Detection of Anomalies in Electric Vehicle Charging Sessions

Dustin Kern, Christoph Krauß, Matthias Hollick

acsd applied cyber security darmstadt

ATHENE National Research Center for Applied Cybersecurity

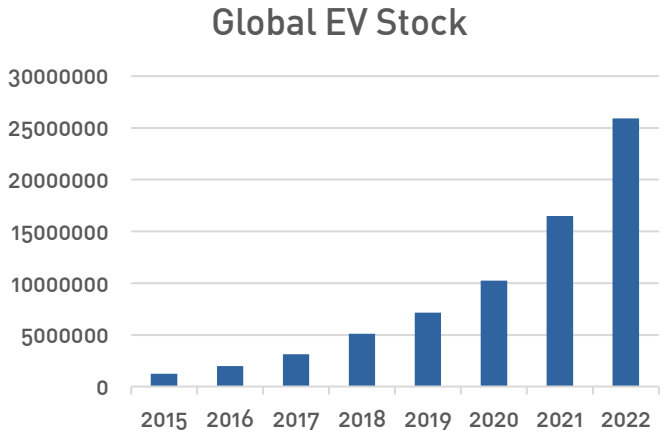
SPONSORED BY
Federal Ministry of Education and Research

HESSEN Hessisches Ministerium für Wissenschaft und Kunst

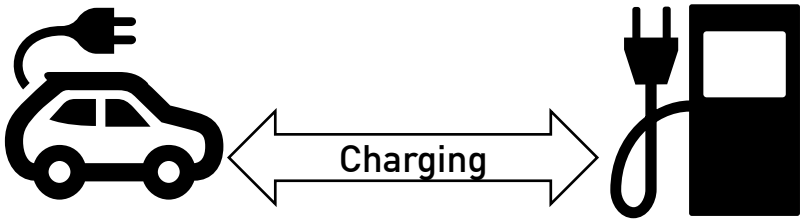
Funded by
DFG Deutsche Forschungsgemeinschaft
German Research Foundation

Introduction

- **Electric Vehicles (EVs)**
  - Growing EV Adoption
  - Charged at Charge Points (CPs)
  - ➢ Cyber-physical threats

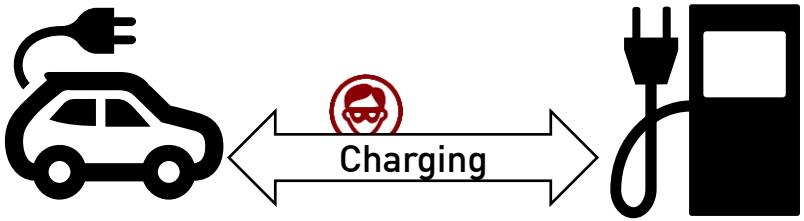


Data Source: https://www.iea.org/data-and-statistics/data-tools/global-ev-data-explorer (accessed 12.06.2023)



Introduction

- **Electric Vehicles (EVs)**
  - Growing EV Adoption
  - Charged at Charge Points (CPs)
  - ➢ Cyber-physical threats
- **EV Charging (high load on grid)**
  - Load balancing
  - Vehicle to Grid (V2G) power flow



Forbes

EDITORS' PICK | May 15, 2019, 08:21am EDT

As More EVs Hit The Road, Blackouts Become Likely

Oliver Wyman Contributor
Oliver Wyman Contributor Group
Aerospace & Defense
Exploring transport & travel's transformative ideas & technologies

POST WRITTEN BY
Members of the Energy Practice at Oliver Wyman

Oliver Wyman's Thomas Fritz, Andrew Perry, Aditya Ranjan, Joerg Staeglich, and Curtis Underwood collaborated to produce this article.

Power outages may not be as severe if cars are encouraged to charge at power stations. GETTY

Source:
https://www.forbes.com/sites/oliverwyman/2019/05/15/as-more-evs-hit-the-road-blackouts-become-likely/

Motivation

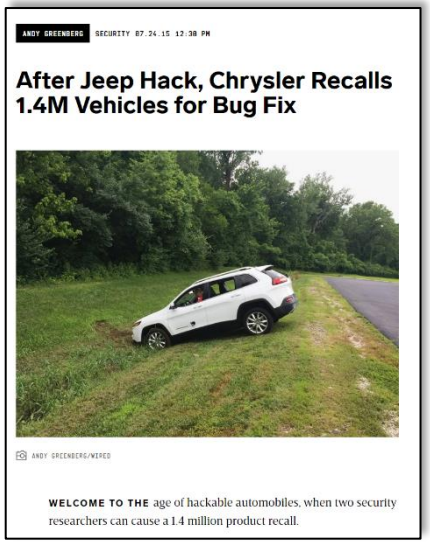
Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks

OCTOBER 11, 2017 // AUTHORS: DONGHUI PARK, MICHAEL WALSTROM

Source:
https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

Motivation

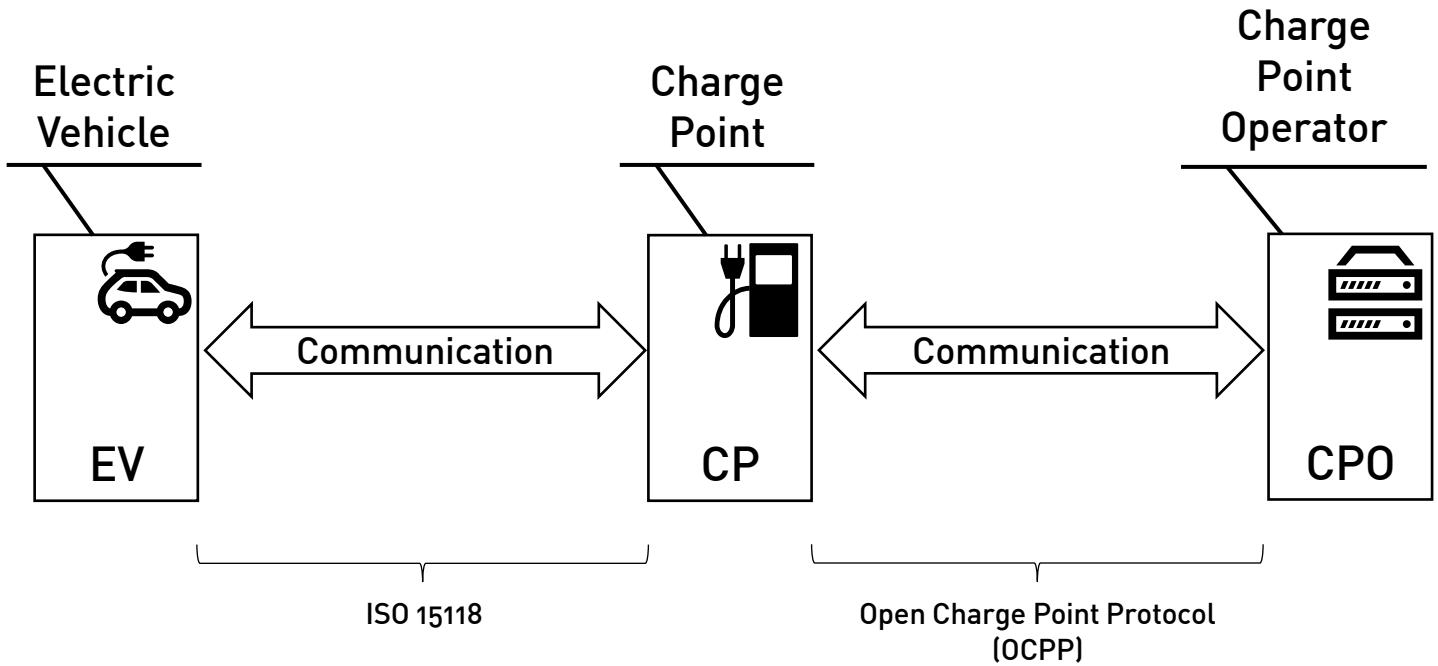
Source: https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/



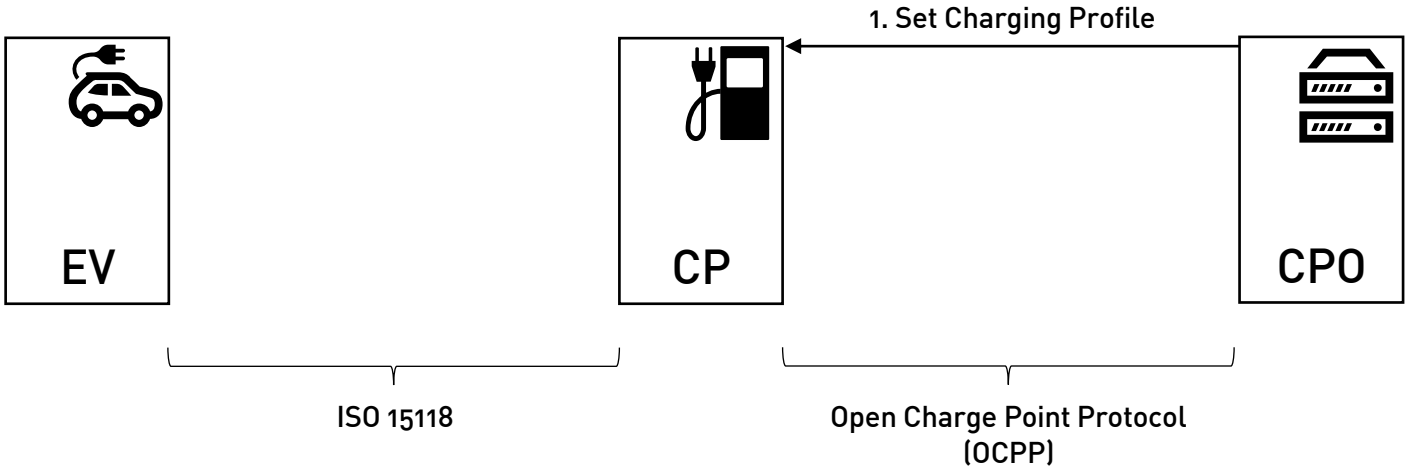
Source: https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/

Source: https://www.pentestpartners.com/security-blog/smart-car-chargers-plug-n-play-for-hackers/

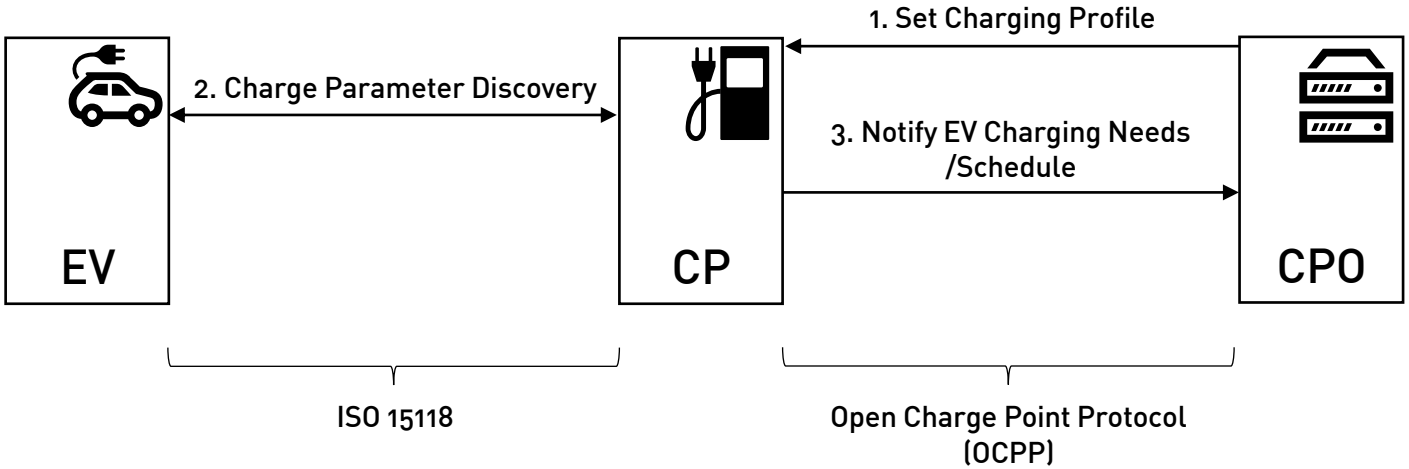
System Model
Overview



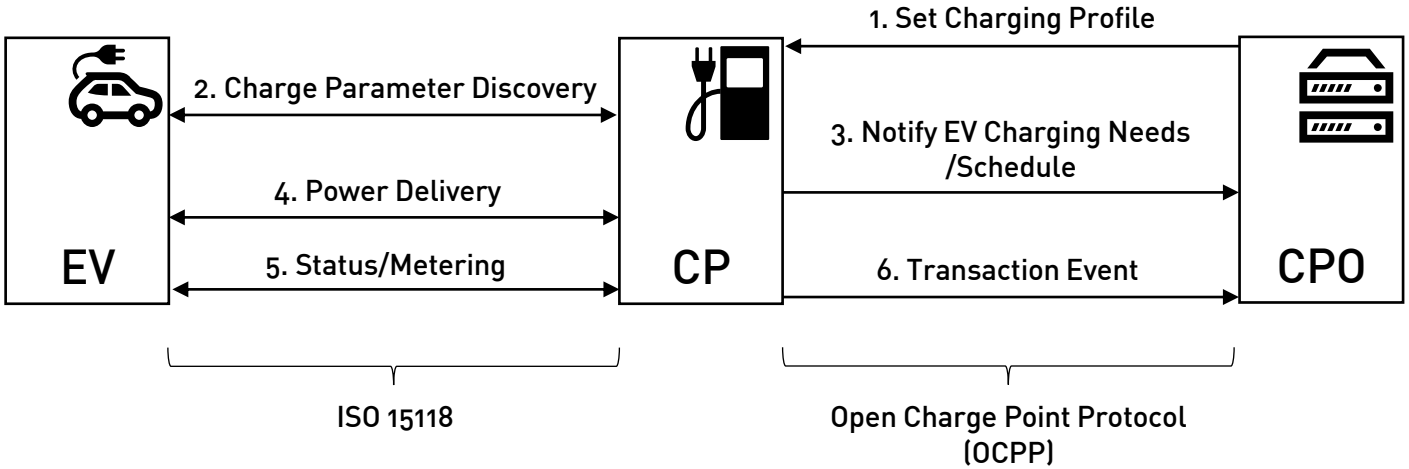
System Model
CPO Charge Profiles



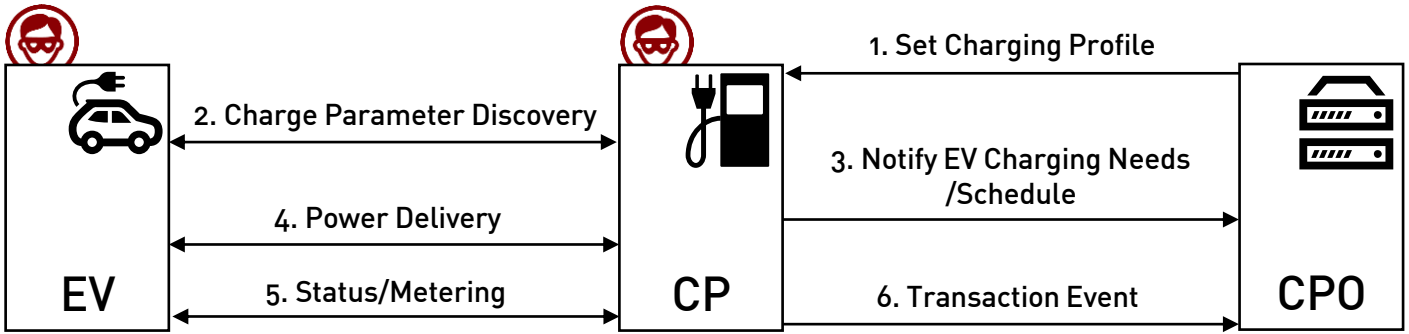
System Model
Charge Parameter Negotiation



System Model
Charge Session

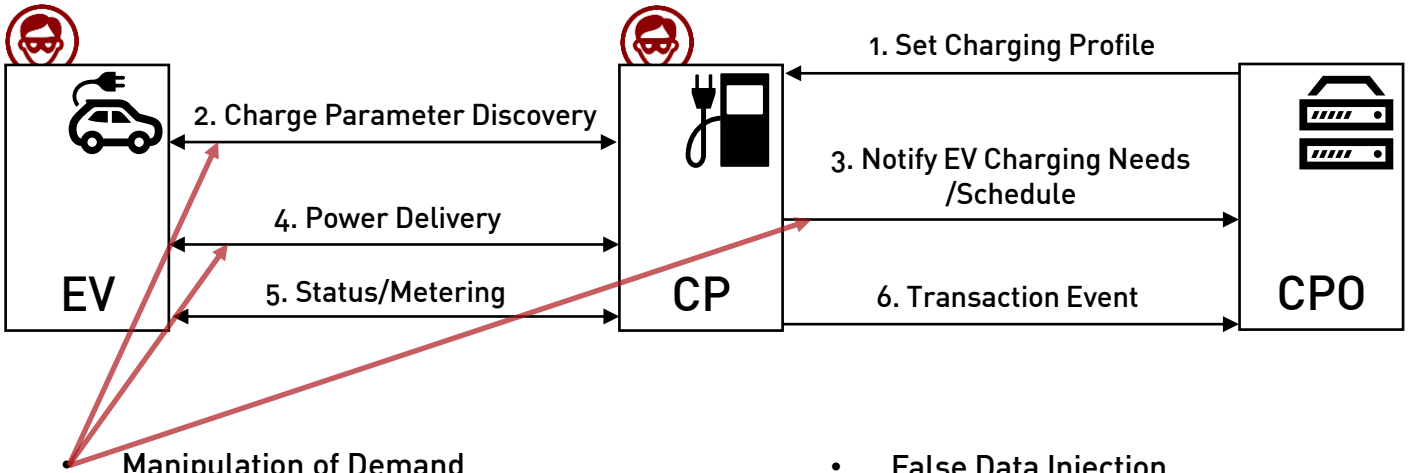


Adversary Model



- Manipulation of Demand
- False Data Injection

Adversary Model

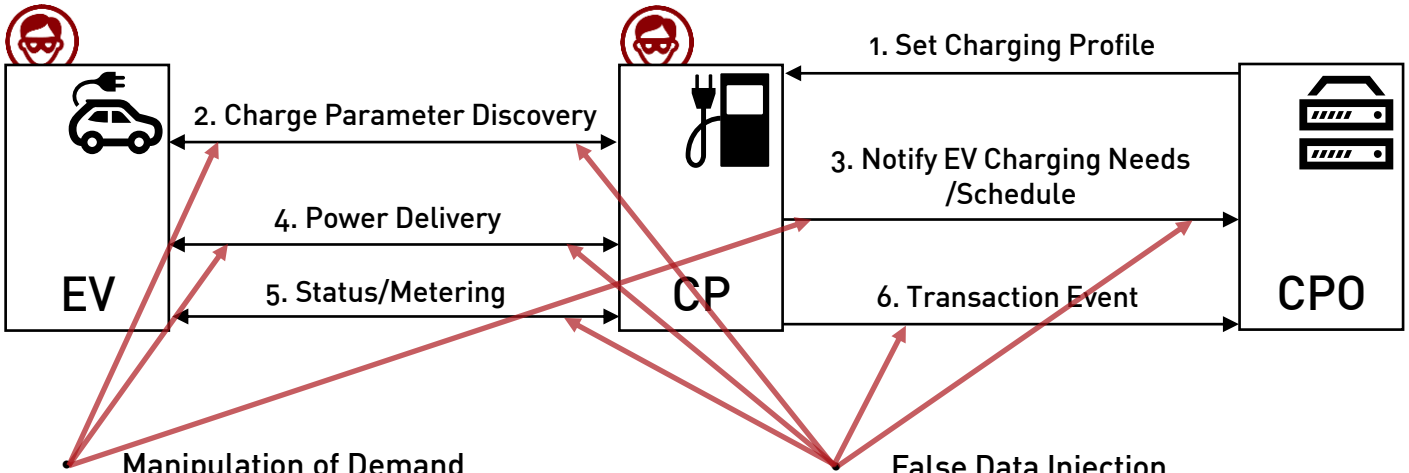


Manipulation of Demand

- ➢ Higher/lower charging speeds
- EV/CP: current or voltage limits
- CP: Charge profiles, tariffs
- EV: Charge profile/tariff selection

- **False Data Injection**

Adversary Model



Manipulation of Demand

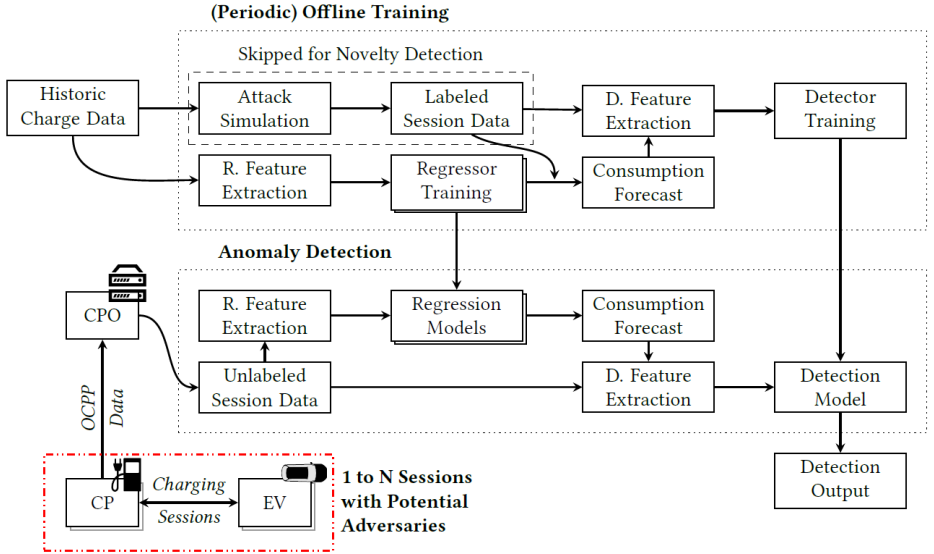
- ➢ Higher/lower charging speeds
- EV/CP: current or voltage limits
- CP: Charge profiles, tariffs
- EV: Charge profile/tariff selection

False Data Injection

- ➢ Inaccurate State Estimation
- EV/CP: Energy amount + departure time, planned consumption over time, charge profile selection
- CP: Meter values

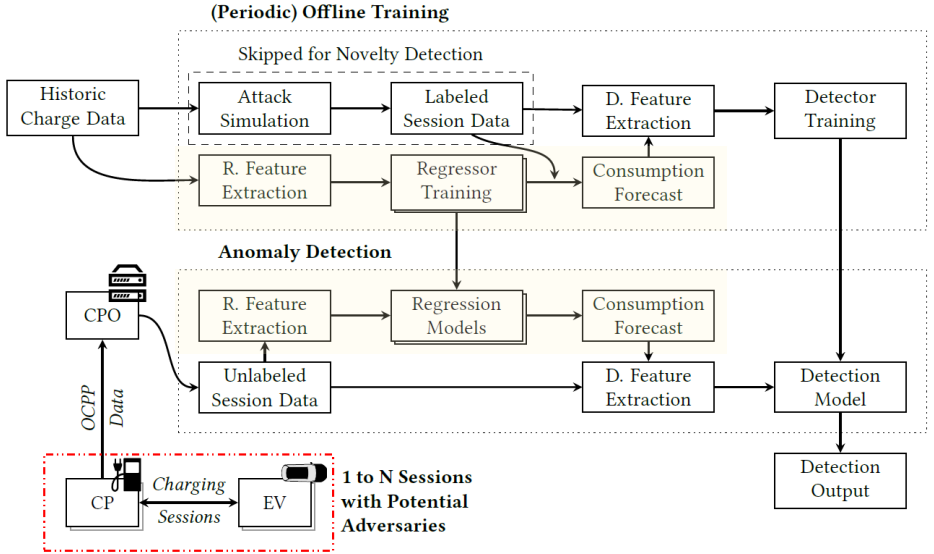
IDS for EV Charge Session Anomalies

- **Hybrid model for anomaly detection:**
  - Semi-supervised regression model
  - Detection model
    - Supervised classification
    - Semi-supervised novelty detection



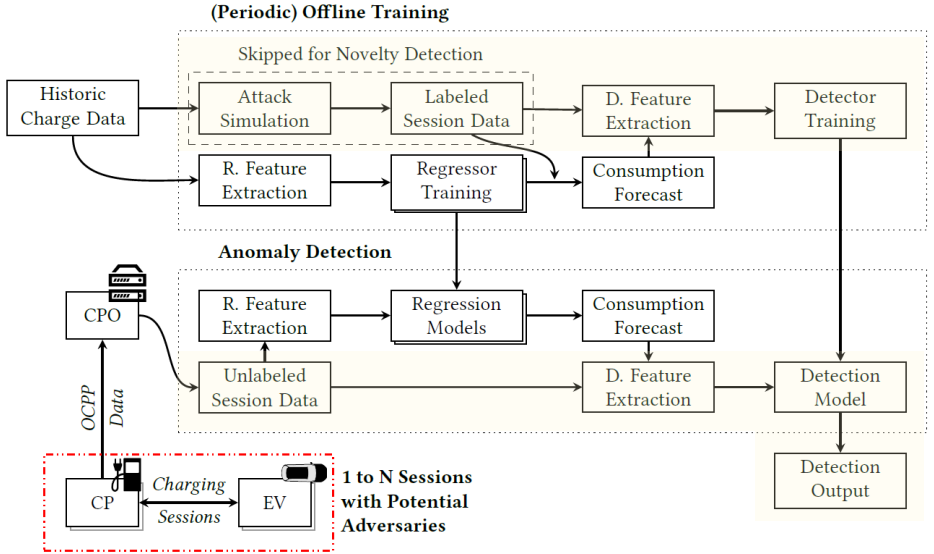
IDS for EV Charge Session Anomalies

- **Hybrid model for anomaly detection:**
  - Semi-supervised regression model
    - Trained on data w/o attacks
    - Generates charge speed predictions
  - Detection model
    - Supervised classification
    - Semi-supervised novelty detection



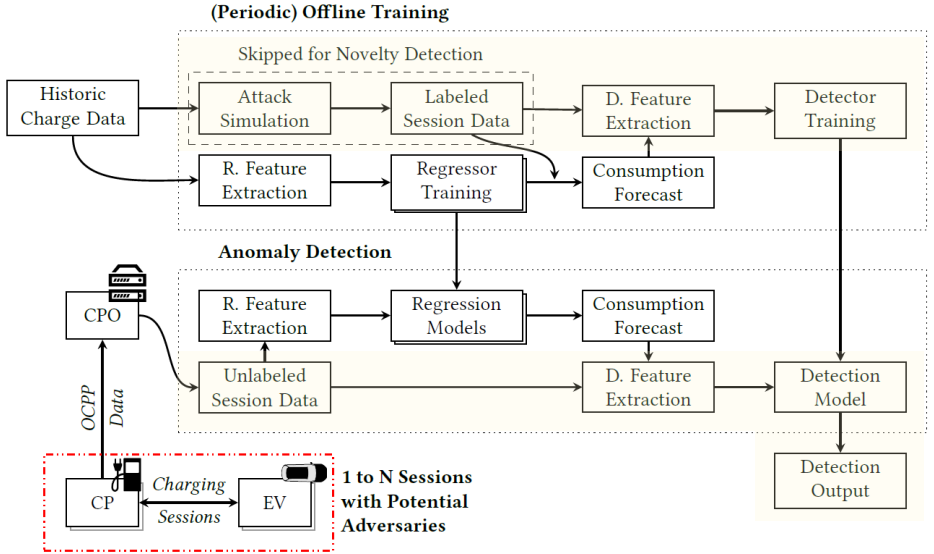
IDS for EV Charge Session Anomalies

- **Hybrid model for anomaly detection:**
  - Semi-supervised regression model
    - Trained on data w/o attacks
    - Generates charge speed predictions
  - Detection model
    - Supervised classification
      - Trained on data w/ simulated attacks
      - ➢ Lower false positives
    - Semi-supervised novelty detection
      - Trained on data w/o attacks
      - ➢ Better generalization



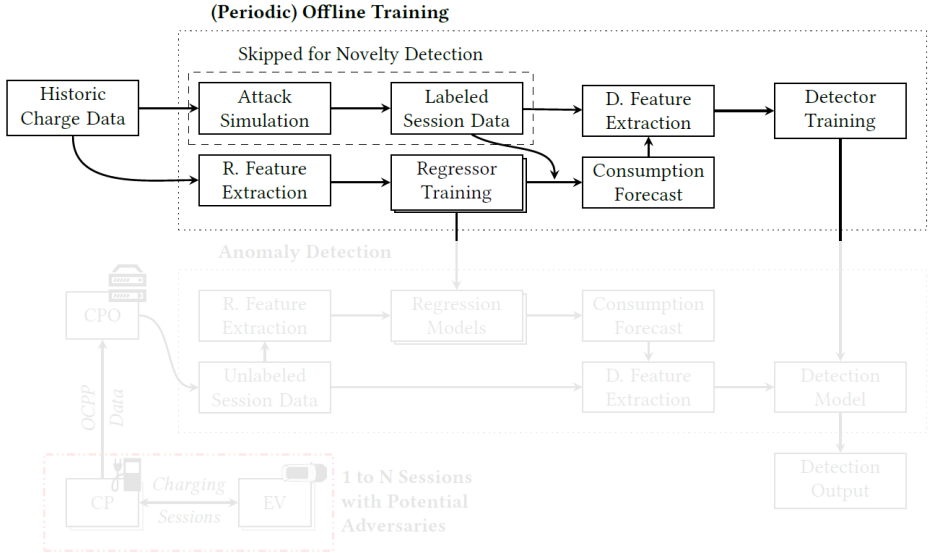
IDS for EV Charge Session Anomalies

- **Hybrid model for anomaly detection:**
  - Semi-supervised regression model
    - Trained on data w/o attacks
    - Generates charge speed predictions
  - Detection model
    - Supervised classification
      - Trained on data w/ simulated attacks
      - ➢ Lower false positives
    - Semi-supervised novelty detection
      - Trained on data w/o attacks
      - ➢ Better generalization
    - Ensemble of classification and novelty detection
      - ➢ Combine advantages



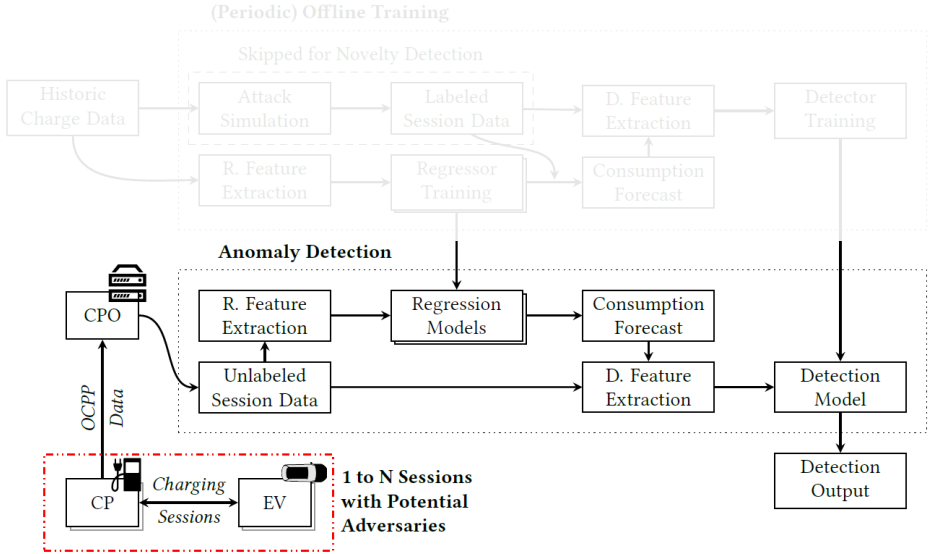
IDS for EV Charge Session Anomalies

- **Offline Training**
  - Based on historic charge session data
  - Feature selection
    - High-level features
    - Charging behavior
    - Consumption predictions
  - Simulated attacks (for classification model)
    - Random anomalies in charging behavior



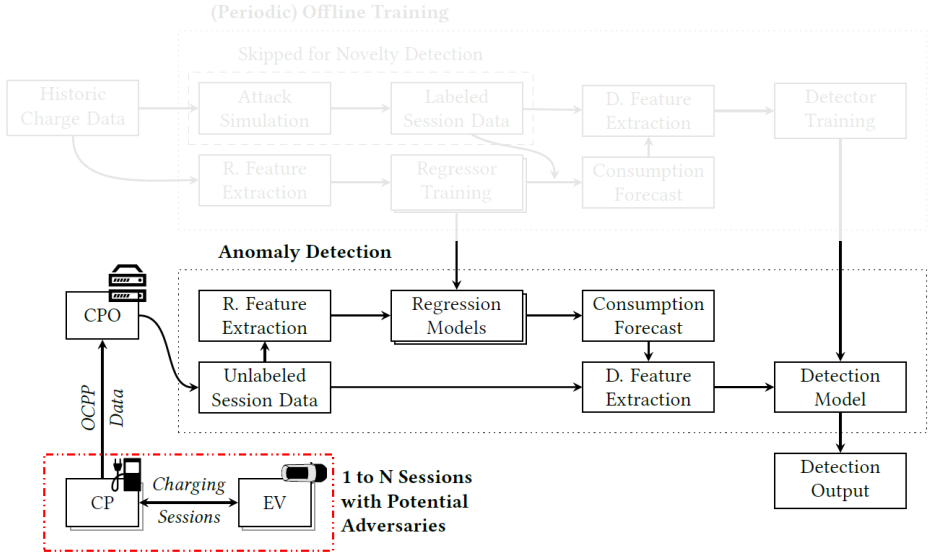
IDS for EV Charge Session Anomalies

- **Anomaly Detection During Live Operation**
  - Process
    - Generate the consumption forecasts
    - Generate the relevant detection features
    - Classify session (normal/anomaly)



IDS for EV Charge Session Anomalies

- **Anomaly Detection During Live Operation**
  - Process
    - Generate the consumption forecasts
    - Generate the relevant detection features
    - Classify session (normal/anomaly)
  - Ensemble detection combining:
    - Classification-based detection
      - \+ High TPR on known/trained-on attacks
      - – Lower TPR for previously unseen attacks
    - Novelty-based detection
      - \+ Generalize better to unseen attacks
      - – Higher FPR
    - Weighted voting tuned towards low FPR

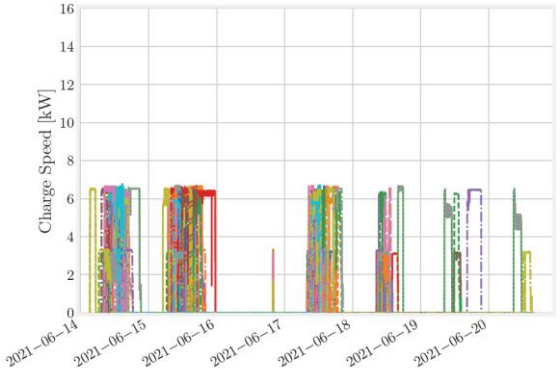


TPR := True Positive Rate
FPR := False Positive Rate

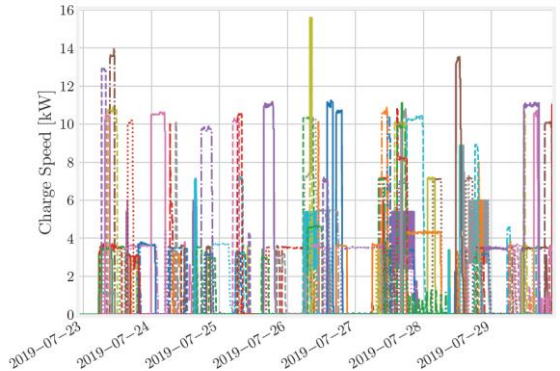
Evaluation – Data Sets

- **3 Adaptive Charging Network (ACN) data sets**
  - ACN Caltech (54 semi-public CPs)
  - ACN JPL (52 workplace CPs)
  - ACN Office (8 workplace CPs)
- **ElaadNL data set**
  - 850 public CPs

➢ **Detailed charging data during each session**



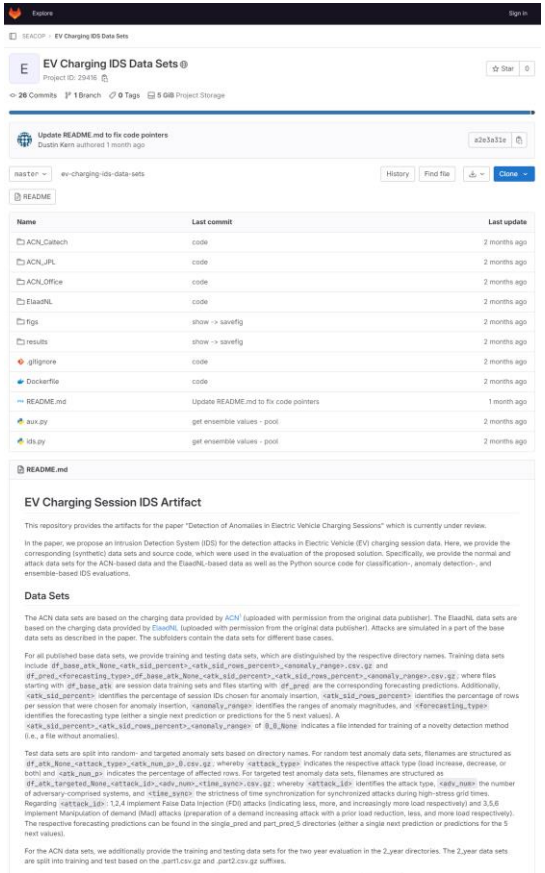
(a) ACN JPL Data Set



(b) ElaadNL Data Set

Evaluation – Attack Data Sets

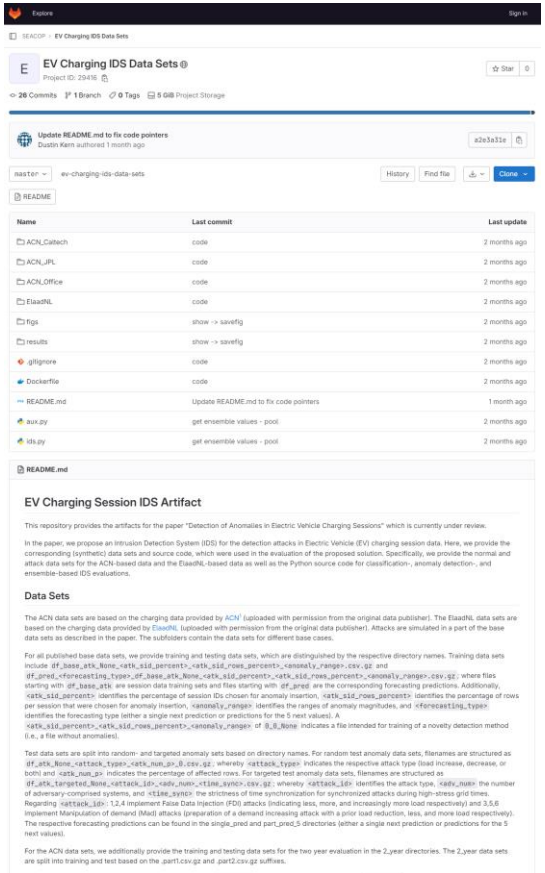
- **11 months of training/validation data**
  - Normal traffic without attacks
  - Simulated attacks for classifier training
- **Several 1 month testing data sets**



- **Data/code provided online: https://code.fbi.h-da.de/seacop/ev-charging-ids-data-sets**

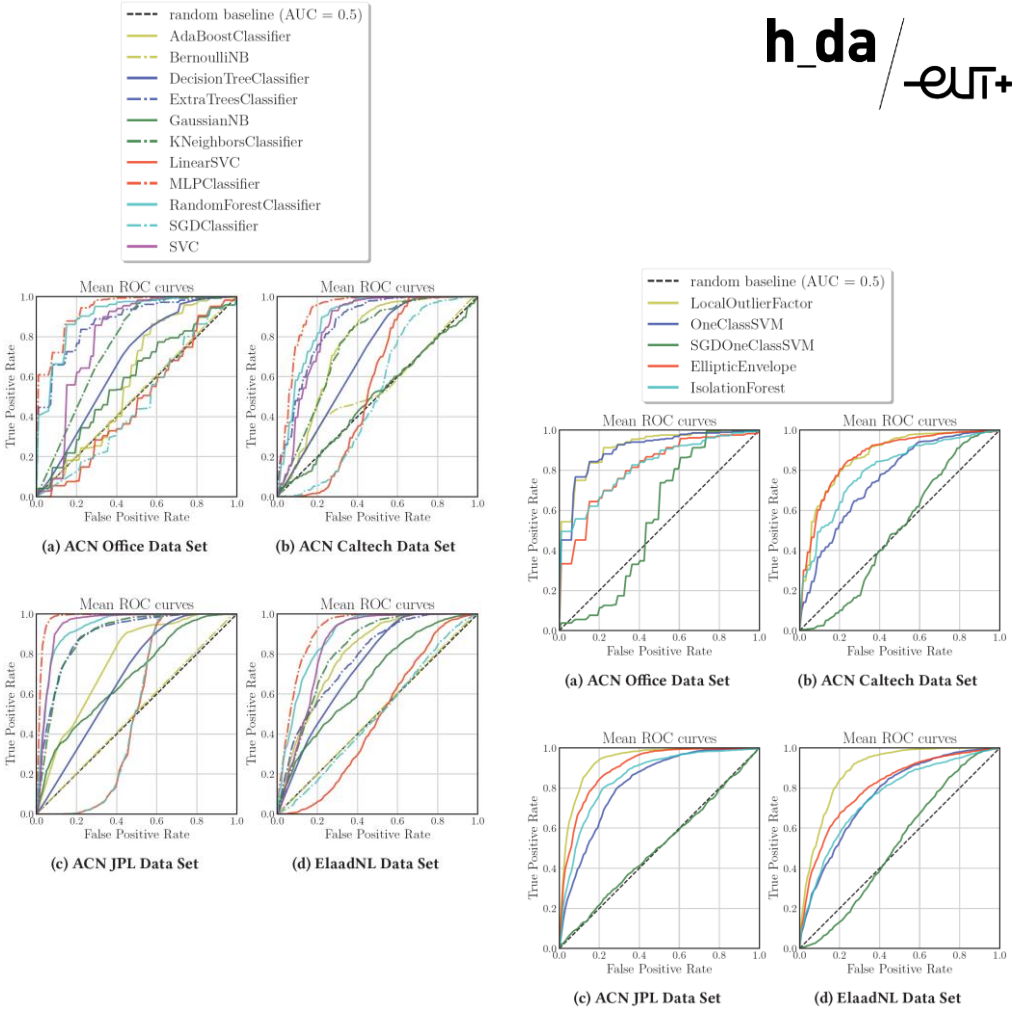
Evaluation – Attack Data Sets

- **11 months of training/validation data**
  - Normal traffic without attacks
  - Simulated attacks for classifier training
- **Several 1 month testing data sets**
  - Manipulation of Demand/False Data Injection
  - Different magnitudes and compromise levels
  - Attack vectors:
    - Synchronized, prepared increase, slow change
  - Fabricated/manipulated data
  - Varying time spans and repetitions
- **Data/code provided online:** https://code.fbi.h-da.de/seacop/ev-charging-ids-data-sets



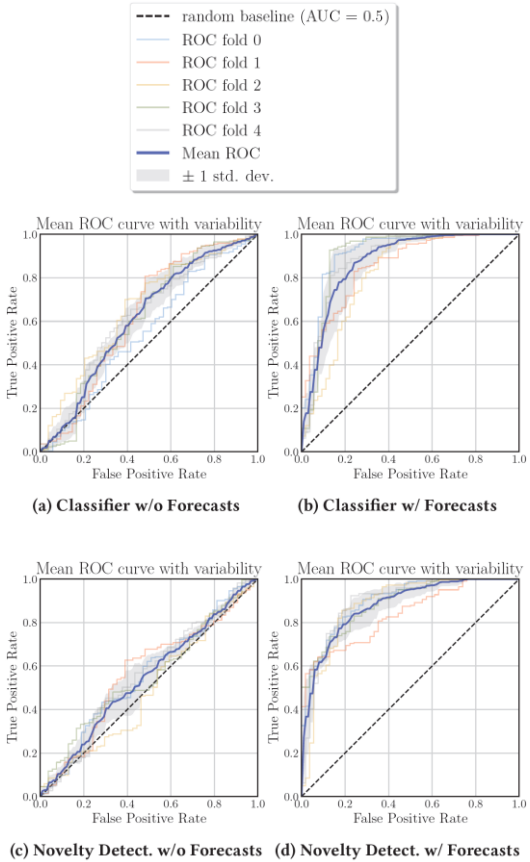
Evaluation – Detection

- Based on sklearn implementations
- Evaluation of fitting algorithms
  - Grid-search-based hyperparameter tuning
  - 5-fold cross validation over training data
  - ➢ MLPClassifier and LocalOutlierFactor



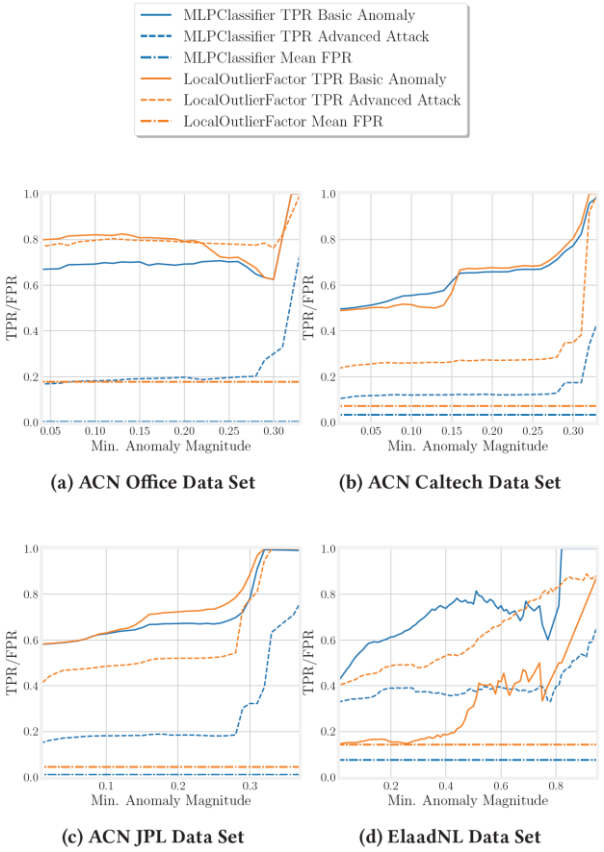
Evaluation – Detection

- **Based on sklearn implementations**
- **Evaluation of fitting algorithms**
  - Grid-search-based hyperparameter tuning
  - 5-fold cross validation over training data
  - ➢ MLPClassifier and LocalOutlierFactor
- **Evaluation of regression-base features**
  - Based on RandomForestRegressor
  - With anomalies during a session
  - 5-fold cross validation over training data



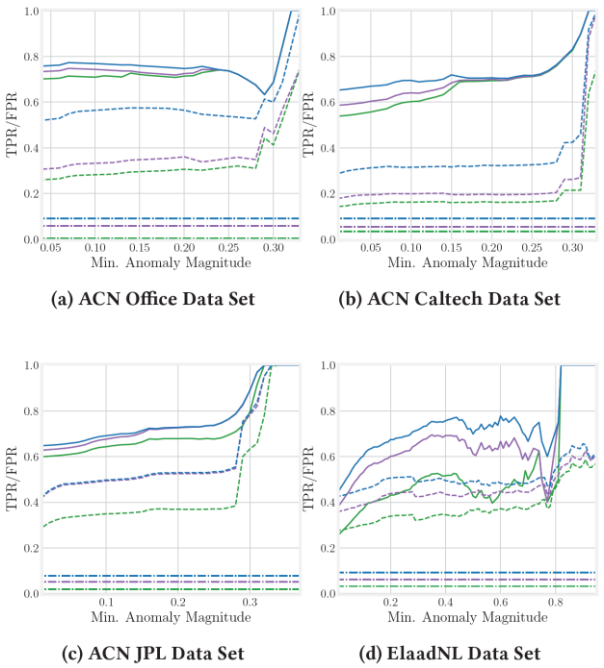
Evaluation – Details

- **Performance on previously unseen data**
  - Random simulated anomalies (same as training)
  - Attacks targeting grid stability (not in training)



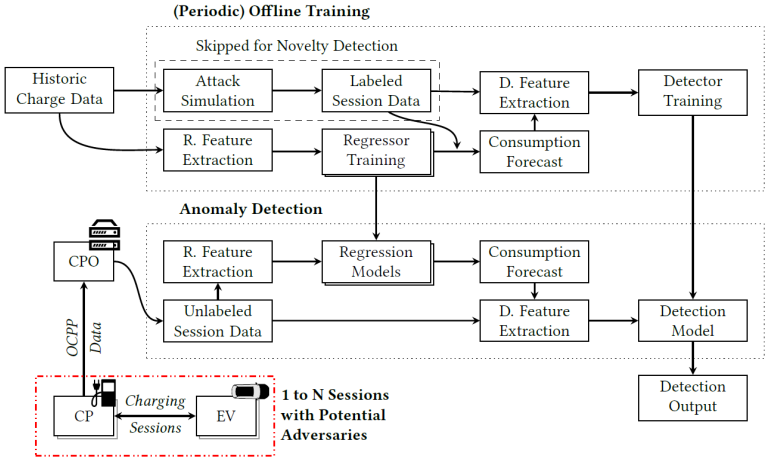
Evaluation – Details

- **Performance on previously unseen data**
  - Random simulated anomalies (same as training)
  - Attacks targeting grid stability (not in training)
- **Evaluation of ensemble**
  - Based on the respective prediction confidence
  - Optimized towards different maximum FPR
  - ➢ Classification and novelty detection can complement each other



Summary

- **EV charging poses cyber-physical threats**
  - E.g., attacks on power grid stability
- **Detection of Anomalies in Electric Vehicle Charging Sessions**
  - Hybrid of regression and anomaly detection
  - Ensemble-based detection
    - Classification model
    - Novelty detection model
- **Evaluation**
  - Shows good design choices and thresholds
  - Good performance of the IDS concept



Thank you for your attention. Questions?

Dustin Kern

dustin.kern@h-da.de