Securing Electric Vehicles in the Power Grid

Chaitra Niddodi, Sibin Mohan, Tim Yardley

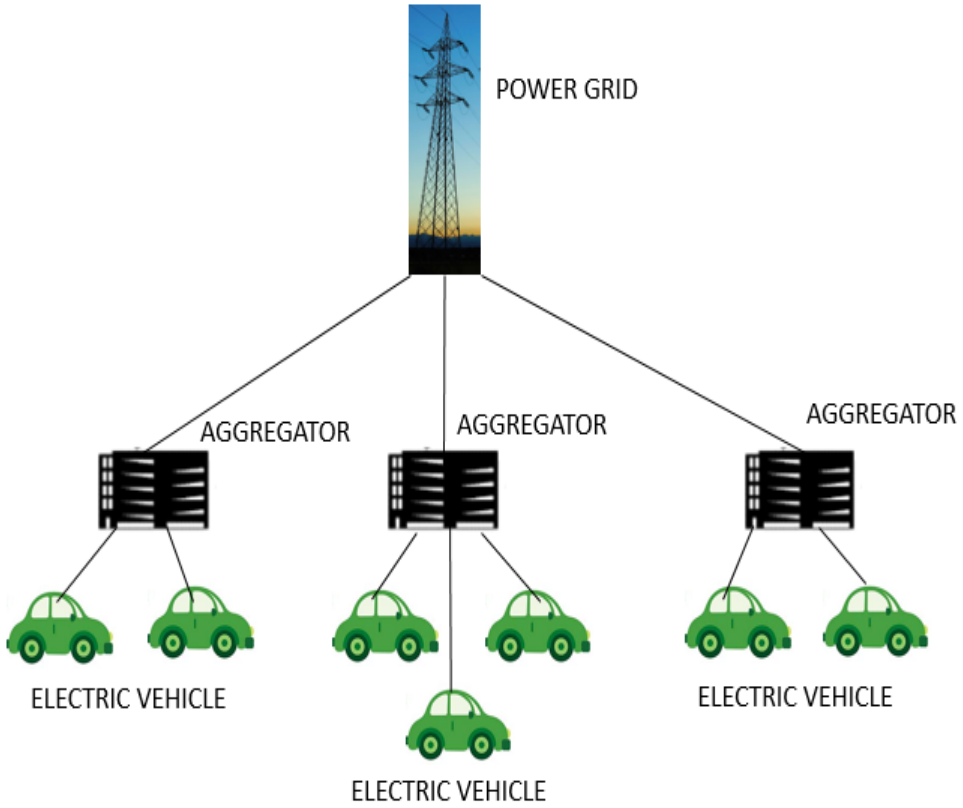
ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

The Electric Power Grid

- With increasing cyber-physical attacks on the Power Grid, security of this critical national infrastructure to ensure its non-disrupted functioning is essential.
- Integration of **Distributed Energy Resources (DERs)** like **Electric Vehicles (EVs)** into the Power Grid entails many security considerations.
- We start by investigating security threats with respect to EVs and propose robust techniques to secure the **Vehicle to Grid (V2G)** system.
- We will later extend these techniques to secure other DERs in the Power Grid.

The V2G System

- The main components of the system are
  - Electric Vehicle
  - Aggregator
  - Power Grid



Security - Approach

- **Component Security**
  - Creating valid states and state transitions for the components.
  - Imposing constraints on the components' behavior.
- **Secure Communication among Components**
  - Validating *data* exchanged among components.
  - Real time verification of *timing requirements* for the communication.
- **Consistency of Cyber States with Physical States**
  - Verifying the data exchanged against readings from physical sensors.

Security - Solution

- Detailed modeling of the V2G system to establish expected system behavior.
- Design a specification based **intrusion detection system (IDS)** to detect anomalous behavior.
- Evaluate IDS based on metrics – *false negatives and false positives.*

THANK YOU