SaTC: TTP: Medium: Collaborative: Exposing and Mitigating Security/Safety Concerns of CAVs: A Holistic and Realistic Security Testing Platform for Emerging CAVs

Projects #: CNS-1930041, CNS-1929771

PIs: Z. Morley Mao (UMich), Qi Alfred Chen (UCI), Yiheng Feng (Purdue)

UNIVERSITY OF MICHIGAN

UCI

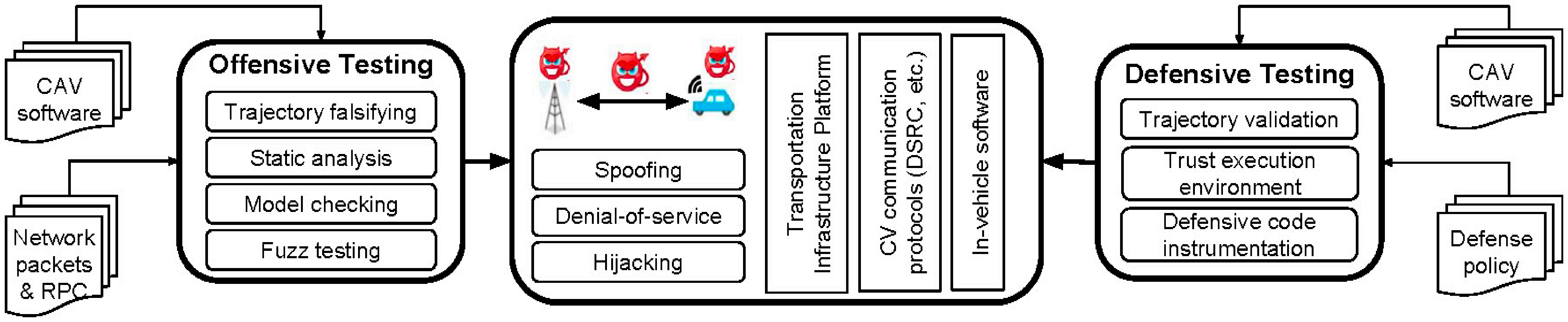
PURDUE UNIVERSITY

Problem & Challenges

- Connected & Automated Vehicle (CAV) technologies enable real-time information sharing and driving automation, with the potential of significantly improving safety and efficiency of transportation system
- However, cyber-security threats may compromise the efficiency of infrastructure operations and the safety of passengers, posing a significant challenge for CAV deployment.
- Our proposal: A novel CAV security/safety testing platform to address the critical needs for assessing CAV security and safety concerns in an effective & realistic manner.

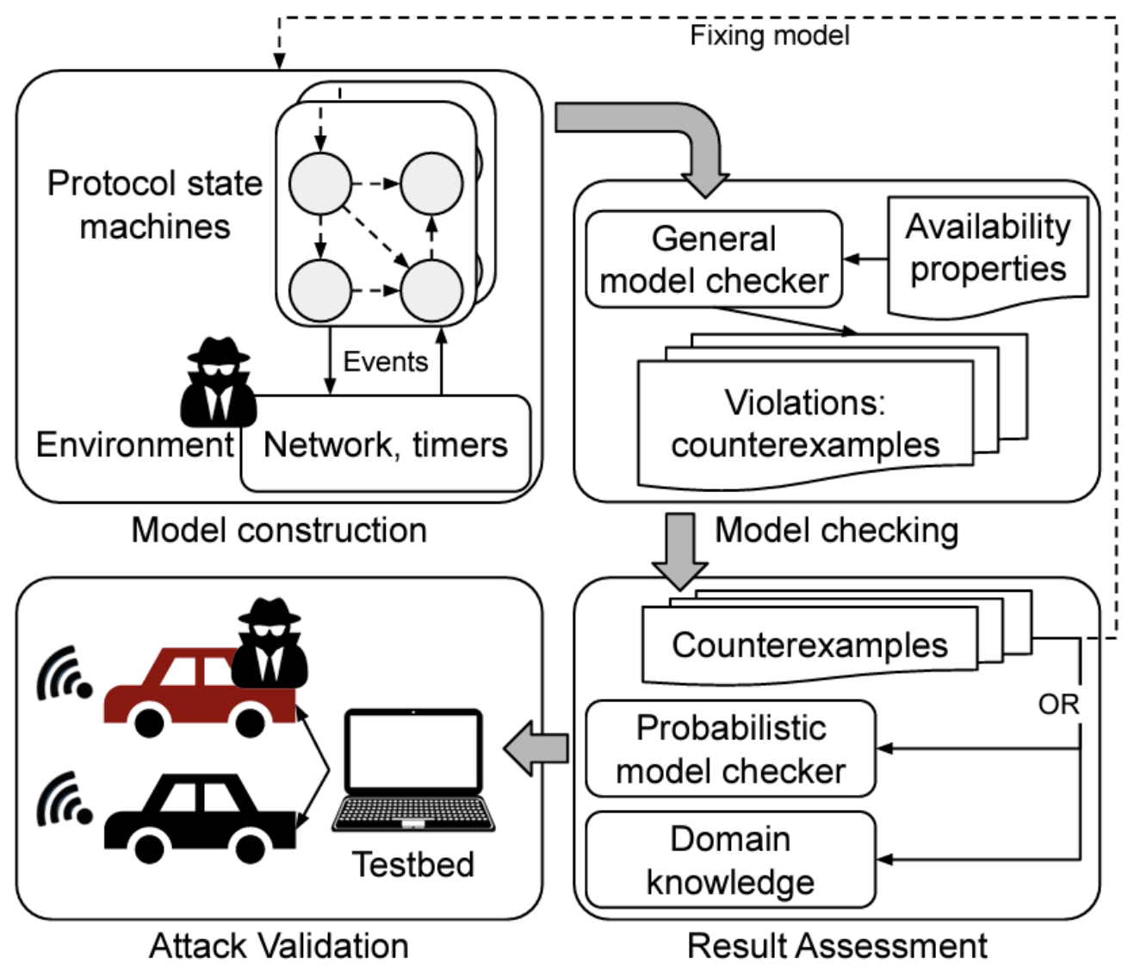
Scientific Impacts

- The first platform to allow comprehensive evaluations of all 3 key CAV components in a unified framework
  - Necessary for systematic analysis of interdependent safety/security issues in the CAV eco-system
- Develop novel testing support by effectively combining techniques in optimization, statistical modeling, machine learning, network emulation, program analysis, & model checking.
- Build and evaluate both offensive and defensive testing support in real world environments



Technical Solutions

- Provide both offensive & defensive testing services that cover 3 key components of CAV ecosystem: (1) transportation infrastructure platform, (2) V2 communication channels, (3) in-vehicle software platform.
- Highlights of new contributions:
  - First comprehensive analysis on CV based traffic signal control system security (TRC'21, IEEE TITS'22)
  - Defensive testing support of detecting anomaly in localization module of autonomous vehicles (TRB'21)
  - Offensive testing support for denial-of-service vulnerabilities in connected vehicle protocols (Usenix Security'21)
  - Offensive testing support for robustness of 3D object detection sensor fusion models (ICIP'20)
  - Defensive testing support of using infrastructure-side camera for detecting CV data spoofing (under submission)
  - Offensive testing support for adversarial robustness of trajectory prediction algorithms (CVPR'22)



Novel model checking support for CV protocols (Usenix Security'21)

Impacts on Society

- Allow hardware manufacturers, software developers, security service providers, and policymakers in the CAV industry & government to conveniently and holistically test their products against latest CAV attacks and study implications to different policies & regulations.
- Allow usage for training & education purposes for both schools and companies, and for facilitating the development of security best practices and standards in the CAV industry.

Impacts on Education & Outreach

- Provide research opportunities for graduate students in CS & civil engineering.
  - Including the recruitment of PI Chen and PI Feng's first Ph.D. students
- Contributed course materials to security and transportation courses at UMich (EECS 388), UCI (CS 134, CS 205), and Purdue (CE 299)
- Allow organizations of the AutoSec (Automotive and Autonomous Vehicle Security) Workshop, which co-located with NDSS since 2021 (top-tier security venue).

Impact on Broader Participation

- Provides opportunities for the PIs to present latest transportation technology and its security topics at URM clubs such as WiSys@UCI and Ensemble@UMich
- Allows recruitment of female and African American undergrad & grad students in research, and contributing to programs such as MiBytes at Michigan, WiSE (Woman in Science and Engineering) at Purdue, and UROP (Undergraduate Research Opportunity Program) at UCI.