Security of Distributed Cyber-Physical Systems with Connected Vehicle Applications

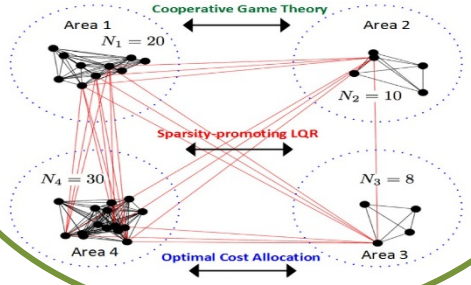
PI : Dr. Pierluigi Pisu
Automotive Engineering Department (CUICAR)
Clemson University
Co-PI : Dr. Richard Brooks
Electrical and Computer Engineering Department
Clemson University
Co-PI : Dr. Jim Martin
School of Computing
Clemson University

CNS-1544910

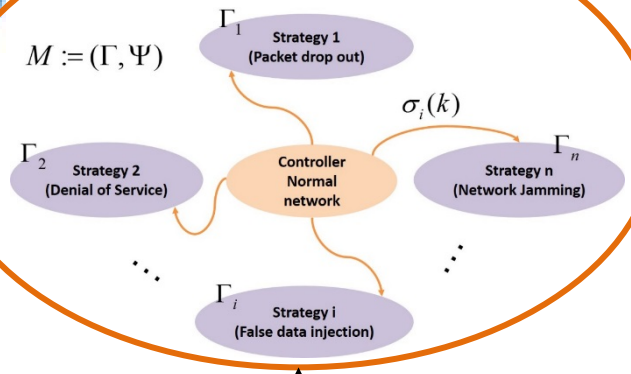
Project introduction

Distributed CPS

Game Theory Approach



Reconfigurable Control



Risk Analysis

Cyber-attack identification
Attack modeling scenarios

Hybrid Observer
&
Active Attack Detection

Problem Statement

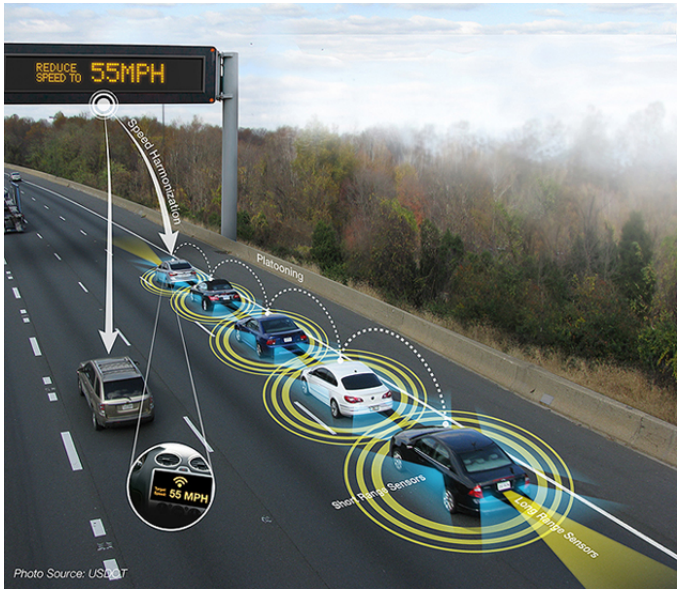
Cooperative ACC (CACC)

❑ Advantages

- ➢ Short following distance
- ➢ Increasing the string stability
- ➢ Fast response to the preceding vehicle
- ➢ Increasing traffic throughput

❑ Issues

- ➢ Communication network failure
- ➢ Cyber-attacks
- ➢ Physical failures



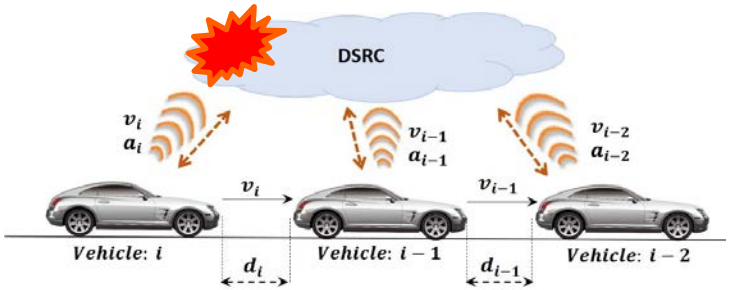
Denial of Service (DoS) Attack

- ➢ Attacker provides several requests to access the network. Therefore, communication network will be busy for real requests
- ➢ Average service time of network increases to transmit a package
- ➢ Denial of Service is not deterministic

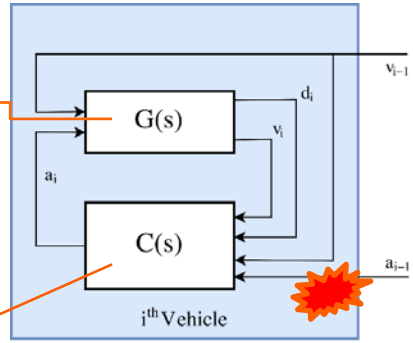
Packet Dropping

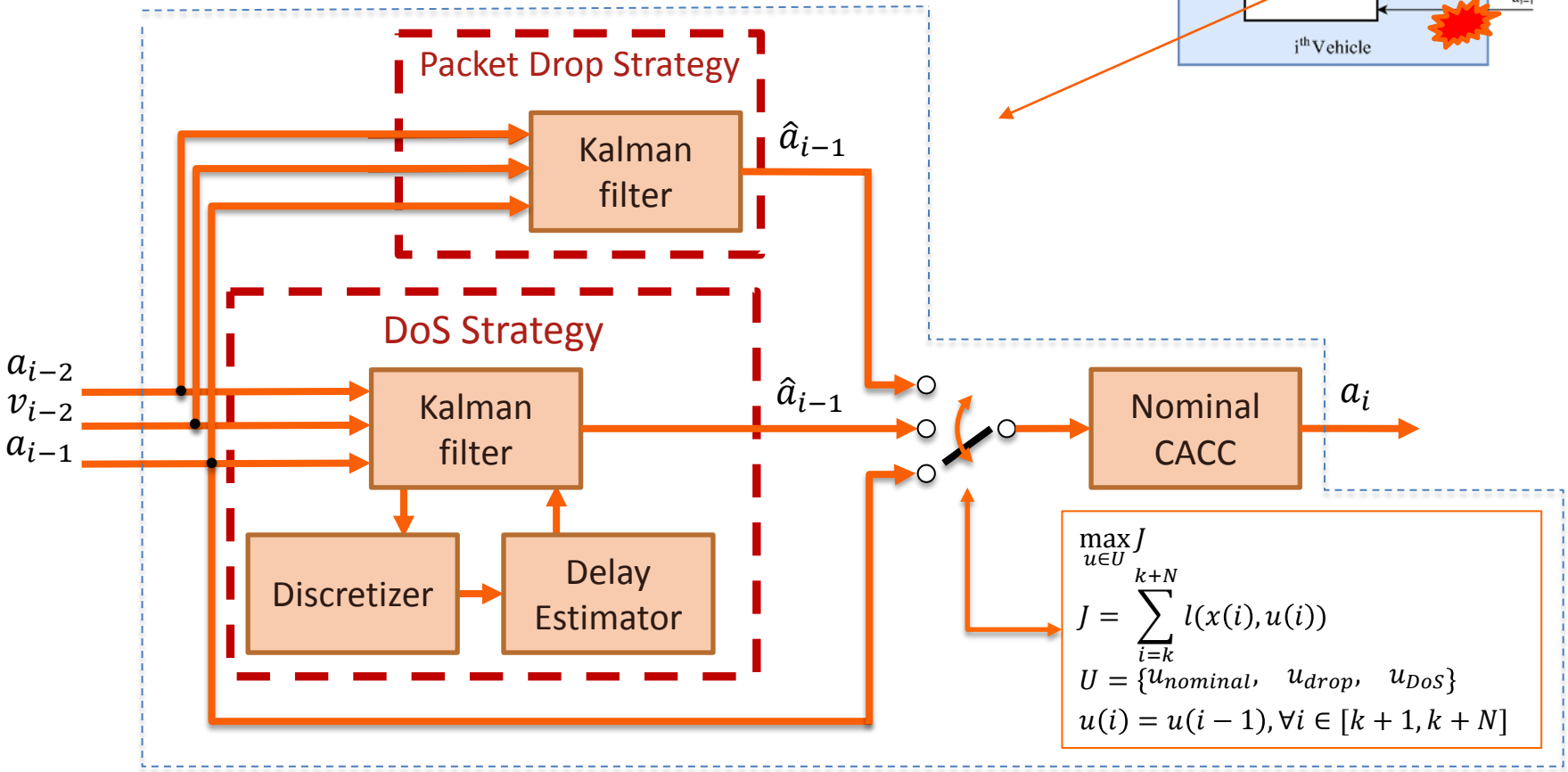
- ➢ Data is transmitted over communication network with limited bandwidth → intermittent packet dropout occurs
- ➢ Losing information
- ➢ Packet drop out is not a deterministic event

Proposed Diagnostics Scheme



G(s) : Vehicle dynamic





Z.Biron, S. Dey, P.Pisu, "Sensor Fault Diagnosis of Connected Vehicles under imperfect Communication Network", DSCC 2016

Z.Biron, S. Dey, P.Pisu, "On Resilient Connected Vehicles under Denial of Service", ACC 2017

G.Savaglia, Z.Biron, P.Pisu, "A Receding Horizon Switching Control Resilient to Communication Failures for Connected Vehicles", DSCC 2017

Simulation Results

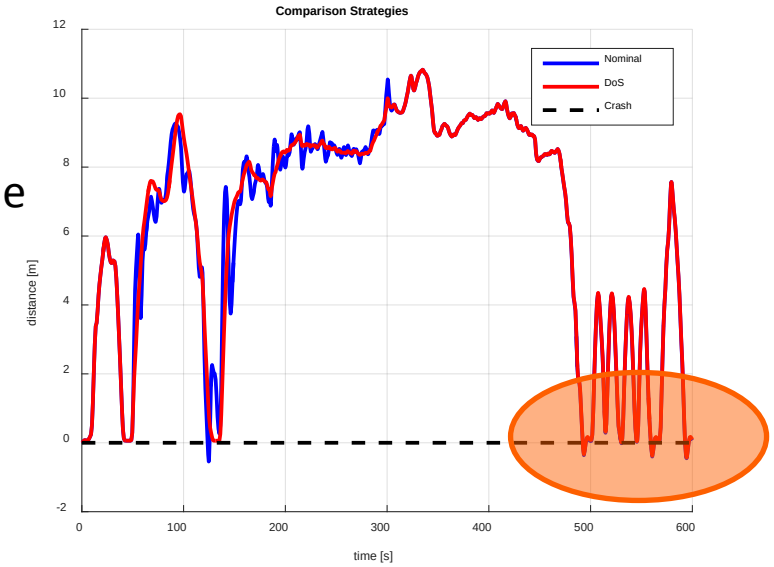
Ad Hoc Strategies

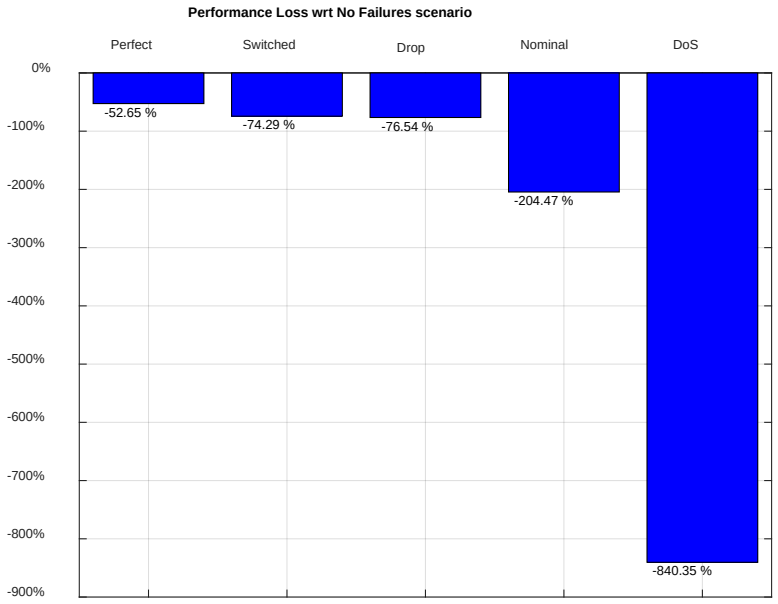
Each strategy can only tackle the correspondent attack, whilst it fails in avoiding crashes during the other.

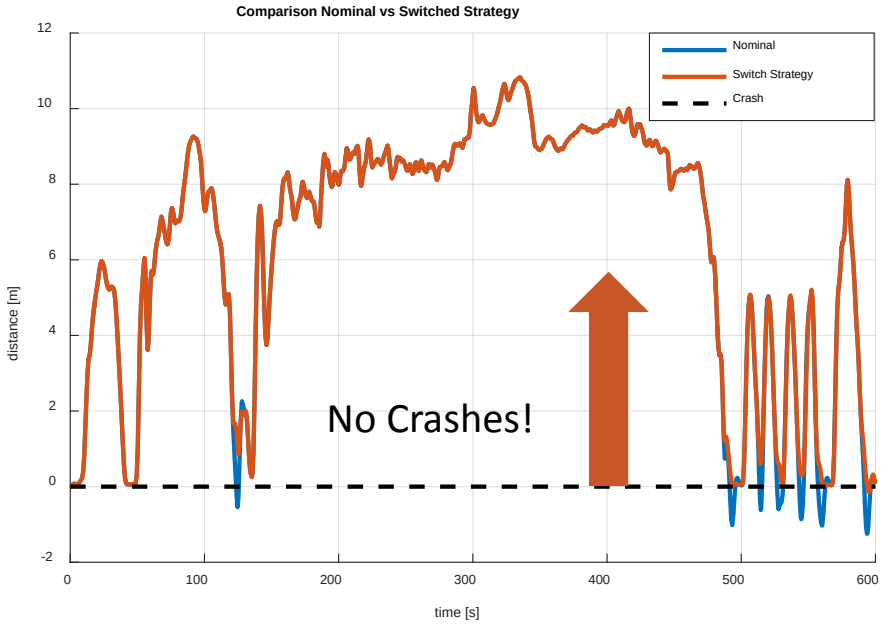
DoS : $50 < t < 300$

Packet Drop : $400 < t < 600$

RMS of jerk is used as comfort performance index







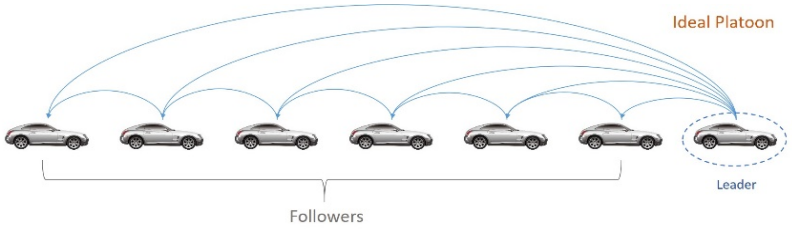
False Data Injection (Ghost Vehicle)

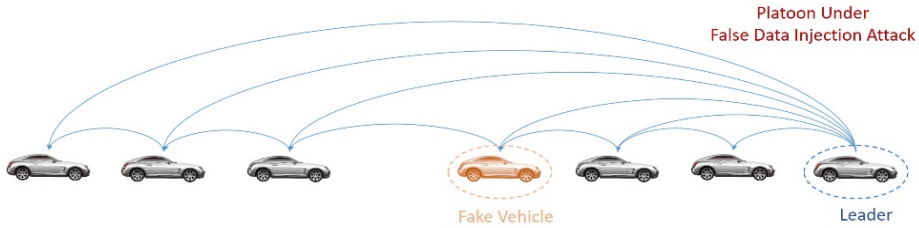
False Data Injection attack is considered as fake vehicles in the platoon of connected vehicles

Vehicles are equipped with CACC strategy and the observer to detect the place of fake vehicles is implemented into the leader of the platoon

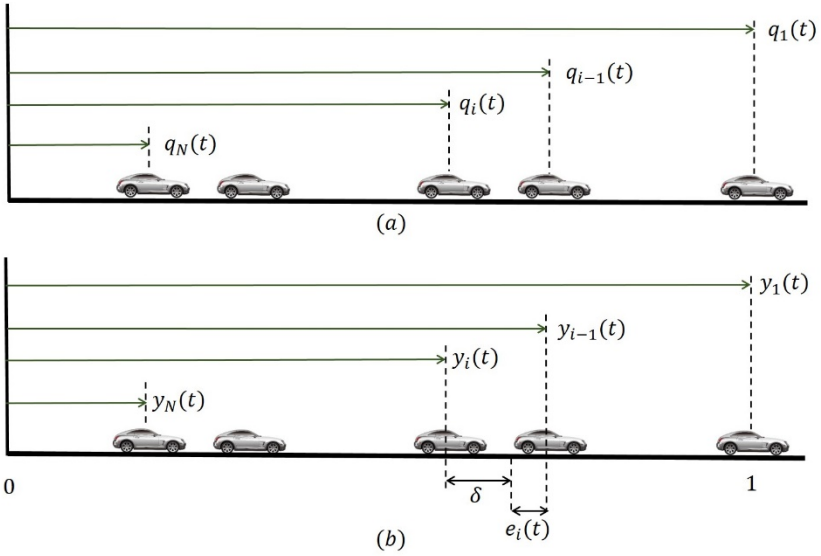
PDE model of the platoon of vehicles eases the health monitoring and analysis

Objective
Detect ghost vehicle injection in the platoon of connected vehicles as false data injection attack





PDE modeling of a platoon of connected vehicles



$$v_t(x,t) = u(x,t)$$

$$\bar{\rho}_t(x,t) = -\rho_0 v_x(x,t)$$

$$u_t(x,t) = \frac{1}{h\rho_0}u_x(x,t) - \frac{k_p}{\rho_0^2}\bar{\rho}(x,t) + \frac{k_d}{\rho_0}v_x(x,t)$$

PDE based observer

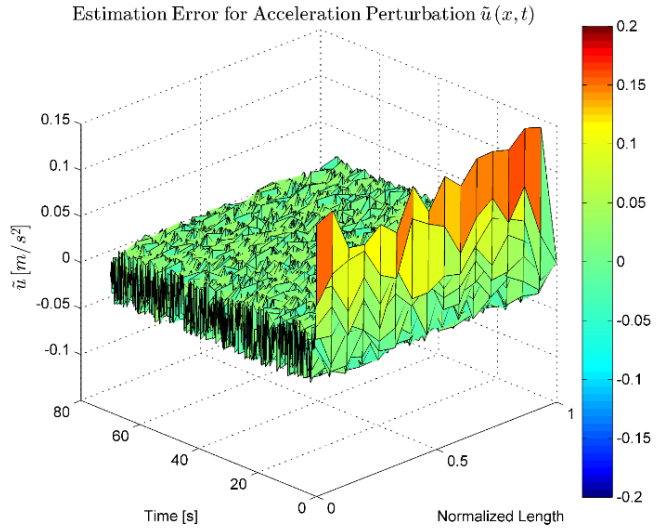
$$\hat{v}_t(x,t) = \hat{u}(x,t) + L_{11}(\tilde{v}(x,t)) + L_{12}(\tilde{u}(x,t))$$

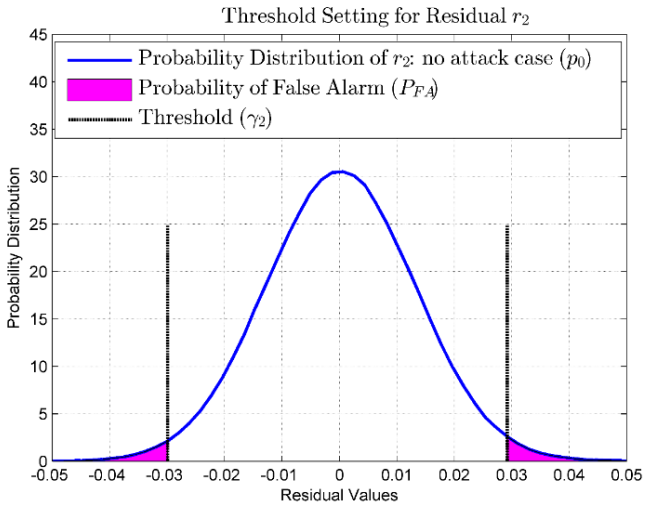
$$\hat{\bar{\rho}}_t(x,t) = -\rho_0 \hat{v}_x(x,t) + L_2(\tilde{u}(x,t))$$

$$\hat{u}_t(x,t) = \frac{1}{h\rho_0}\hat{u}_x(x,t) - \frac{k_p}{h\rho_0^2}\hat{\bar{\rho}}(x,t) + \frac{k_d}{h\rho_0}\hat{v}_x(x,t) + L_3\tilde{u}(x,t)$$

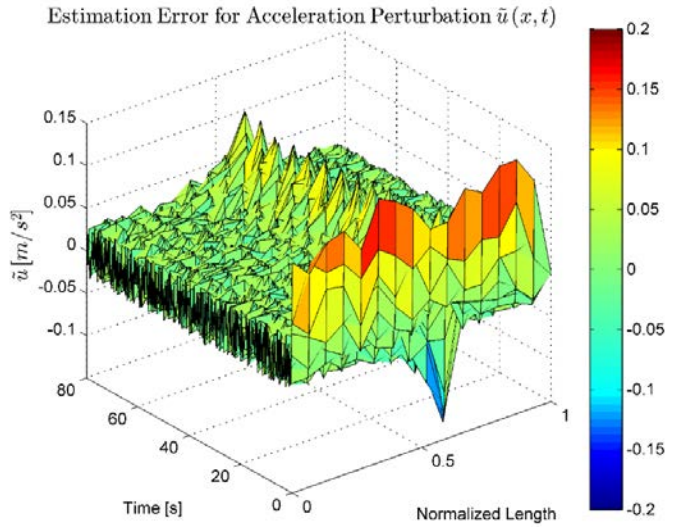
False Data Injection (Ghost Vehicle): Residuals in the Presence of Attack

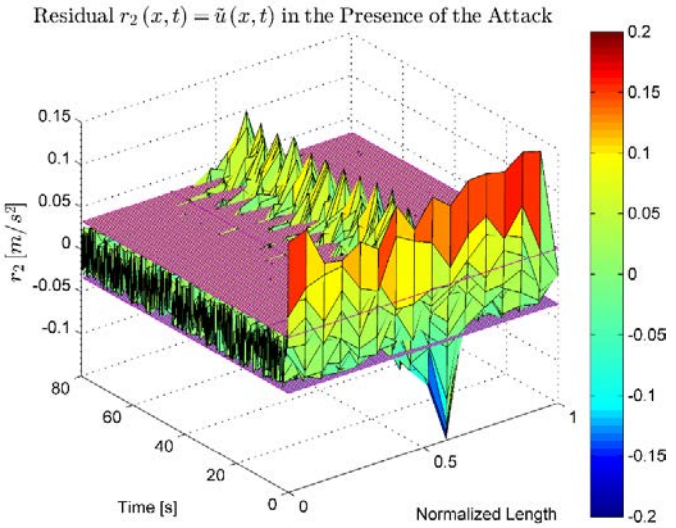
No Attack Injected





Fake Vehicle Injected

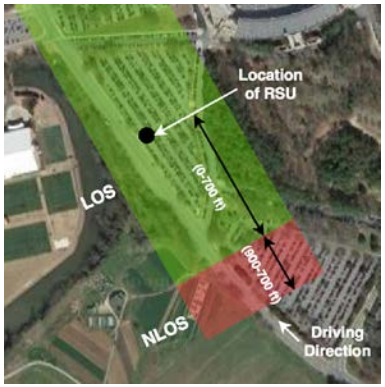


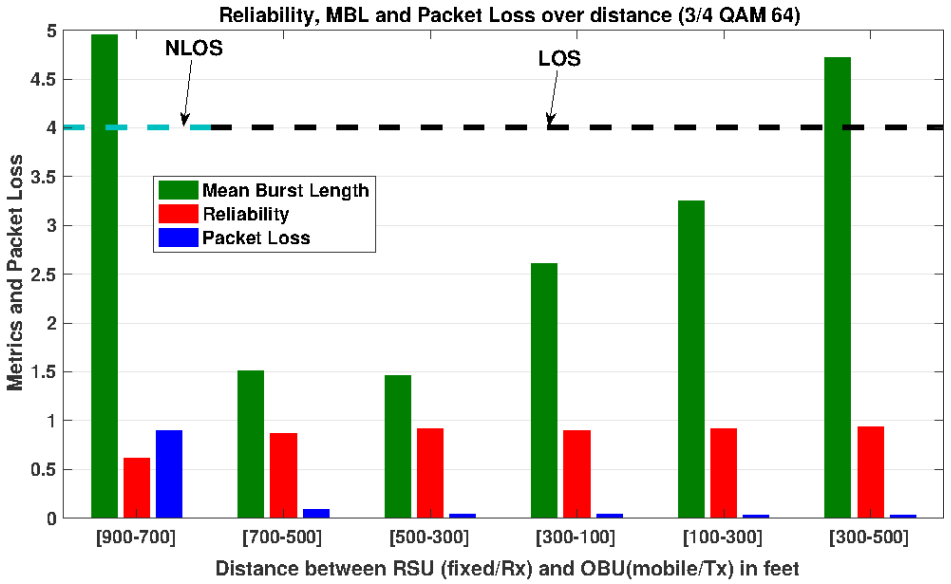


DSRC Tests performed in US-Ignite Connected Vehicle testbed located in Clemson University

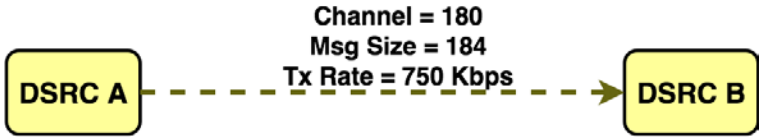
Driving through a region with No-Line of Sight before driving through a region with good Line of sight. Performance metrics:

- Reliability
- Packet Loss Rate (PLR)
- Mean Burst Length (MBL)





Denial of Service Attack on DSRC network



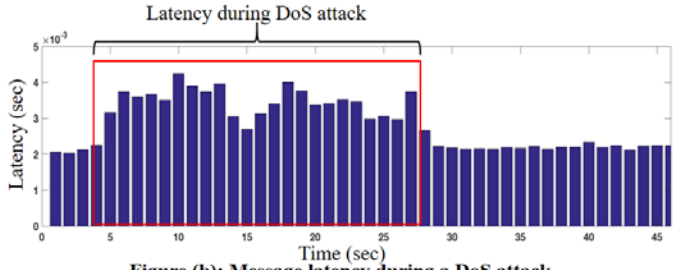
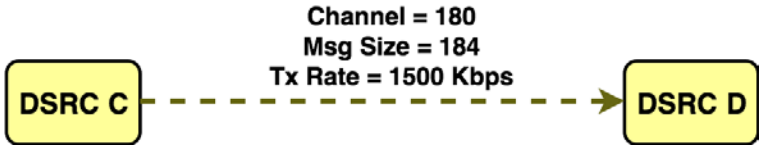


Figure (b): Message latency during a DoS attack



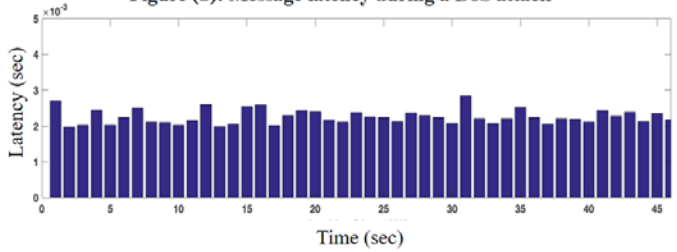


Figure (a): Base case without DoS attack

Thank you

Dr. Pierluigi Pisu

Associate Professor
Leader of the Connected Vehicle Technology Consortium

Project Leader of Deep Orange 8 and 10
Dept. of Automotive Engineering and CU-ICAR
Dept. of Electrical and Computer Engineering
Clemson University

Email : pisup@clemson.edu