Linking2Source: Security of In-Vehicle Networks via Source Identification

Challenge:

Protecting connected and autonomous vehicles, which utilize the traditional in-vehicle networks (e.g., CAN, LIN, etc.), against ever-expanding attack surfaces is a challenging problem.

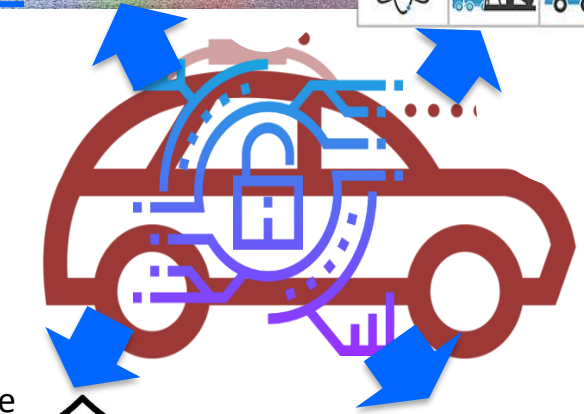
Scientific Impact:

- Robust, reliable and real-time attack detection, localization, and prevention.
- Proposed solutions are extendable beyond the automotive application domain, e.g., aviation.

Solution:

A layered framework to mitigate cyber-attacks on IVNs using

- **physical fingerprinting** to link the in-vehicle network packets to "the" transmitting ECU;
- **behavioral fingerprinting** to detect deviations in the network traffics due to the compromised ECU(s);
- **vehicle physics** to safeguard against sensing/actuation layer attacks by detecting misbehaviors – which may be caused by cyberattacks, device faults, and external disturbances.



Broader Impact and Broader Participation:

- Broader impacts are envisioned in several areas, including automotive cybersecurity, CPS security, smart infrastructure, and sensor integrity verification.
- The UM-Dearborn CyberAuto Challenge aims at filling the growing shortfall in the trained workforce in cybersecurity.

Project Info.: Award # CNS-2035770

Hafiz Malik (PI) & Alireza Muhammadi (Co-PI) University of Michigan-Dearborn, MI, Email: {hafiz, amohmmad}@umich.edu