Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
UNIVERSITÀ DEGLI STUDI DI MILANO

FORESEEN

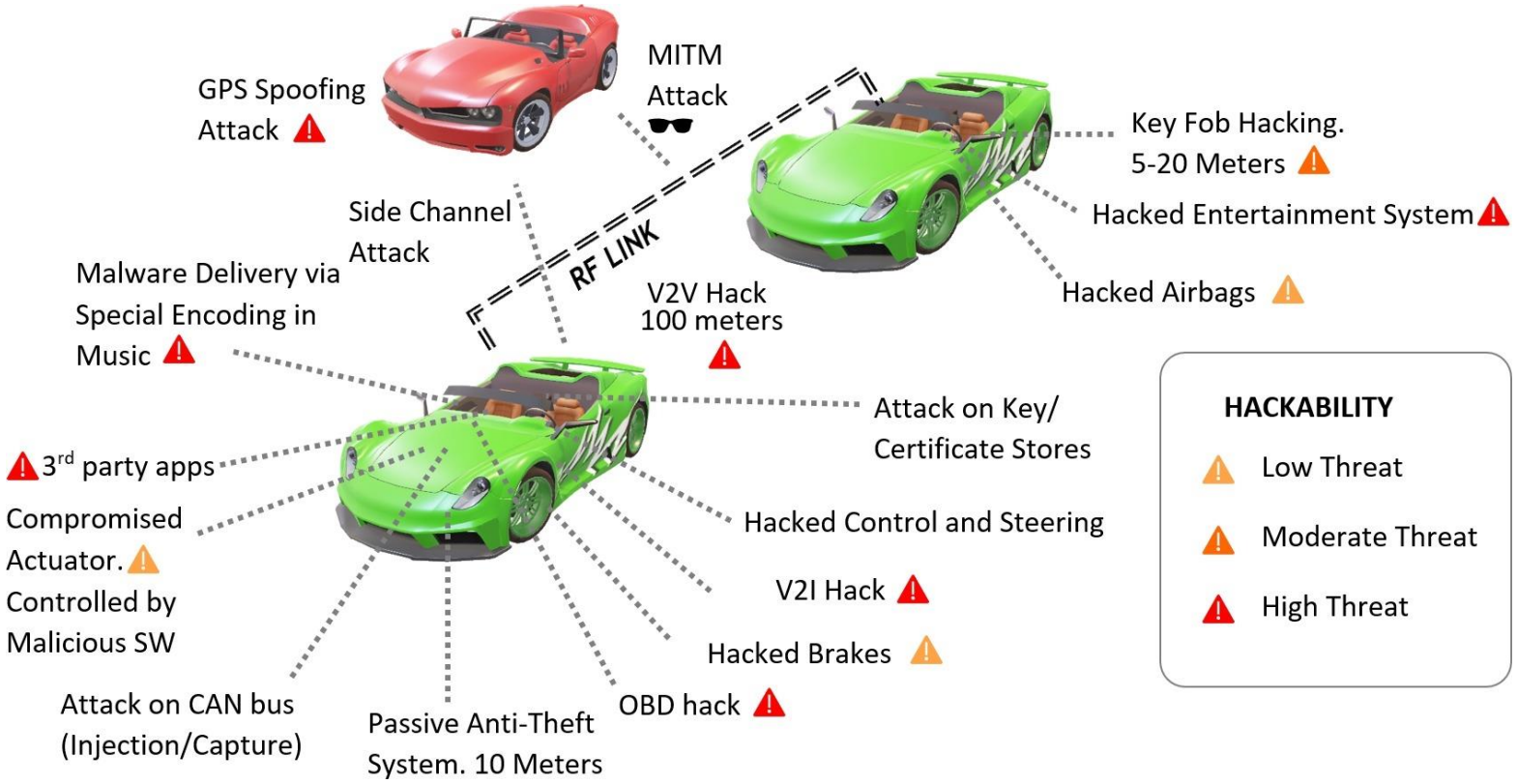
Technical meeting

Connets Lab

Platooning

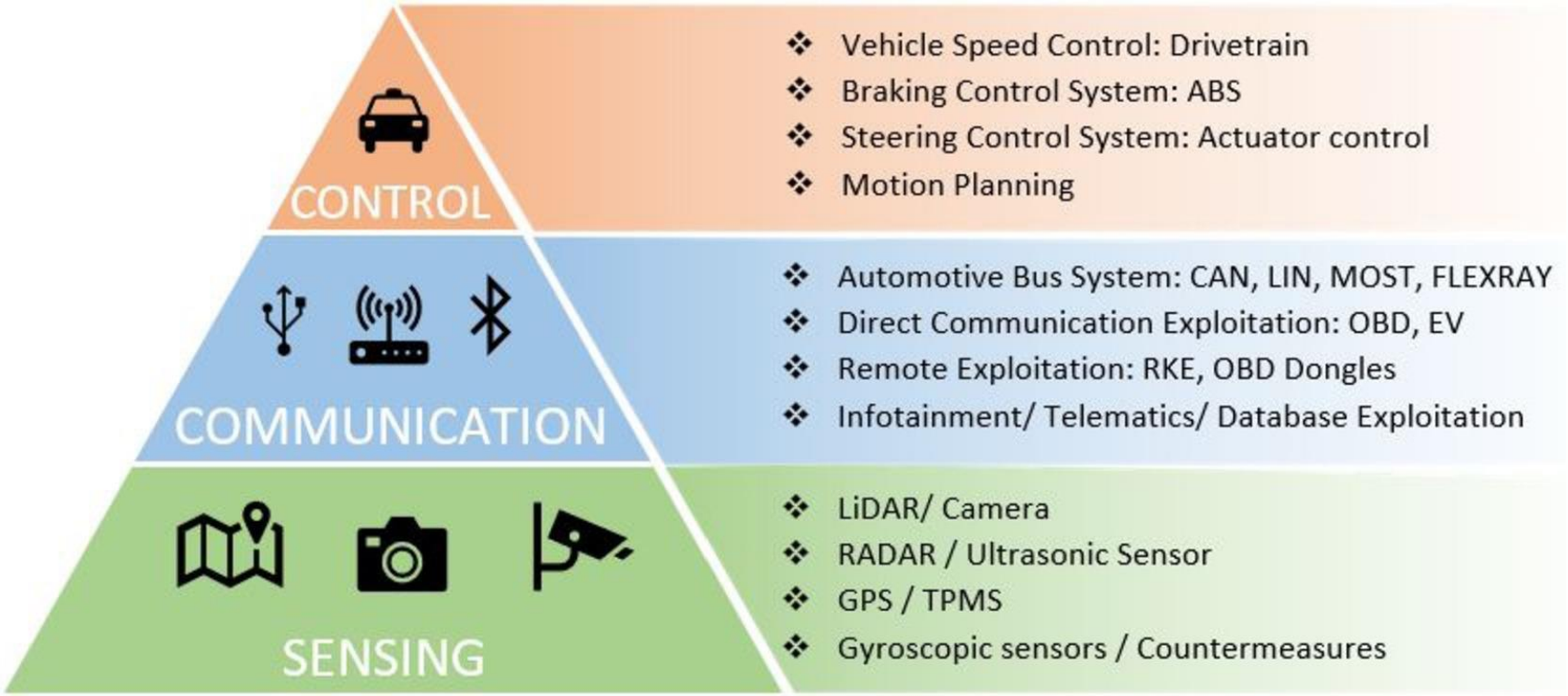
Security Aspects of Intra/Inter-Vehicle Communications

Cyber vulnerabilities in a vehicular ecosystem



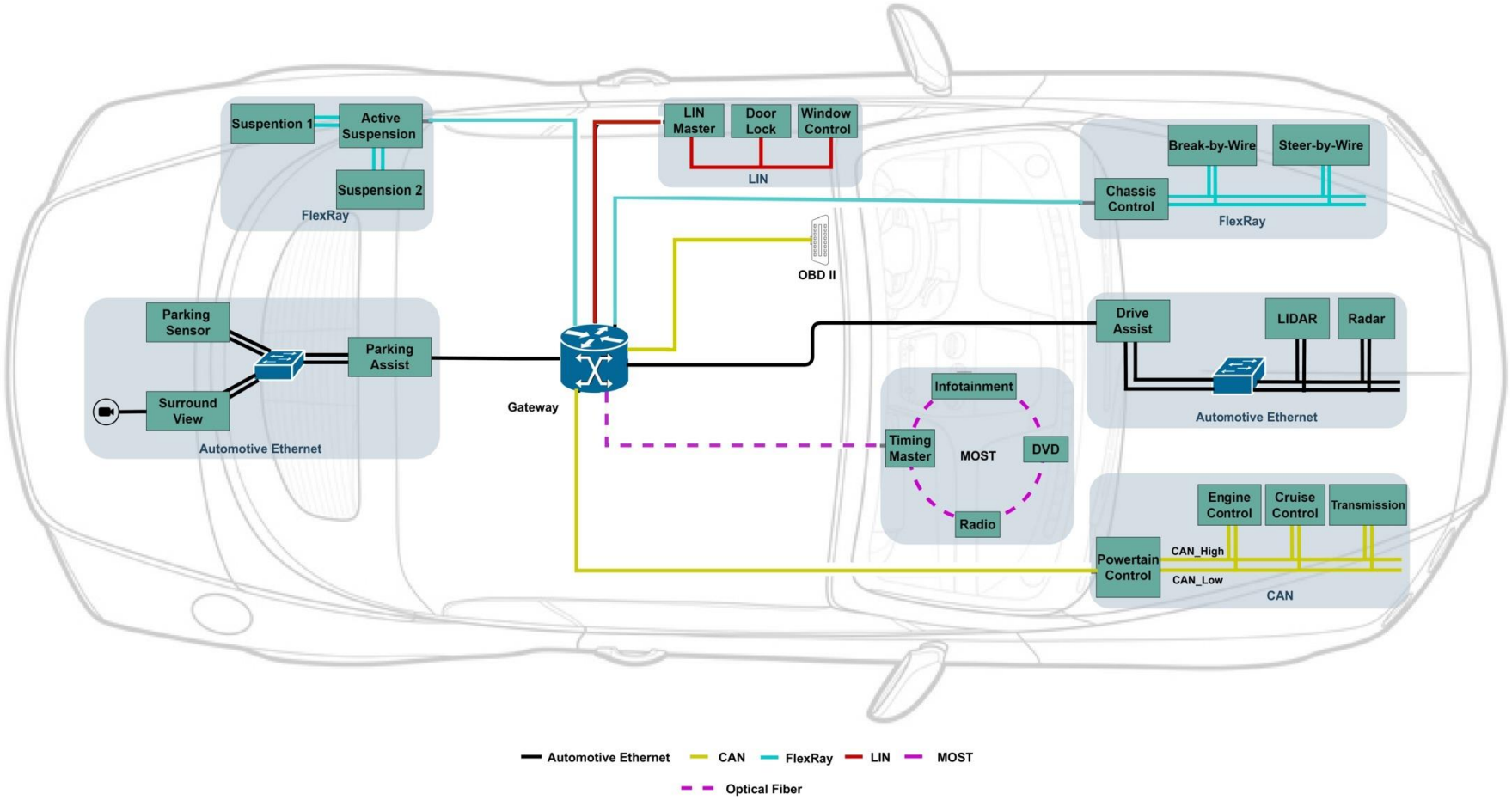
Zeinab El-Rewini, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, Prakash Ranganathan, Cybersecurity challenges in vehicular communications, Vehicular Communications, Volume 23, 2020, 100214, ISSN 2214-2096, https://doi.org/10.1016/j.vehcom.2019.100214.

The Autonomous Vehicular Sensing-Communication-Control framework



Zeinab El-Rewini, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, Prakash Ranganathan, Cybersecurity challenges in vehicular communications, Vehicular Communications, Volume 23, 2020, 100214, ISSN 2214-2096, https://doi.org/10.1016/j.vehcom.2019.100214.

Intra-Vehicular Communication Threats



Controller Area Network (CAN)

Powertrain

Local Interconnect Network (LIN)

Body control (instruments, door, light remote keyless...)

FlexRay

(Safety & Chassis control)

Media Oriented System Transport (MOST)

(infotainment)

Ethernet

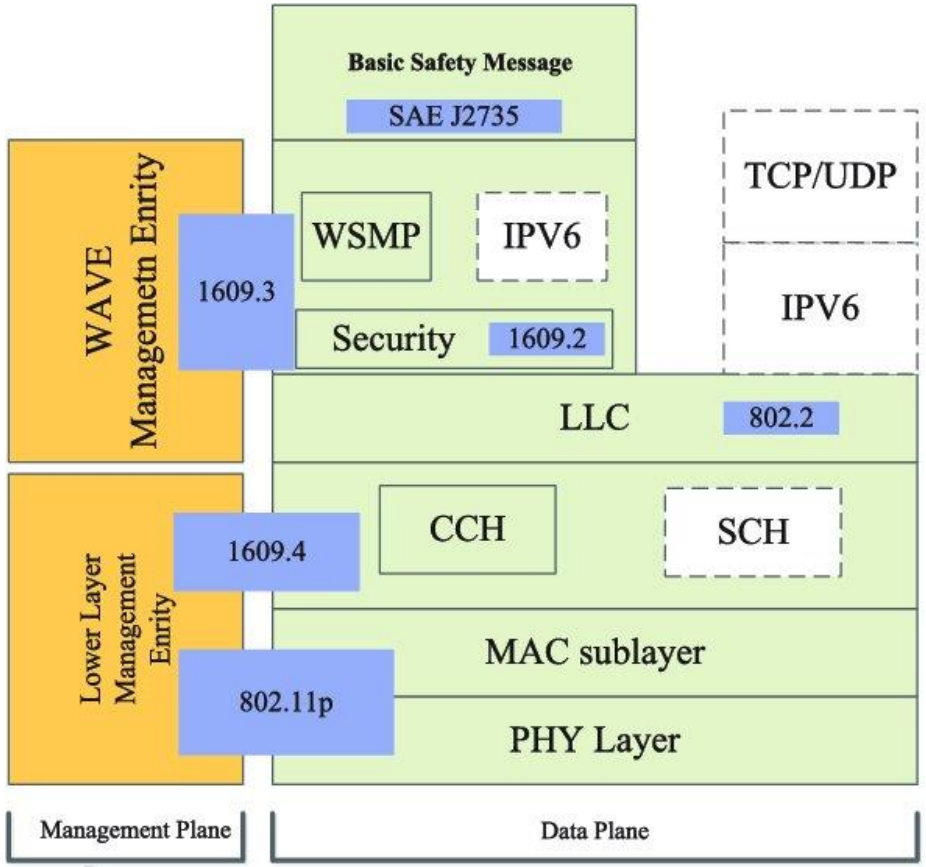
Akib Anwar, Anika Anwar, Lama Moukahal, Mohammad Zulkernine, Security assessment of in-vehicle communication protocols, Vehicular Communications, Volume 44, 2023, 100639, ISSN 2214-2096, https://doi.org/10.1016/j.vehcom.2023.100639.

Intra-Vehicular Communication Threats
(Via Infotainment & OBD port)

Attacks

- **Masquerading: attacker masquerades as legitimate node**
- **Message spoofing: illegitimate/inaccurate messages**
- Eavesdropping: unauthorized access to vehicular messages
- **Injection: fake messages injected into bus**
- **Relay: resent valid frames to impede real-time functioning**
- ***DoS***
- Bus-off: specific for CAN bus protocol causing increment of ECU transmit error counter

Inter-vehicular Communication Threats



V2V

IEEE 802.11p +
WAVE (Wireless Access in Vehicular Environment)

IEEE 1609.2 offers a security layer for connected vehicular environment

Platoon messages are "Basic Safety Message"

Inter-vehicular Communication Threats

- **Illusion attack:** false event created
- **Bogus information attack:** attacker generates fake messages to make other vehicles choose different path (e.g. Lane changing)
- **Sybil attack:** attacker declares itself as multiple nodes
- **Timing attack:** add some time delay on purpose (other vehicle believe info is timing)
- **Impersonation attack**
- **Alteration/Replay attack**
- **Jamming**
- **DoS (DSRC & Cellular)**

Attack	Property	Ease of attack	Detection probability
Eavesdropping	Confidentiality	High	Low
GPS Spoofing	Authentication, Privacy	High	Low
Alteration/Replay	Integrity, Authentication	High	Low
Magnetic	Privacy, Integrity, Availability, Real-time Constraint	High	Low-Driver, High-System
Identity tracking	Location, Privacy	High	Low-at High Traffic Density
Sybil	Authentication, Availability	High	Moderate
Denial of service	Authentication, Availability	High	High
Timing	Availability, Real-time Constraint	High	High
Bogus information	Integrity, Authentication	Moderate	Low-Driver, Moderate-System
Black hole	Availability, Confidentiality, Integrity	Moderate	Moderate
Man-in-the-middle	Confidentiality, Integrity, Authentication	Moderate	Moderate
Injection	Integrity	Moderate	Moderate-Driver, High-System
Blinding	Privacy, Integrity, Real-Time constraint	Moderate	High
Illusion	Authentication, Integrity	Low	Low-Driver/System
Impersonation	Integrity, Authentication	Low	High

Table 4. Potential cyber attacks in V2X communications

J. Petit and S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," in IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 2, pp. 546-556, April 2015, doi: 10.1109/TITS.2014.2342271.

Possible scenarios to investigate

- On-board attack: one or more vehicles are compromised and send wrong data to other platoon vehicles
  - OBU is compromised
  - Communication is ok (V2V/V2N)

- V2V communication attack
  - Internal – one or more vehicles are compromised and acts non-cooperatively (timing attack, relay,...)
  - External – jamming/DoS from outside, other vehicles/RSU

- V2N communication attack
  - Jamming/DoS at BS level
  - DoS at Edge level
- Control Law attack ?? (gain values, target values)