Wireless Network Security
Spring 2016

Patrick Tague

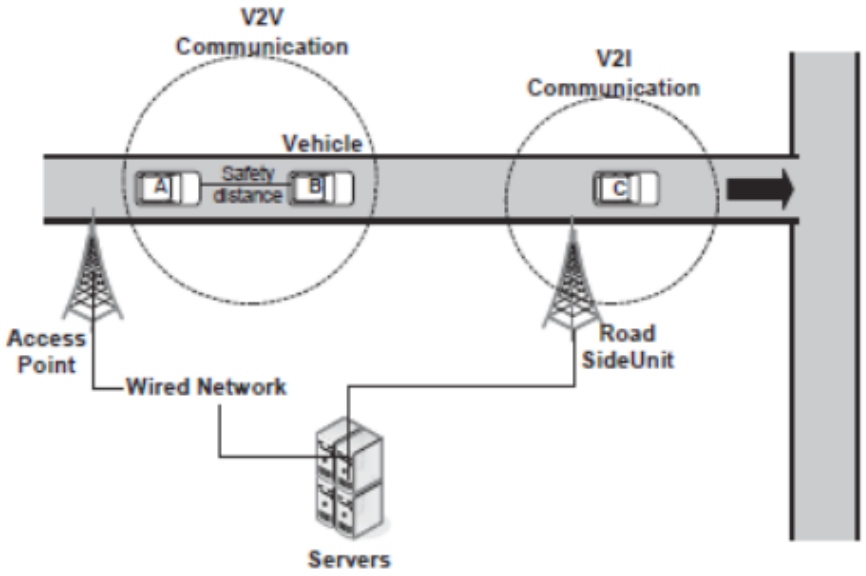
Class #19 – Vehicular Network Security & Privacy

Class #19

- Review of some vehicular network stuff
- How wireless attacks affect vehicle safety
- Brief mention of vehicle network privacy challenges

Vehicular Networks

- Vehicular (ad hoc) network
  - Cars talk amongst each other, w/ roadside units and w/ devices within the vehicles



- Applications of interest:
  - Automated driver safety management
  - Passive road quality / condition monitoring
  - In-car entertainment
  - Navigation services
  - Context-aware rec's:
    - "This alternate route would be faster, and it would go past your favorite Primanti Bros."

Vehicular Network Components

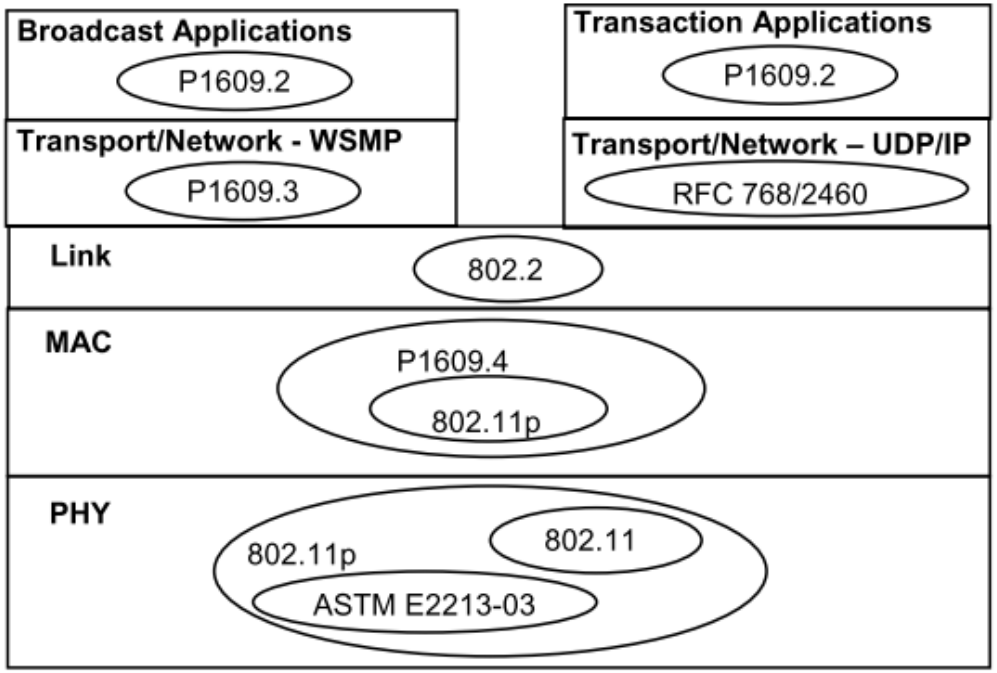
- User devices interact with the vehicle using WiFi, Bluetooth, NFC, visual channels, etc.
- On-board sensors communicate with a controller using low-power RF, e.g., 802.15.4 for TPMS
- Mobile network connectivity (e.g., GSM, LTE)
- Safety messaging systems between vehicles

802.11p and DSRC

- 802.11p extends the 802.11 standard to include vehicular communications in the 5.9 GHz band
  - Allows dynamic comms without setting up a BSS (i.e., no SSID) for fast decentralized operation
  - No association, no authentication, no access control…
  - Also includes mechanisms for channel management and synchronization
- Dedicated Short Range Communication
  - One- and two-way communication based on the 802.11p standard
  - Builds on the older ASTM E2213-03 PHY standard

WAVE

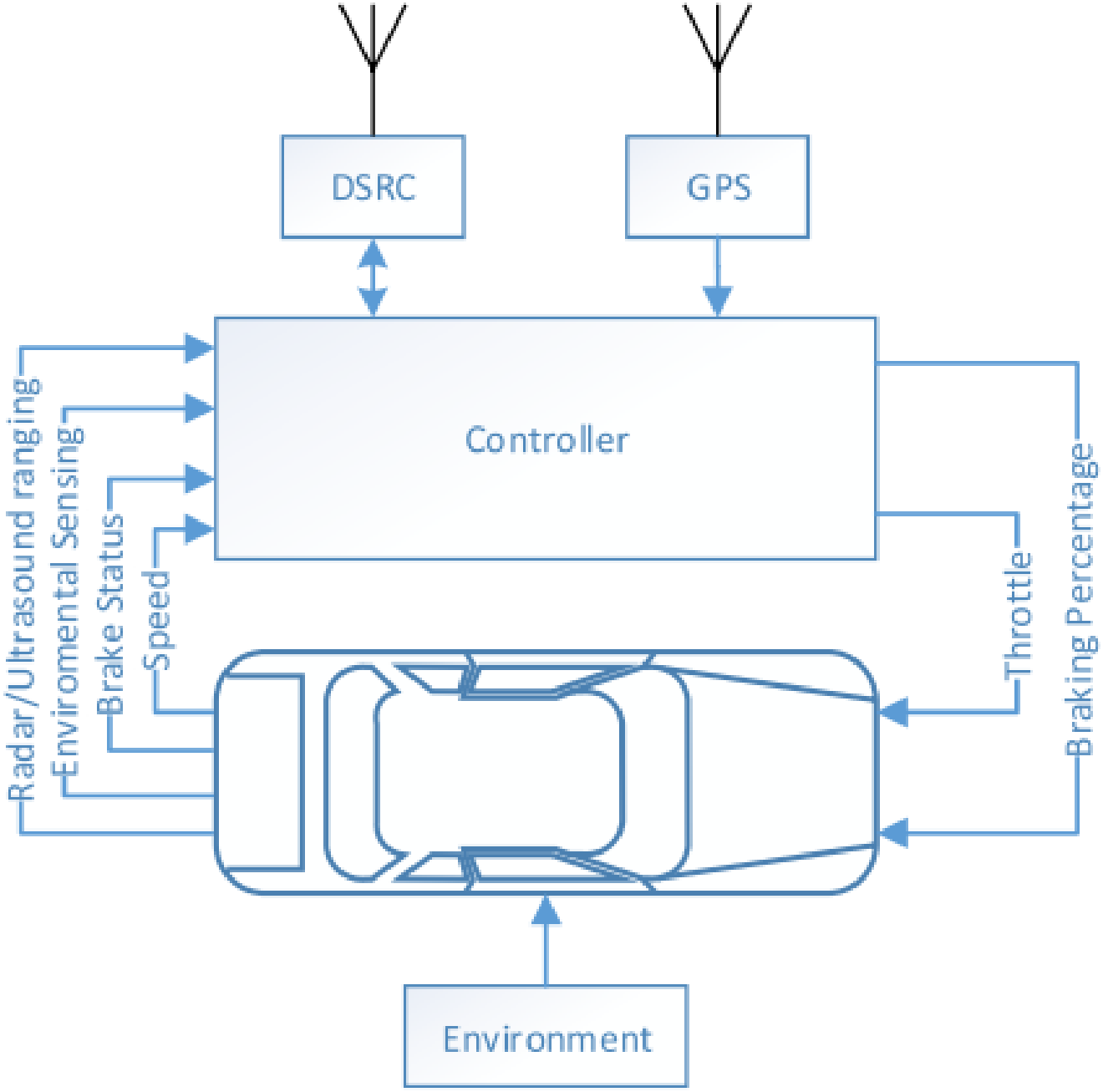
- Wireless Access in Vehicular Environments
  - Wireless stack for vehicle-to-vehicle and vehicle-to-infrastructure communications
  - Based on IEEE P1609 standard family
  - Built on top of the 802.11p / DSRC foundation



What kinds of vehicle safety systems are built on top of this wireless stack?

Vehicle Safety Systems

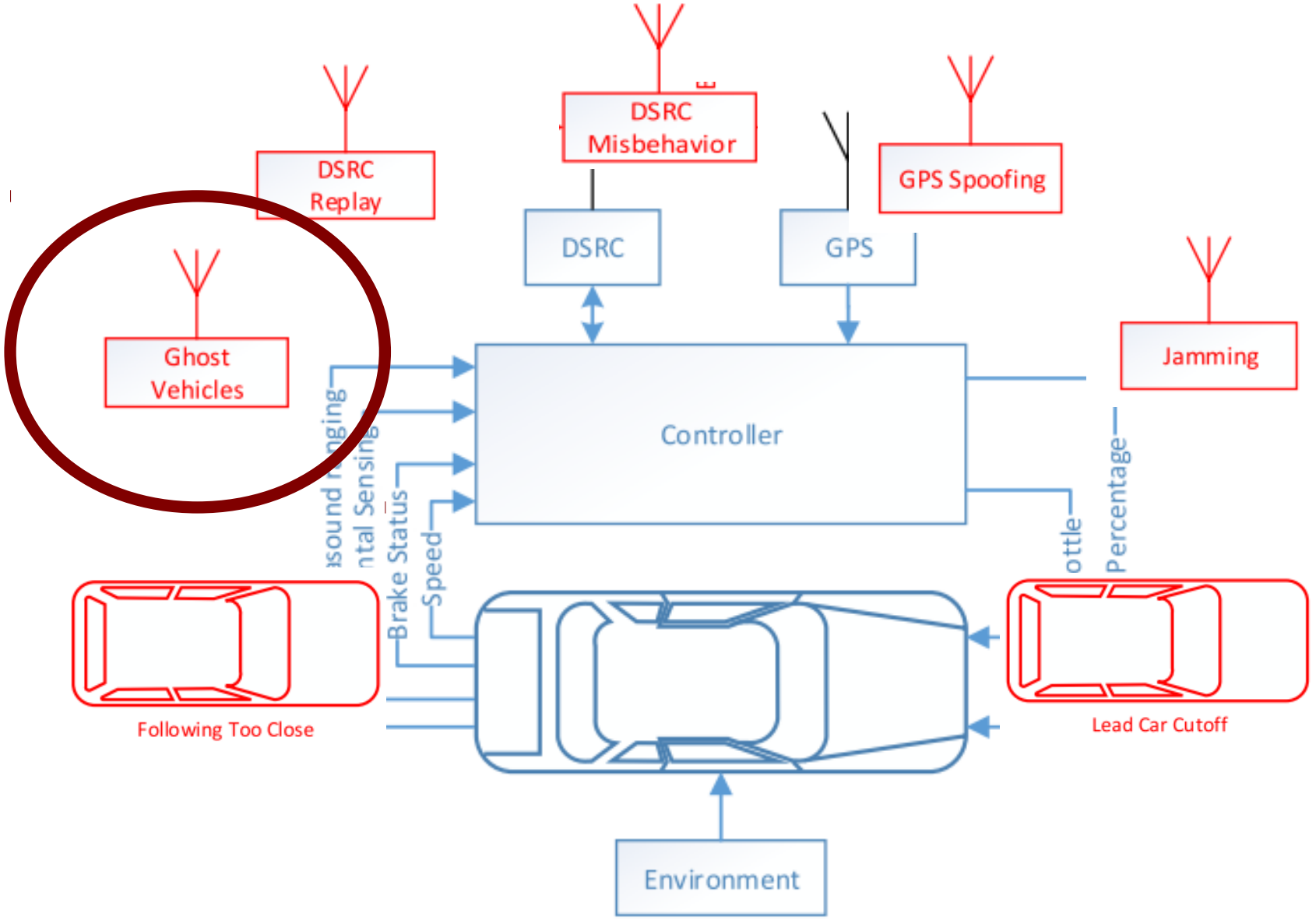
- New vehicles have various wireless subsystems
  - Driver alerts, ex: tire pressure monitoring
    - Valve sensors report to a TPMS controller – wireless because they're inside the wheels…
  - Adaptive cruise control, Platooning
    - Controller receives signals from a variety of sources, including other vehicles, RSUs, road beacons/monitors, etc.
  - Crash avoidance, Self-braking
    - Alerts come from other vehicles, sensors, etc.
  - Self-driving
    - All of the above and more…



Networked Controllers

- Any time you put a network inside a control loop, the network affects the controller
  - Lost packets ==> lost control
  - Spoofed packets ==> poor decisions
  - GPS errors ==> wrong controller world view
  - Network/compute overhead ==>control delay ==> reduced accuracy
  - All of these have potentially bad side-effects in the context of vehicle safety systems

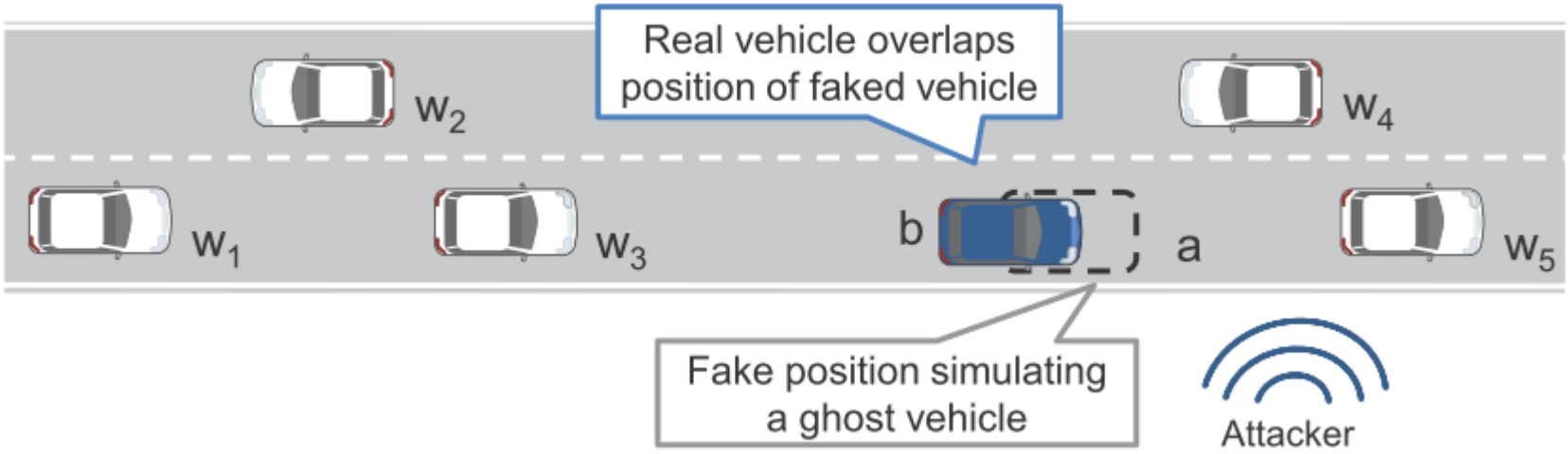
Other than general wireless comms issues, what are some potential threats?



Ghost Vehicles

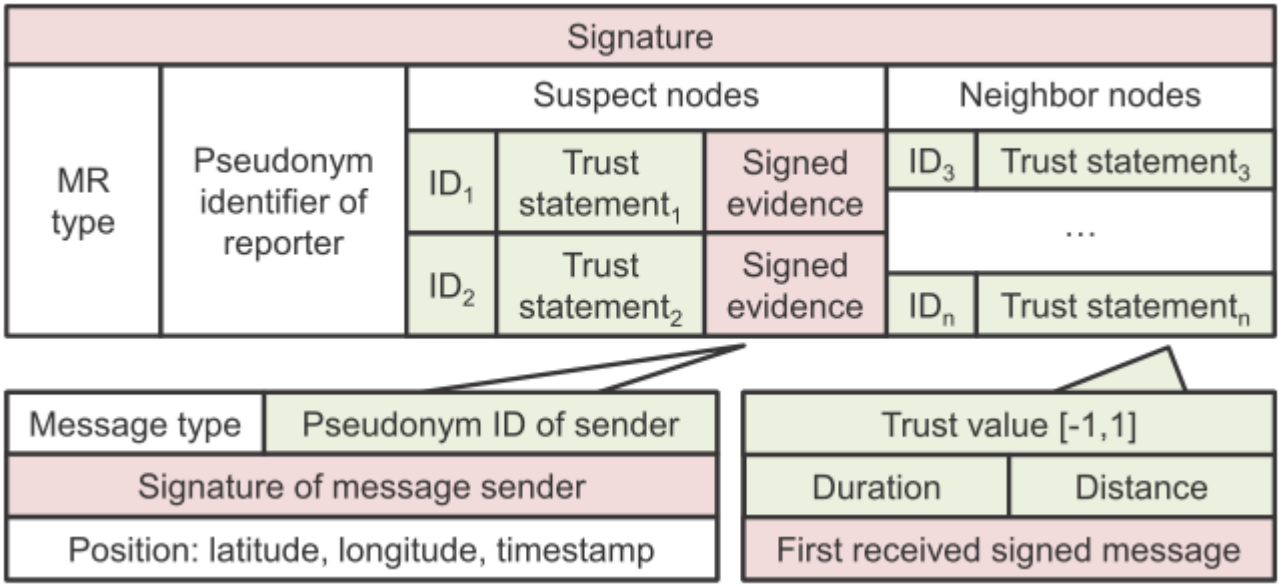
[Bißmeyer et al., VANET 2012]

- Ghost vehicles result from falsified reports, often by a Sybil attacker
  - Insider can properly sign and protect reports, so detection must rely on somehow invalidating reports
  - Trust and reputation system?



Misbehavior Evaluation

- Misbehavior detection systems can detect inconsistencies in reported mobility data
  - Local detection is limited to observable area (i.e., limited by communication range)
  - Also limited to short validity lifetime of mobility data
  - Subject to ID changes by attackers, dynamic tactics

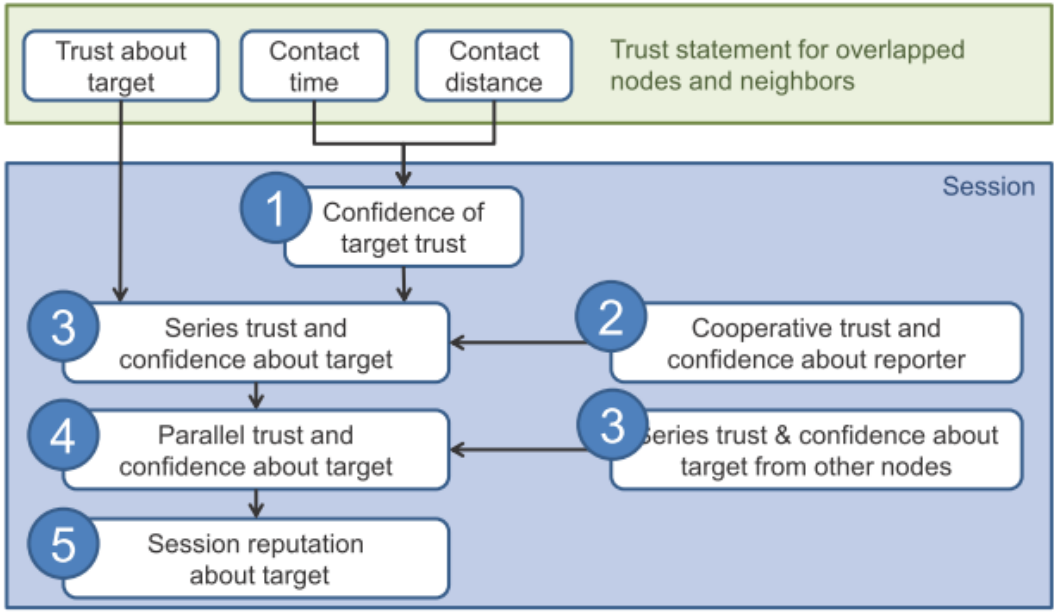


Some Assumptions

- Vehicles can switch between pseudonym certificates arbitrarily
- Position information is very accurate
  - GPS, relative positioning approaches
  - Additional sensors: cameras, radar
- The availability of connection between local nodes and the central entity is not guaranteed
  - Excluding attackers is the goal over the long run
  - Latency is not a big concern

Reputation Evaluation

- Reputation is computed centrally by a Misbehavior Evaluation Authority (MEA) using misbehavior reports from witnesses and info from suspects
  - **Trust**: the observed tendency to behave as expected, takes values in [-1,1], defaults to 0
  - **Confidence**: level of certainty in the trust value, essentially a weighting in [0,1]
  - **Reputation:** essentially trust x confidence, values in [-1,1]



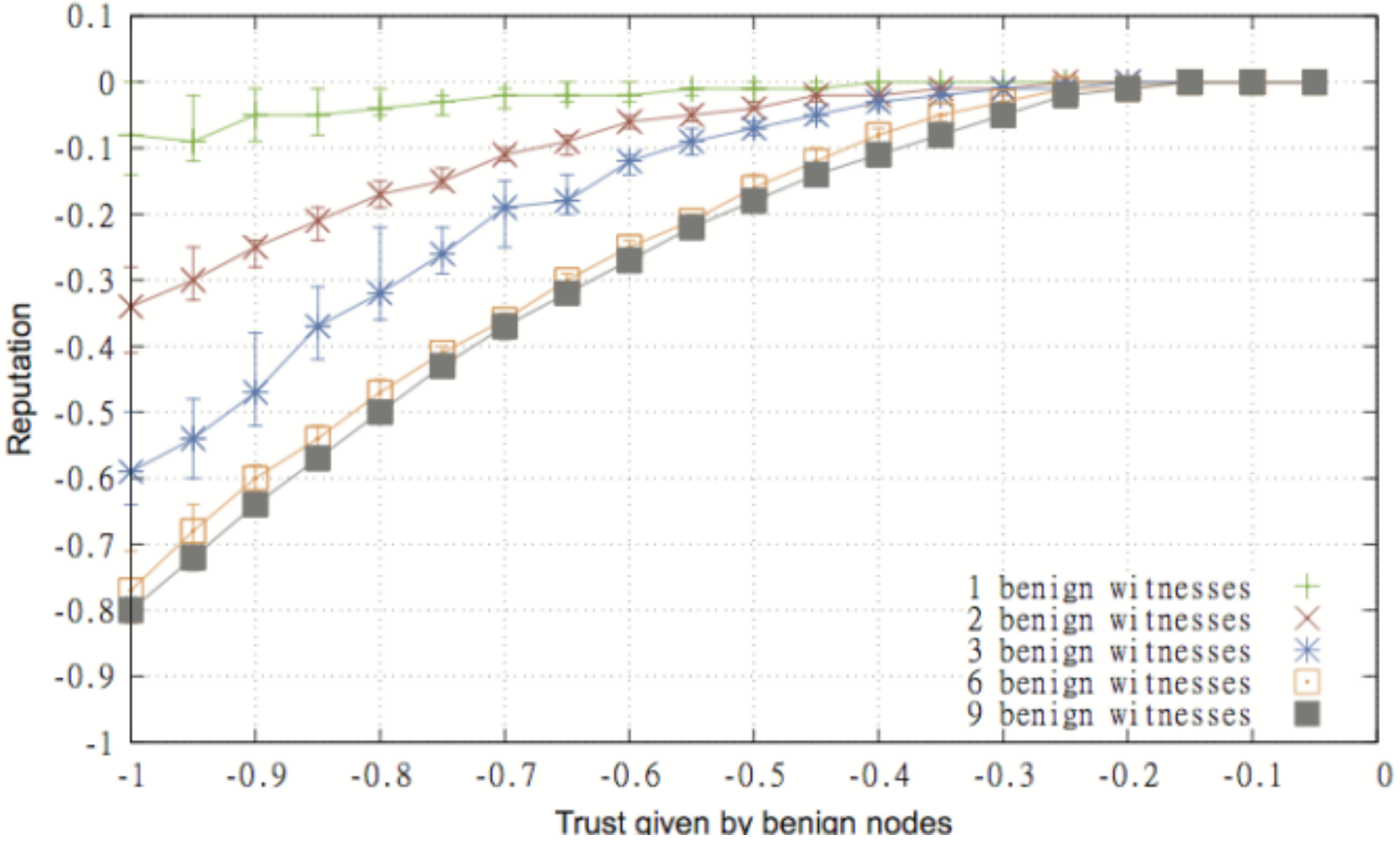
Ghost Identification

- Vehicles with “beyond a threshold” negative reputation can be identified as ghosts

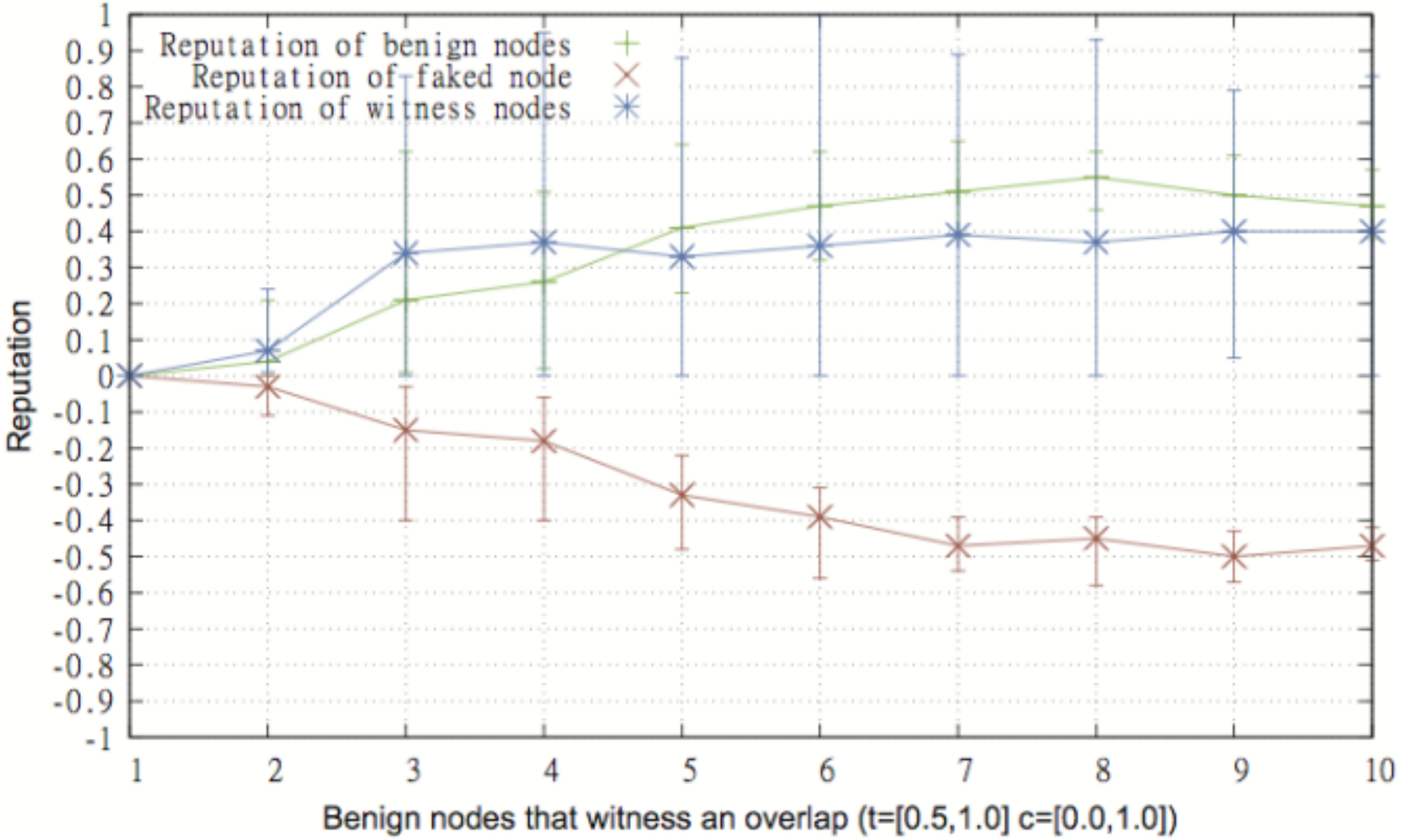
- **Q:** How serious is a false negative (declaring a real car when it's a ghost)?

- **Q:** How serious is a false positive (declaring a ghost when it's a real car)?

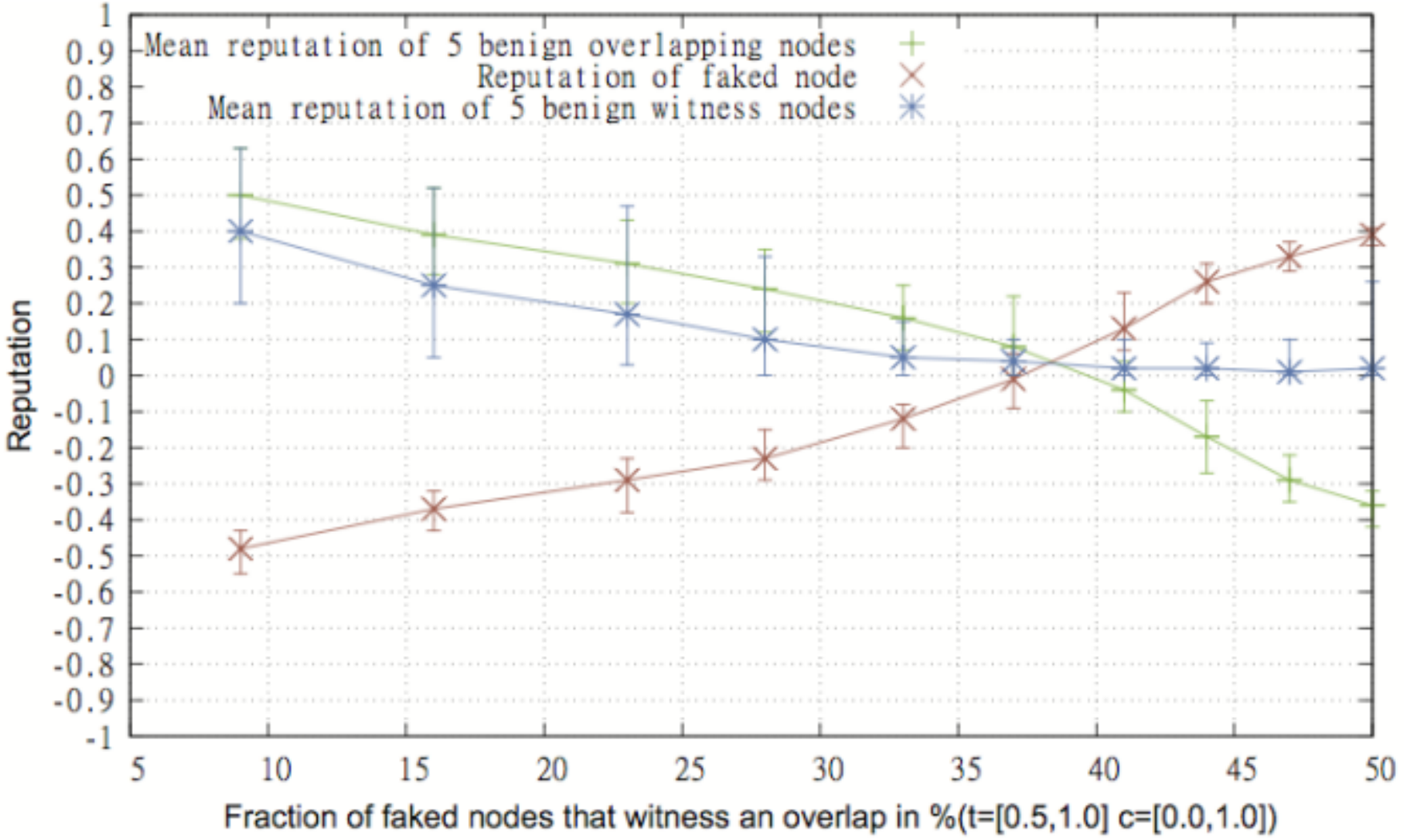
Evaluation

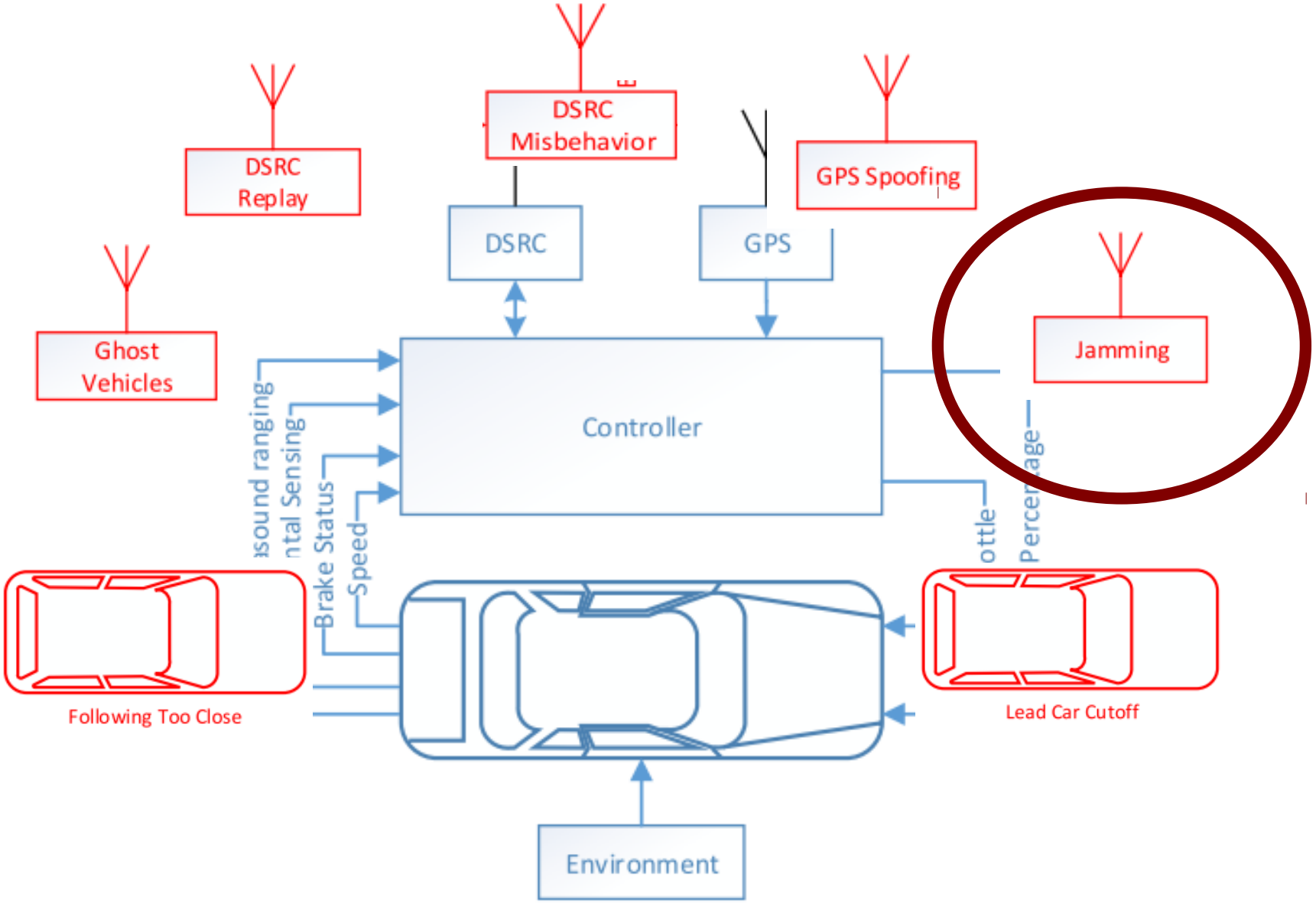


Evaluation



Evaluation

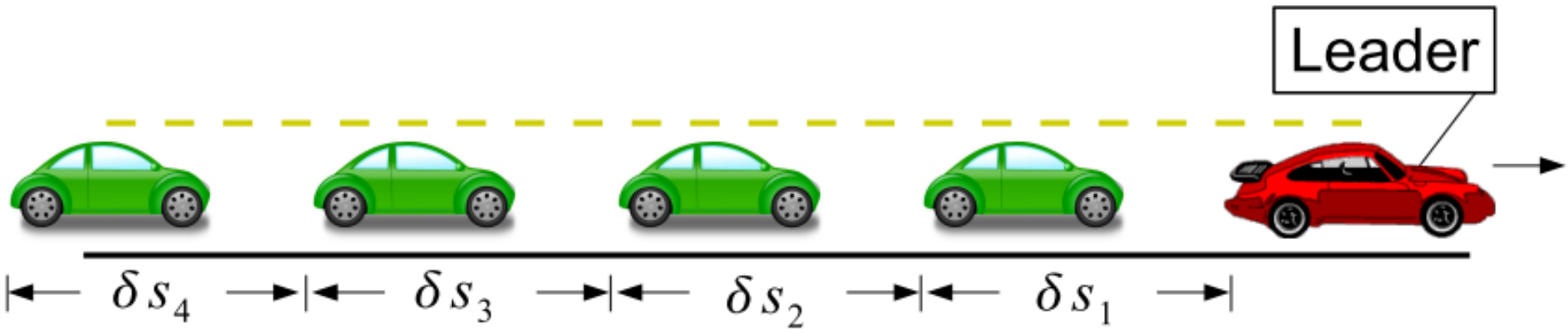




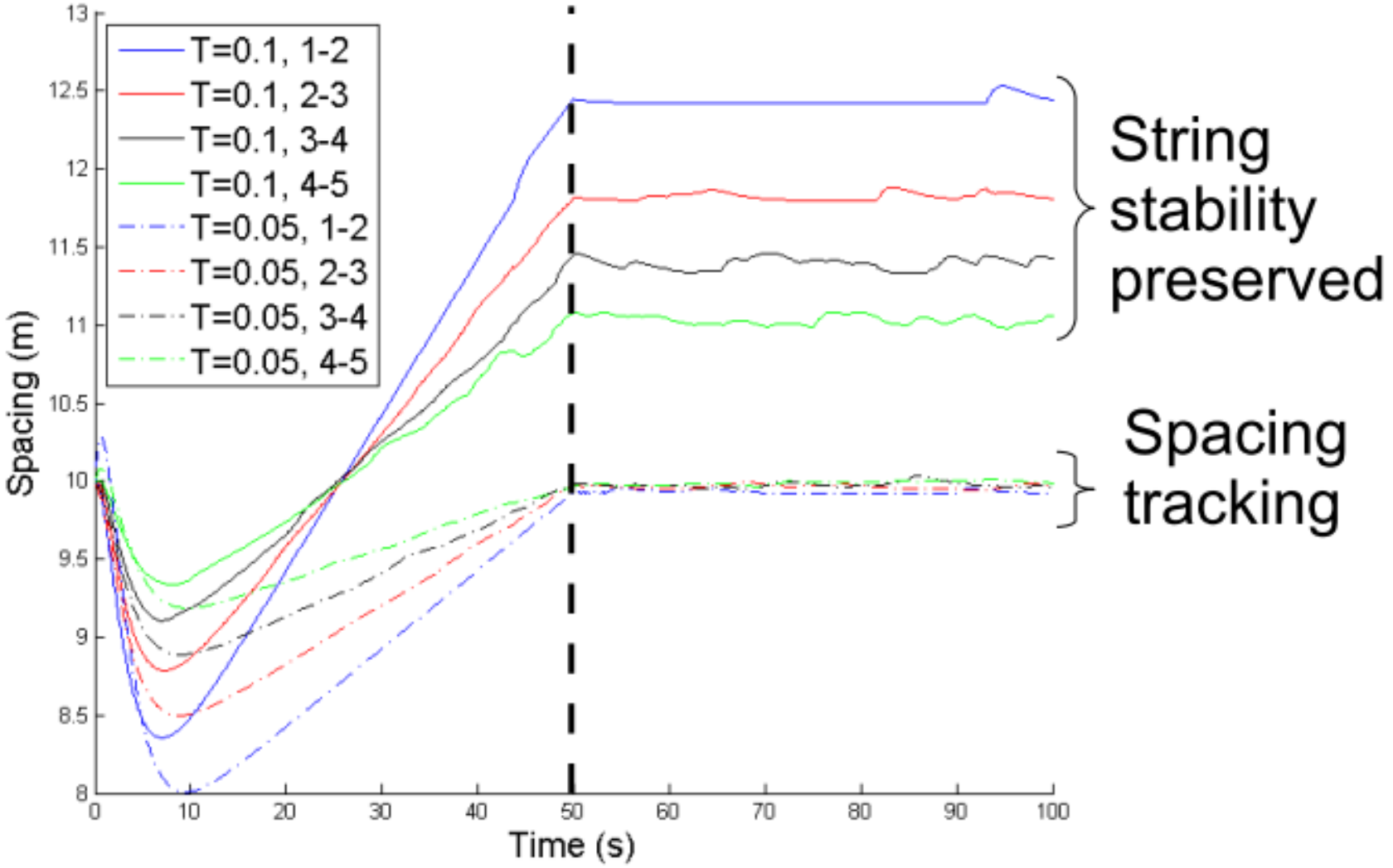
[Some slides courtesy of Jason Haas]

DSRC Evaluation

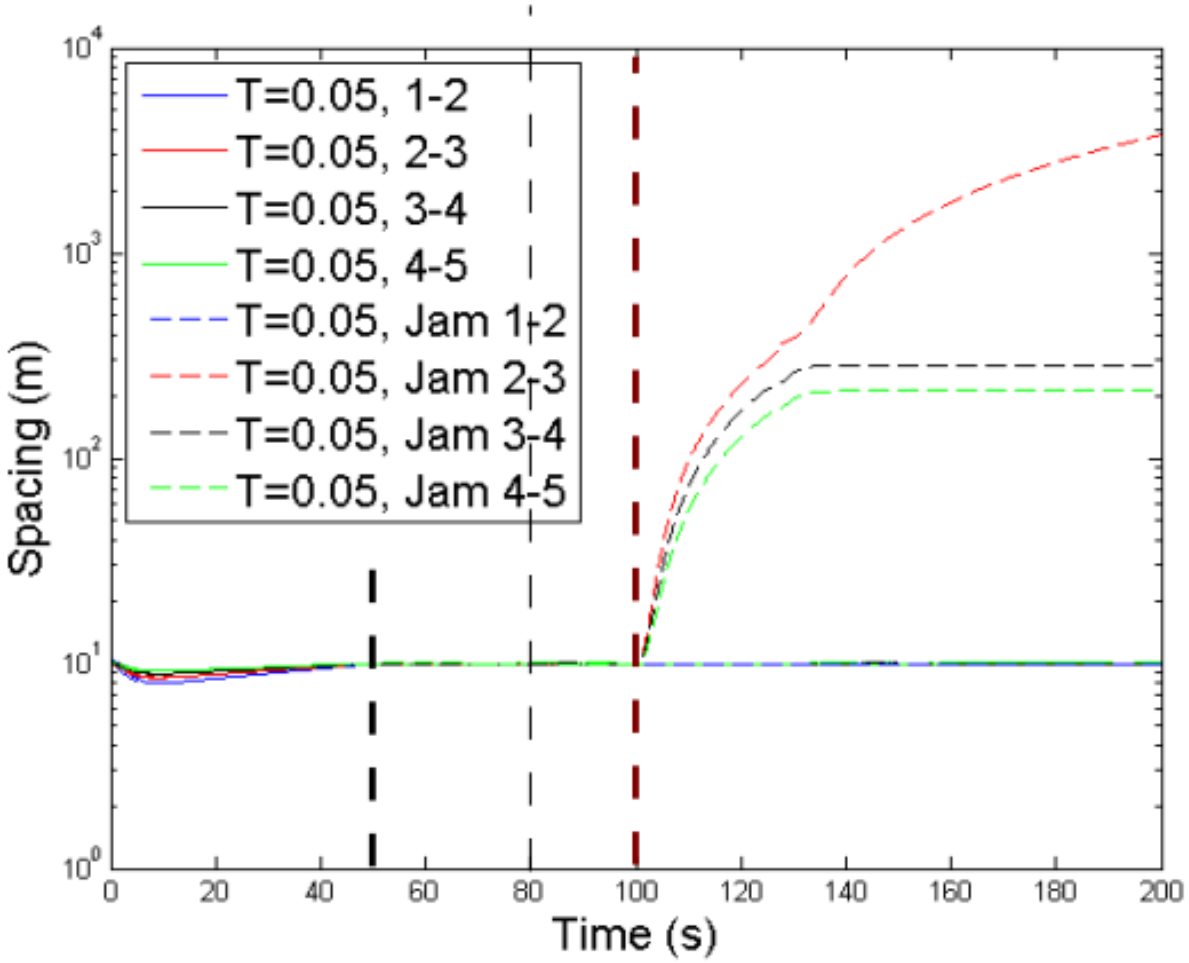
- UIUC DSRC Simulator: accurate modeling of vehicular networking environment
  - 5 vehicles: 1 leader, 4 followers
  - 10m ideal and initial spacing
  - Lead vehicle accelerates at 1 m/s^2
- Compare control (no failure) to jamming scenario
  - Attacker knows preceding vehicle's state



Control (No Jammer)



Effect of Jammer

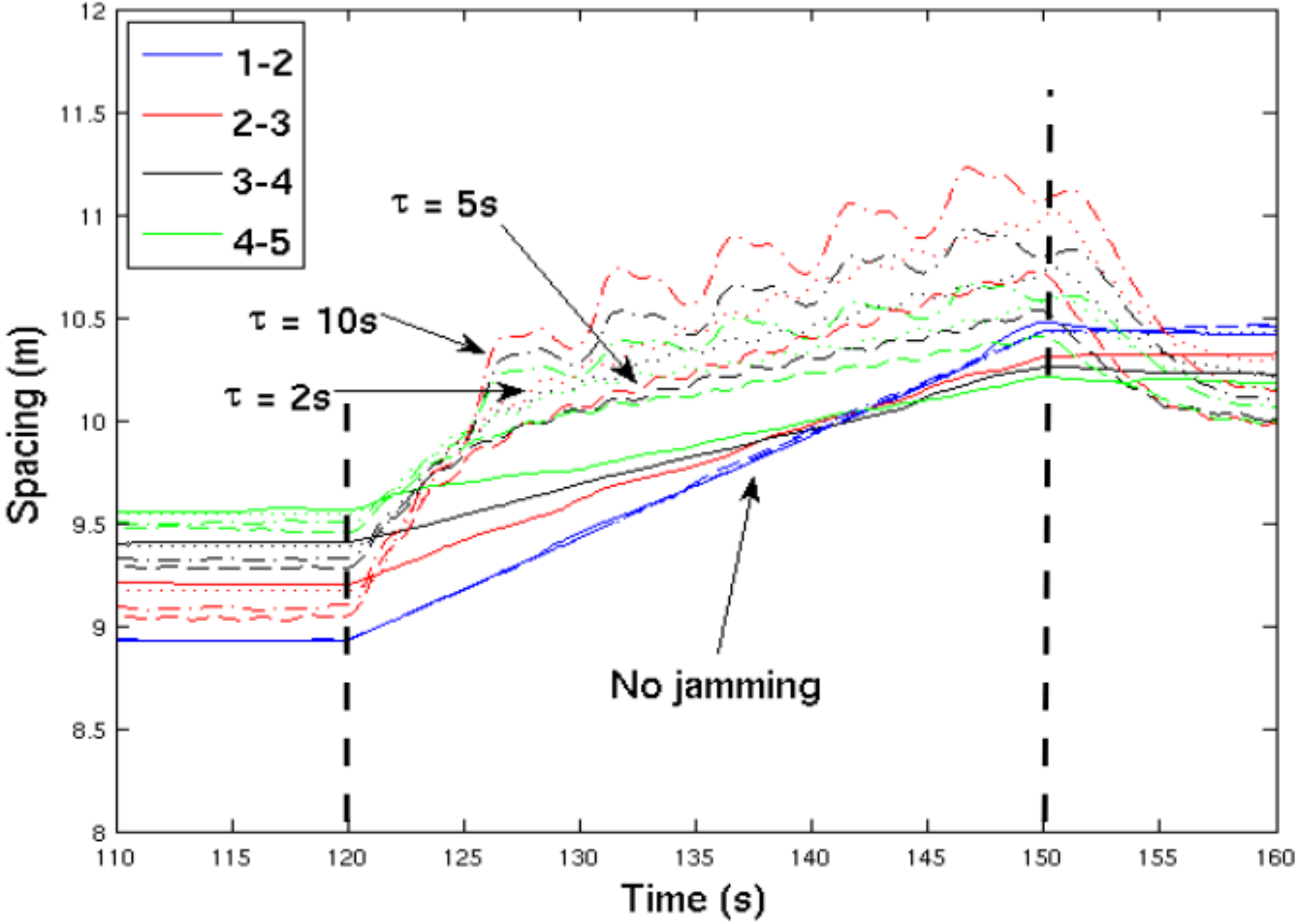


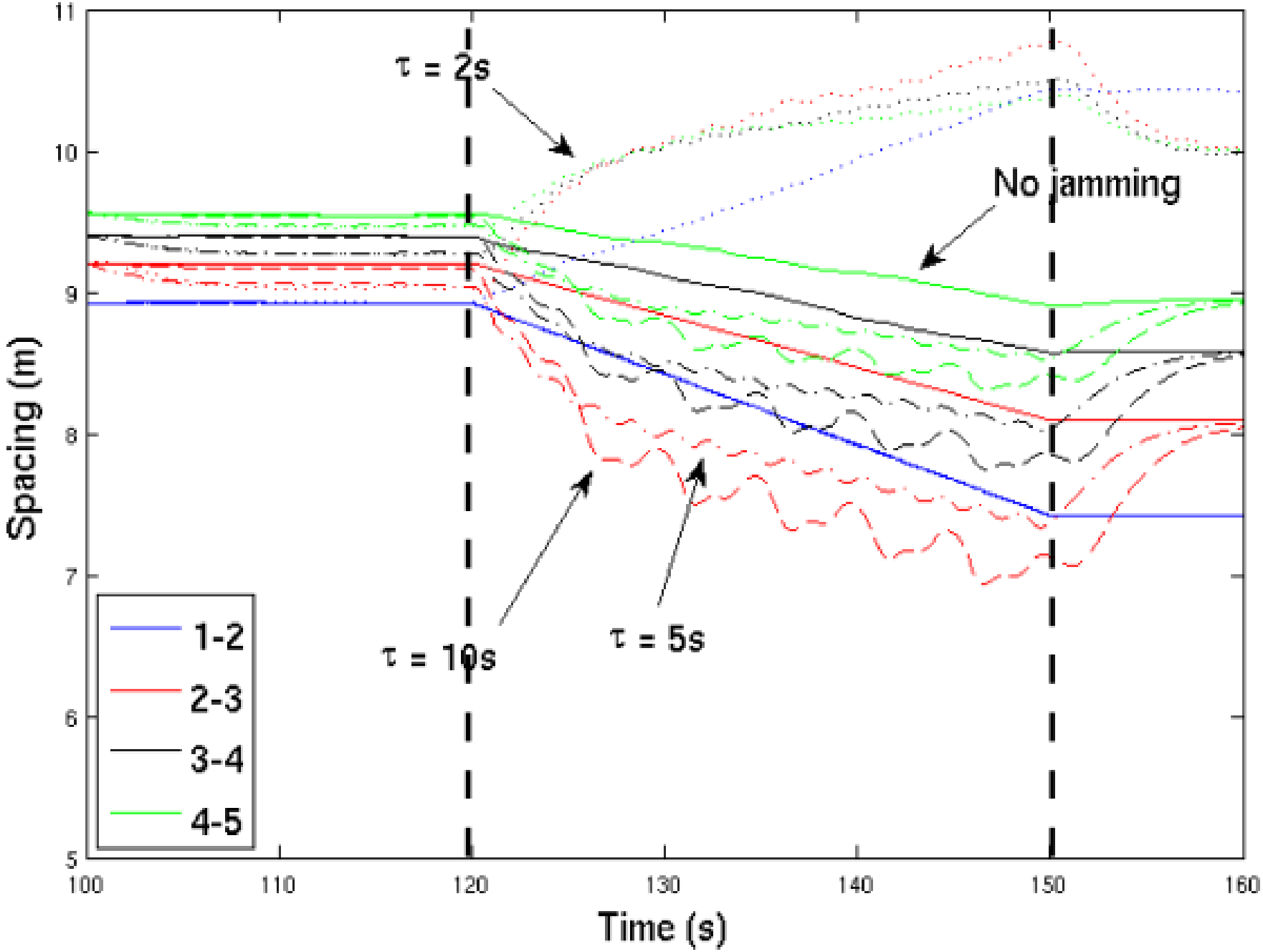
- DSRC position broadcast at 20 Hz
- Leader speed limit: 50 m/s
- Jammer turns on at 100s

Pretty easy to detect

More Interesting Jamming

- New jammer strategy: jam during acceleration
  - 50% duty cycle, variable period in {2, 5, 10}s
  - Jammer turns on at 100s
- More interesting lead vehicle behavior as well:
  - Starts at 30m/s
  - Accelerate/decelerate at 1m/s^2 from 120-150s





What about privacy issues in vehicular networks?

Vehicular Network Privacy

- Everything we talked about previously regarding network privacy applies to vehicles

- However, vehicles have many wireless subsystems combined into a single platform
  - Several wireless identities (DSRC, WiFi, LTE, TPMS, etc.) and non-wireless identities being used (license plate number, visual identity, etc.)
  - Many apps/services operating simultaneously with different requirements
  - Identity/pseudonym management may need to consider all of these jointly, consider many trade-offs

Conclusions

- Some of the most fundamental threats / misbehaviors in wireless have serious and sometimes unpredictable effects on vehicles

- Open problem: how to design vehicle controllers that are robust to wireless threats? … wireless protocols that provide guarantees for vehicle control?

Apr 12:
IoT Security & Privacy