THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY
http://radionavlab.ae.utexas.edu

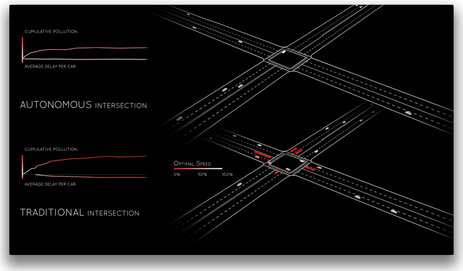
Secure Perception in Connected Vehicles

LAKSHAY NARULA, AND TODD E. HUMPHREYS

WNCG Wireless Networking & Communications Group

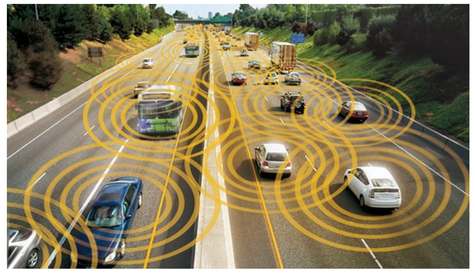
THE CONNECTED VEHICLE DREAM

Connected vehicles enable technologies such as Automated Intersection Management and platooning that help make roadways efficient, safe, and eco-friendly.



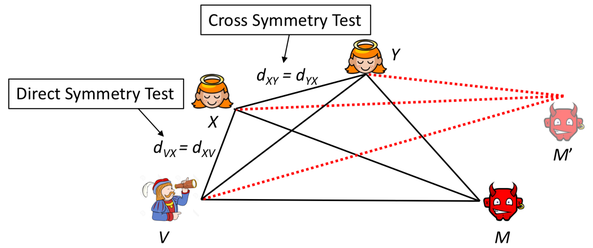
TALKING OVER DSRC

Dedicated Short-Range Communications (DSRC) protocol enables connected vehicles to exchange safety messages with minimal latency.



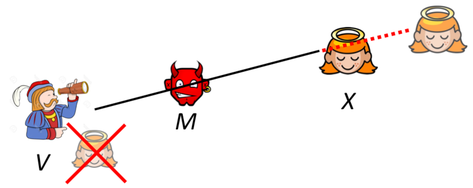
NEIGHBOR POSITION VERIFICATION

Fiore et al. [1]: An **internal attack can be detected** as long as the number of honest verifiers is greater than the number of colluding internal attackers.



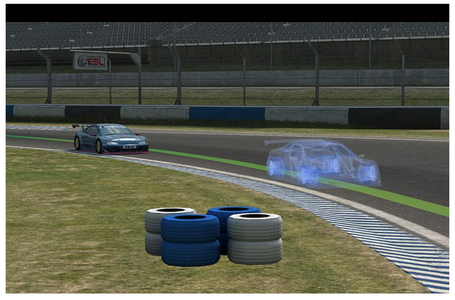
MAN-IN-THE-MIDDLE

Such verification schemes make the connected vehicle system **susceptible to MITM attacks**. A MITM could **tarnish the reputation of an honest node** by delaying the claims made by the honest node.



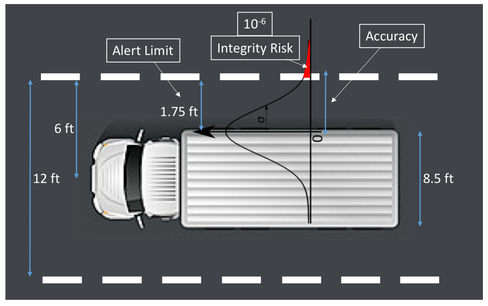
PHANTOM AND INVISIBLE CARS

- DSRC is vulnerable to **MITM and Internal attacks**.
- **Secure self-localization** is an open challenge.
- What is *misbehavior* and how do we deal with malicious actors?

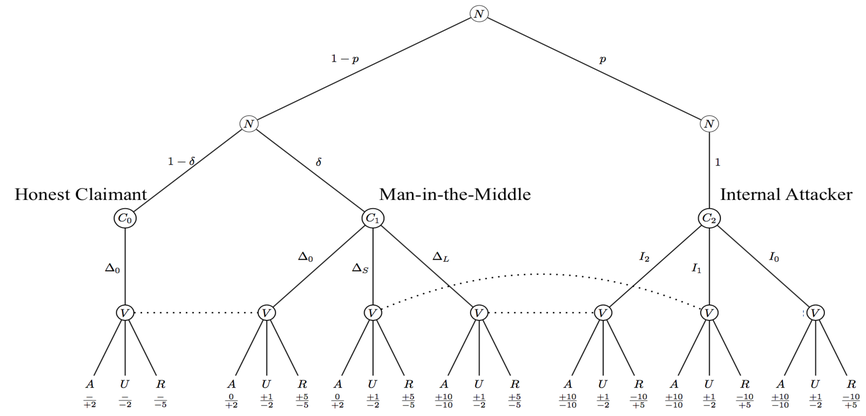


ACCURACY REQUIREMENTS

A connected vehicle must detect and address misbehavior before it is too late. Safe operation of vehicles demands **decimeter-accurate** own-vehicle positioning and **meter-accurate** neighbor position verification.



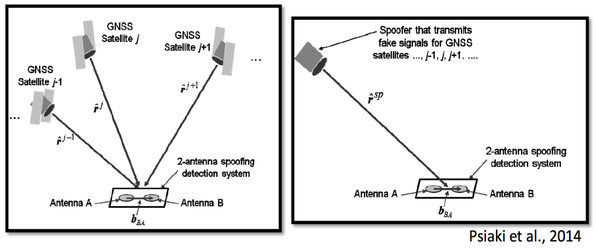
GAME THEORETIC ANALYSIS OF CONNECTED VEHICLES



SECURE SELF-LOCALIZATION

GPS is the most common mode of own-vehicle positioning. The UT Radionavigation Lab has previously demonstrated GPS spoofing as well as anti-spoofing techniques. Pincer and Two-Antenna defense are the most effective spoofing countermeasures.

- Received Power Monitoring
- Distortion Monitoring
- **Angle-of-Arrival Diversity**



Psiaki et al., 2014

INTERNAL ATTACKS

In a safety-of-life application such as high-speed driving, it is essential to take stock of all possible attacks. **However, DSRC assumes that certified vehicles always advertise true position and velocity.**

An **internal attacker could claim false position** and/or velocity under current DSRC security model. Alternatively, a **MITM could replay out-of-date claims**.

Connected vehicles **must verify** the claims made by their neighbors to the accuracy specified above.

At the same time, **such paranoia must not nullify the utility of connected vehicles.**

TWO-ANTENNA DEFENSE DEMO

An implementation of the two-antenna spoofing detection mechanism was demonstrated on the University of Texas at Austin campus. Two-antennas also make the centimeter-accurate RTK solution robust.

CONCLUSIONS

- Connected vehicles must use communications as one of the many *sensors* for secure perception.
- Secure centimeter-accurate positioning systems are a must-have for all safe connected vehicles. Two-antenna RTK is one such system.
- Anti-spoofing systems for DSRC must be developed to defend against false location and velocity claims.
- Significant revamp of DSRC credential management policy is recommended.

[1] Fiore, Marco, Claudio Ettore Casetti, Carla-Fabiana Chiasserini, and Panagiotis Papadimitratos. "Discovery and verification of neighbor positions in mobile ad hoc networks." *IEEE Transactions on Mobile Computing* 12, no. 2 (2013): 289-303.