CPS: Synergy: Securing the Timing of Cyber-Physical Systems

Qi Zhu (Northwestern); Nael Abu-Ghazaleh, Zhiyun Qian, Fabio Pasqualetti, Matthew Barth (UC Riverside)

2018 NSF Cyber-Physical Systems Principal Investigators' Meeting

Challenges of Timing Attacks

- CPS functionality is affected by both the data values of operations and the time those operations are conducted.
- Timing-based security attacks: compromise functionality by changing the timing of computation or communication operations.
- Broad attack surface across cyber and physical domains.
- Timing attacks could be stealthy, and difficult to defend against at real time under limited resources.

Framework

Thrust A: Analyze Timing-based Attack Surface and Strategies

A1. Identification and Analysis of Timing-based Attack Surface

- Wireless jamming and flooding at physical layer; denial-of-service on TCP/IP or WAVE; compromised nodes on CAN, Ethernet or other buses; partially compromised computation nodes.

A2. Investigate Precise and Stealthy Timing-based Attack Strategies

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

Thrust B: Cross-Layer Analysis of Timing Attacks

B1. Analysis of System Properties under Timing Aberration

- Analyze the impact of timing aberration on system properties, e.g., safety, performance, liveness, deadlock-free, fairness, robustness.
- Safety and mobility applications for vehicular networks.

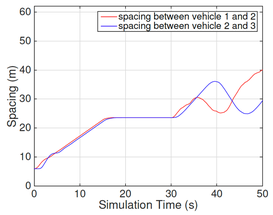
B2. Cross-Layer Timing Analysis for Timing Attacks

- Correlate system-level timing changes with local timing changes.

Thrust C: Cybersecurity and Control-based Defense

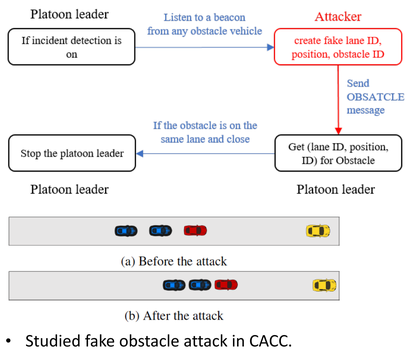
- Design of protocols that are robust to timing aberration.
- System interconnection adaptation for improving resilience to timing attacks. System level control-based detection mechanisms.

Thrust A

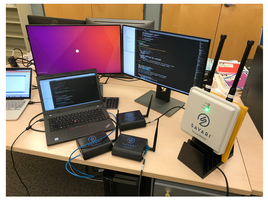


CACC (collaborative adaptive cruise control) under flooding attacks:

- Assumed 40% packet lost during 30s to 50s.
- Spacing increased from 24m to 30-40m.



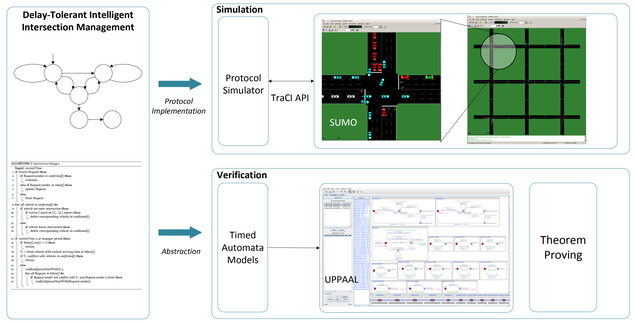
- Studied fake obstacle attack in CACC.
- Considered other attack types and applications.

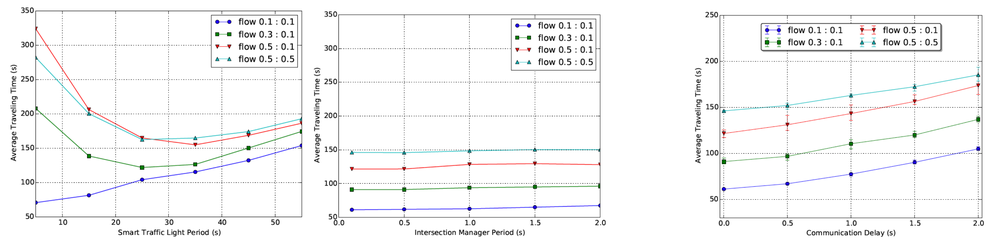


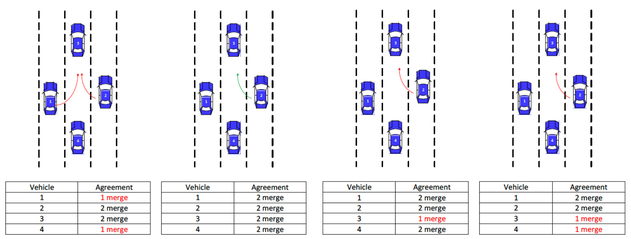
Experimental platform with commercial DSRC transceivers:

- One road side unit and four on-board units.
- Assessed jamming and attack on Chrony for time synchronization.

Thrust B & C







Vehicle	Agreement
1	1 merge
2	2 merge
3	2 merge
4	1 merge

Vehicle	Agreement
1	2 merge
2	2 merge
3	2 merge
4	2 merge

Vehicle	Agreement
1	2 merge
2	2 merge
3	1 merge
4	2 merge

Vehicle	Agreement
1	2 merge
2	2 merge
3	1 merge
4	1 merge

- Proposed partial consensus formulation for generalizing the development of secure connected vehicle protocols.

Developed delayed-tolerant autonomous intersection design:

- Proved system's safety, liveness, and deadlock-free properties under timing attacks.
- Demonstrated 10-25% performance improvement over back pressure based smart traffic lights in normal operation condition.
- Studied the impact of timing attacks on system performance and derived guidance for vehicle design at lower SW/HW and communication layers.

- Bowen Zheng, et al. "Delay-Aware Design, Analysis and Verification of Intelligent Intersection Management", SMARTCOMP, 2017.
- Bowen Zheng, et al. " Timing and Security Analysis of VANET-based Intelligent Transportation Systems", ICCAD, 2017.
- Hengyi Liang, et al. "Network and System Level Security in Connected Vehicle Applications", ICCAD, 2018.
- Bowen Zheng, et al. "Design and Analysis of Delay-Tolerant Intelligent Intersection Management," submitted to TCPS.
- Qi Zhu and Alberto Sangiovanni-Vincentelli, "Co-design Methodologies and Tools for Cyber-Physical Systems," Proceedings of the IEEE, 2018.
- Chung-Wei Lin, et al. "Platform-Based Design for Automotive and Transportation Cyber-Physical Systems," Springer, in preparation.

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 to address 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, robotic systems.
- Enable close collaboration with industry and explore potential technology transfer.
- Integrate findings into Northwestern and UCR curriculum and extend to K-12 through Lego Mindstorm.

Northwestern University

UC RIVERSIDE UNIVERSITY OF CALIFORNIA

Industry Collaborator: TOYOTA InfoTechnology Center, U.S.A., Inc.

PI: Qi Zhu (qzhu@northwestern.edu)

Award ID#: 1839511