Living on the Electric Vehicle and Cloud Era: A Study of Cyber Vulnerabilities, Potential Impacts, and Possible Strategies

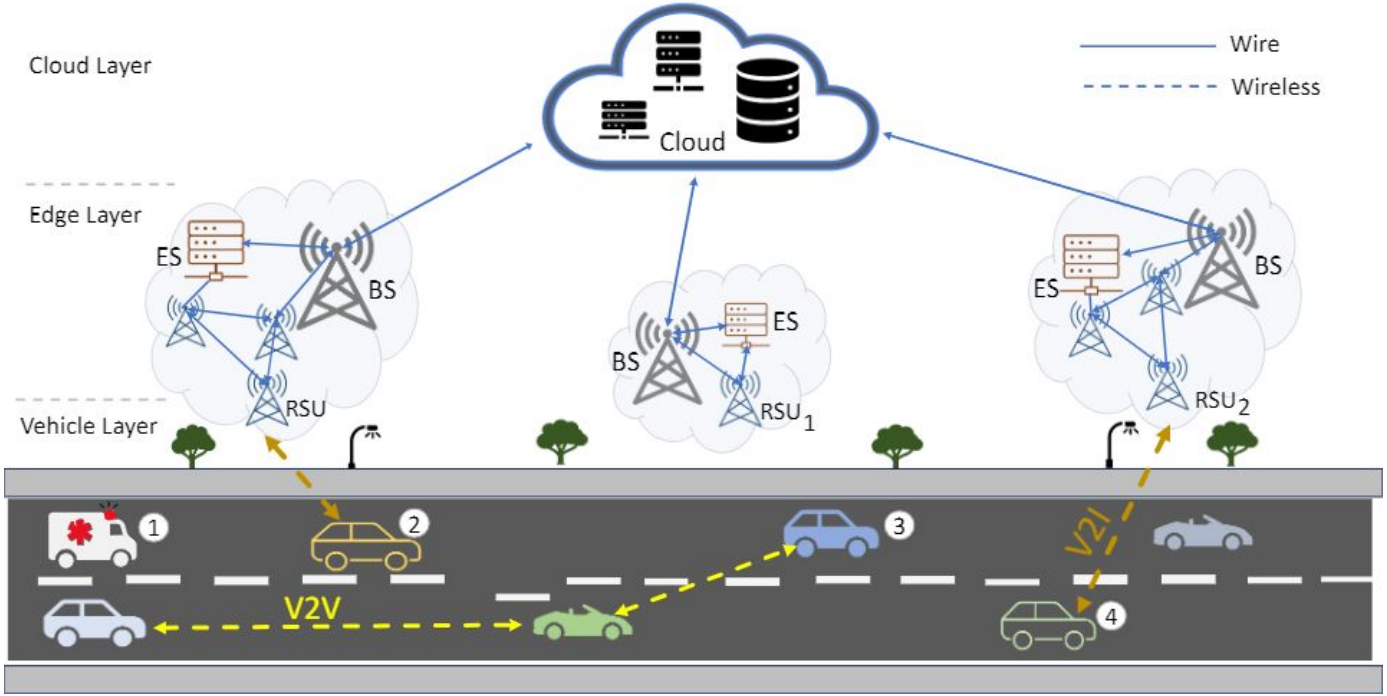
Long Vu, Kun Suo, Md Romyull Islam,
Nobel Dhar, Tu Nguyen, Selena He, Yong Shi

Kennesaw State University

OUTLINE

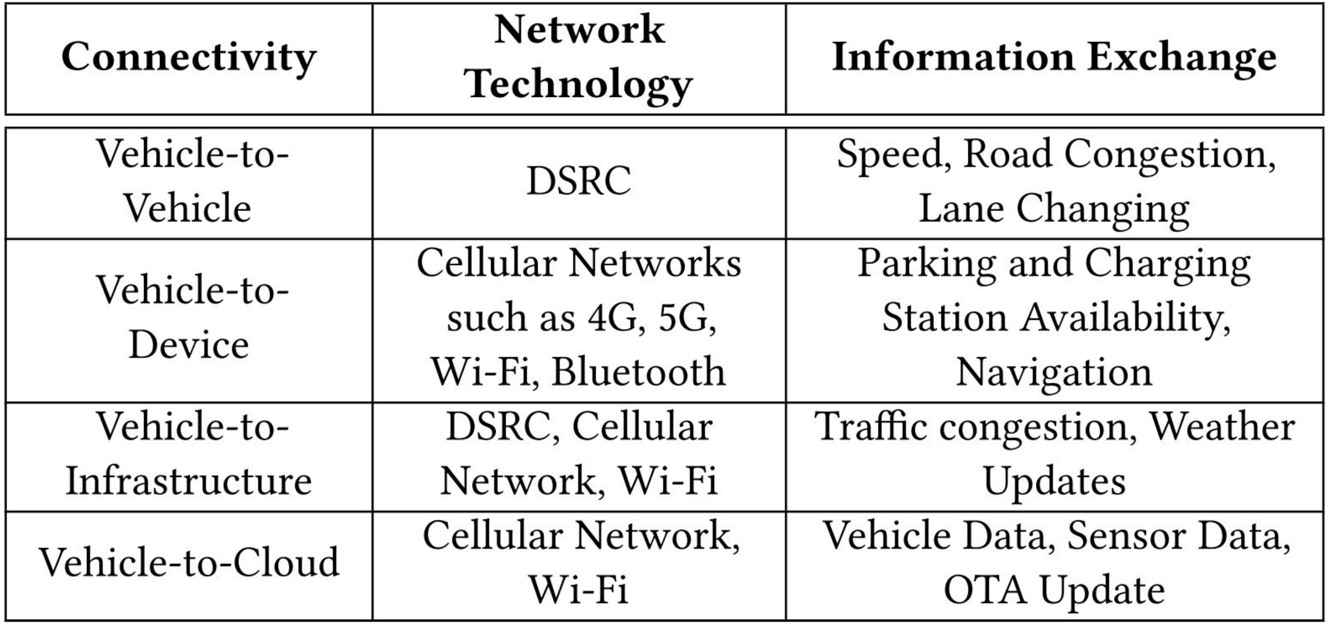
1. The Connection between EVs & Outside World
2. EV Cyber Vulnerabilities & Impacts
3. Security Strategies
4. Current Limitations & Future Research Directions
5. Conclusion

The Connection between EVs & Outside World



3 Layers of Communication

The Connection between EVs & Outside World



Connectivity	Network Technology	Information Exchange
Vehicle-to-Vehicle	DSRC	Speed, Road Congestion, Lane Changing
Vehicle-to-Device	Cellular Networks such as 4G, 5G, Wi-Fi, Bluetooth	Parking and Charging Station Availability, Navigation
Vehicle-to-Infrastructure	DSRC, Cellular Network, Wi-Fi	Traffic congestion, Weather Updates
Vehicle-to-Cloud	Cellular Network, Wi-Fi	Vehicle Data, Sensor Data, OTA Update

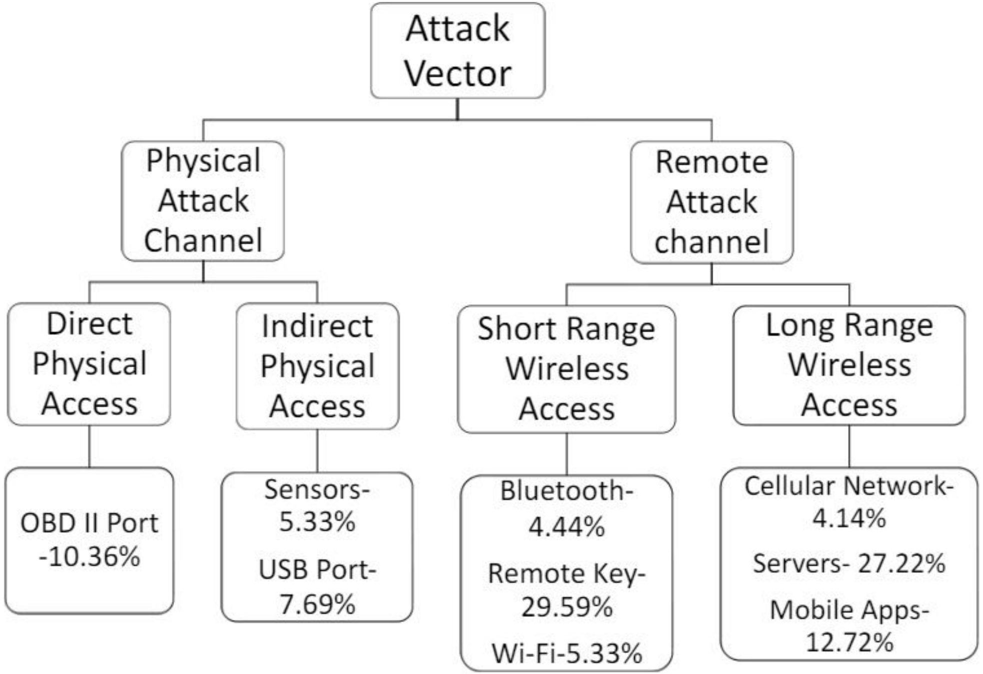
Types of V2X Connectivity, Technology and Data

Overview of This Research

- We scrutinize the **potential attack vectors** that EVs are vulnerable to and the **consequential impact** on vehicle operations
- We outline both **general and specific strategies** aimed at thwarting these cyberattacks
- We **anticipate future developments** aimed at enhancing EV performance and reducing security risks

EV Cyber Vulnerabilities & Impacts

EV Cyber Vulnerabilities



Common Attack Vectors on EV System

Types of EV Attacks

Eavesdropping

Jamming

Message Spoofing/Forgery

Replay Attack

Man-in-the-Middle

Sybil Attack

Fake Attack

Denial-of-Service

Malware

Tracking

Impacts of Attack on EVs

Loss of Mobility

Data Leakage

Remote Control & Safety Risks

Financial Losses & Reputation Damage

Security Strategies

Strategies Against Attacks

Software Update

Restrict In-vehicle Wireless Services

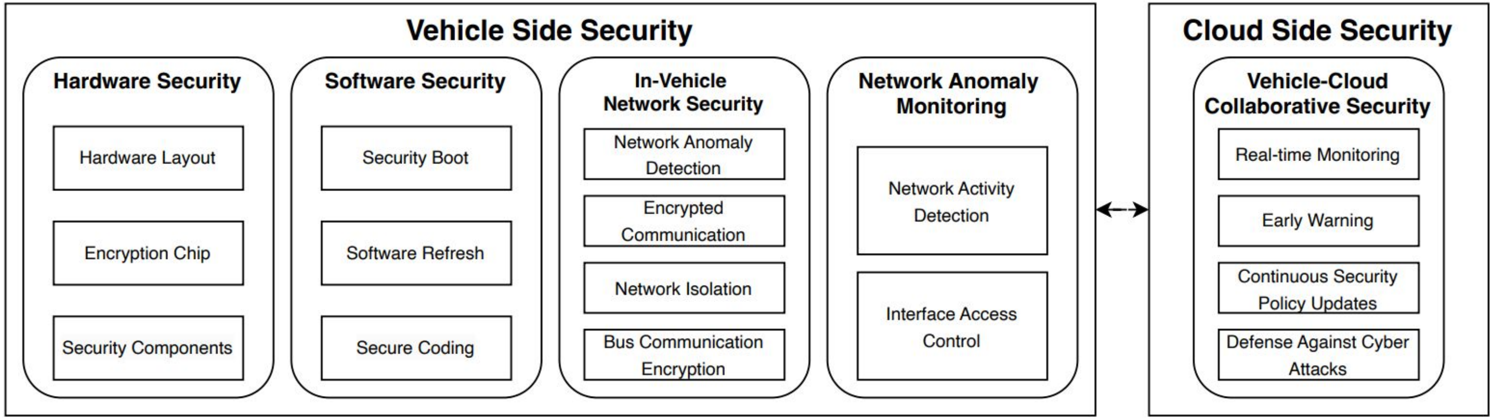
Avoid Untrusted Apps and Services

Other Measurements

EV Cyber Security Defense Lines

- **Vehicle side:**
  - Security software and hardware architecture design
  - In-vehicle network security architecture
- **Cloud side:**
  - Vehicle-cloud collaborative security
  - Up-to-date security policies

Security Strategies



Security Architecture Design Components

Current Limitations & Future Research Directions

- **EV Charging Infrastructure**
  - Limited station availability; vulnerable to cyberattacks
    -> need secure protocols and intrusion systems
- **Safety and Privacy**
  - Increased cyber-attack risk for connected EVs
    -> need better privacy techniques and cyber-security protocols.
- **Vehicle and Grid Interaction**
  - V2G/G2V needs secure cloud platforms
    -> focus on *security and privacy in data transactions*

Conclusions

- **Adoption and Benefits of EVs**
  - EV are gaining popularity due to multiple benefits (lower emissions, reduced noise, higher efficiency, superior technology)
- **This Research**
  - explores the integration of EVs with cloud connectivity and identifies potential cybersecurity threats; assesses the impacts and proposes strategies to mitigate these risks.
- **Contribution**
  - examine the potential attack vectors that EVs might be susceptible to and the resulting impact on the vehicle.
  - a valuable resource for researchers interested in EV platforms and cybersecurity issues related to EVs

Thank You!