Electric Vehicles

CPS and IoT Security

Alessandro Brighente

Master Degree on Cybersecurity

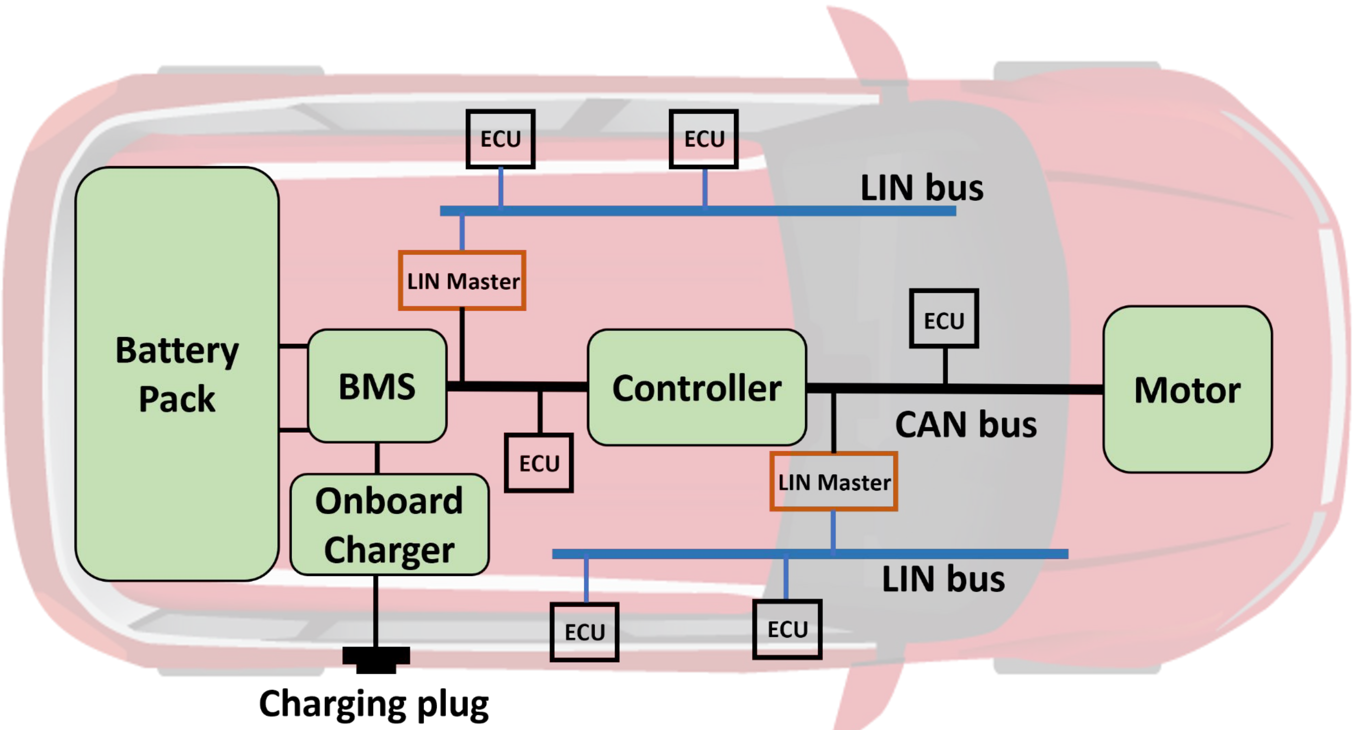
Università degli Studi di Padova

SPRITZ Security & Privacy Research Group

Electric Vehicles

- Recent climate crisis demands green alternatives to replace technologies with high environmental impact
- Electric Vehicles (EVs) have been proposed as a green alternative, where electric batteries are employed as a power source
- Governments are incentivizing the adoption of EVs thanks to the deployment of a large number of Electric Vehicle Supply Equipment (EVSE) in public charging infrastructure
- Ban of gas-fueled cars

Components of EVs



Components of EVs

- **Battery:** The battery is where the charge is stored in the form of Direct Current
- Batteries are usually combined in packs and connected in series or parallel to increase the voltage and Ampere/hour they can deliver to the EV
- Batteries suitably combined are enclosed into a metal casing to prevent damage
- The case usually includes a cooling system to avoid damage due to batteries overheating

Components of EVs

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- **Battery Management System:** manages all operations regarding the battery
- Manages the current output and the charging and discharging of the battery by keeping it in a safe operating area
- Monitors each battery in the pack and measures each cell's voltage, current, and temperature
- Is instructed with a threshold limit for each of them and disconnects the load if values exceed the threshold value

Components of EVs

SPRITZ Security & Privacy Research Group
Università degli Studi di Padova

- **Battery/On-Board Charger:** provides an interface between the charging system and the EV battery
- The charger converts the input voltage to DC and passes it to the battery for storage
- It prevents possible damages to the battery or the supply system (e.g., overheating) by limiting the power flow

Components of EVs

- **Controller:** handles the flow of current from the battery to the EV associated with all operations, ranging from motors-related operations to powering the infotainment system
- Receives the input from the driver to control the acceleration, brake pressure, and driving mode and converts the energy in the battery from DC to AC
- The controller converts the generated AC to DC such that the energy can be stored in the battery

Components of EVs

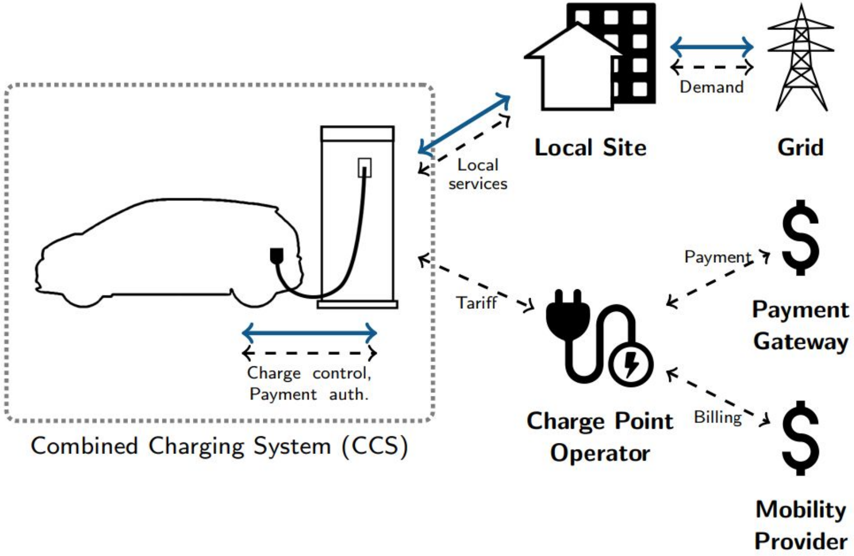
SPRITZ
Security & Privacy
Research Group

Università
degli Studi
di Padova

- **Electric Motor:** the motor is powered by the EV battery
- The electric motor communicates with sensors and actuators in the EV that control the amount of thrust required
- There exist many implementations of electric motors
- The most commonly used for EVs are AC induction due to their lower cost implementation thanks to the absence of permanent magnets

Losing the Car Keys

- Physical layer attack against the Combined Charging System
- Exploit electromagnetic side channel attacks to tamper with the Power Line Communication (PLC)
- The unintentional wireless channel is sufficient to recover messages in the vast majority of cases



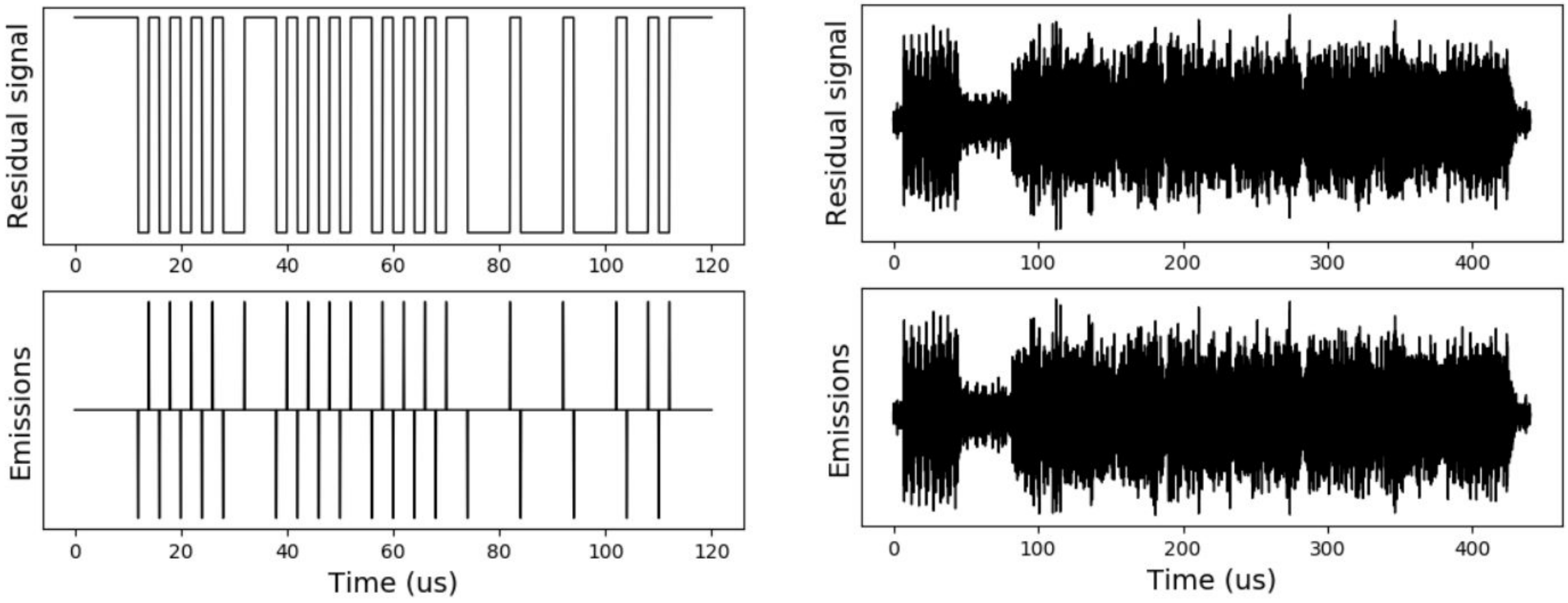
Side Channel in PLC

- PLC design assumes differential signalling, wherein two transmission lines are driven with equal but opposite signals
- However, practical implementations of PLC circuit connect one of the transmission lines to the ground
- The resulting single-ended signalling creates a suitable antenna for emission or inference

Threat Model

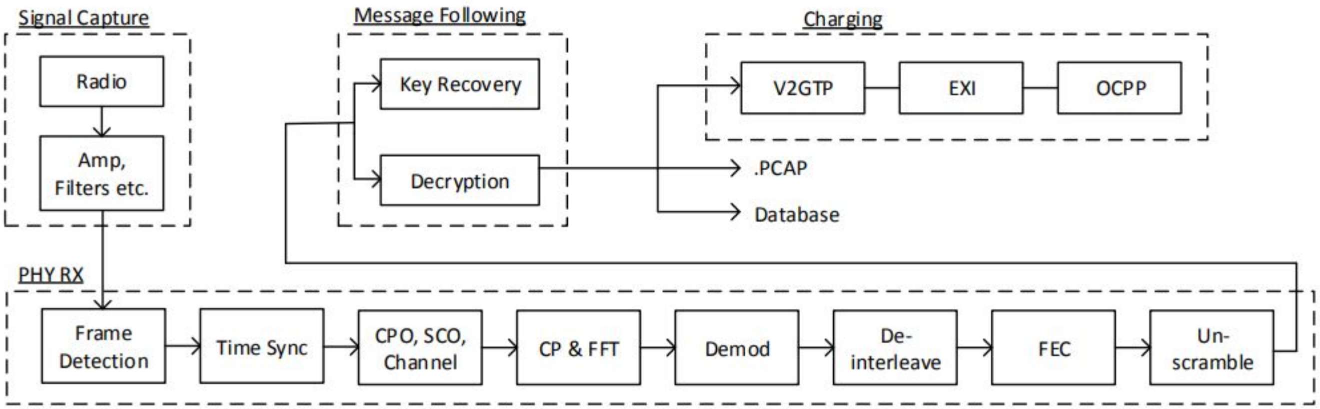
- We consider a passive attacker, eavesdropping the charging process via unintended radiations
- Eavesdrop general purpose communication between EV and charger
- The attacker can get closer, but cannot modify or tamper the equipment
- The data collection can be done both in presence or remotely

Emission Examples



Eavesdropping Tool

- Task of the attacker: maximize the signal to noise ratio and bandwidth of the receiver
- Challenge: any exposed component might be generating unintended EM signals
- The tool resembles a HomePLug GreenPHY receiver



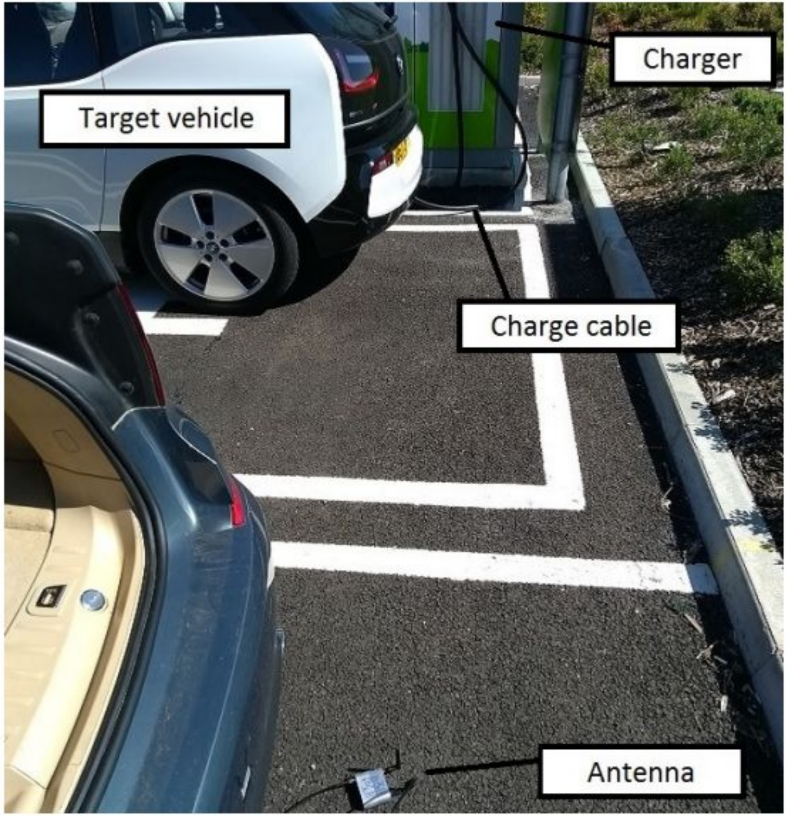
Measurement Campaign

- Three different EV models, collecting a total of 54 unique charging sessions
- Use the eavesdropping tool to reconstruct the digital information
- The receiver antenna can be both inside the car, outside of it, or at a certain number of bays away

Measurement Campaign

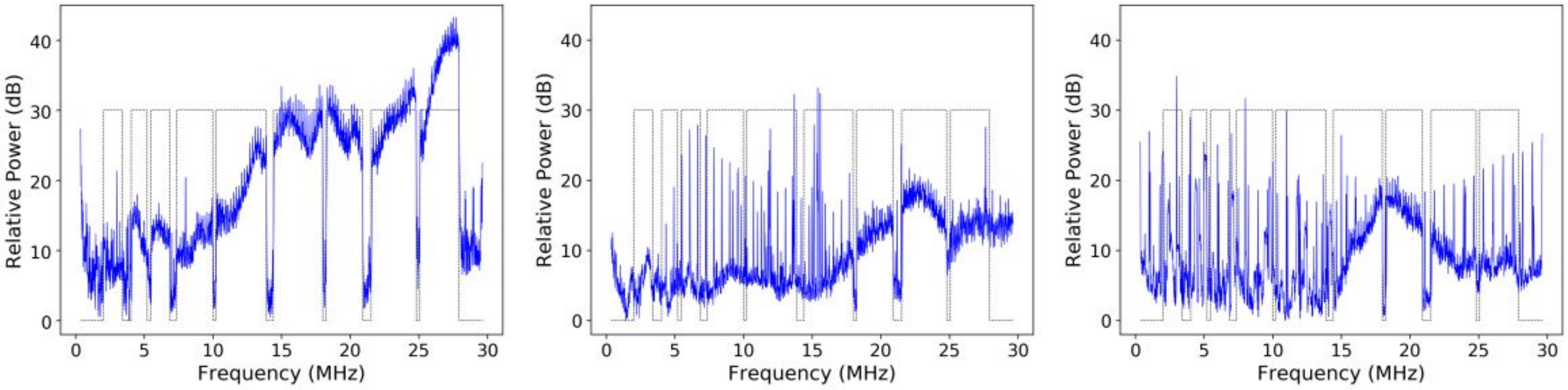
SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA



Eavesdropped Communication

- Measured signals at different locations
- Overlaid HPGP spectrum to show where communication occurs
- Every site displays some form of unintentional communication
- We see the effect of distance from the transmitter



(a) Antenna by cable (site H) (b) Antenna in bay behind (site F) (c) Antenna in next bay (site G)

Message Recovery

- Thanks to the received signals and its high SNR, decoding has a high success probability
- In the best case (in car, peak SNR = 20 dB, BW = 12 MHz) the rate of correctly decoded CRC is 100 %
- The proposed approach is also valid in case of multiple EVs simultaneously charging
- The success rate however varies from 24.3% to 94.8%

Communication Security

SPRITZ
Security & Privacy
Research Group

Università
degli Studi
di Padova

- The first phase is capturing the initialization of the charging session
- If that is the case, thanks to the attack it is possible to examine the network membership key exchange
- Since there is no encryption, if the message is received intact it is possible to determine the network membership key
- Successful in 31 cases when considering single EV
- When considering side-by-side vehicles, successful in extracting one NMK in 4 session, and both NMK in one

Communication Security

- As the vehicle and charger establish a network, the vehicle undertakes the discovery protocol to find a charge controller and the two established a TCP connection
- However, there is no establishment of TLS tunnel
- This leaves the high level protocols exposed
- There is still an open debate on the type of PKI to deploy, which limits the applicability of TLS
- Currently, infrastructures rely on the physical security of location and cabling

Attacks to EVs and Infrastructure

- Electric Vehicles and their charging infrastructure are cyber-physical systems
- We discuss how the different threat vectors can lead to multiple types of attack, undermining the communication security or jeopardizing the privacy of the users
- We discuss attacks based on the current exchanged during the charging process and the communication protocols needed to establish connections or to manage the chagrin process

EV Charging Profiling

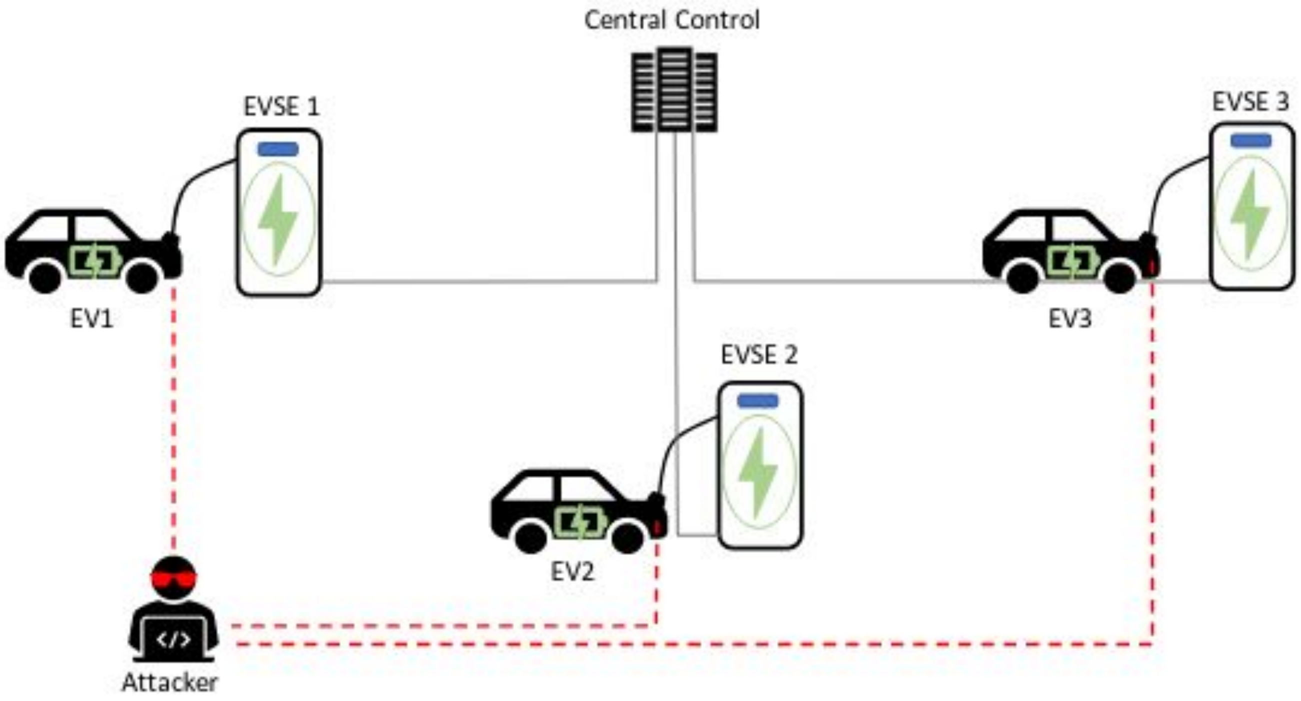
Motivation:

- Public infrastructures are easily accessible by anyone
- Attackers can physically tamper the charging infrastructure to collect sensitive data

Goal:

- Exploit physical charging information to identify vehicles
- Malicious purposes: e.g., Tracking
- Benign purposes: e.g., Authentication

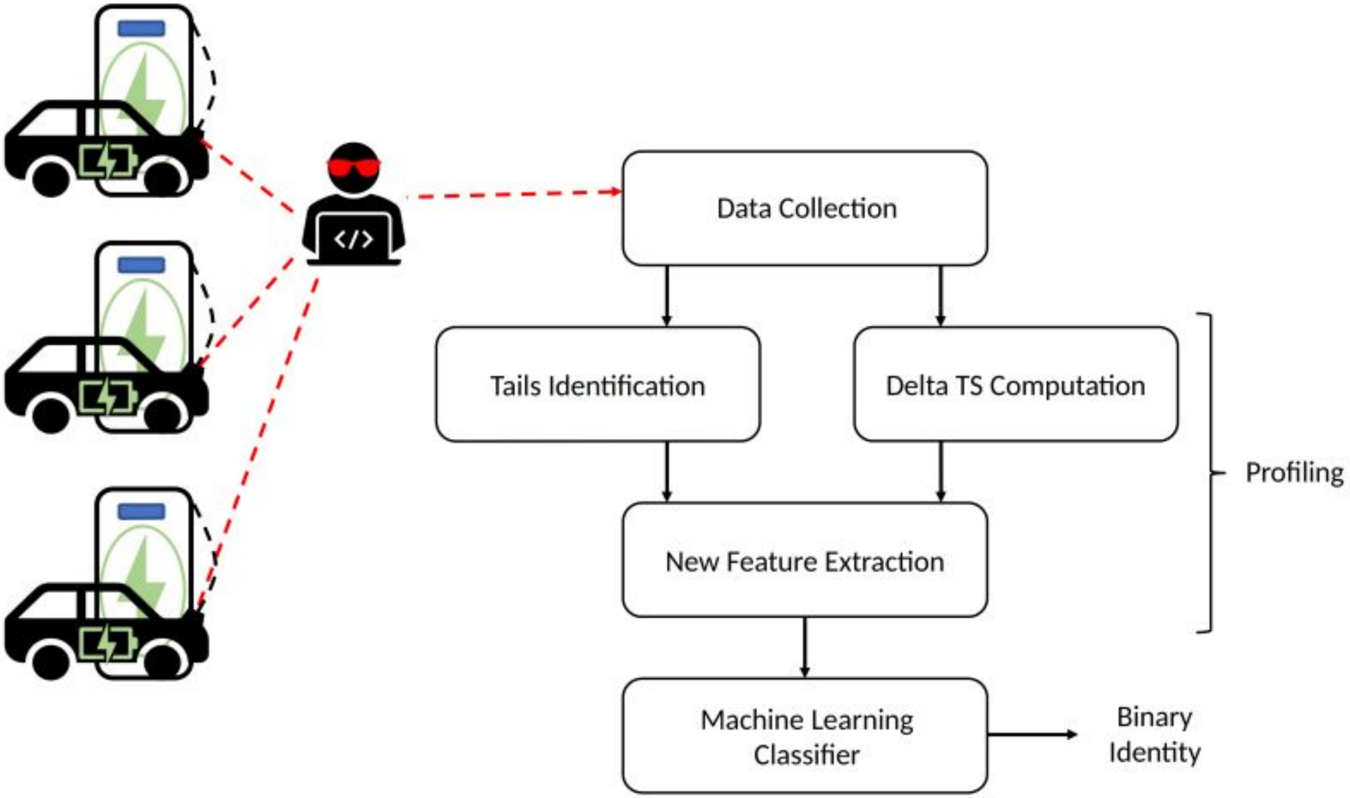
System & Threat Models



Attack Methodology

SPRITZ
Security & Privacy
Research Group

Università
degli Studi
di Padova

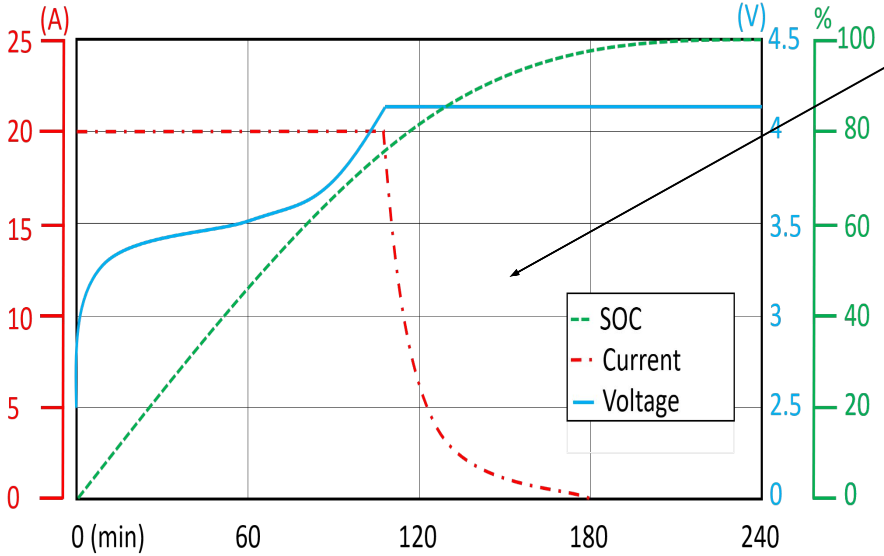


Dataset

- Data of charging sessions of real devices from [1]
- TS data connect connected to users identifiers
- Total number of EVs considered: 187
- Information:
  - vehicle identifier
  - arrival and departure time
  - kwh delivered
  - current and pilot time series
  - disconnection time

Tail Identification and Extraction

- Batteries charging model: constant current-constant voltage
- Tails include features to recognize the battery model [2]
- Objective: design an algorithm to identify and extract tails



Tail of the current time series

Tail Extraction Algorithm

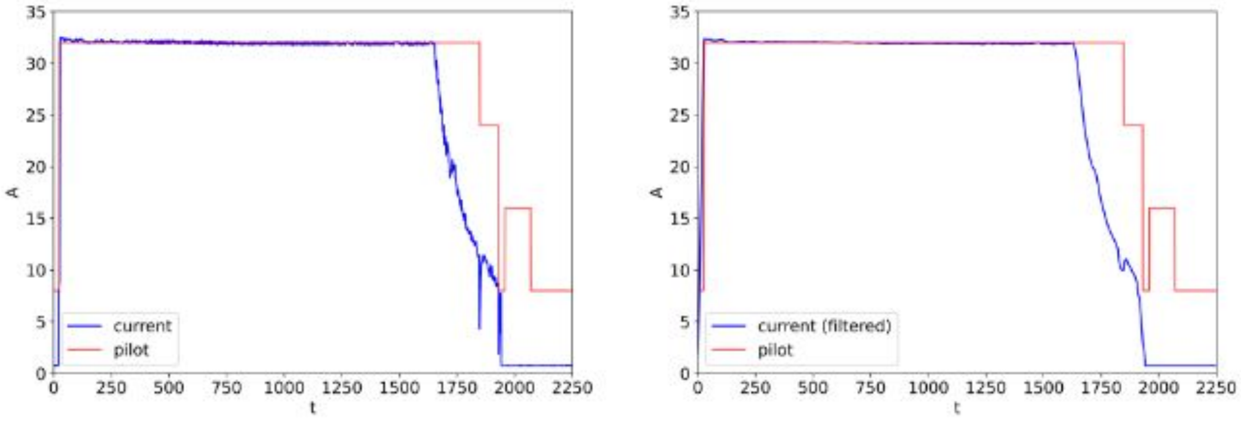
SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- Input: set C, P of filtered current and pilot time series, respectively
- Output: set TC , TP of current and pilot tails, respectively
- Steps:
    - Identify current TS ending point (zero values thereafter)
    - Identify backward ascending trend
    - Given the tail timestamp values, extract tail for both current and pilot
    - Add them to the sets TC , TP of current and pilot tails, respectively
- Feature set: 18 features including mean, variance, slop, time duration, min and max values.

Delta TS computation

- The charging itself also characterize the battery
- Pilot ≠ Current absorbed
- Objective: Characterize the normal charging behavior
- -> Compute Delta TS = Difference between pilot and absorbed currents



(a) Raw current profile.

(b) Current filtered with a moving average filter with $N_{avg} = 25$.

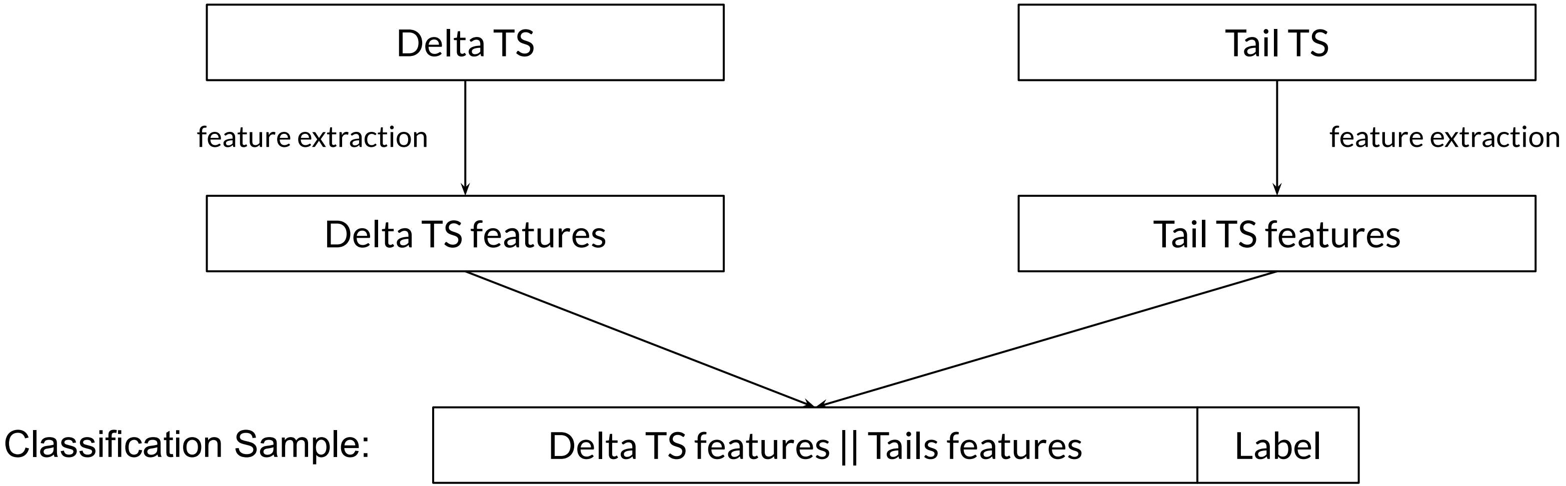
Features Extraction

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- Deleted not complete charges
- Automated Features extraction from TS
  - TSFresh: Lot of features for time series classification
- Classification sample:
  - <u>Delta</u> TS features || <u>Tails</u> features

Features Extraction



Machine Learning Classifiers

- Implemented classifiers:
  - Support-Vector Machine (SVM)
  - k-Nearest-Neighbours (kNN)
  - Decision Tree (DT)
  - Logistic Regression (LR)
  - Random Forest (RF)
  - ADA Boost (ADA)
- Unbalance ratio parameter Q
- Hyperparameter selected via grid search
- Performance measure: precision (P), recall (R), and F1
  - To cope with unbalancing: G-Mean
- Classification problem as Authentication

Results - Number of Features

- $F1$ scores for different ratios Q
- Same model kNN
- Varying the NoF from 10 to 200.
- Negligible increase from 100 features up
- We selected NoF = 100

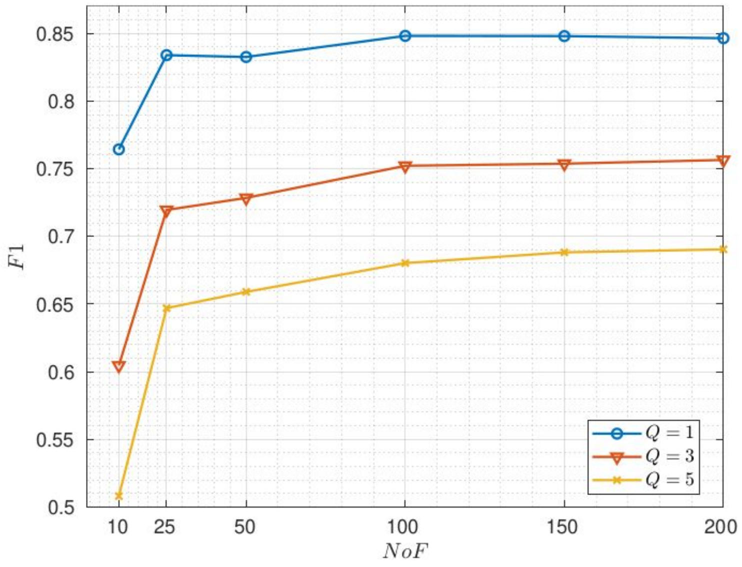
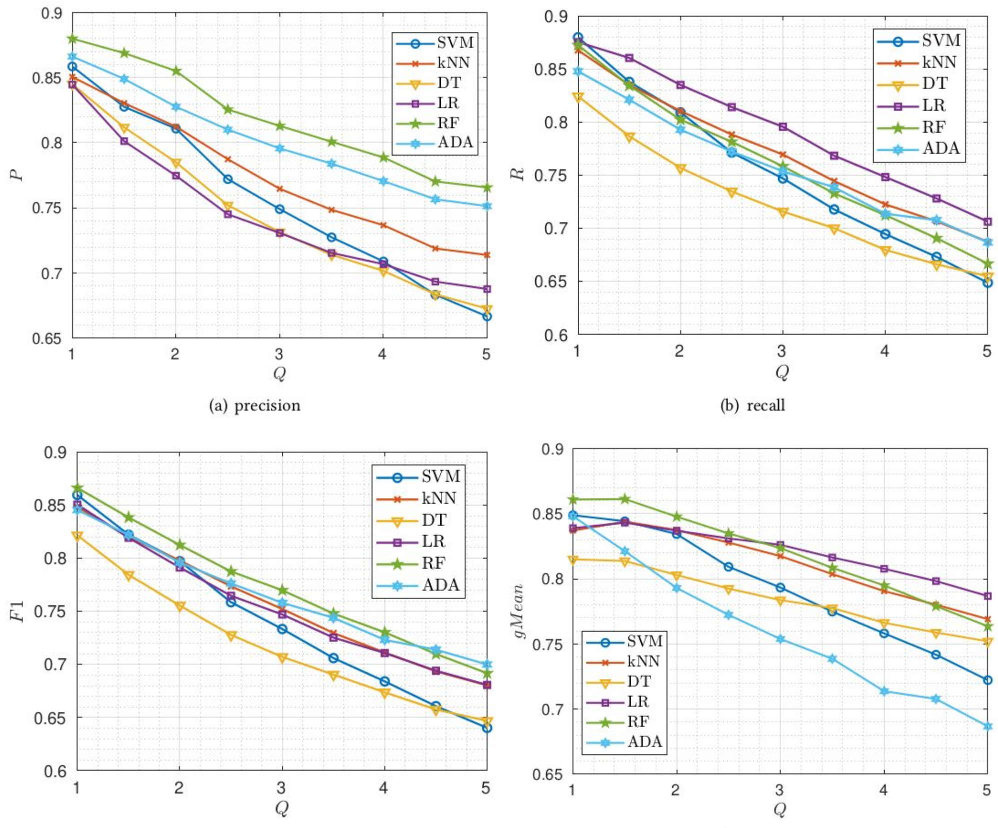


Fig. 5. $F1$ score of kNN classifier with different numbers of features NoFs.

Results - Unbalance Effect



(a) precision (b) recall (c) $F1$ (d) G-Mean