilience to timing attacks.
- Cyber-security detection mechanisms: 1) detecting temporal anomalies using time-series analysis, 2) detecting the footprint of the delay attack.
- Design of secure time synchronization protocols.

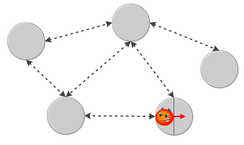
Threats of Timing Attacks



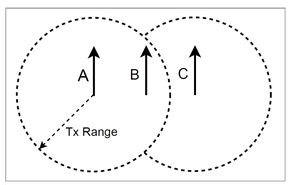



Malicious node outside of the system

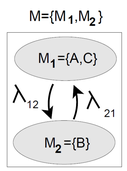

Malicious node participating in the system

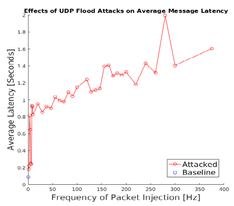

Partially compromised node

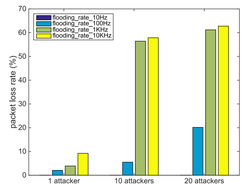
Thrust A



Flow-In-the-Middle (FIM) attacks

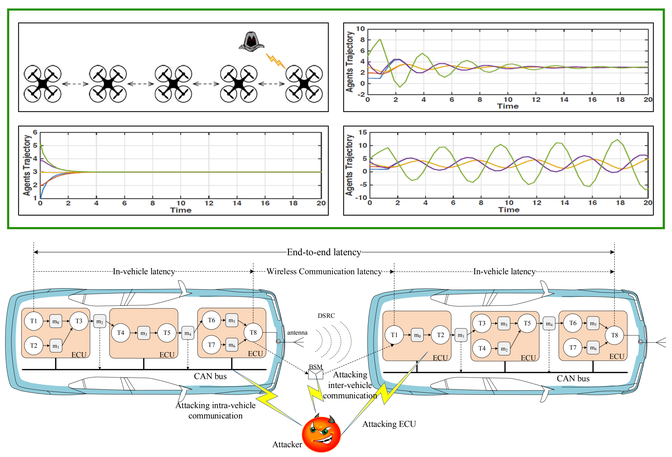






Timing attacks on communication links

Thrust B



Thrust C

Control-Based Detectors

Cyber-Security Monitors on Communication and Computation

Scientific Impacts

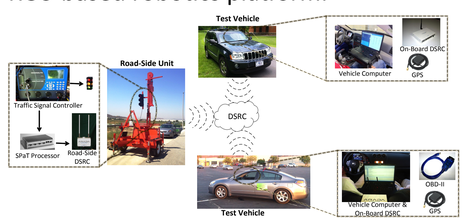
- Discover new timing-based attack surface and threat models.
- Develop novel cross-layer methodologies for analyzing the impact of timing attacks on system properties.
- Develop novel run-time detection and mitigation techniques as well as design-time protection strategies for timing attacks.
- Provide insights for addressing system robustness under general timing variations.

Broader Impacts

- Address little-studied timing attacks and design secure CPS in critical sectors, e.g., automotive and transportation systems, industrial automation, robotics.
- Enable close collaboration with industry and potential technology transfer.
- Integrate findings into UCR curriculum and extend to K-12 through Lego Mindstorm.

Evaluation

- Test vehicles with custom sensors (LiDAR, IMUs, radar, cameras, …) and DSRC.
- Road-side unit with DSRC (e.g., a portable traffic signal controller).
- Simulation platforms (SUMO, NS-3, ...).
- ROS-based robotics platform.



UC RIVERSIDE UNIVERSITY OF CALIFORNIA
PI: Qi Zhu (qzhu@ece.ucr.edu)
Industry Collaborator: TOYOTA INFOTECHNOLOGY CENTER, U.S.A., INC.