

# Detection of Anomalies in Electric Vehicle Charging Sessions

Dustin Kern, Christoph Krauß, Matthias Hollick



SPONSORED BY



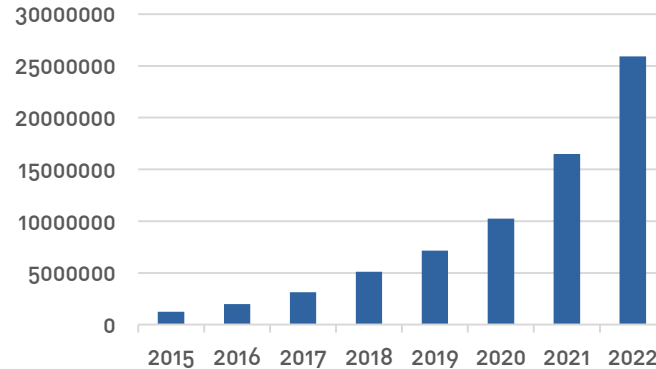
Funded by



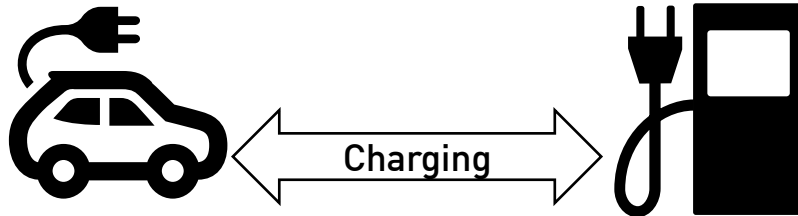
# Introduction

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

## Global EV Stock

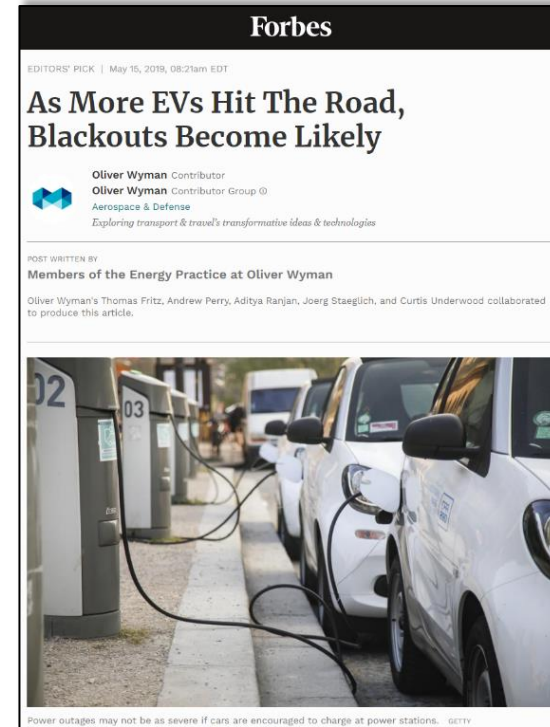
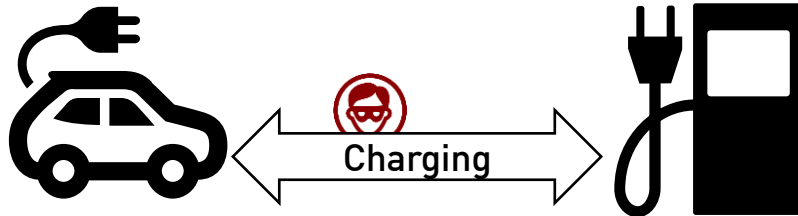


Data Source:  
<https://www.iea.org/data-and-statistics/data-tools/global-ev-data-explorer>  
(accessed 12.06.2023)



# 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



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://jisis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/>

# Motivation

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

OCTOBER 11, 2017 // AUTHORS: [DONGHUI PARK](#), [MICHAEL WALSTROM](#)



Source:

<https://jisis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/>



Source:

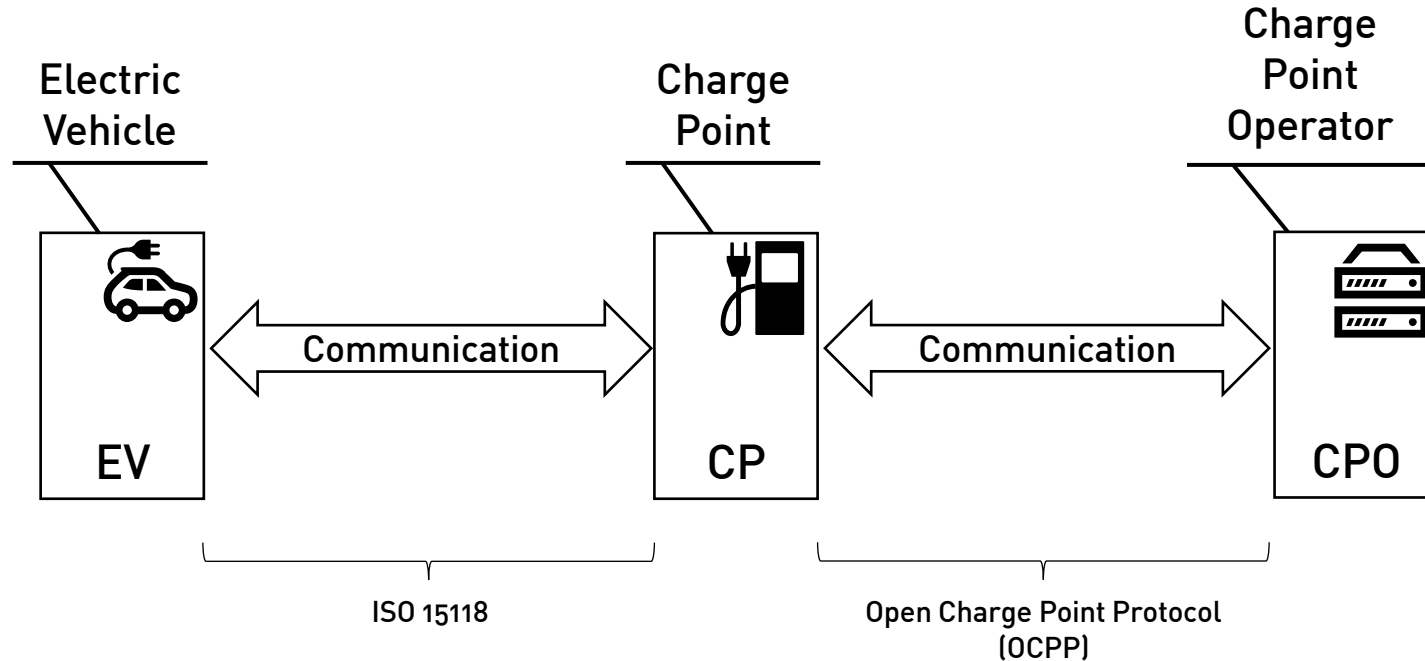
<https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/>



Source:

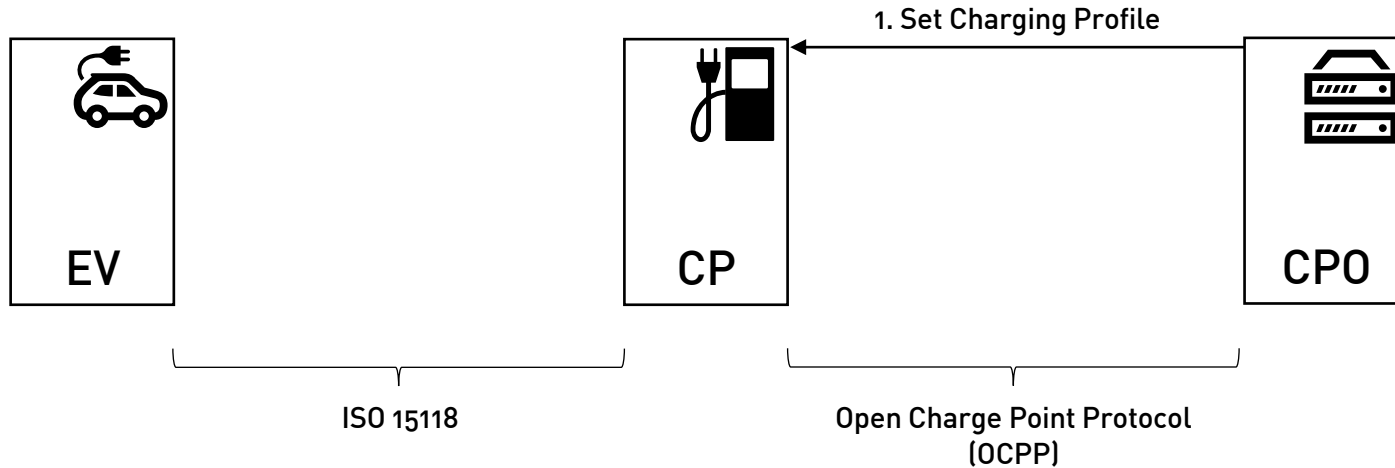
<https://www.pentestpartners.com/security-blog/smart-car-chargers-plug-n-play-for-hackers/>

# System Model Overview



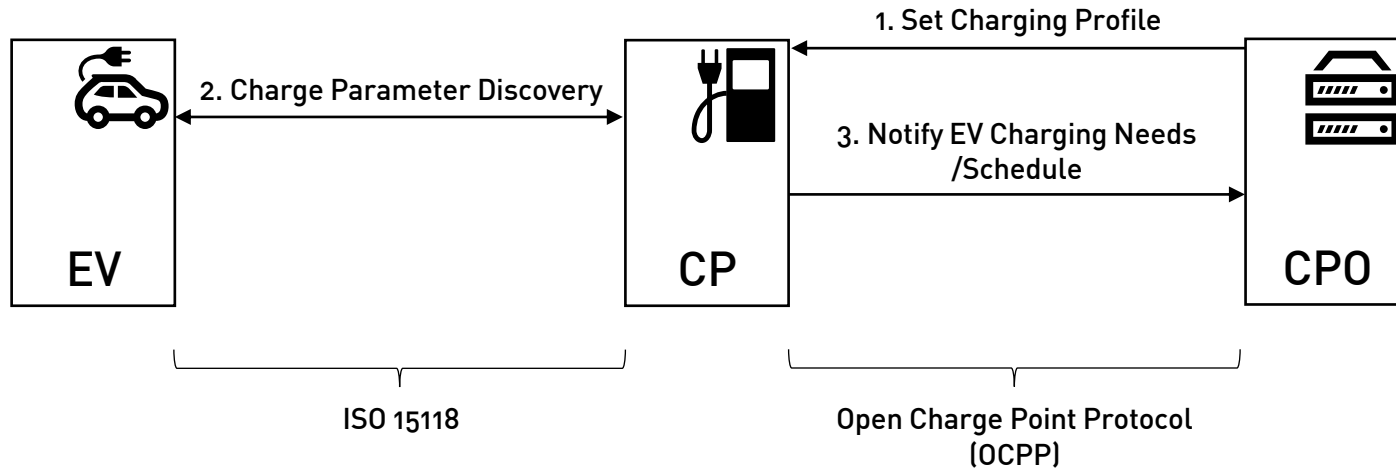
# System Model

## CP0 Charge Profiles



# System Model

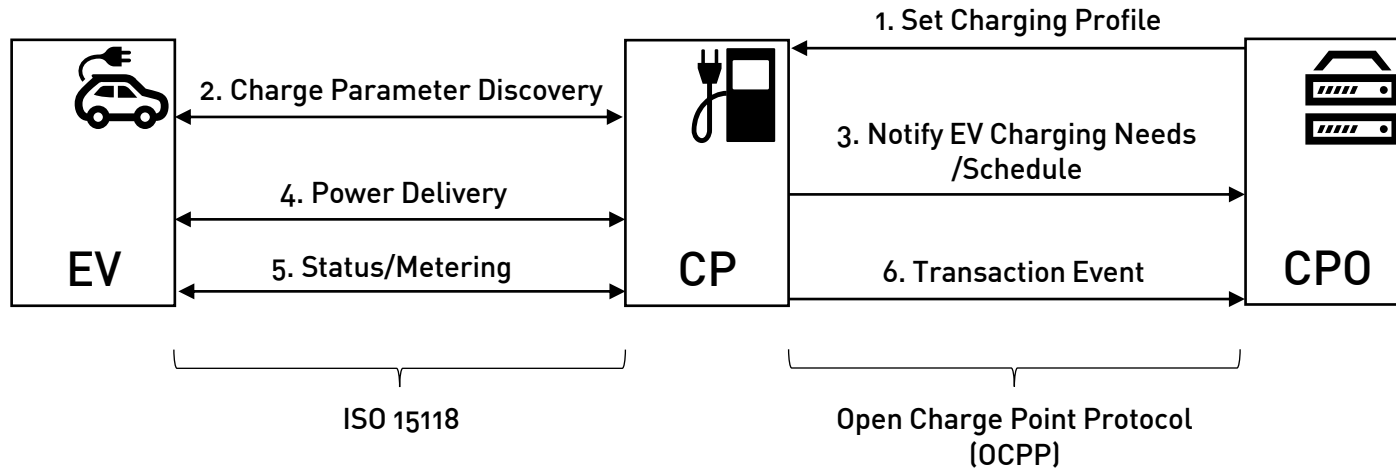
## Charge Parameter Negotiation



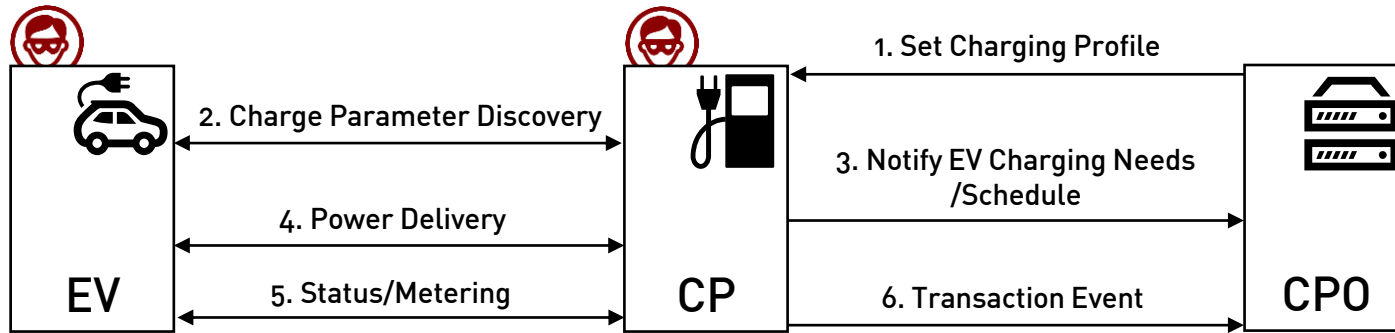


# System Model

## Charge Session



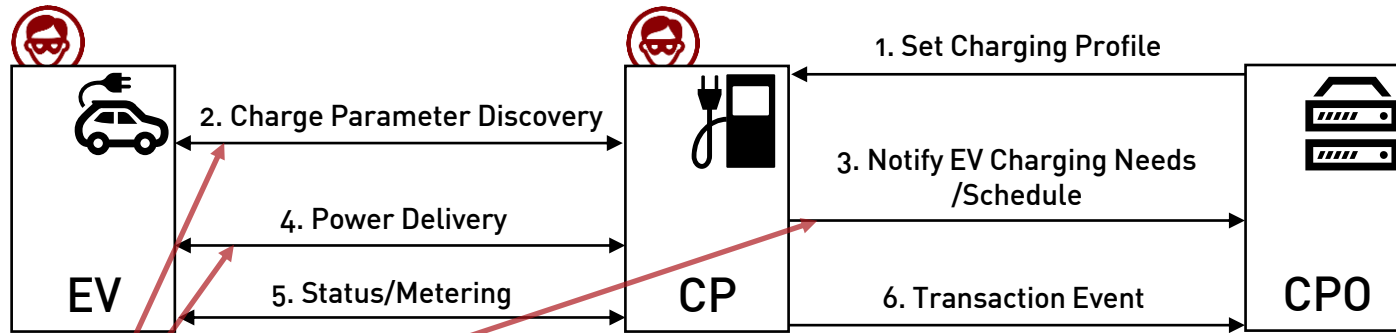
# Adversary Model



- Manipulation of Demand

- False Data Injection

# Adversary Model

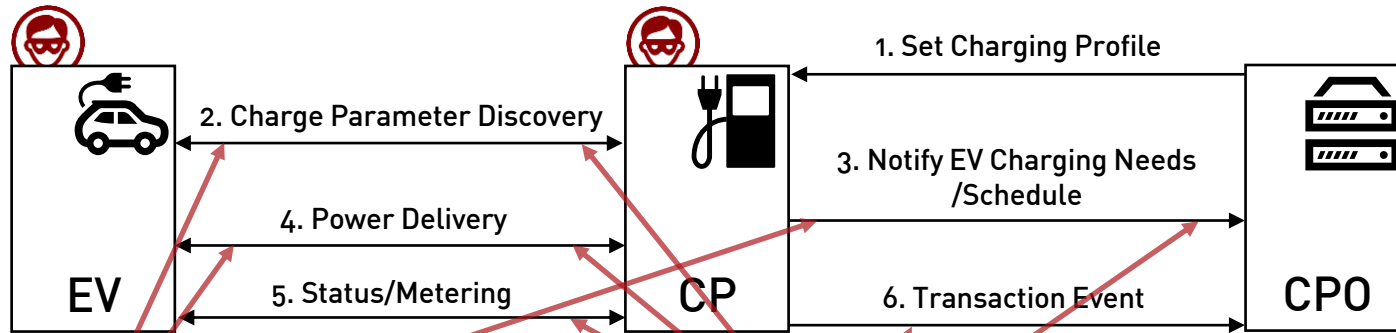


## Manipulation of Demand

- 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

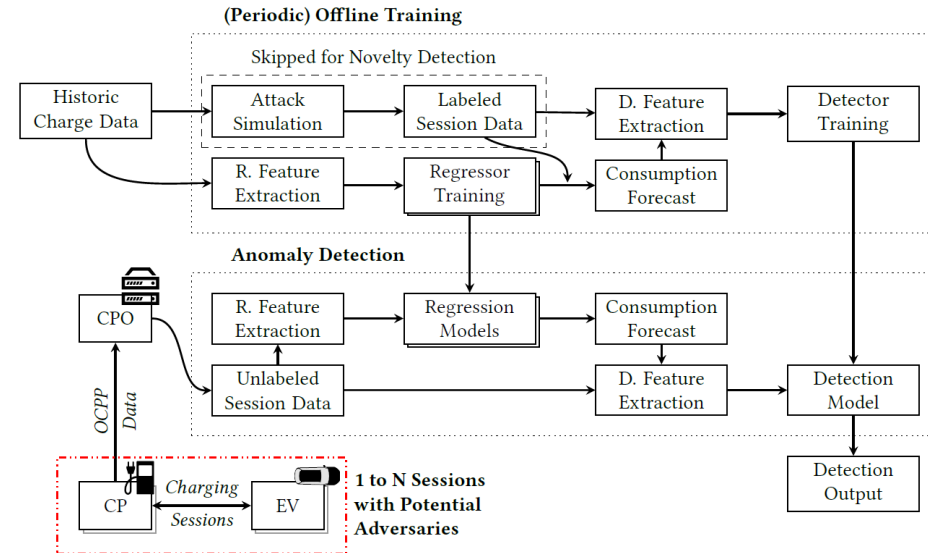
- Higher/lower charging speeds
  - EV/CP: current or voltage limits
  - CP: Charge profiles, tariffs
  - EV: Charge profile/tariff selection

## False Data Injection

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

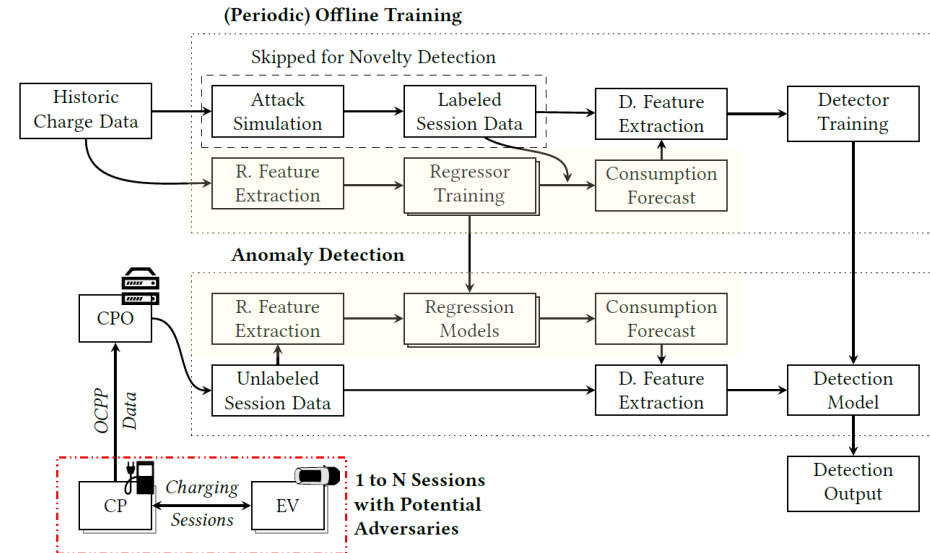
# IDS for EV Charge Session Anomalies

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



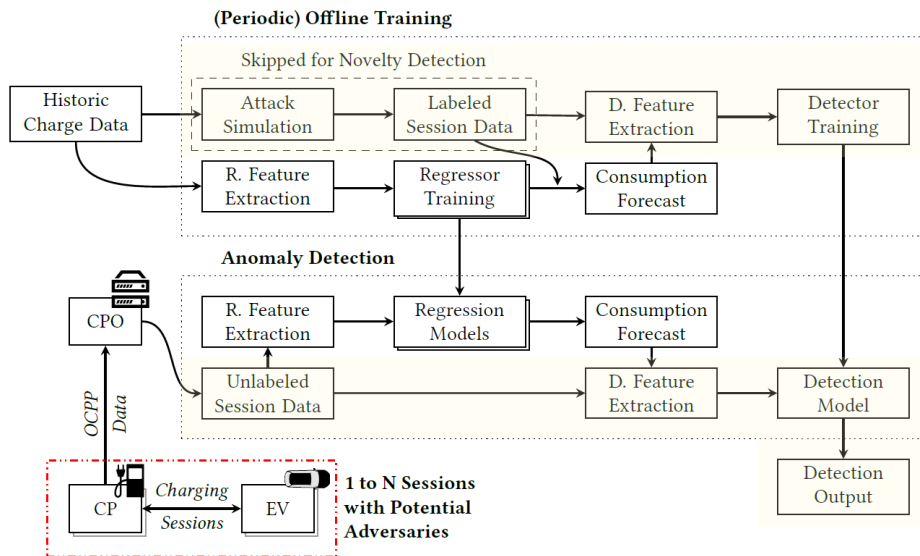
# IDS for EV Charge Session Anomalies

- 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



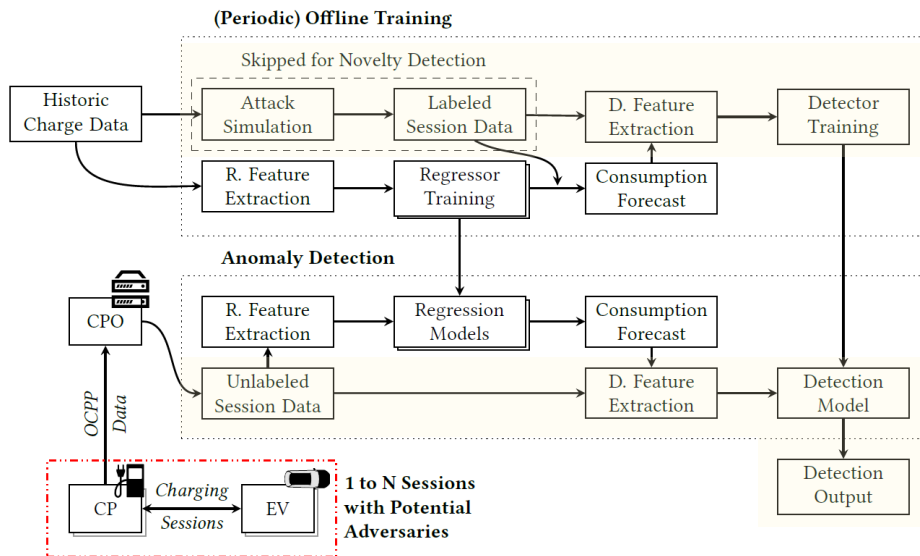
# IDS for EV Charge Session Anomalies

- **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

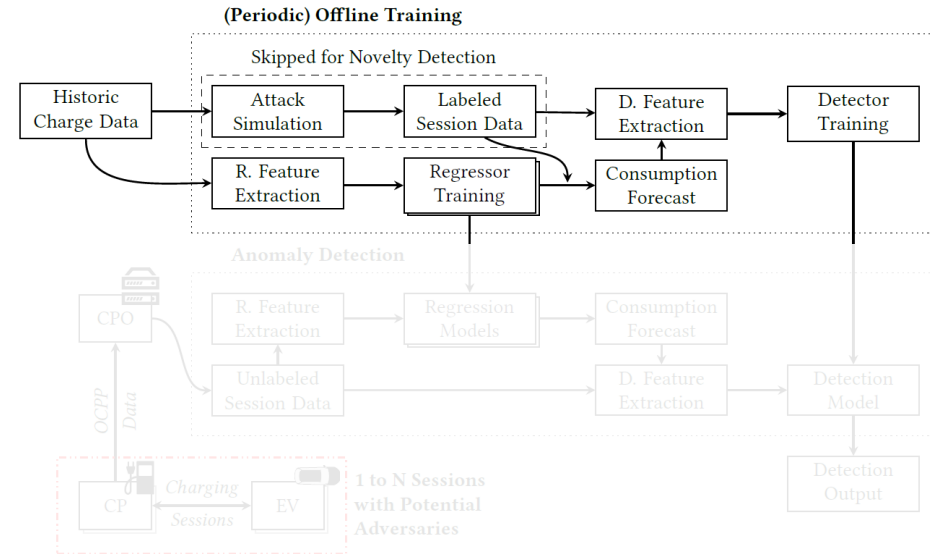
- **Hybrid model for anomaly detection:**
  - Semi-supervised regression model
    - Trained on data w/o attacks
    - Generates charge speed predictions
  - Detection model
    - Supervised classification
      - Trained on data w/ simulated attacks
        - Lower false positives
    - Semi-supervised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





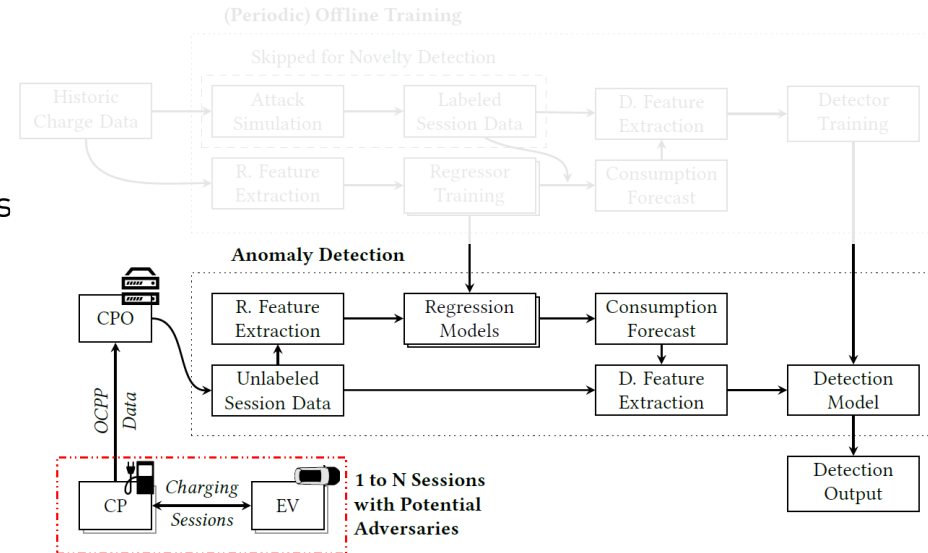
# IDS for EV Charge Session Anomalies

- **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



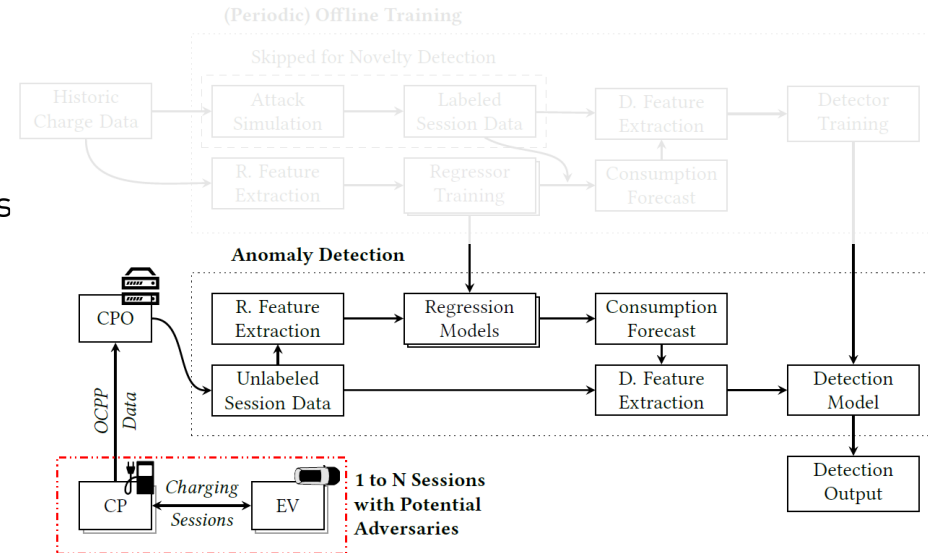
# IDS for EV Charge Session Anomalies

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



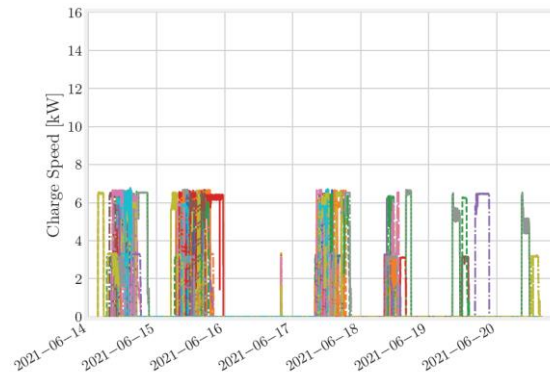
# IDS for EV Charge Session Anomalies

- **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

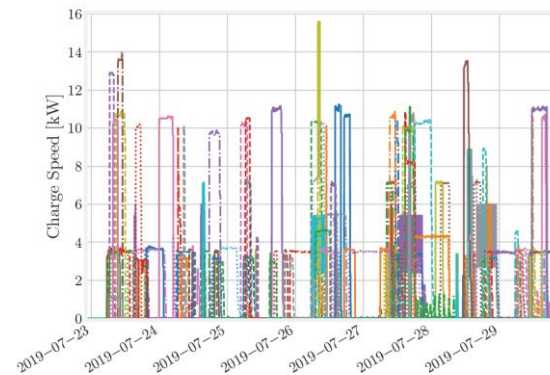


# Evaluation – Data Sets

- 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>



Ev Charging IDS Data Sets

Project ID: 20418

28 Commits 1 Branch 0 Tags 5 GB Project Storage

Update README.md to fix code pointers  
Dustin Kahn authored 1 month ago

ev-charging-ids-data-sets

| Name        | Last commit                           | Last update  |
|-------------|---------------------------------------|--------------|
| ACN_Cattech | code                                  | 2 months ago |
| ACN_ILPL    | code                                  | 2 months ago |
| ACN_Office  | code                                  | 2 months ago |
| ElaadNL     | code                                  | 3 months ago |
| figs        | show -> savefig                       | 2 months ago |
| results     | show -> savefig                       | 2 months ago |
| gfigstore   | code                                  | 2 months ago |
| Dockerfile  | code                                  | 2 months ago |
| README.md   | Update README.md to fix code pointers | 1 month ago  |
| aux.py      | get ensemble values - pool            | 2 months ago |
| ids.py      | get ensemble values - pool            | 2 months ago |

**EV Charging Session IDS Artifact**

This repository provides the artifacts for the paper "Detection of Anomalies in Electric Vehicle Charging Sessions" which is currently under review.

In the paper, we propose an Intrusion Detection System (IDS) for the detection attacks in Electric Vehicle (EV) charging session data. Here, we provide the corresponding (synthetic) data sets and source code, which were used in the evaluation of the proposed solution. Specifically, we provide the normal and attack data sets for the ACN-based data and the ElaadNL-based data as well as the Python source code for classification-, anomaly detection-, and ensemble-based IDS evaluations.

**Data Sets**

The ACN data sets are based on the charging data provided by ACN<sup>1</sup> (uploaded with permission from the original data publisher). The ElaadNL data sets are based on the charging data provided by ElaadNL (uploaded with permission from the original data publisher). Attacks are simulated in a part of the base data sets as described in the paper. The subfolders contain the data sets for different base cases.

For all published base data sets, we provide training and testing data sets, which are distinguished by the respective directory names. Training data sets include `df_base_att_name_<atk_sid_percent>-<atk_sid_rows_percent>-<anomaly_range>-csv.gz` and `df_pred_<forecasting_type>-df_base_att_name_<atk_sid_percent>-<atk_sid_rows_percent>-<anomaly_range>-csv.gz`, where files starting with `df_base_attk` are session data training sets and files starting with `df_pred` are the corresponding forecasting predictors. Additionally, `<atk_sid_percent>` identifies the percentage of session IDs chosen for anomaly insertion, `<atk_sid_rows_percent>` identifies the percentage of rows per session that were chosen for anomaly insertion, `<anomaly_range>` identifies the ranges of anomaly magnitudes, and `<forecasting_type>` identifies the forecasting type (either a single next predictor or predictors for the 5 next values). A `<atk_sid_percent>-<atk_sid_rows_percent>-<anomaly_range>-df_0_0_0.csv` indicates a file intended for training of a novelty detection method (i.e., a file without anomalies).

Test data sets are split into random- and targeted anomaly sets based on directory names. For random test anomaly data sets, filenames are structured as `df_test_name_<attack_type>-<atk_sid_rows_percent>-<atk_sid_rows_percent>-<anomaly_range>-csv.gz`, where `<attack_type>` indicates the respective attack type (load increase, decrease, or both) and `<atk_sid_rows_percent>` indicates the percentage of affected rows. For targeted test anomaly data sets, filenames are structured as `df_att_targeted_name_<attack_sid>-<csv_num>-<time_window>-csv.gz`, where `<attack_sid>` identifies the attack type, `<csv_num>` the number of adversary-compromised systems, and `<time_window>` the time interval for synchronized attacks during high-stress grid times.

Regarding `<attack_sid>`: 1, 2 implement False Data Injection (FDI) attacks (indicating less, more, and increasingly more load respectively) and 3, 5, 6 implement Manipulation of demand (Mand) attacks (preparation of a demand increasing attack with a prior load reduction, less, and more load respectively). The respective forecasting predictions can be found in the `single_pred` and `part2_pred` sub-directories (either a single next predictor or predictors for the 5 next values).

For the ACN data sets, we additionally provide the training and testing data sets for the two year evaluation in the `2_year` directories. The `2_year` data sets are split into training and test based on the `part1.csv.gz` and `part2.csv.gz` suffixes.

# 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>



EV Charging IDS Data Sets

Project ID: 20416

28 Commits 1 Branch 0 Tags 5 GB Project Storage

Update README.md to fix code pointers  
Dustin Kahn authored 1 month ago

ev-charging-ids-data-sets

| Name        | Last commit                           | Last update  |
|-------------|---------------------------------------|--------------|
| ACN_Cattech | code                                  | 2 months ago |
| ACN_ILPL    | code                                  | 2 months ago |
| ACN_Office  | code                                  | 2 months ago |
| ElaadNL     | code                                  | 3 months ago |
| figs        | show -> savefig                       | 2 months ago |
| results     | show -> savefig                       | 2 months ago |
| gfigstore   | code                                  | 2 months ago |
| Dockerfile  | code                                  | 2 months ago |
| README.md   | Update README.md to fix code pointers | 1 month ago  |
| aux.py      | get ensemble values - pool            | 2 months ago |
| ids.py      | get ensemble values - pool            | 2 months ago |

EV Charging Session IDS Artifact

This repository provides the artifacts for the paper "Detection of Anomalies in Electric Vehicle Charging Sessions" which is currently under review.

In the paper, we propose an Intrusion Detection System (IDS) for the detection attacks in Electric Vehicle (EV) charging session data. Here, we provide the corresponding synthetic data sets and source code, which were used in the evaluation of the proposed solution. Specifically, we provide the normal and attack data sets for the ACN-based data and the ElaadNL-based data as well as the Python source code for classification-, anomaly detection-, and ensemble-based IDS evaluations.

**Data Sets**

The ACN data sets are based on the charging data provided by ACN<sup>1</sup> (uploaded with permission from the original data publisher). The ElaadNL data sets are based on the charging data provided by ElaadNL (uploaded with permission from the original data publisher). Attacks are simulated in a part of the base data sets as described in the paper. The subfolders contain the data sets for different base cases.

For all published base data sets, we provide training and testing data sets, which are distinguished by the respective directory names. Training data sets include `df_base_atsk_none_<atk_sid_percent>_<atk_sid_rows_percent>_<anomaly_range>_csv.gz` and `df_ensemble_<forecasting_type>_df_base_atsk_none_<atk_sid_percent>_<atk_sid_rows_percent>_<anomaly_range>_csv.gz`, where files starting with `df_base_atsk` are session data training sets and files starting with `df_ensemble` are the corresponding forecasting predictors. Additionally, `<atk_sid_percent>` identifies the percentage of session IDs chosen for anomaly insertion, `<atk_sid_rows_percent>` identifies the percentage of rows per session that were chosen for anomaly insertion, `<anomaly_range>` identifies the ranges of anomaly magnitudes, and `<forecasting_type>` identifies the forecasting type (either a single next predictor or predictors for the 5 next values). A `<atk_sid_percent>_<atk_sid_rows_percent>_<anomaly_range>` of `0_0_None` indicates a file intended for training of a novelty detection method (i.e., a file without anomalies).

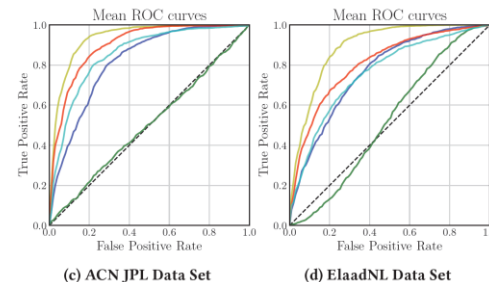
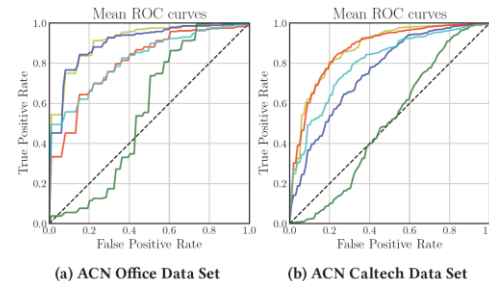
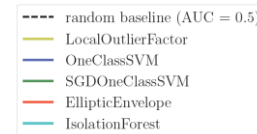
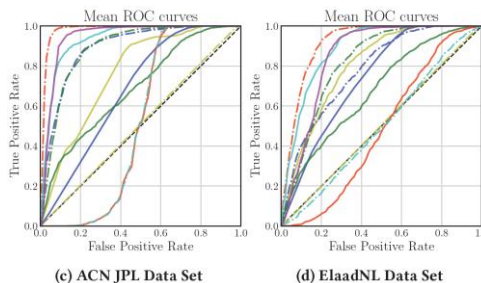
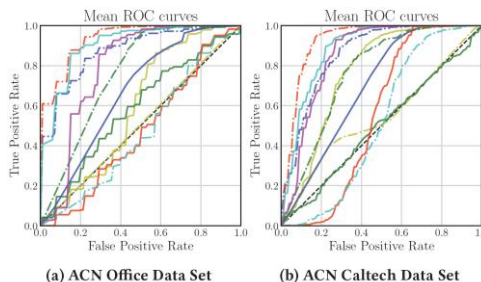
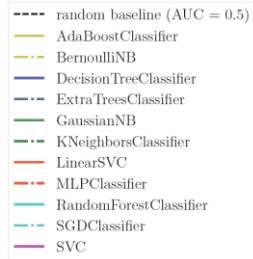
Test data sets are split into random- and targeted anomaly sets based on directory names. For random test anomaly data sets, filenames are structured as `df_atsk_none_<attack_type>_<atk_sid_rows_percent>_<atk_sid_rows_percent>_<anomaly_range>_csv.gz`, whereby `<attack_type>` indicates the respective attack type (load increase, decrease, or both) and `<atk_sid_rows_percent>` indicates the percentage of affected rows. For targeted test anomaly data sets, filenames are structured as `df_atsk_targeted_none_<attack_type>_<adv_num>_<time_window>_csv.gz`, whereby `<attack_type>` identifies the attack type, `<adv_num>` the number of adversary-compromised systems, and `<time_window>` the time span for synchronization for synchronized attacks during high-stress grid times.

Regarding `<attack_sid>`: 1,2 implement False Data Injection (FDI) attacks (indicating less, more, and increasingly more load respectively) and 3,5,6 implement Manipulation of demand (Mand) attacks (preparation of a demand increasing attack with a prior load reduction, less, and more load respectively). The respective forecasting predictions can be found in the `single_ensemble` and `part2_ensemble` directories (either a single next predictor or predictors for the 5 next values).

For the ACN data sets, we additionally provide the training and testing data sets for the two year evaluation in the 2\_year directories. The 2\_year data sets are split into training and test based on the `part1.csv.gz` and `part2.csv.gz` suffixes.

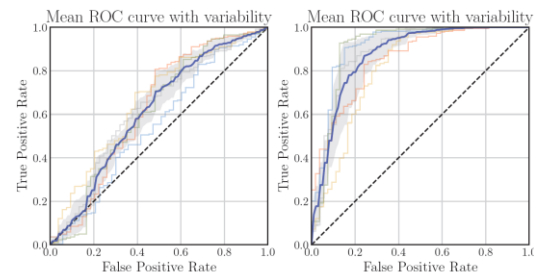
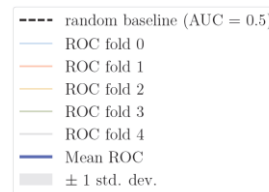
# Evaluation – Detection

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



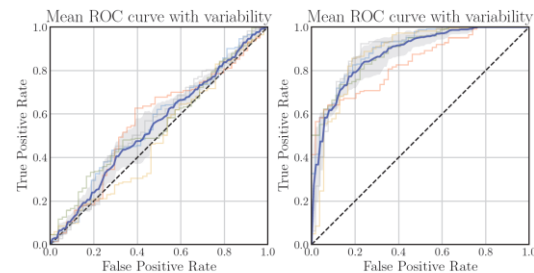
# Evaluation – Detection

- 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



(a) Classifier w/o Forecasts

(b) Classifier w/ Forecasts



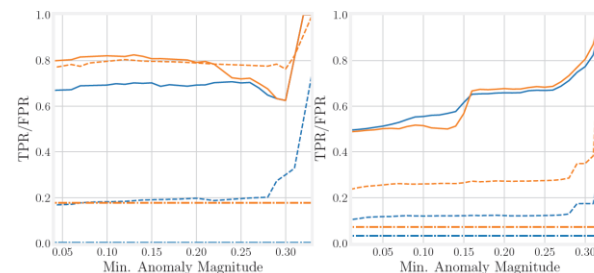
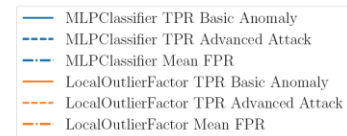
(c) Novelty Detect. w/o Forecasts

(d) Novelty Detect. w/ Forecasts



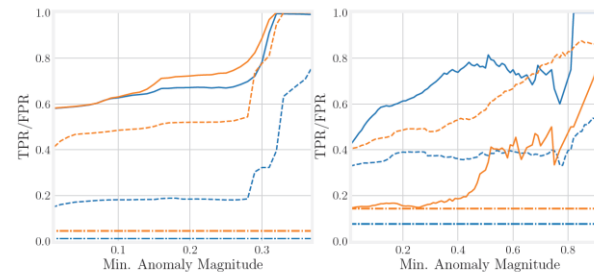
# Evaluation – Details

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



(a) ACN Office Data Set

(b) ACN Caltech Data Set

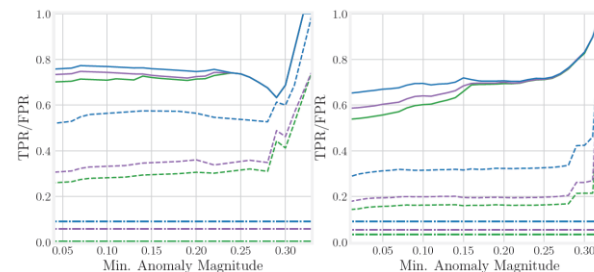
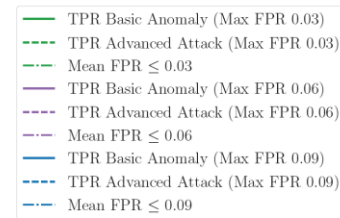


(c) ACN JPL Data Set

(d) ElaadNL Data Set

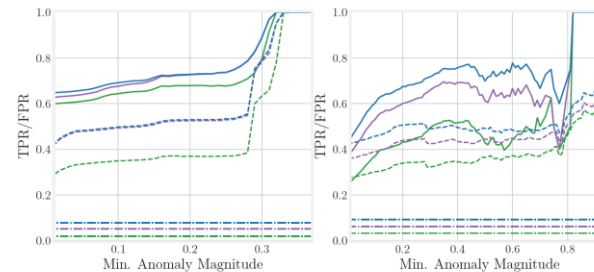
# Evaluation – Details

- 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



(a) ACN Office Data Set

(b) ACN Caltech Data Set

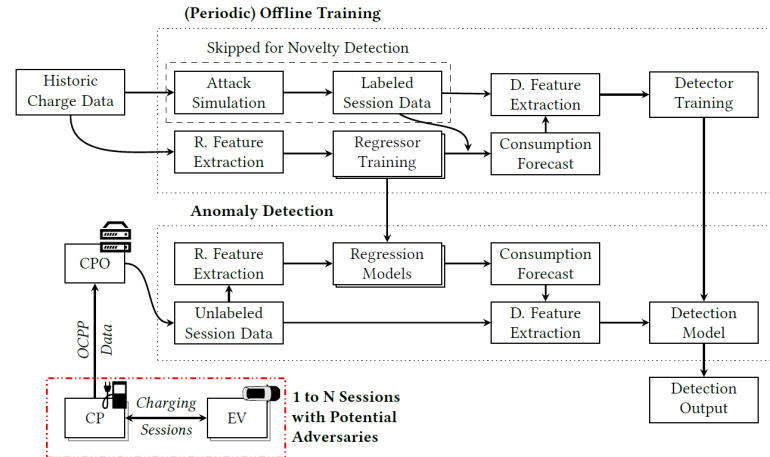


(c) ACN JPL Data Set

(d) ElaadNL Data Set

# 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

