IEEE Globecom

December 4-8, 2022
Rio de Janeiro, Brazil // Hybrid: In-Person and Virtual Conference

False Data Injection Attacks against Low Voltage Distribution Systems

P. Radoglou-Grammatikis, **P. Sarigiannidis***, et al.

University of Western Macedonia

psarigiannidis@uowm.gr

Under H2020 ELECTRON & SDN-microSENSE

SDN-µSense

Authors & Contributors

University of Western Macedonia

https://ithaca.ece.uowm.gr/

Panagiotis Radoglou Grammatikis

Panagiotis Sarigiannidis

Alexandros-Apostolos A. Boulogeorgos

Innovation Hub of Public Power Corporation S.A

https://innovationhub.dei.gr/

Christos Dalamagkas

International Hellenic University

https://www.cs.ihu.gr/

Thomas Lagkas

Innovative Energy and Information Technologies LTD

https://www.ieit.eu/

Magda Zafeiropoulou,

Maria Atanasova

Pencho Zlatev

Kingston University London

https://www.kingston.ac.uk/

Vasileios Argyriou

Hellenic Mediterranean University

https://hmu.gr/en/home/

Evangelos K. Markakis

University of Peloponnese

https://www.uop.gr/

idm@uop.gr

This project has received funding from the European Union's Horizon 2020 research and innovation programmes under grant agreement No 101021936 (ELECTRON) and No 833955 (SDN-microSENSE) .

Introduction, Relevant Works & Contributions

Introduction

Industrial Internet of Things and Smart EPES

In the era of hyper-connected digital economies, the smart technologies play a vital role in the operation of the electrical grid, transforming it into a new paradigm.

Legacy Systems

The presence of legacy systems, such as ICS/SCADA remains a crucial issue, raising multiple threats and vulnerabilities.

Insecure Communication Protocols

Both smart and legacy EPES assets use insecure communication protocols that do not comprise essential authentication and authorization mechanisms.

Existing Countermeasures

Despite the effectiveness of existing cybersecurity solutions they cannot mitigate coordinated EPES cyberattacks, such as Advanced Persistent Threats (APTs)

Lack of Datasets & Privacy

The existing countermeasures are not certified dynamically, ensuring their sufficiency.

False Data Injection Attacks

FDI attacks refer to unauthorised activities that can violate both the confidentiality and integrity of the involved systems. The goal is to inject malicious data, such as wrong measurements, that can affect the normal operation of the target system.

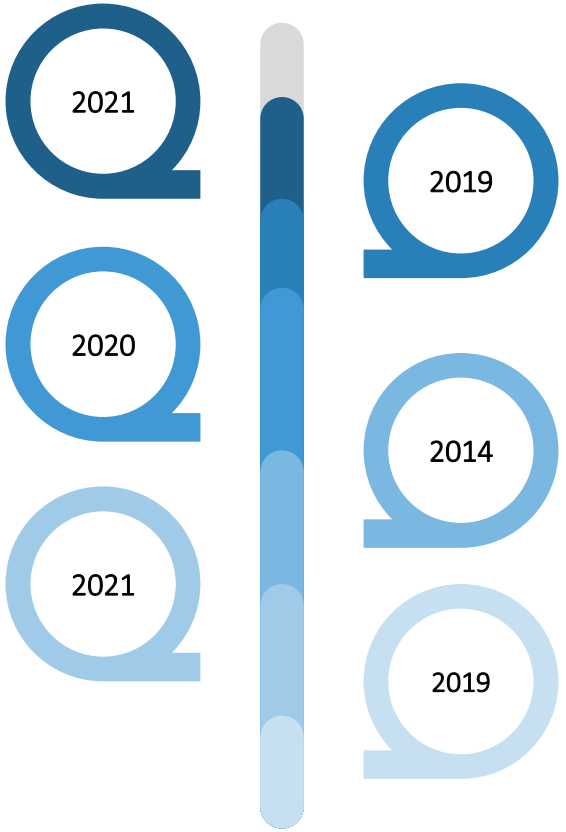
Related Work

Previous works related to False Data Injection Attacks against Electrical Power and Energy Systems

M. A. Husnoo et al.
False Data Injection Threats in Active Distribution Systems: A Comprehensive Survey

A. S. Musleh, G. Chen, and Z. Y. Dong
A Survey on the Detection Algorithms for False Data Injection Attacks in Smart Grids

P. Zhuang and H. Liang
False data injection attacks against state-of-charge estimation of battery energy storage systems in smart distribution networks



P. I. Radoglou-Grammatikis and P. G. Sarigiannidis
Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems

N. Komninos, E. Philippou, and A. Pitsillides
Survey in smart grid and smart home security: Issues, challenges and countermeasures

A. Ghosal and M. Conti
Key management systems for smart grid advanced metering infrastructure: A survey

Contributions

Three main contributions

C1: FDI Modelling

Two FDI cyberattacks are investigated. The first attack targets the communication between the ADMS and a smart meter, while the second attack targets the communication between the ADMS and a smart inverter.

C2: FDI Implementation

Implementation of the FDI cyberattacks via a real testbed emulating an Active Distribution Management System and smart inverters

C3: FDI Detection

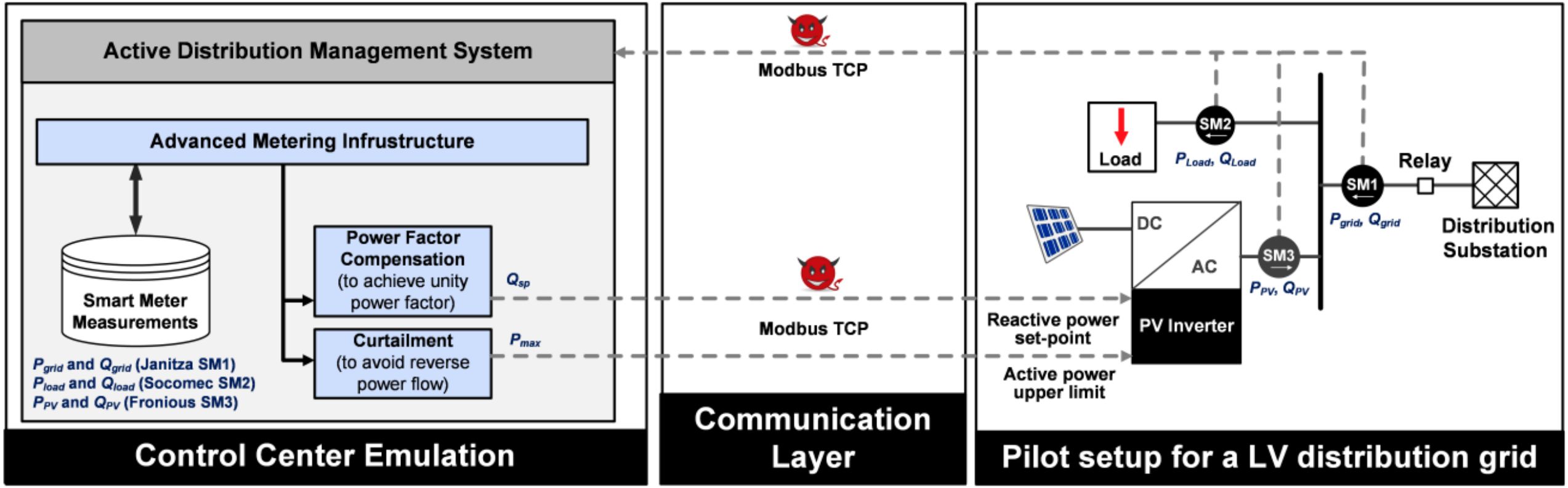
Intrusion Detection System (IDS) for FDI attacks taking full advantage of autoencoders

IEEE GLOBECOM®

Testbed

LV Distribution System Testbed

Four Main Components



LV Distribution System Testbed

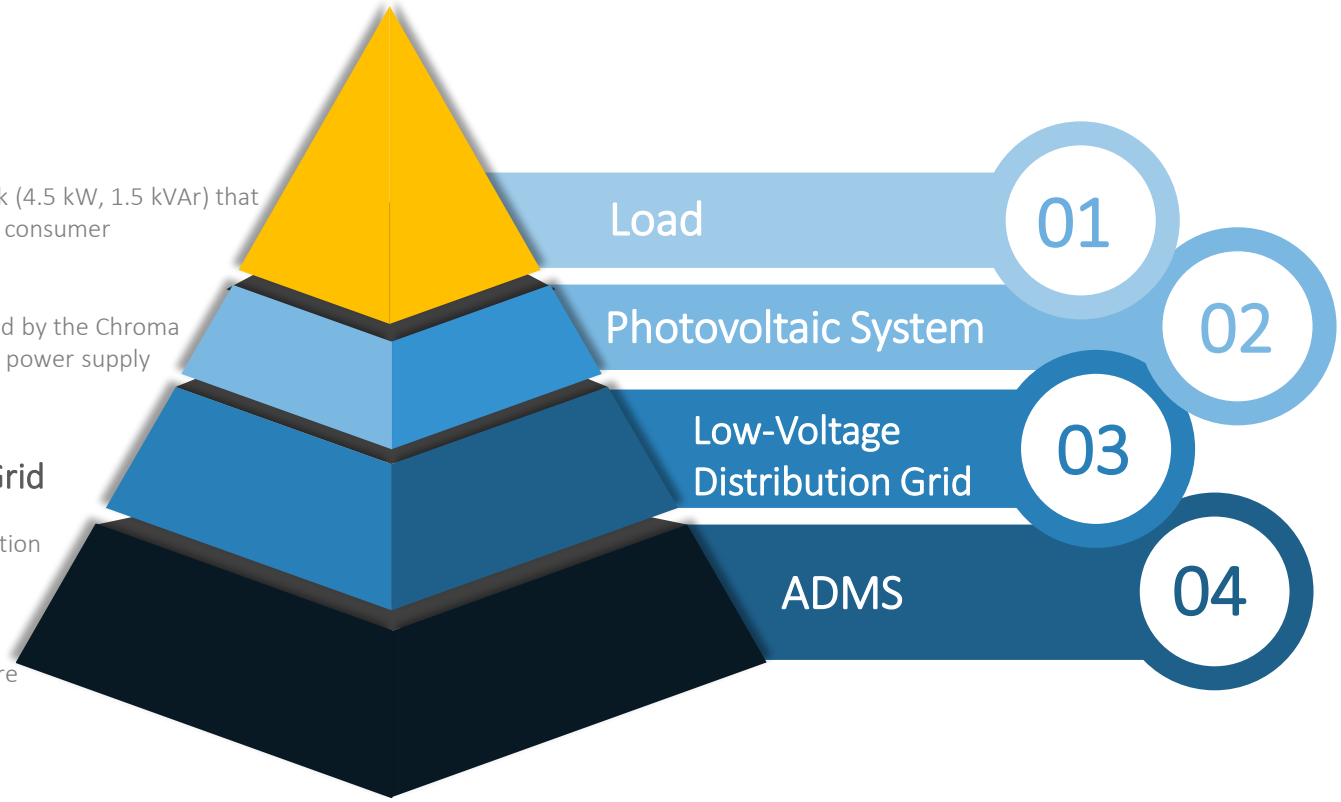
Architectural Components

Load
A controllable three-phase load bank (4.5 kW, 1.5 kVAr) that emulates the load consumption of a consumer

Photovoltaic System
The PV power generation is emulated by the Chroma 62150H-1000S device, which is a DC power supply with emulation capabilities.

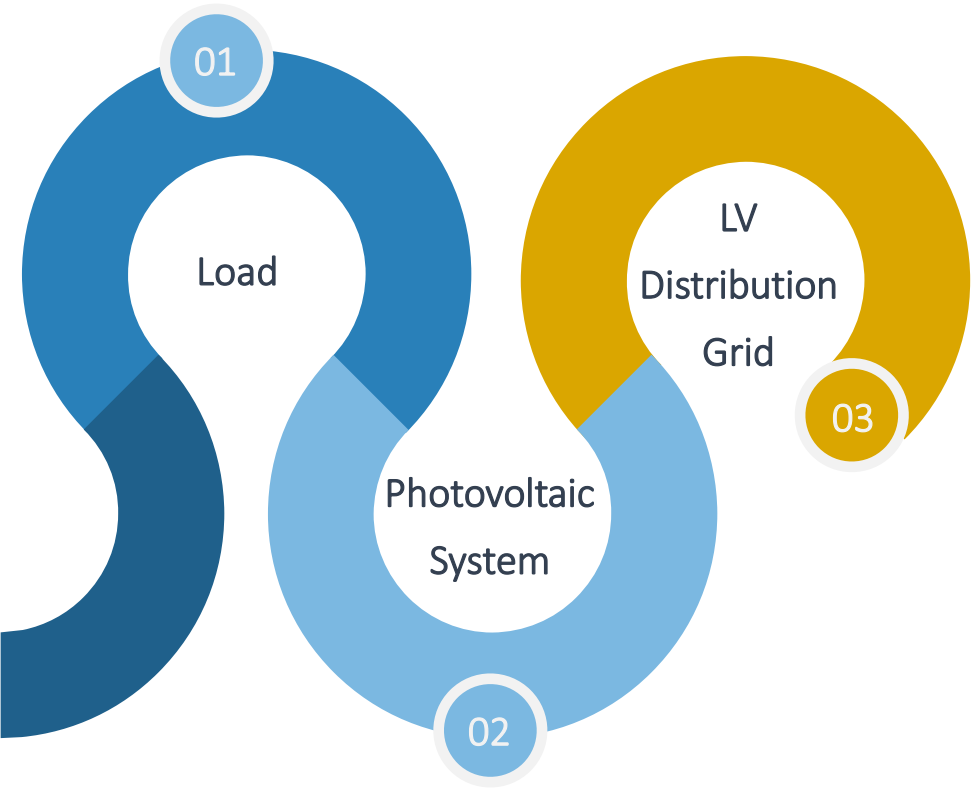
Low-Voltage Distribution Grid
Both the load and the PV system are integrated into a small scale distribution grid

ADMS
The ADMS emulate the control centre of the operator.



Load, Photovoltaic System, LV Distribution Grid

Description of Architectural Components



Load

A controllable three-phase load bank (4.5 kW, 1.5 kVAr) that emulates the load consumption of a consumer. This load is monitored by a **SOCOMEC DIRIS A-40** energy meter (**SM2**), which retrieves the values of both the active and reactive load consumption (P_{Load}, Q_{Load}).

Photovoltaic System

The PV power generation is emulated by the **Chroma 62150H-1000S** device, which is a DC power supply with emulation capabilities. The DC generator is integrated into the distribution grid via a commercial inverter, **Fronius Symo 5 kW** (**SM3**), The DC generator is integrated into the distribution grid via a commercial inverter **Modbus/TCP**. **Modbus/TCP** is also used by the ADMS to monitor the active and reactive power P_{PV} and Q_{PV}. The reactive power regulation setpoint (Q_{sp}) can be issued to control the reactive power injection, while the maximum active power (P_{max}) can limit the active power generation

LV Distribution Grid

Both the load and the PV system are integrated into a small scale distribution grid and the overall active and reactive power exchange with the grid (P_{Grid} and Q_{Grid}) are measured by the smart meter: **Janitza UMG 604** energy meter (**SM1**). **Modbus/TCP** is used again by the ADMS to collect these measurements.

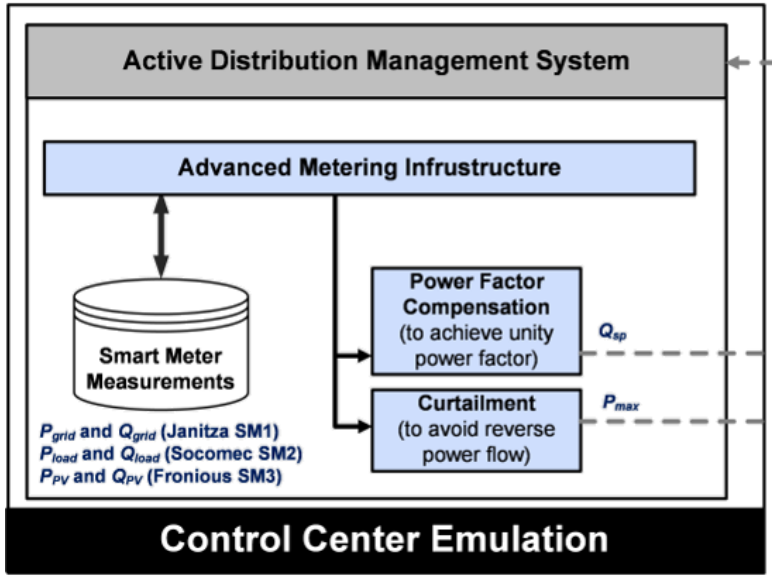
Active Distribution Management System

Description of Architectural Components

01

Advanced Metering Infrastructure

- Receives P_{Grid}, Q_{Grid} from SM1
- Receives P_{Load}, Q_{Load} from SM2
- Receives P_{PV}, Q_{PV} from SM3



02

Power Factor Compensation Scheme

- Compensate the reactive power consumed by the load in order to achieve a unity power factor for the distribution grid.
- The reactive power setpoint (Q_{sp}) is generated to control the reactive power injection of the PV inverter.
- To achieve a Q_{Grid} near to zero, the power factor compensation scheme sets $Q_{sp} = Q_{Load}$.

03

Curtailment Scheme

- Prevent any intensive reverse power flow conditions.
- Active power flows from the low-voltage side (consumers and prosumers) to the rest of the distribution grid.
- To limit the reverse active power flow to 10% of the nominal transformer value (i.e., -500 W), the maximum power generation by PV systems should be limited to 110% of the real-time active power consumption.
- Set-point for the upper limit of the inverter is set as $P_{max} = 1.1 \times P_{Load}$ to limit the generation according to the demand and therefore to limit the reverse power flow from the low-voltage distribution grid.

False Data Injection Attacks

IEEE Globecom 2022 // December 4-8, 2022
Rio de Janeiro, Brazil // Hybrid: In-Person and Virtual Conference

False Data Injection Attacks

Summary

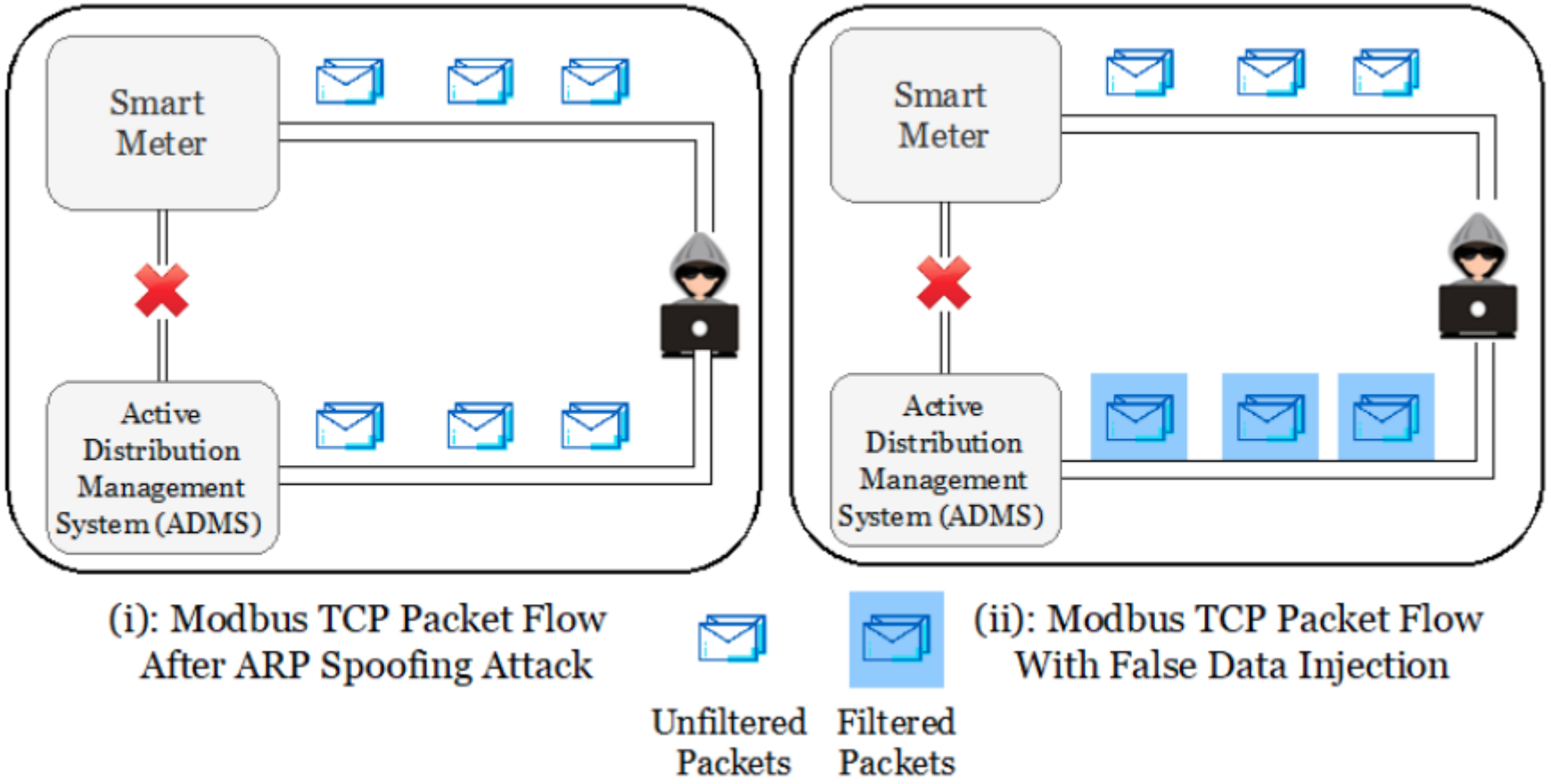
Attack Scenario A

Attacking Smart Meter Measurements

Attack Scenario B

Attacking Control Signals

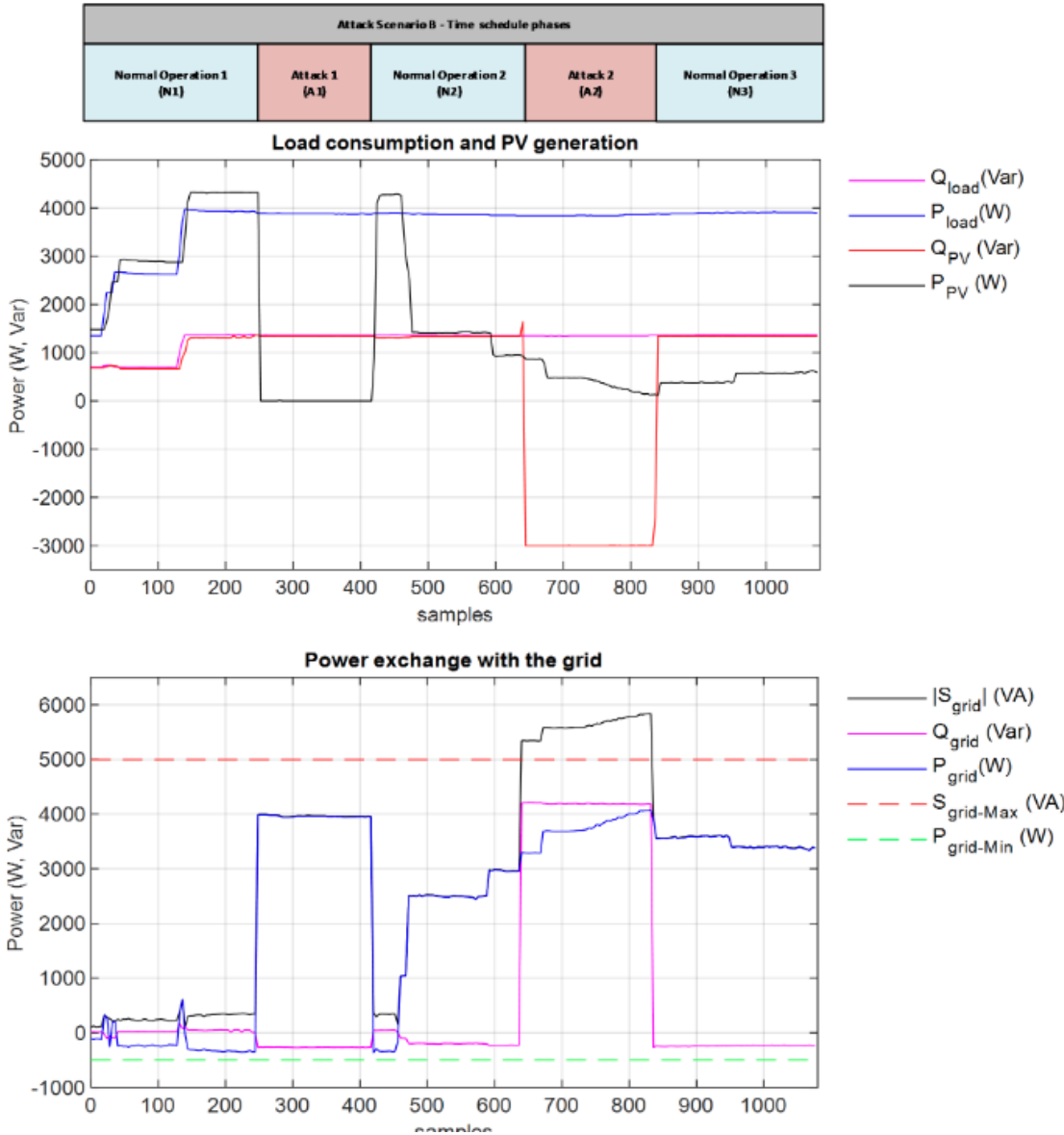
False Data Injection Attacks



Attacking Smart Meter Measurements

Attack Phase 1 (A1) - Q_{Load} = -3 kVar

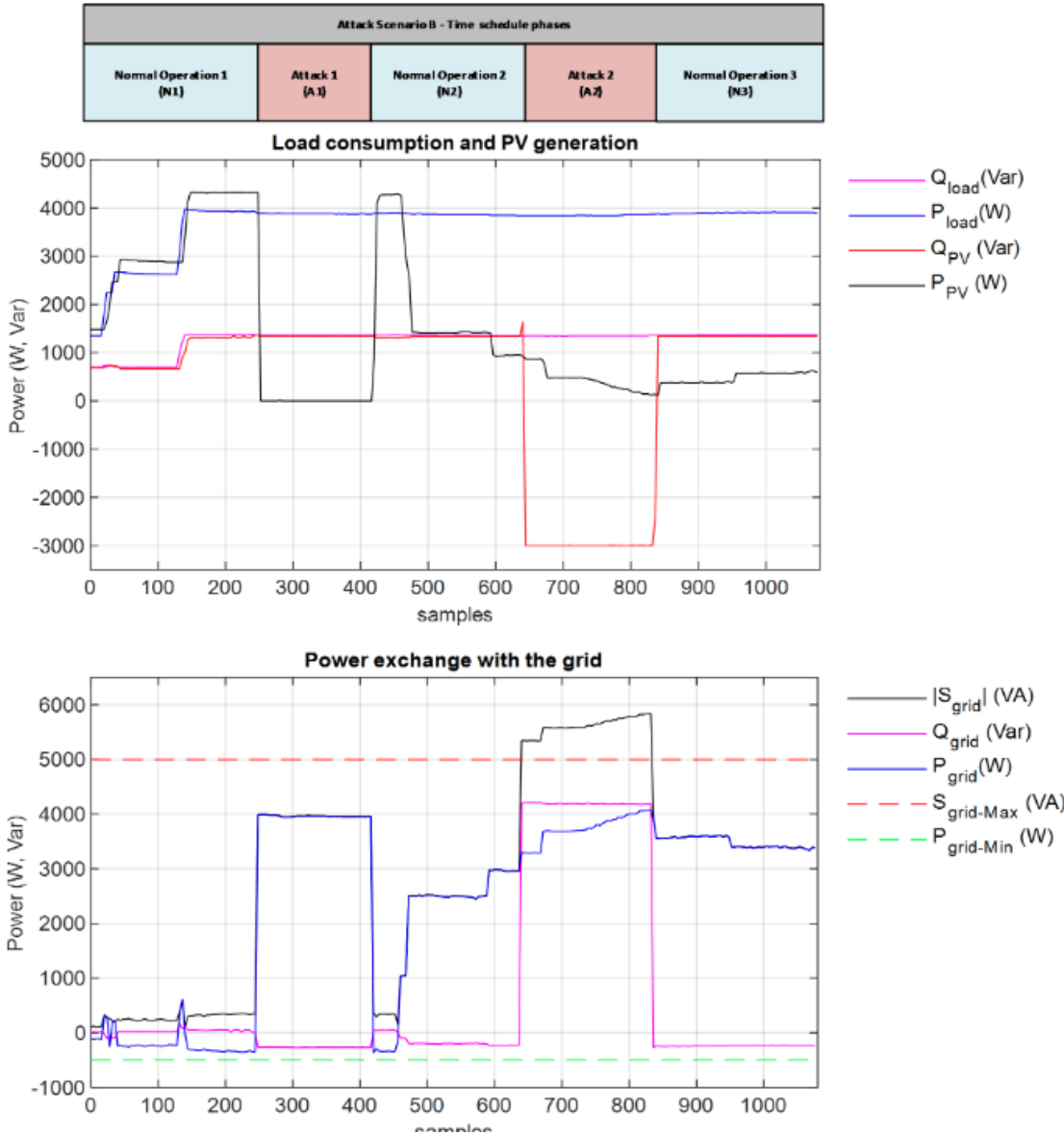
- **Goal**: Modify the load measurements **P_{Load}** and **Q_{Load}**
- **Normal Phases**: N1-N4, **Attack Phases**: A1-A3
- **Attack Phase #1: Q_{Load} = - 3Kvar**: The inverter is violated and injects -3000 Var (inductive) instead of 1380 Var (capacitive).
- The reactive power changes from near to 0 Var (during normal operation) to a high value (near to 4200 Var).
- Significant increase in the grid energy losses since it increases the current flow in the distribution lines.
- Overloading conditions in the distribution grid
- Such conditions can trip the protection relay of the distribution substation, resulting in a regional blackout for the LV distribution grid.



Attacking Smart Meter Measurements

Attack Phase 2 (A2) - P_{Load} = 50W

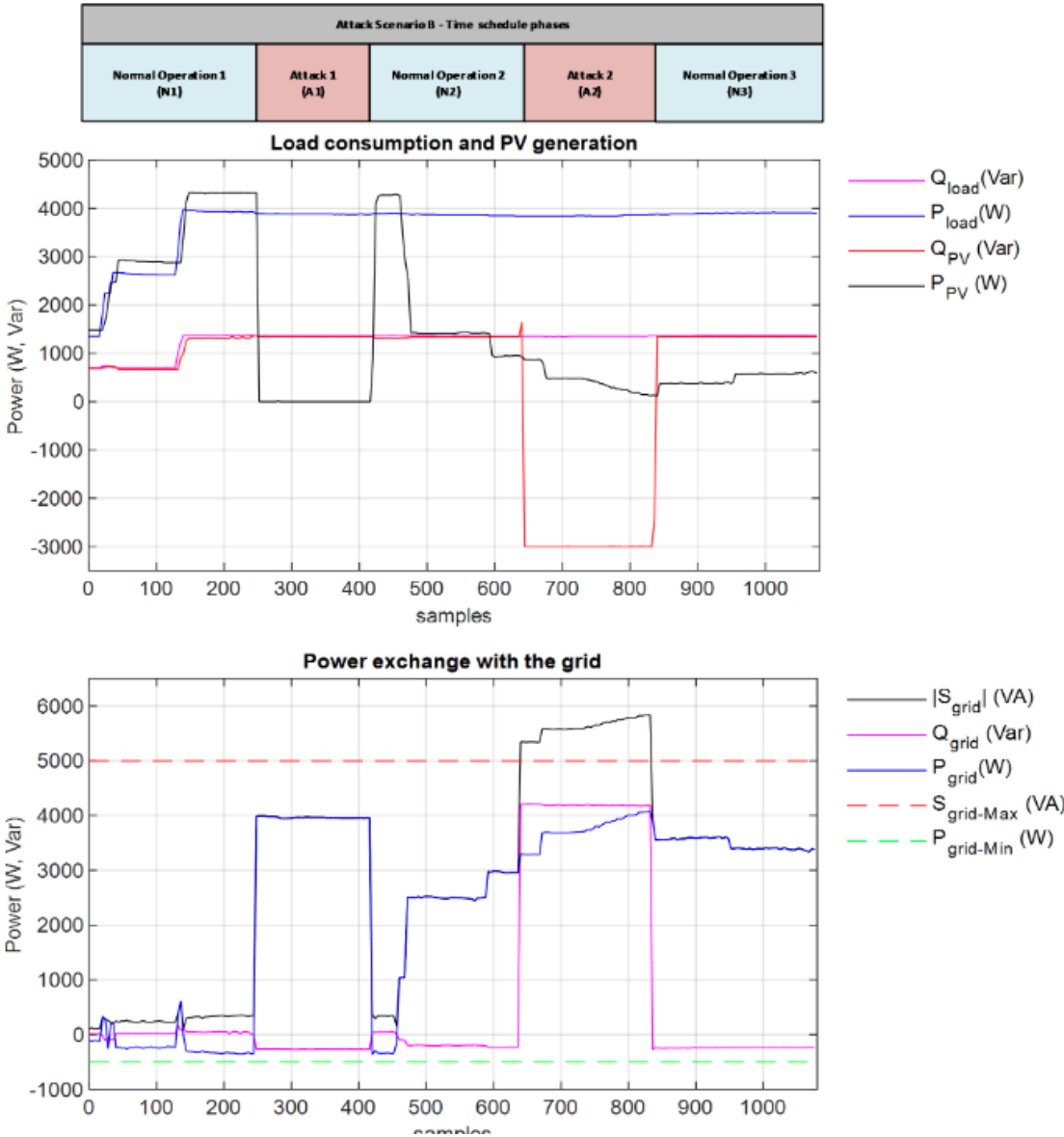
- **Goal**: Modify the load measurements $\mathbf{P_{Load}}$ and $\mathbf{Q_{Load}}$
- **Normal Phases**: N1-N4, **Attack Phases**: A1-A3
- Attack Phase 2 (A2) - $\mathbf{P_{Load}}$ = 50W: Modifies P_{Load} to 50W.
- As a result, the billing of the consumer can be violated since the overall energy consumption is reduced by the attacker.
- While $\mathbf{P_{Load}}$ is reduced by the attacker, the power generation of the PV system is also affected, producing a loss of the PV energy that results in a profit loss for the prosumer.
- The reduction of the PV generation increases the active power of the grid ($\mathbf{P_{Grid}}$ and $\mathbf{S_{Grid}}$), which can potentially lead to overloading conditions under specific circumstances



Attacking Smart Meter Measurements

Attack Phase 3 (A3) - P_{Load} = 4500 W

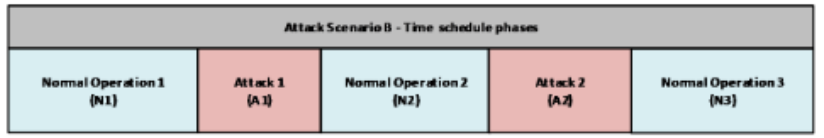
- **Goal**: Modify the load measurements $\mathbf{P_{Load}}$ and $\mathbf{Q_{Load}}$
- **Normal Phases**: N1-N4, **Attack Phases**: A1-A3
- Attack Phase 3 (A3) - $\mathbf{P_{Load}}$ = 4500W: Modifies P_{Load} to 4500W.
- As a result, the billing of the consumer can be violated since the overall energy consumption appears to be increased
- $\mathbf{P_{Load}}$ leads to increased PV generation compared to the consumption, leading to intense reverse power flow conditions.
- This attack causes an intense reverse power flow of -2000 W which exceeds the reverse power limit ($\mathbf{P_{grid-Min}}$) of the transformer (i.e., -500 W) and can lead to cascading events for the distribution grid

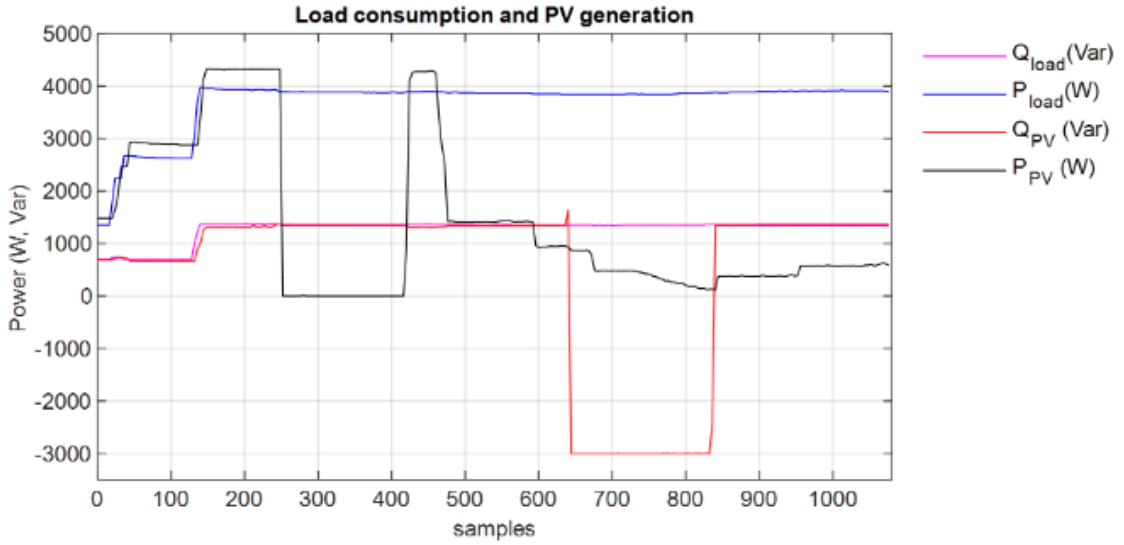


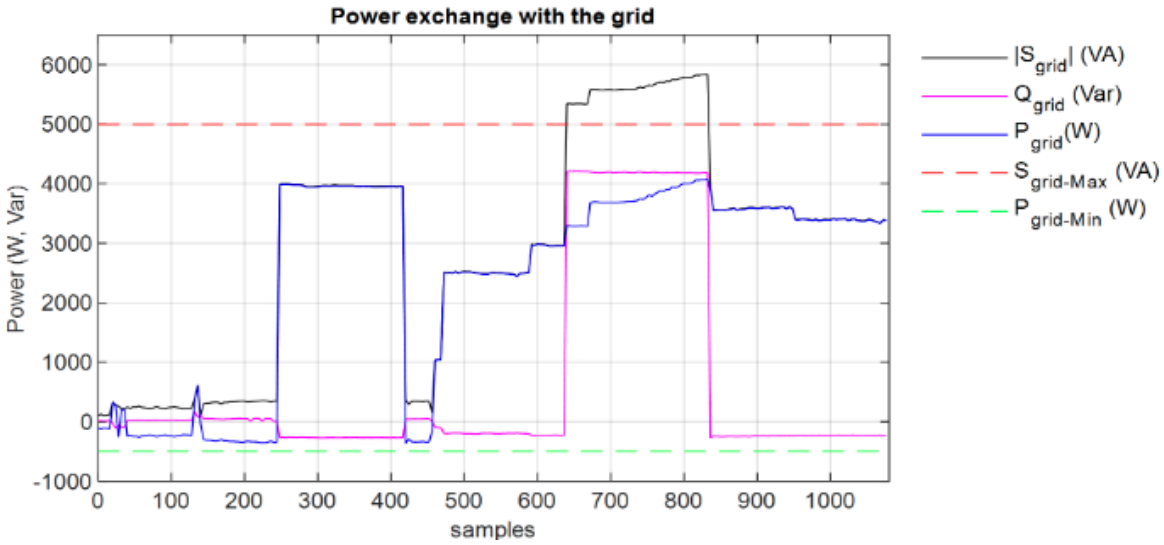
Attacking Control Signals

Attack Phase 1(A1) - P_{max} = 0

- **Goal**: Target Q_{sp} and P_{max}. Modify the reactive power injection Q_{PV} and reduce the active power production P_{PV}, thus affecting the overall operation of the distribution grid
- **Normal Phases**: N1-N3, **Attack Phases**: A1-A2
- Attack Phase 1 (A1) - P_{max} = 0: Modifies P_{max} to 0.
- The active power is limited to 0 W. The controller uses the active power to control the reactive power of the PV inverter
- An intense loss of the PV generation is observed, associated with an intense loss of profit for the prosumer.
- The reduction of the PV generation leads to an increase in the net power of the grid P_{grid} which under specific circumstances can also lead to overloading conditions.



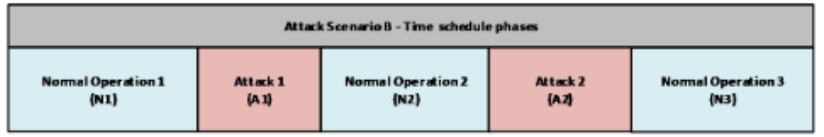


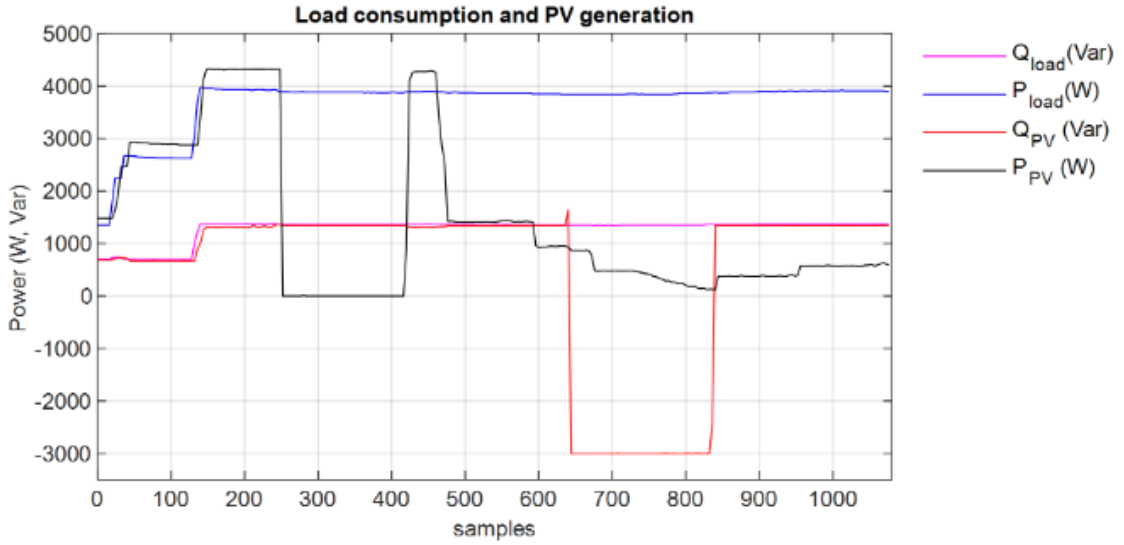


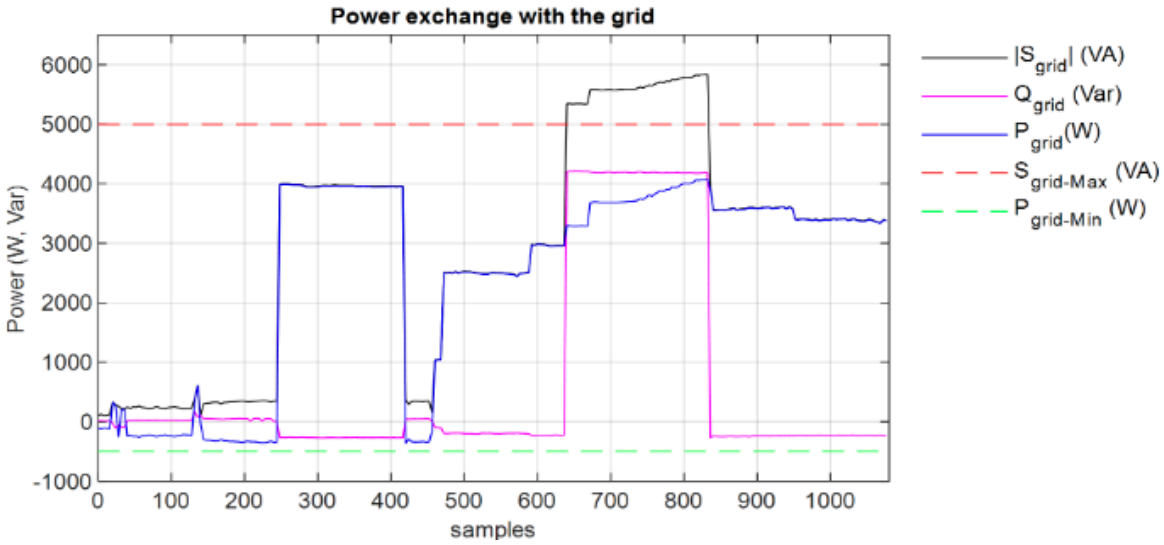
Attacking Control Signals

Attack Phase 2(A2) - Q_{sp} = -3000 Var

- **Goal**: Target **Q_{sp}** and **P_{max}**. Modify the reactive power injection **Q_{PV}** and reduce the active power production P_{PV}, thus affecting the overall operation of the distribution grid
- **Normal Phases**: N1-N3, **Attack Phases**: A1-A2
- Attack Phase 2 (A2) - **Q_{sp}** = -3000 Var
- During this attack phase, the FDI attack sets the reactive power setpoint of the PV inverter to a high negative value (i.e., -3000 Var).
- The falsified operation of the inverter increases the overall reactive power exchange with the grid (Q_{grid}).
- The increased reactive power results in intense energy losses on the distribution grid lines, while under specific circumstances (i.e., increased net active power), this consumption can result in overloading conditions



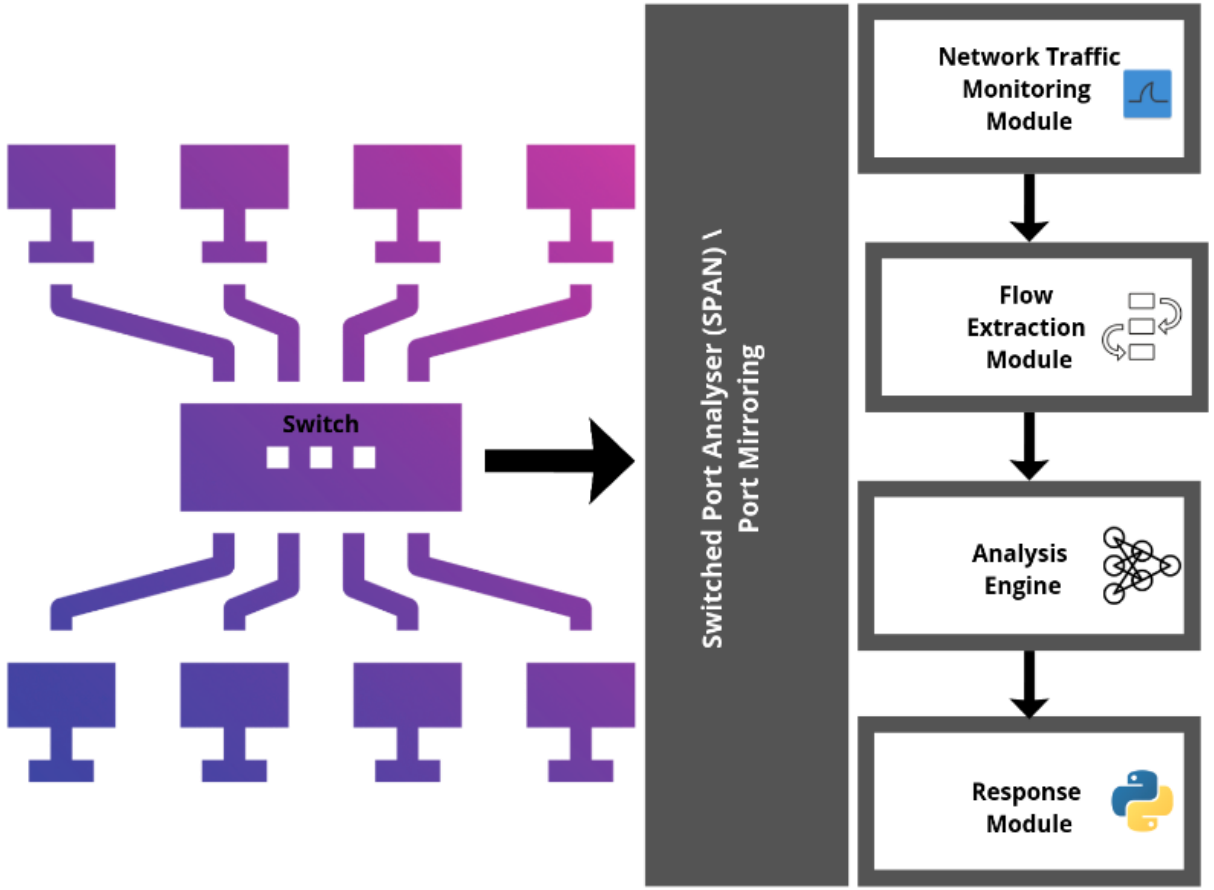




Proposed Intrusion Detection System

Proposed Intrusion Detection System

Architecture



Network Traffic Monitoring Module

Responsible for monitoring and capturing the Modbus/TCP traffic

Flow Extraction Module

Responsible for extracting network flow statistics based on the Modbus/TCP traffic

Analysis Engine

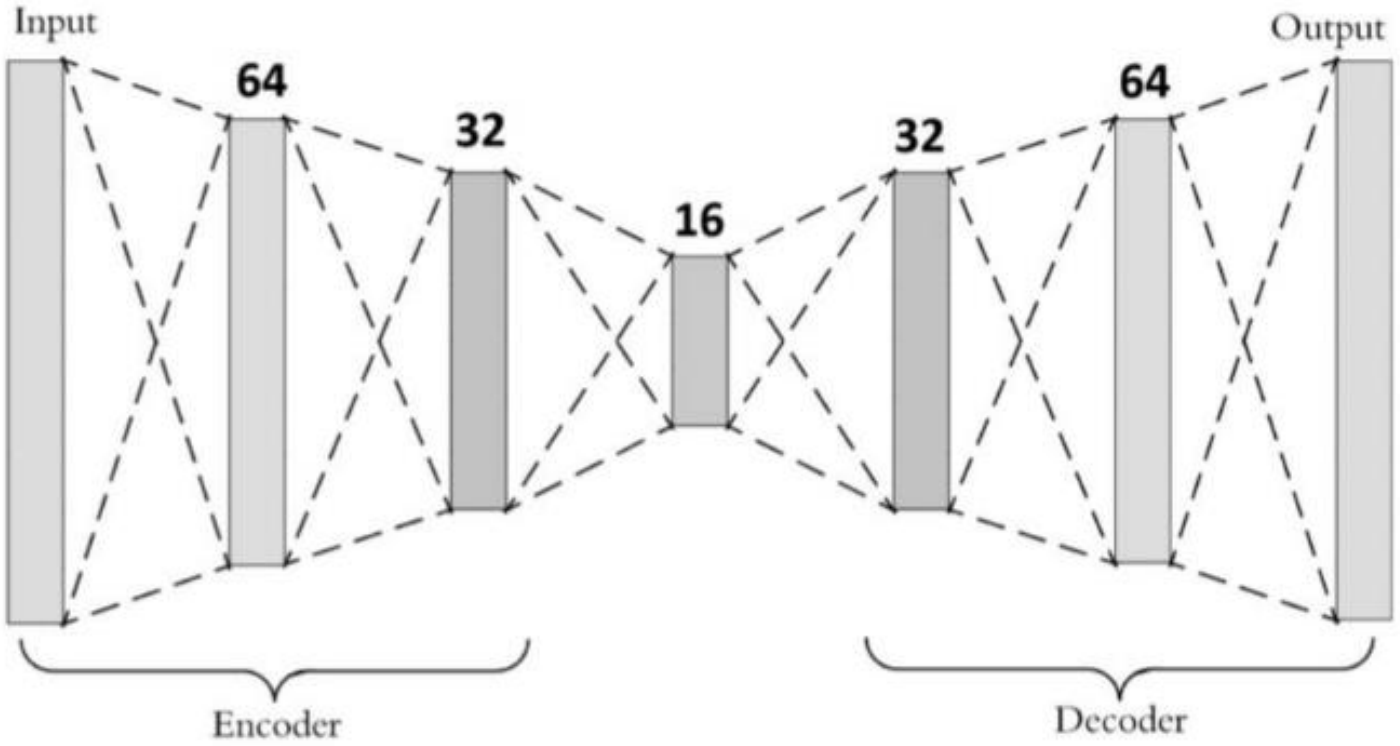
It takes over the intrusion detection process based on the flow statistics and autoencoder

Response Module

Notifies about the presence of security events

Proposed Autoencoder

Architecture



maps input data $x \in X = \mathbb{R}n$ to an output x' ∈ X. It consists of an encoder f : X → Z and a decoder g : Z → X, each implemented as a deep neural network. The encoder and decoder together result the output x' = g(f(x))

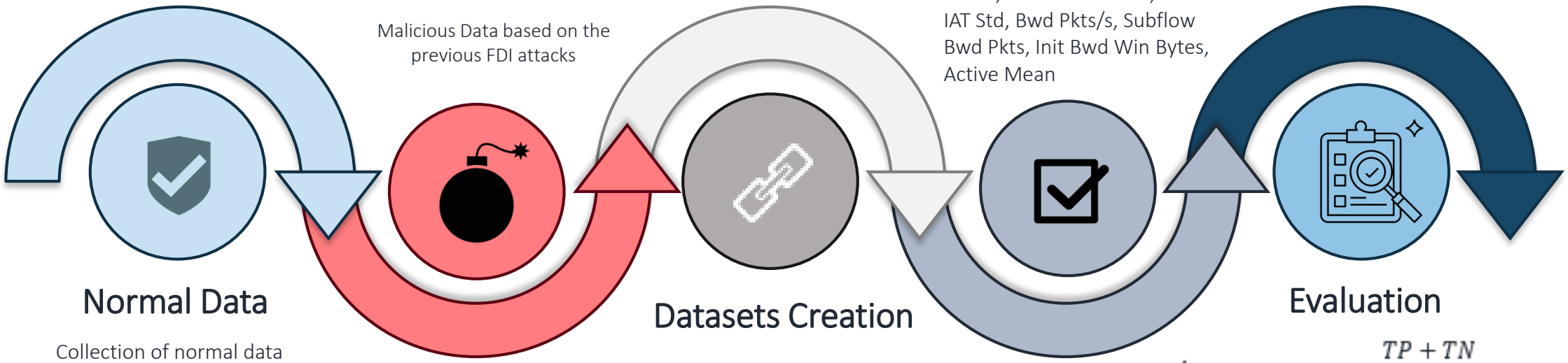
The low-dimensional latent representation of x is obtained from the encoder and is defined as z = f(x) ∈ Z = Rm (m << n). The autoencoder avoids to become an identity function and the training process aims to minimise the reconstruction error L(x, x')

Anomalies are detected by measuring the reconstruction error L(x,x') and comparing it with a threshold T, classifying all operational data samples y with L(y, g(f(y))) > T as anomalies. T is estimated heuristically based on the reconstruction error L of all normal training data samples. The threshold T in order to be more robust is selected to be a large percentile of the reconstruction error T = p0.9(L(x, x')| x ∈ X) or if a validation dataset is available is selected to maximise the performance for the validation data.

Evaluation Results

Evaluation Strategy

Methodology & Metrics



Normal Data

Collection of normal data based on the normal conditions of the previous testbed

Malicious Data

Malicious Data based on the previous FDI attacks

Datasets Creation

Data creation and pre-processing based on the previous data

Feature Selection

Flow Duration, TotLen Fwd Pkts, Fwd Pkt Len Mean. Fwd Pkt Len Mean, Bwd Pkt Len Std, Flow IAT Std, Bwd Pkts/s, Subflow Bwd Pkts, Init Bwd Win Bytes, Active Mean

Evaluation

$$Accuraccy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$TPR = \frac{TP}{TP + FN}$$

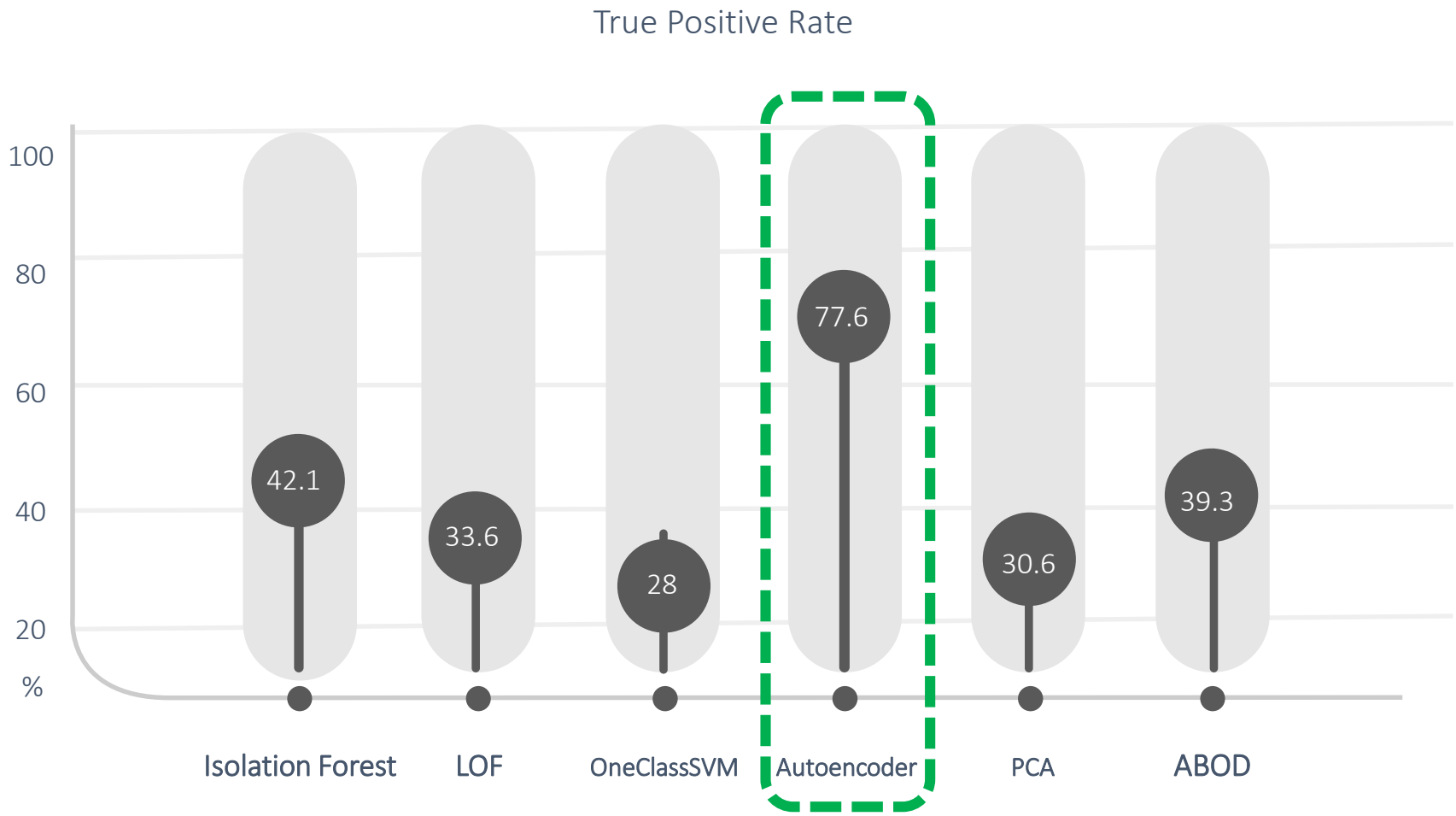
$$FPR = \frac{FP}{FP + TN}$$

$$F1 = \frac{2 \times Precision \times TPR}{Precision + TPR} \text{ where } Precision = \frac{TP}{TP + FP}$$

Evaluation

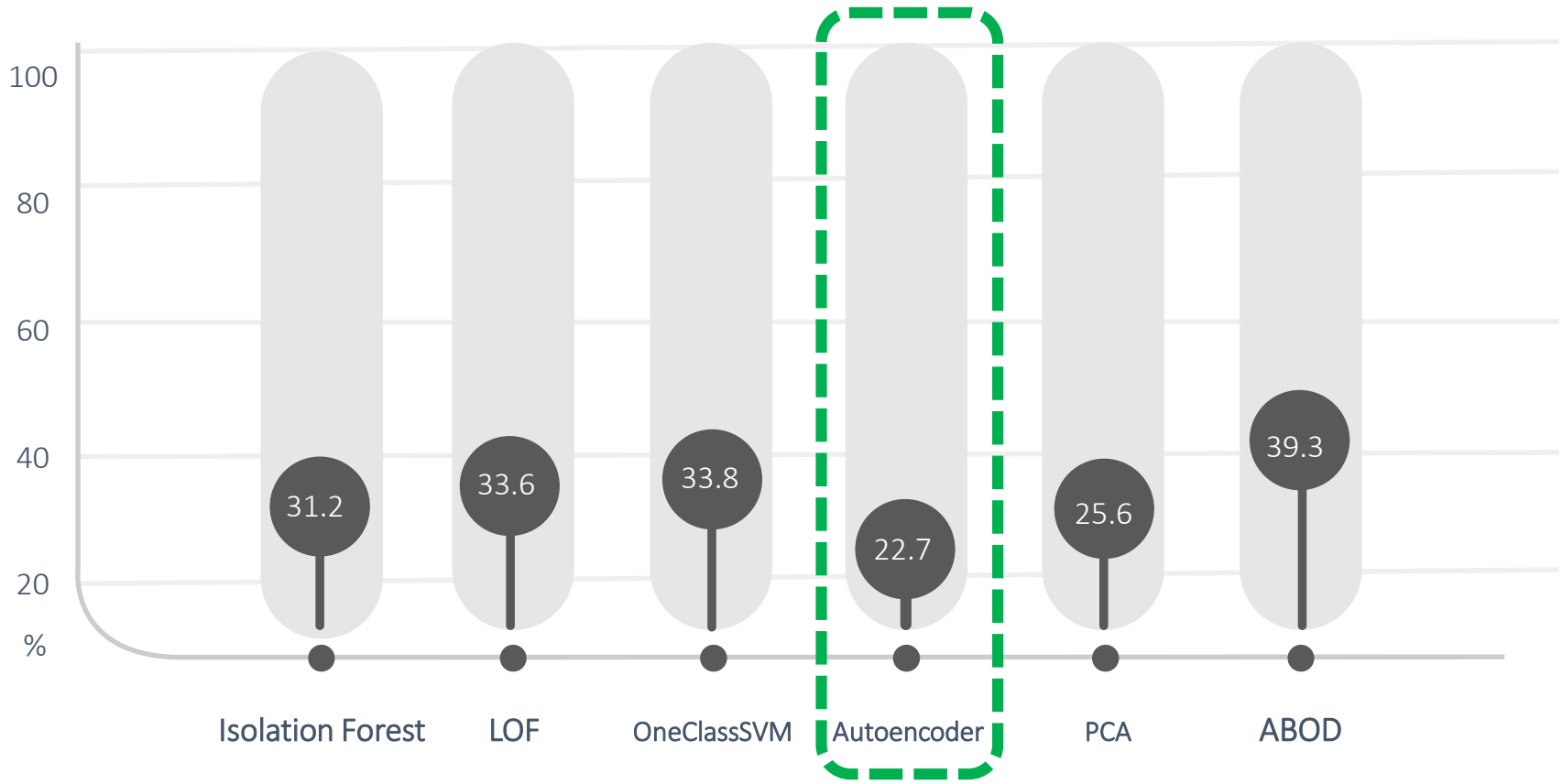

Accuracy
100
80
60
40
20
%
54.9
50.2
43.2
86.4
48.7
53.4
Isolation Forest
LOF
OneClassSVM
Autoencoder
PCA
ABOD

Evaluation


True Positive Rate
100
80
60
40
20
%
42.1
33.6
28
77.6
30.6
39.3
Isolation Forest
LOF
OneClassSVM
Autoencoder
PCA
ABOD

Evaluation

False Positive Rate



Evaluation


F1-Score
100
80
60
40
20
%
54.9
45.8
38.2
85.5
45.3
54.9
Isolation Forest
LOF
OneClassSVM
Autoencoder
PCA
ABOD

Conclusions & Future Work

Conclusions & Future Plans

Despite the smart technologies, severe security issues arise…

Introduction, Rationale & Objectives

1

Goal

Investigation of FDI attacks against LV Distribution Systems

FDI Attacks Modelling

2

Two FDI Attack Scenarios

(a) FDI attack between a smart meter and the ADMS and (b) FDI attack between an inverter and the ADMS.

FDI Attacks Implementation

3

Modbus/TCP Security Vulnerabilities

Both scenarios take full advantage of the Modbus/TCP protocol, which does not include any authentication and authorization mechanisms.

FDI Attacks Detection

4

FDI Attacks Detection

Detecting successfully the previous cyberattacks through an autoencoder. The evaluation results demonstrate the efficiency of the proposed IDS

Future Plans

5

Future Works

FDI attacks against Medium and High Voltage Distribution Systems using IEEE C37.118

Thank You & Q/A

Contact us

ithaca (at) uowm (dot) gr

https://ithaca.ece.uowm.gr/el/

https://www.linkedin.com/in/ithaca-lab/

https://www.youtube.com/channel/UClAuHbgmxirMxDy9zQt97Ew

Thank You

Q/A ?