KOÇ UNIVERSITY Cryptography, Security, and Privacy Research Group

Connected Vehicle Problems and Solutions

Barış Kaplan and İlter Erol Gürol

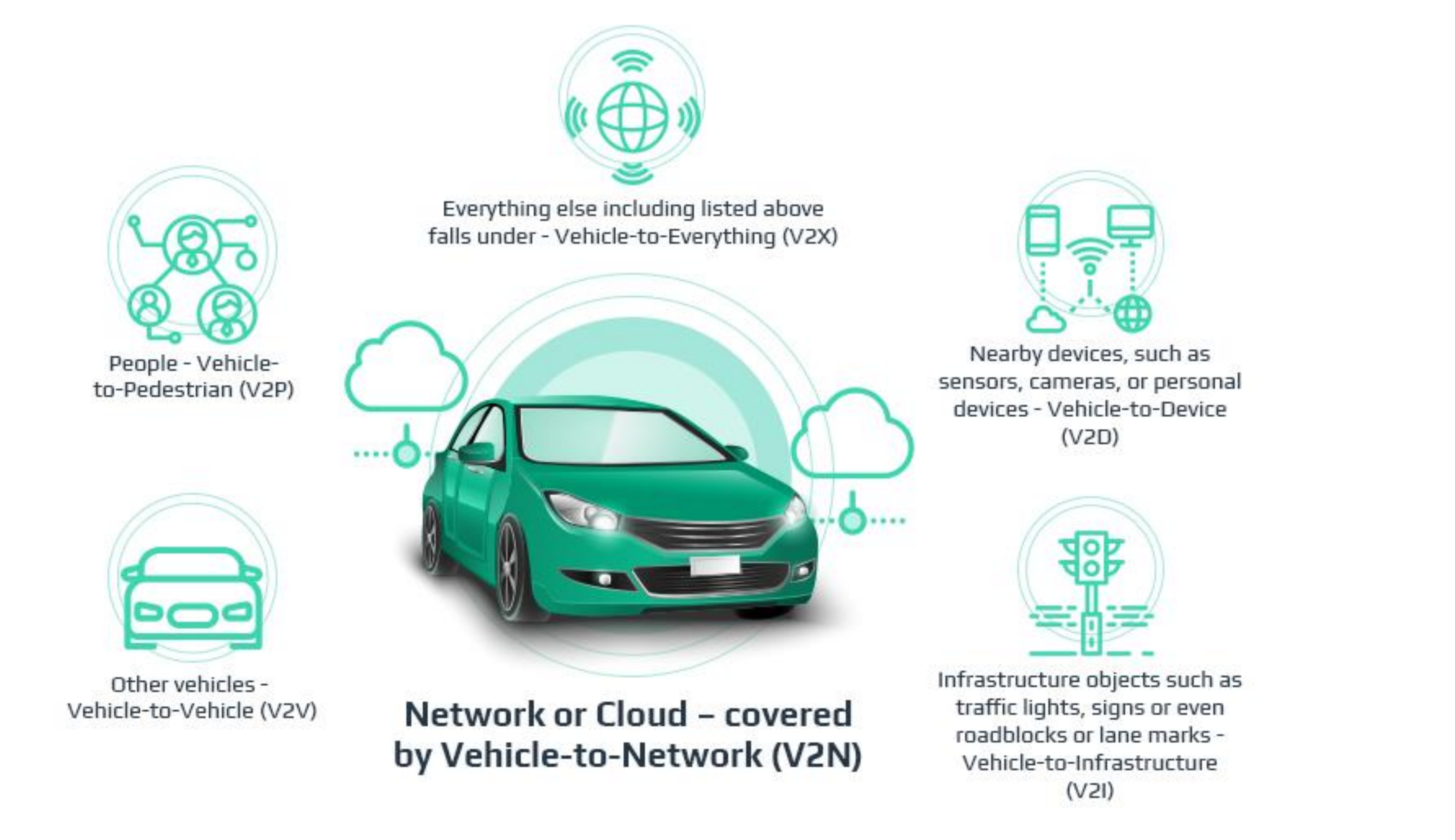
- Manipulation of EM and GPS Signals

- ECU Flashings and Code Changes

- Data Poisoning Attacks and Learning Attacks

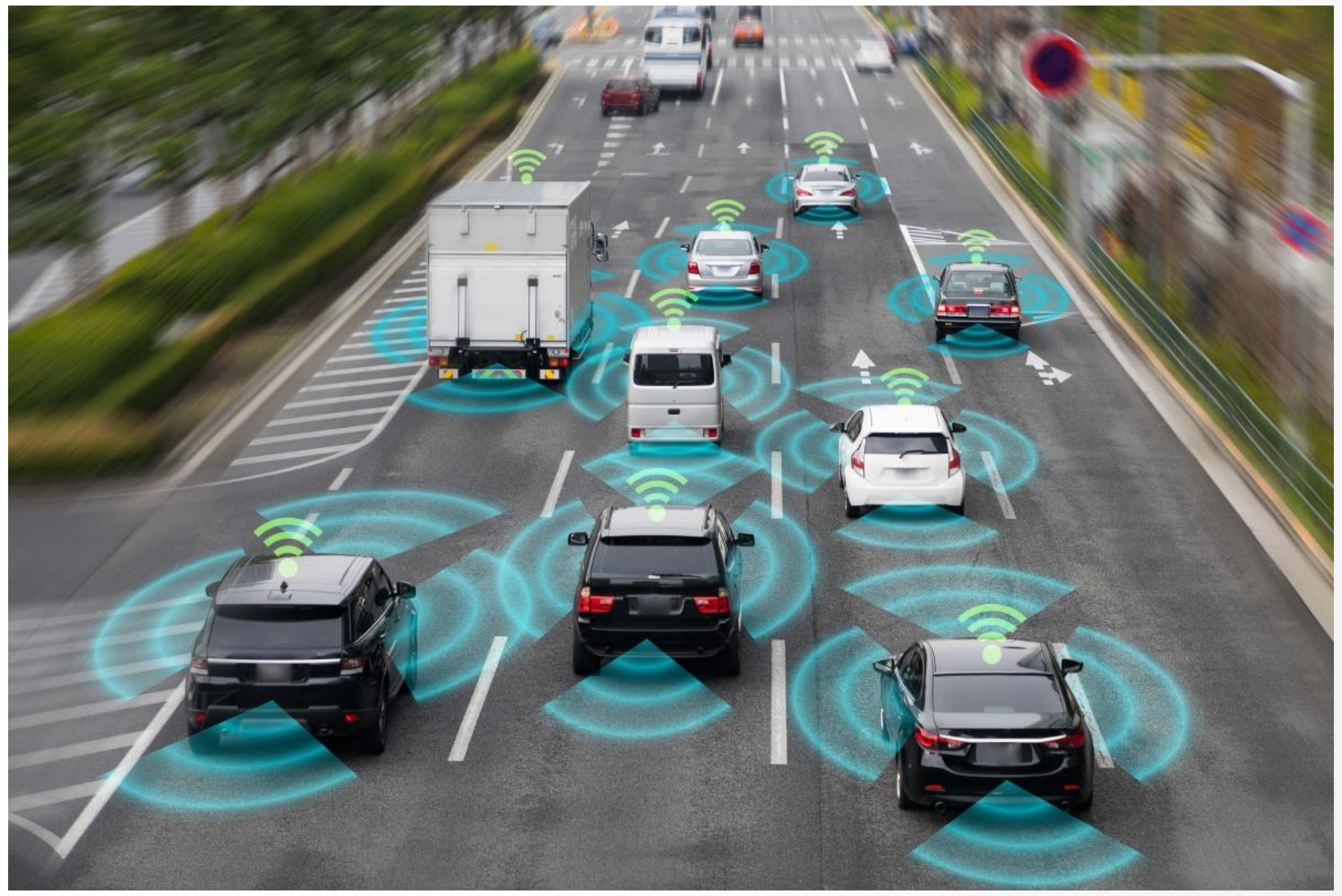
- Denial of Service Attacks, Impersonation Attacks, Replay Attacks, Routing Attacks, Eavesdropping Attacks, Priority Attacks, and Data Falsification Attacks

- Communication Protocol Attacks


Everything else including listed above falls under - Vehicle-to-Everything (V2X)
People - Vehicle-to-Pedestrian (V2P)
Nearby devices, such as sensors, cameras, or personal devices - Vehicle-to-Device (V2D)
Other vehicles - Vehicle-to-Vehicle (V2V)
Network or Cloud – covered by Vehicle-to-Network (V2N)
Infrastructure objects such as traffic lights, signs or even roadblocks or lane marks - Vehicle-to-Infrastructure (V2I)

Taken from: https://intellias.com/v2x-basics-connected-vehicle-technology/

- For preventing the eavesdropping, data falsification, replay priority, routing, DOS, impersonation, and priority attacks; blackbox modelling, authenticity checks, and integrity checks are applied.
- For preventing the learning , and data poisoning attacks; black-box modelling is applied.
- For preventing the manipulation of GPS signals, the GPS signals are compared from the adjacent CAVs. For preventing the manipulation of the EM signals, the output signals are randomly modulated.
- For preventing the ECU Flashings, and code alterations; integrity checks are done.
- For preventing the communication protocol attacks, safer communication protocols can be commercially used.



Taken from: https://www.smartcitiesworld.net/news/news/siemens-unveils-connected-vehicle-app-3194

Poster designed as part of the Computer and Network Security course by Alptekin Küpçü