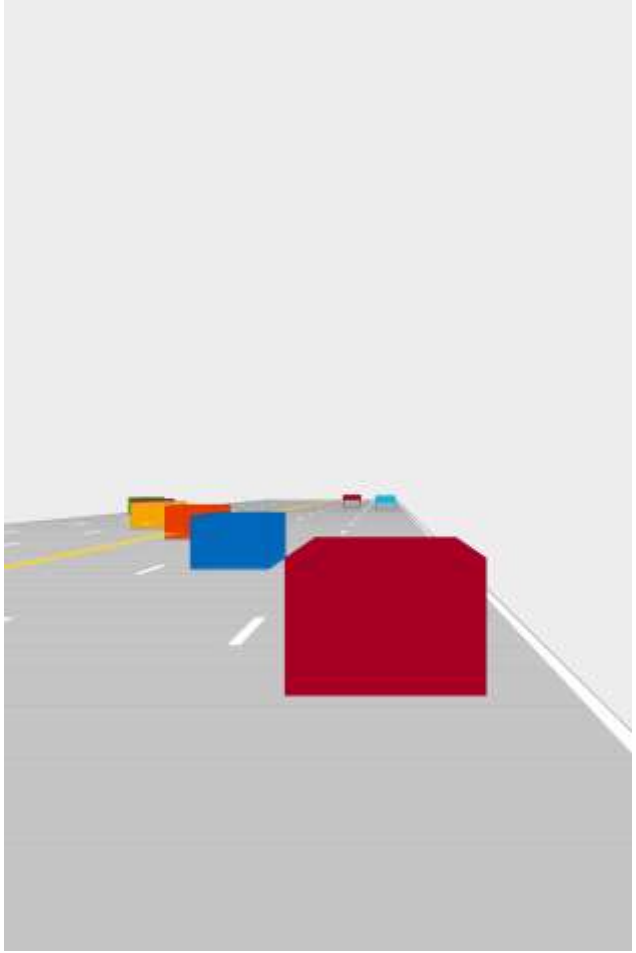
Cyber-Security for Automation: The Challenge

Virtual, 9 -10 September

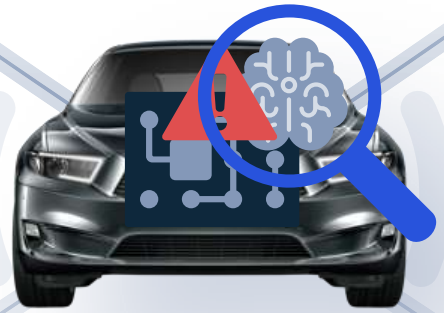
SUMMER SCHOOL 2020

Dr. Jonathan Petit
Director, Engineering

Qualcomm



Automated Vehicle: a complex threat landscape



Radar
Bad weather conditions, long range, low light situations

Camera
Interprets objects / signs, practical cost and FOV

Lidar
Depth perception, medium range

Ultrasonic
Low cost, short range

Users / Operator
Local or remote

V2X wireless sensor
See through, 360° non-line of sight sensing, extended range sensing

3D HD maps
HD live map update, sub-meter level accuracy of landmarks

Precise positioning
GNSS positioning, dead reckoning, VIO

Cloud / Edge
AI, crowdsourcing, data collection, infotainment

Process information from diverse sensors

Immense compute resources
Sensor fusion
Machine learning
Path planning

Simplified Perception Process

Attacks on Detection

https://youtu.be/C-JxNHKqgtk

https://www.youtube.com/watch?v=sNaENlLZYSo

Attacks on Detection (Evasion)

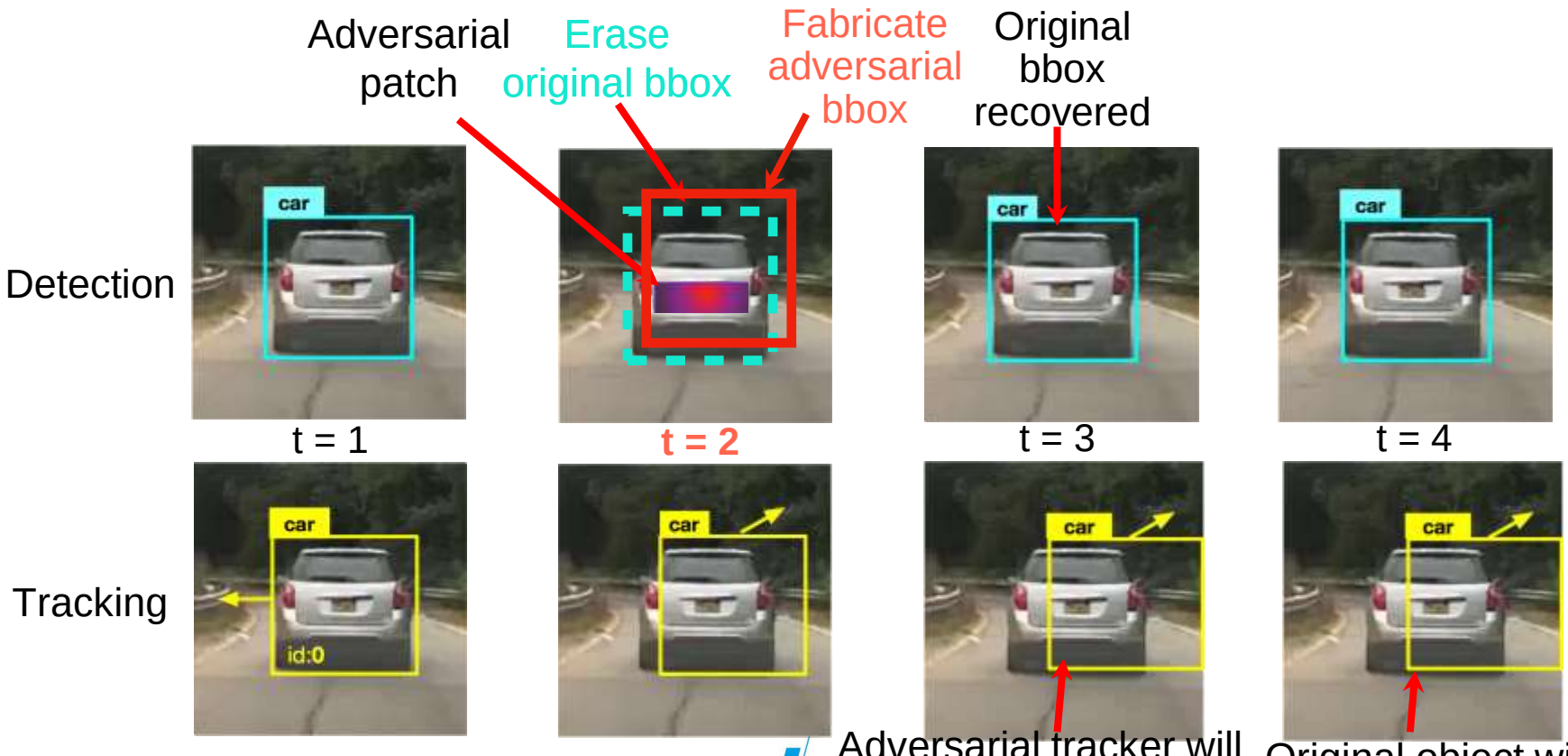
https://www.youtube.com/watch?v=GOjNKQtFs64

https://www.youtube.com/watch?v=6QSsKy0I9LE

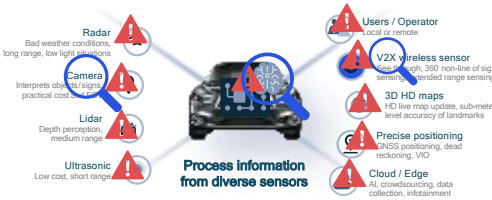
Attacks on Perception (Segmentation): Affects Optical Flow

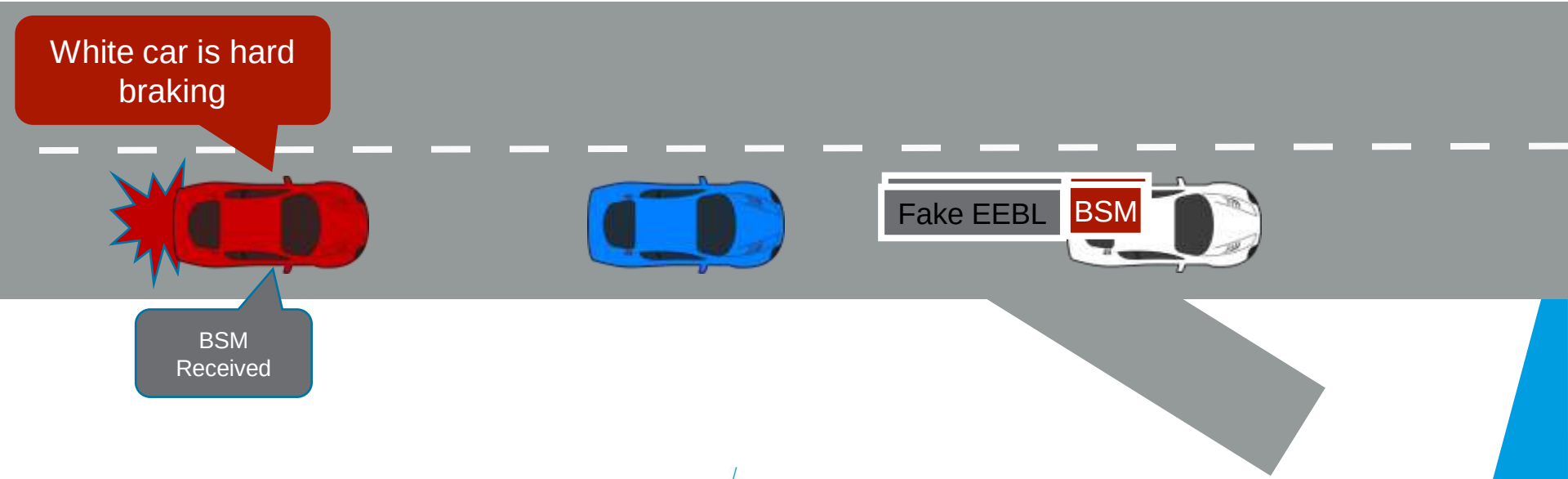
https://www.youtube.com/watch?v=FV-oH1aIdAI

Attack on Tracking [Chen et al., AML workshop CVPR'19 https://arxiv.org/pdf/1905.11026v1.pdf]



Example of V2X Misbehavior: Fake EEBL





Attacks on V2X

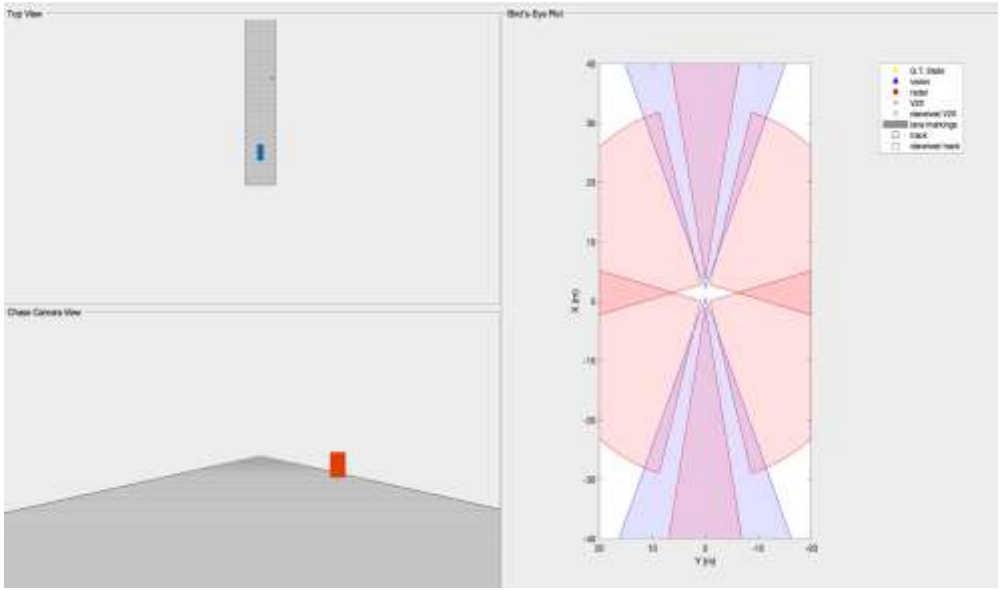
- I-SIG (left) / Position jump (right)

https://www.youtube.com/watch?v=3iV1sAxPuL0

For more detail on V2X attack: https://www.youtube.com/watch?v=xTaksVG9Qi4

Attacks on V2X (Detection and Tracking)

- Track Database Poisoning



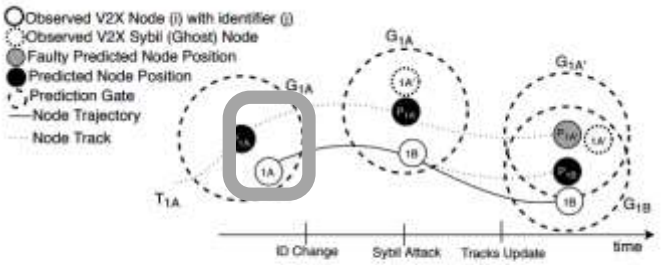
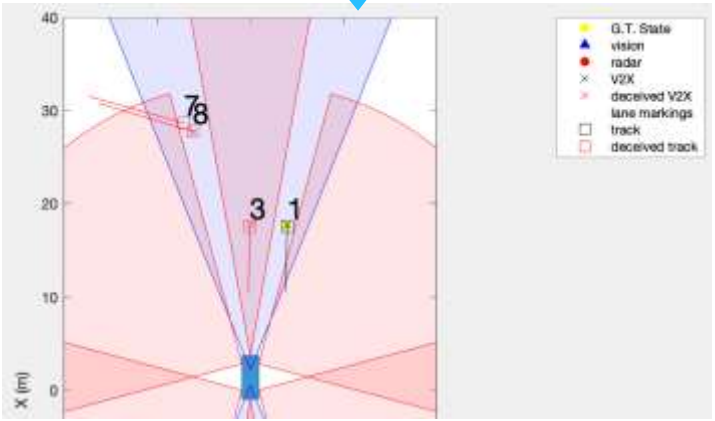
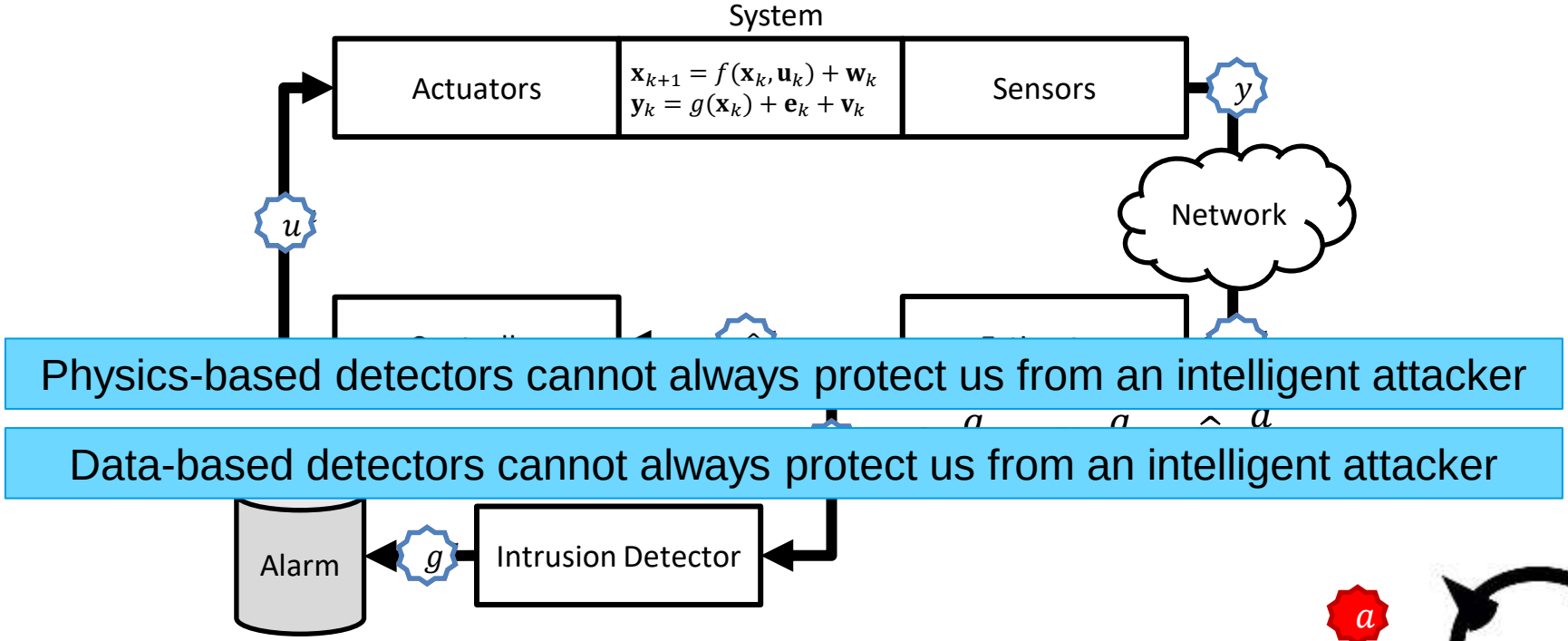


Figure 3: Tracking Poisoner



Attacks on Control

Pajic et al.,"Attack-Resilient State Estimation for Noisy Dynamical Systems" IEEE Transactions on Control of Network Systems, 2017.
Khazraei and M. Pajic, “Perfect Attackability of Linear Dynamical Systems with Bounded Noise,” ACC 2020.
A. Khazraei and M. Pajic, “Attack-Resilient State Estimation with Intermittent Data Authentication,” Automatica, submitted



Open Challenges

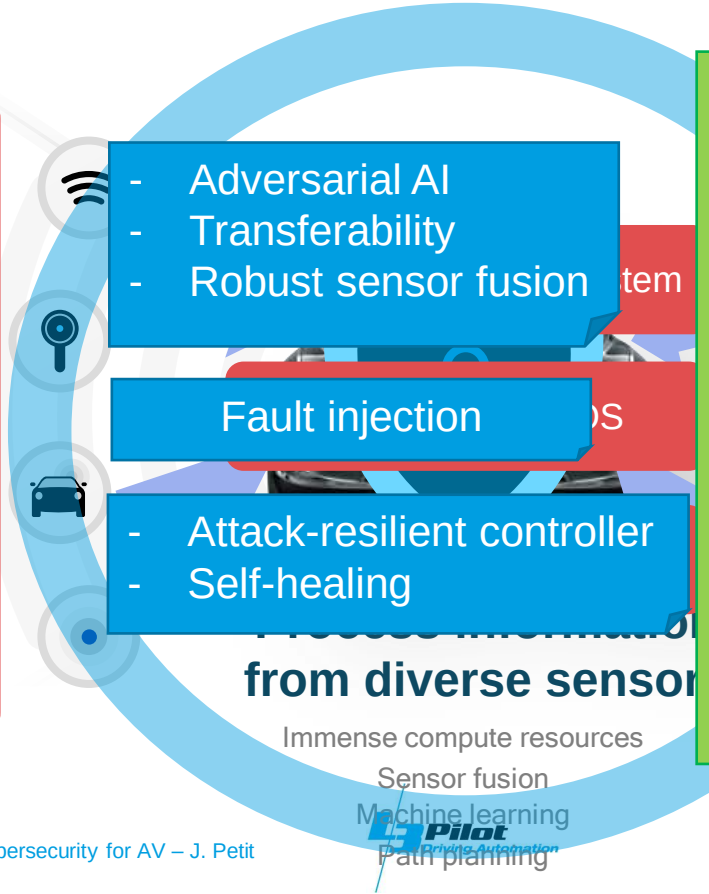
- Increase sensor confidence
- Add HSM

Resilient sensors

- Adversarial AI
- Transferability
- Robust sensor fusion

Fault injection

- Attack-resilient controller
- Self-healing



STANDARDIZATION

V2X
- Authentication / encryption: IEEE 1609.2
- Misbehavior detection and reporting: ETSI TR 103 460 (TS will start soon)

Automated Driving: n/a ☹

Automotive:
- UNECE WP.29.79
- ISO21434
- ETSI ISG Securing Artificial Intelligence

Thank you for your kind attention.

Dr. Jonathan Petit
petit@qti.qualcomm.com

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 723051.