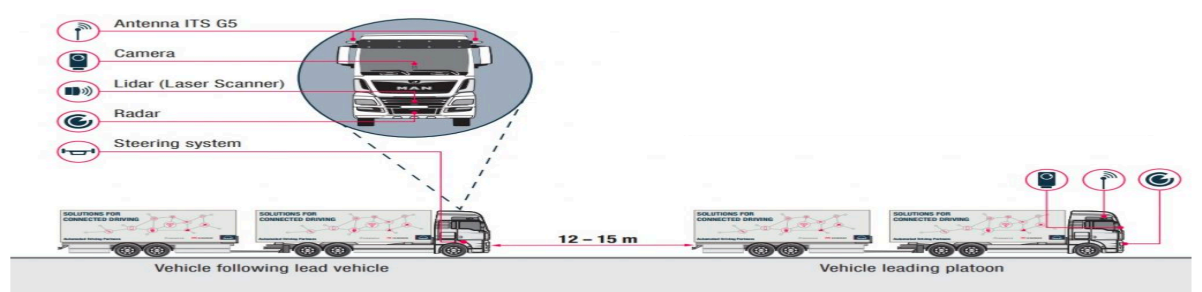
ATTACK RESILIENT STRATEGIES FOR CONTROLLER AREA NETWORKS AND TRUCK PLATOONS

KALANA SAHABANDU, ZACHARY CHEUNG, GRADUATE STUDENTS, NETWORK SECURITY LAB, UW

TRUCK PLATOONING

- Truck Platooning is a line of trucks following a leader while maintaining a smaller gap between each truck.
- Examples of current truck platooning projects are:
  - California PATH - United States
  - KONVOI – Germany
  - Energy ITS - Japan

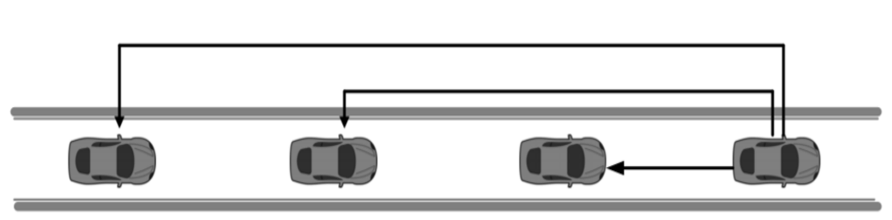


MOTIVATION FOR TRUCK PLATOONING

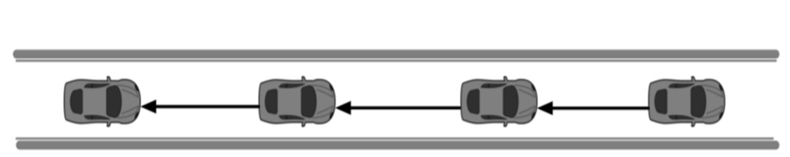
- There are three reasons why truck drivers would consider Platooning:
  - **Environmental** Perspective - Platoons save fuel and put out less emissions into the atmosphere.
  - **Social** Perspective – Platoons reduce roadway congestion and increase pipeline capacity per lane.
  - **Truck Driver's** Perspective – Platoons are safe and comfortable to ride in.

CURRENT COMMUNICATION TECHNOLOGIES

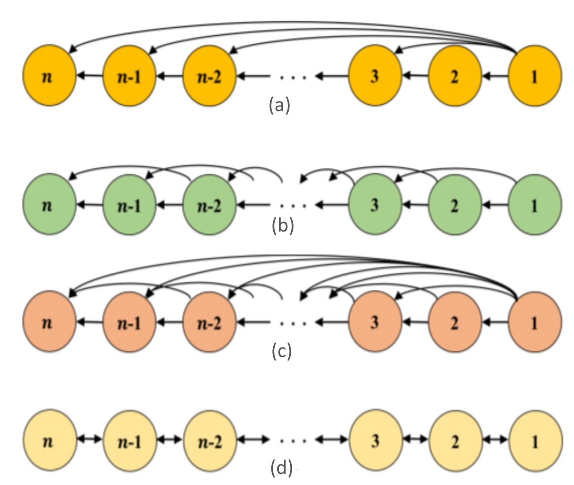
1. **802.11p Wireless Communication:**
   - Extension for 802.11 for Local Area Networks (WLANs) providing wireless communications in Vehicular Environments.
   - Optimized for data-exchange between high speed vehicles and between roadside infrastructures.
   - Bandwidth can vary between 5.8 – 5.925 GHz
2. **Secondary Wireless Communication:**
   - Infrared or Visible Light Communication can be used to improve the robustness of the communication in the event of failures with the primary wireless communication.
3. **Adaptive Cruise Control (ACC) and Cooperative Adaptive Cruise Control (CACC):**
   - ACC is a form of vehicle control that manages the velocity, acceleration, and brakes of a vehicle according to the sensor measurements of what is in front of the vehicle.
   - CACC: combination of ACC with 802.11p Wireless Communication that allows data of velocity, acceleration, and brakes to be directly shared between vehicles and improve string stability.
4. **Sensors for Detection:**
   - RADAR
   - LIDAR
   - Ultrasonic
   - Cameras



Centralized Topology



De-centralized Topology

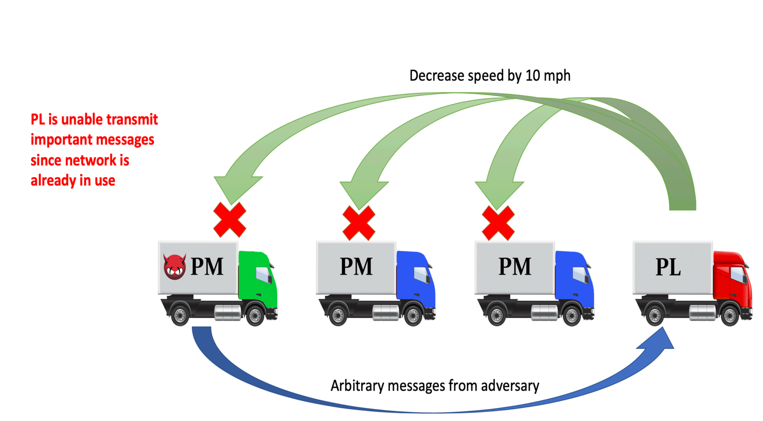


Hybrid Topology Models:
a) Predecessor-leader following b) Two predecessor-following c) Two predecessor-leader following d) Bidirectional

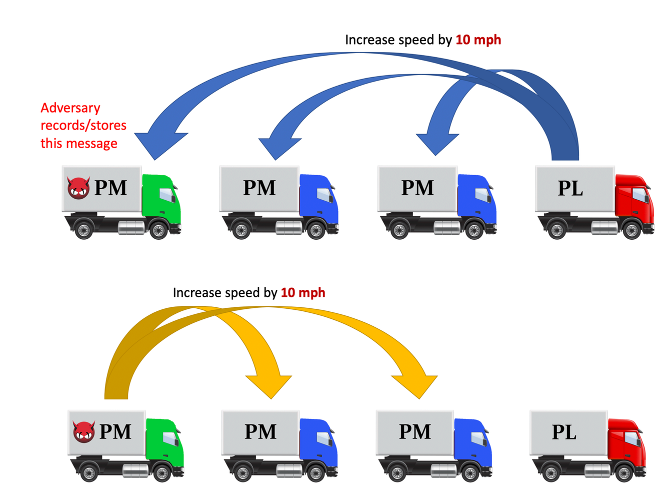
COMMUNICATION TOPOLOGIES

1. **Centralized Topology:** The Leader sends and receives messages to all members of the platoon.
2. **Decentralized Topology:** The Leader sends and receives messages to the follower behind it and the message is propagated throughout the line of platoon members.
3. **Hybrid Topology:** A combination of the Centralized and Decentralized Topology.
   a) Predecessor-leader following
   b) Two predecessor-following
   c) Two predecessor-leader following
   d) Bidirectional

TRUCK PLATOONING RISKS



Denial of Service (Dos) Attack



Replay Attack

- There are two categories of risks involved when being a part of a Truck Platoon:
  - **Communication Risks:**
    - Jamming attacks
    - Message Falsification attacks
    - Sybil attacks
    - Replay Attacks
    - Denial of Service (DoS) attacks
  - **Physical Risks:**
    - Intra-Platoon gap reactions to unexpected events:
      - Small gaps pose large risk when a potential collision occurs
      - Large gaps can be interrupted by other drivers and reduce fuel economy
    - Hardware Failures:
      - Sensors and Controllers such as ECUs can fail and stop unexpectedly
      - Mechanical components such as the brakes, engine, and tires wear out over extended usage, especially over long distances.
    - Responsible Leader Selection for managing the platoon
      - A suitable leader must be chosen who can lead a platoon to its destination and manage communication and information between all vehicles.

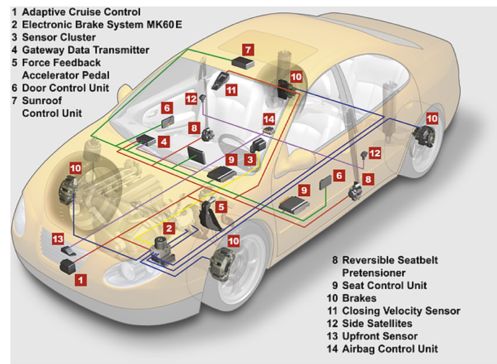
OUR CONTRIBUTIONS AND RESEARCH

- We performed more research on existing leader selection algorithms and systems as there is currently not much sufficient information about the subject.
  - Leader Selection is important to ensure the safety of the platoon and reduce emissions and increase fuel efficiently.
- We simulated Truck Platoons using VENTOS, an open-source traffic simulator
  - Various Platoon scenarios can be simulated with different kinds of road structures and vehicles.
  - Speed, Acceleration, Intra-Platoon Gap, Emissions, and other valuable data can be acquired at each time step of the simulation.

NEED FOR CAN BUS SECURITY

<u>**Motivation for CAN bus security**</u>:

- CAN bus connects in-vehicle Electronic Control Units (ECUs)
- Developed for closed networks – **NO encryption or authentication**.
- Addition of outward-facing ECUs violate the closed network assumption and introduce cyber vulnerabilities.
- **Intrusion Detection System** (IDSs)


In-vehicle CAN bus.

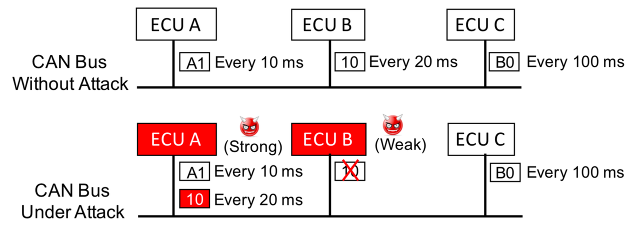
<u>**Main contributions:**</u>

- We propose the **cloaking attack** that bypasses an IDS' detection.
- We **analyze and formally model** the attack success probability of the cloaking attack on both the State-of-the-Art (SOTA) and the Network Time Protocol (NTP)-based clock skew-based IDSs.
- We **demonstrate and evaluate our attack** on hardware testbeds.

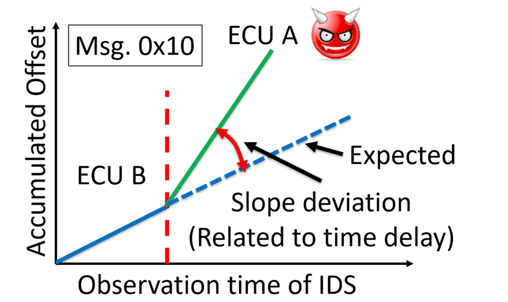
ATTACK SCENARIOS

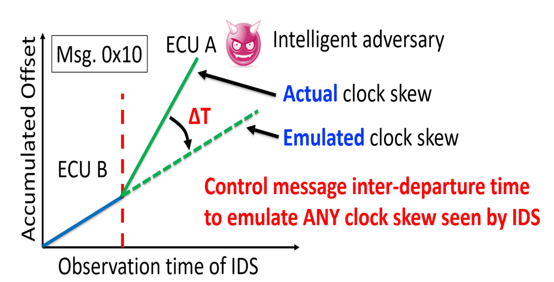
<u>**We consider an adversary who can**</u>

- Physically/remotely compromise one or more in-vehicle ECUs.
- Stop legitimate messages – **suspension attack**,
- Inject spoofed messages – **fabrication attack**,
- Both at the same time – **masquerade attack**.



CLOCK SKEW-BASED IDS AND CLOAKING ATTACK





<u>Key observations</u>:

- Local clocks have **distinct clock skew** - difference in frequency.
- CAN messages are periodic.
- Clock skew can be estimated via message inter-arrival times.
- **Clock skew-based IDS**.

<u>Strategy of cloaking attack</u>:

- Compromise the victim ECU; change the period of the spoofed message from every T sec to **every (T+ΔT) sec** to match the victim's clock skew.

REFERENCES AND SPONSORS

[1] S. Checkoway, et al., "Comprehensive experimental analyses of automotive attack surfaces," in Proceedings of the 20th USENIX Conference on Security, ser. SEC'11. Berkeley, CA, USA, , 2011, pp. 6–6.
[2] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in 25th USENIX Security Symposium (USENIX Security 16). Austin, TX, 2016.
[3] S. Sagong, X. Ying, A. Clark, L. Bushnell and R. Poovendran, "Cloaking the Clock: Emulating Clock Skew in Controller Area Networks". 9th ACM/IEEE ICCPS 2018, Porto, Portugal. (**Best Paper Finalist**)
[4] X. Ying, S. Sagong, A. Clark, L. Bushnell and R. Poovendran. "Shape of the Cloak: Formal Analysis of Clock Skew-Based Intrusion Detection System in Controller Area Networks". IEEE Transactions on Information Forensics and Security, 2019.

ELECTRICAL & COMPUTER ENGINEERING
UNIVERSITY of WASHINGTON

ADVISORS: RADHA POOVENDRAN, LINDA BUSHNELL

COLLABORATORS: ANDREW CLARK (WPI), SANG UK SAGONG (UW), XUHANG YING (UW)

SPONSORS: NATIONAL SCIENCE FOUNDATION (NSF), OFFICE OF NAVAL RESEARCH (ONR), ARMY RESEARCH OFFICE (ARO)