IEEE

DCOSS-IoT 2023

IEEE DCOSS-IoT 2023

IoTI5 2023 - 5th International Workshop on IoT Applications and Industry 5.0

Coral Bay, Pafos, Cyprus // June 19-21, 2023

False Data Injection Attacks against High Voltage Transmission Systems

Panagiotis Radoglou-Grammatikis, Magda Zafeiropoulou, Maria Atanasova, Pencho Zlatev, Sofia Giannakidou, Thomas Lagkas, Vasileios Argyriou, Evangelos K. Markakis, Ioannis Moscholios and Panagiotis Sarigiannidis*

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

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.

Under H2020 ELECTRON & SDN-microSENSE

Authors & Contributors

University of Western Macedonia

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

Panagiotis Radoglou Grammatikis

Panagiotis Sarigiannidis

Alexandros-Apostolos

A. Boulogeorgos

K3Y Ltd

https://k3ylabs.com/

Sofia Giannakidou

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) .

Related Work

Similar Works of FDIs against the smart electrical grid

M. Ahmed and A-S. K. Pathan

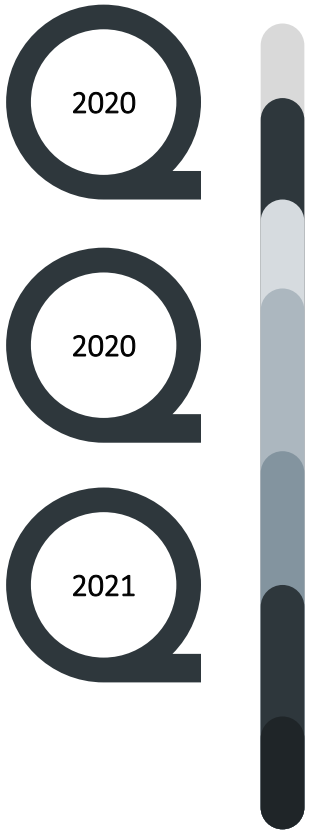
False data injection attack (fdia): an overview and new metrics for fair evaluation of its countermeasure

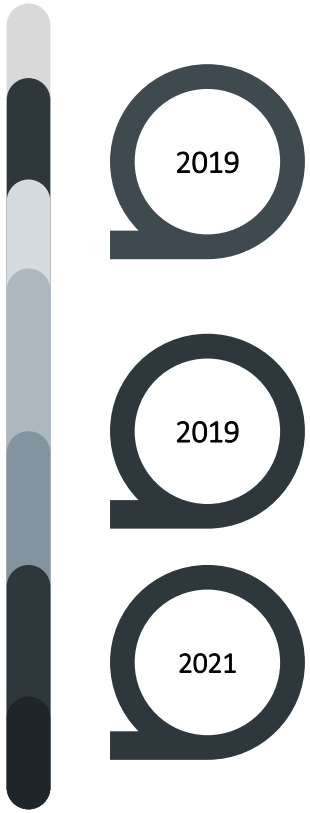
A. Sayghe, Y. Hu, I. Zografopoulos, X. Liu, R. G. Dutta, Y. Jin, and C. Konstantinou

Survey of machine learning methods for detecting false data injection attacks in power systems

C. Chen, Y. Chen, J. Zhao, K. Zhang, M. Ni, and B. Ren

"Data-driven resilient automatic generation control against false data injection attack





P. I. Radoglou-Grammatikis and P. G. Sarigiannidis

Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems

A. S. Musleh, G. Chen, and Z. Y. Dong

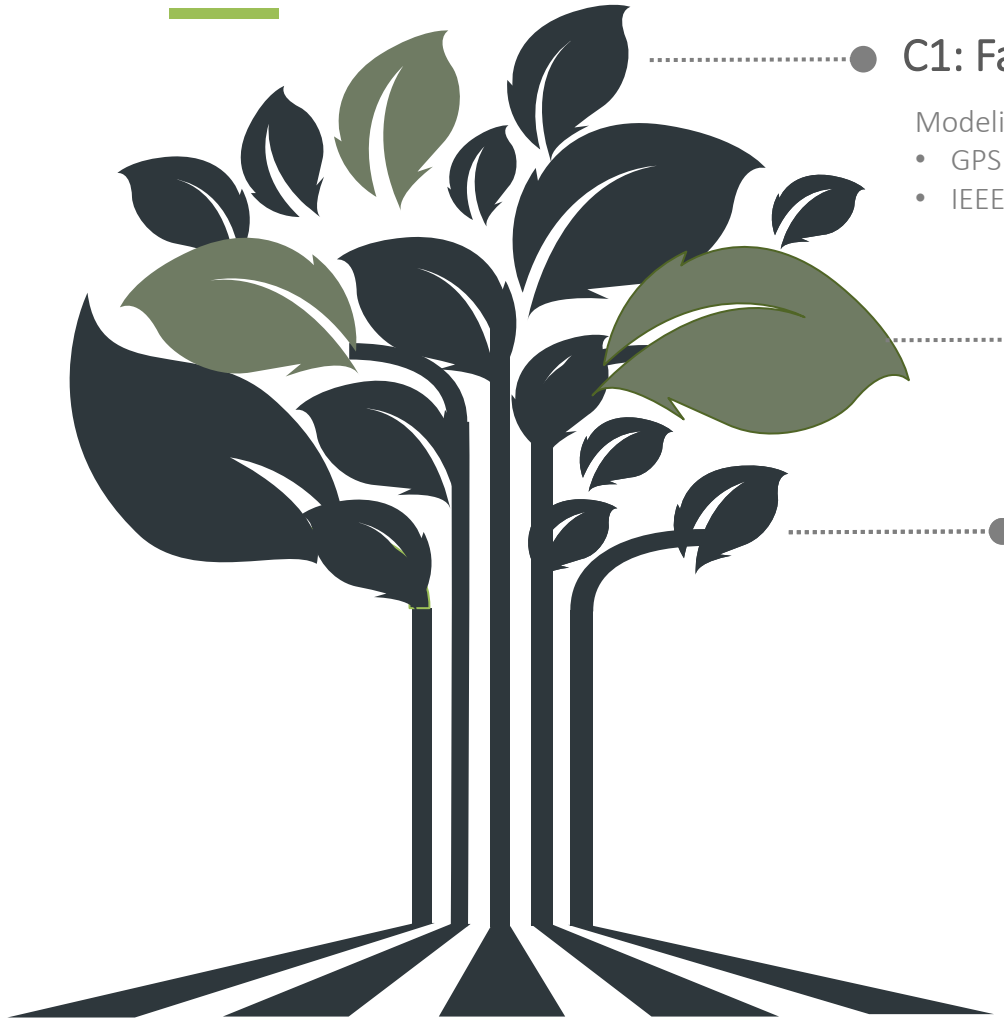
A survey on the detection algorithms for false data injection attacks in smart grids

P. Radoglou-Grammatikis et al.

Sdn-based resilient smart grid: The sdn-microsense architecture

Challenges & Contributions

FDI against HV & Detection



C1: False Data Injection Attacks against HV Voltage System

Modeling two attack scenarios against High-Voltage Distribution System

- GPS Spoofing
- IEEE C37.118 False Data Injection Attacks

C2: Detection of False Data Injection Attacks

ML/DL-based detection of the previous false data injection attacks.

Challenges

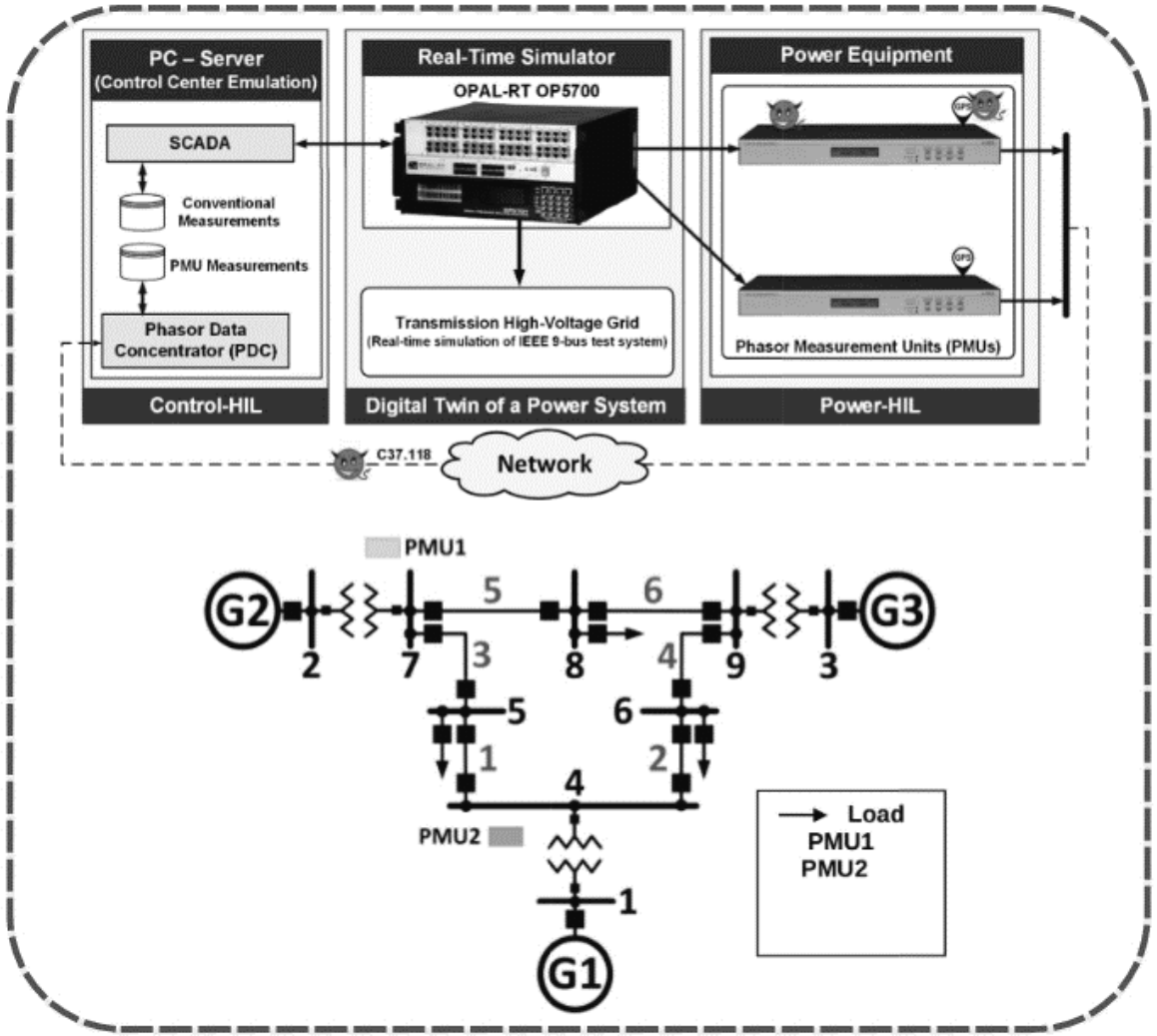
- Lack of (a) an understanding of the complicated relationships between real intrusion alerts and (b) the precision required to piece together attack actions taking place on different systems over long periods.
- Lack of appropriate intrusion detection datasets for tackling False Data Injection attacks
- The false data injection attacks range from environment to environment based on their characteristics. Therefore, their timely detection is challenging.

Testbed & Attack Scenarios

Testbed

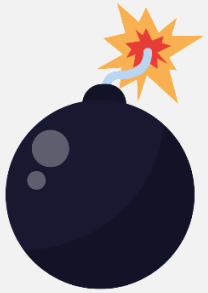
IEEE 9-Bus Transmission Grid Model

- Three generators and nine buses based on the IEEE 9-bus transmission grid model
- PMU1 and PMU2 have been deployed at two buses PMUs were integrated into HIL which provides measurements from OPAL-RT
- Current phasor measurements from six transmission lines and voltage phasor measurements from two buses (substations) are recorded by the PMUs and sent to the PDC through IEEE C37.118.
- PMU1 is responsible for monitoring the voltage and current phasors of bus 7, while PMU2 monitors the voltage and current phasors of bus 4
- PDC aligns the PMU measurements according to their GPS timestamps and stores them in a database at the control center



Attack Scenarios

Two Attack Scenarios



GPS Spoofing Attacks

{GPS spoofing attacks against PMUs involve manipulating GPS signals received by the devices, leading to inaccurate measurements and potential disruption of power grid operations.}

IEEE C37.118 False Data Injection Attacks

{False data injection attacks against the IEEE C37.118 protocol involve injecting fabricated or manipulated data into communication channels, potentially compromising the reliability and security of the power grid.}

GPS Spoofing Attack

Modelling & Implementation

- The attacker executes a MITM attack between PMUs and PDC.
- The attacker intercepts the unencrypted IEEE C37.118 network traffic
- The attacker performs a GPS spoofing attack against PMU2 to cause an offset error of approximately 7 ms

TABLE I: Results of the GPS receiver clock offset error and the voltage phase angle shift

No	GPS Receiver Clock Offset Error (ms)	Phase Angle Shift (degree)
1	6.77	121.86
2	6.86	123.48
3	6.90	124.20
4	7.05	126.90
5	7.19	129.42

GPS Spoofing Attack

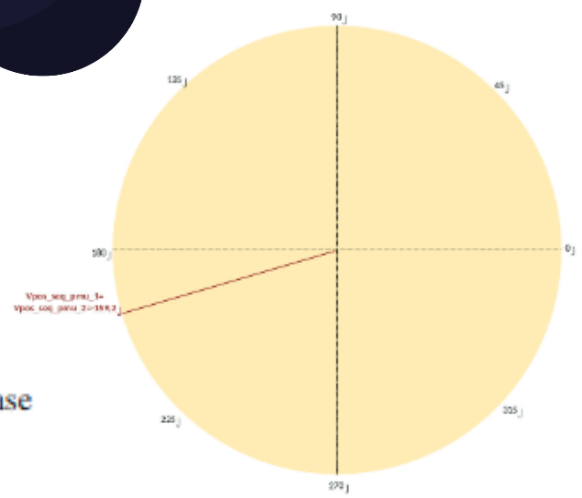


Fig. 2: Phasor Measurement at Bus 4 from PMU1 and PMU2 before the GPS Spoofing Attack

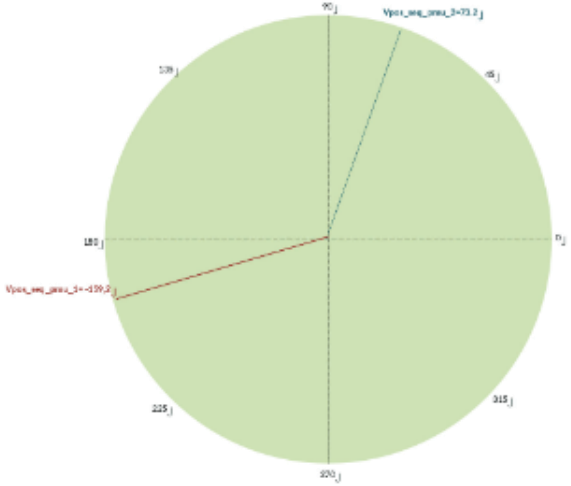


Fig. 3: Phasor Measurement at Bus 4 from PMU1 and PMU2 after the GPS Spoofing Attack

IEEE C37.118 False Data Injection

The attacker executes a MITM attack between PMUs and PDC.

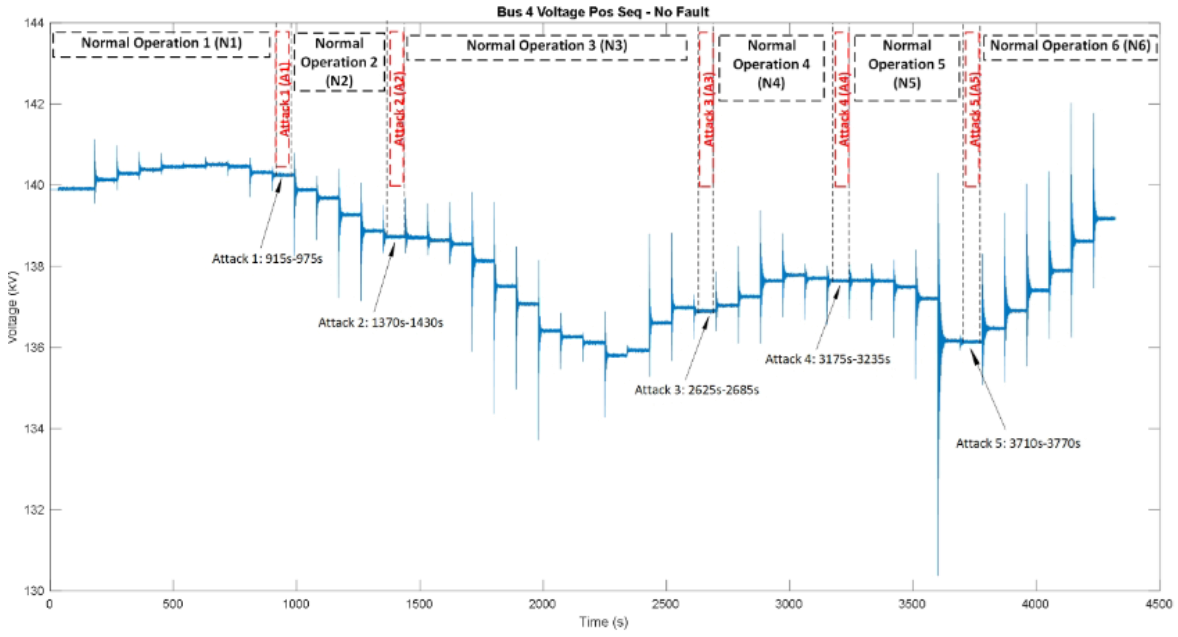
The attacker intercepts the unencrypted IEEE C37.118 network traffic

The following attacks were executed against PMU1:

- **Current magnitude and angle attack at line 7-2**, by increasing the phasor's magnitude by 50% of its nominal value.
- **Voltage magnitude attack at bus 7 and current magnitude attack at line 7-2**, by increasing the phasor's magnitude by 50% of its nominal value.
- **Current magnitude attack at line 7-5**, by increasing the phasor's magnitude by 50% of its nominal value.
- **Current angle attack at line 7-5**, by setting phase angle to 90°
- **Voltage magnitude and angle attack at bus 7**, by increasing the phasor's magnitude by 50% of its nominal value and setting phase angle to 90°.

The ML TCP/IP IDS detects successfully the previous attacks and sends the security events to XL-SIEM. Finally, XL-SIEM normalizes and visualizes the security events

IEEE C37.118 FDIA



IEEE C37.118 False Data Injection

The attacker executes a MITM attack between PMUs and PDC.

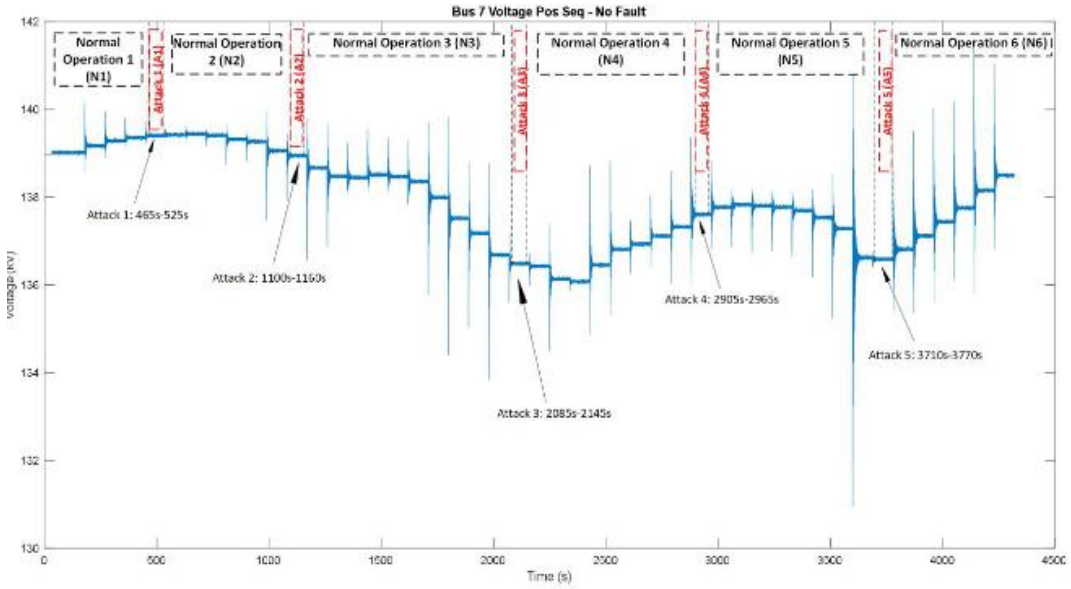
The attacker intercepts the unencrypted IEEE C37.118 network traffic

The following attacks were executed against PMU2:

- **Voltage magnitude attack at bus 4**, by increasing the phasor's magnitude by 50% of its nominal value.
- **Current magnitude attack at line 4-1**, by increasing the phasor's magnitude by 50% of its nominal value.
- **Voltage angle attack at bus 4**, by setting phase angle to 90°.
- **Current angle attack at line 4-1**, by setting phase angle to 90°

The ML TCP/IP IDS detects successfully the previous attacks and sends the security events to XL-SIEM. Finally, XL-SIEM normalizes and visualizes the security events

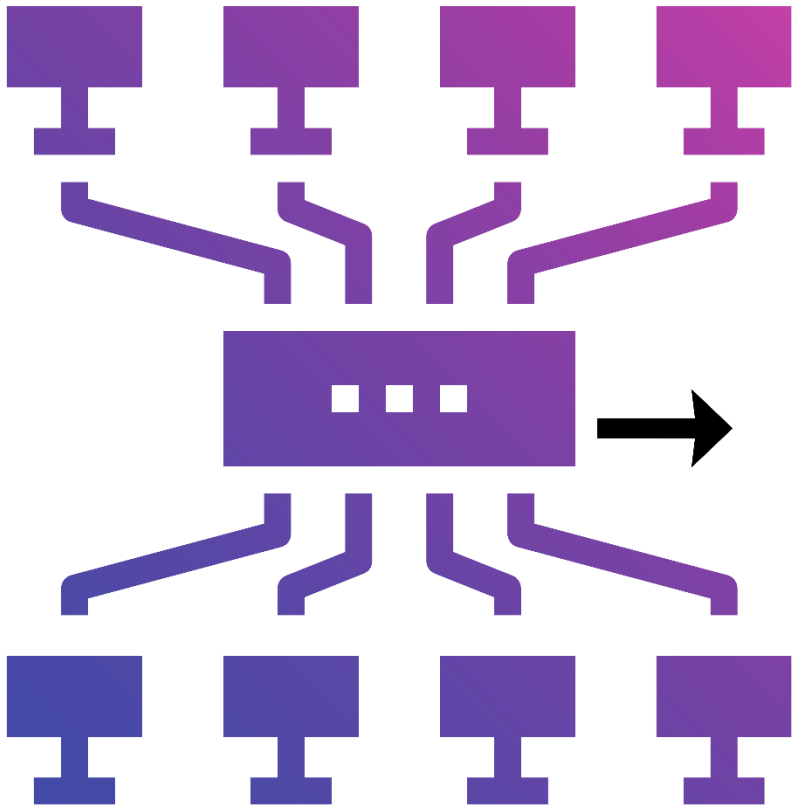
IEEE C37.118 FDIA

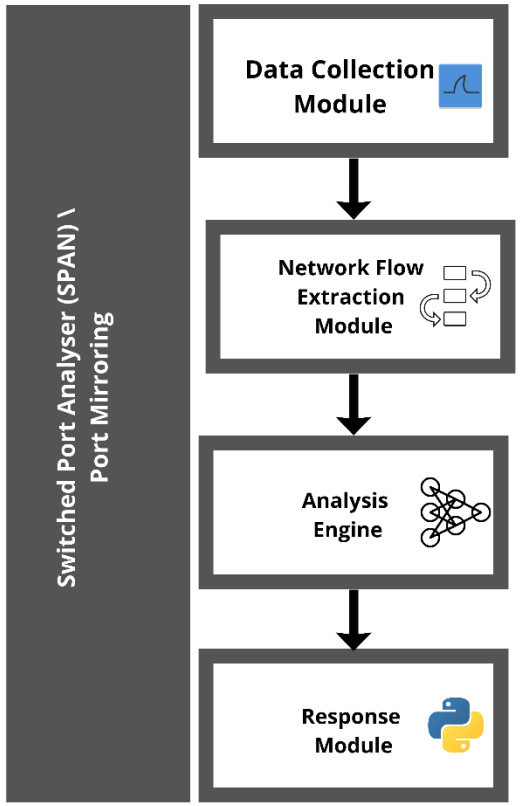


Proposed Intrusion Detection System

Proposed Intrusion Detection System

Architectural Design





Data Collection Module

PMU Measurements (such as positive sequence voltage magnitude and angle), monitoring and capturing the Modbus/TCP traffic

Network 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

ML-based Detection

Detection of FDI with ML Methods

Detection of GPS Spoofing Attacks with Random Forest

- Random Forest is an ensemble learning algorithm that combines multiple decision trees to make predictions.
- It can be used for both classification and regression tasks.
- Each decision tree in the Random Forest is built on a randomly sampled subset of the training data and a random subset of the features.
- The final prediction is made by aggregating the predictions of all the individual trees (classification: voting).
- Random Forest reduces overfitting and improves generalization by using randomization and combining multiple models.
- It handles missing values and maintains good accuracy even with a large number of input features.
- It is computationally efficient and can handle large datasets.
- Random Forest is resistant to outliers and noise in the data.

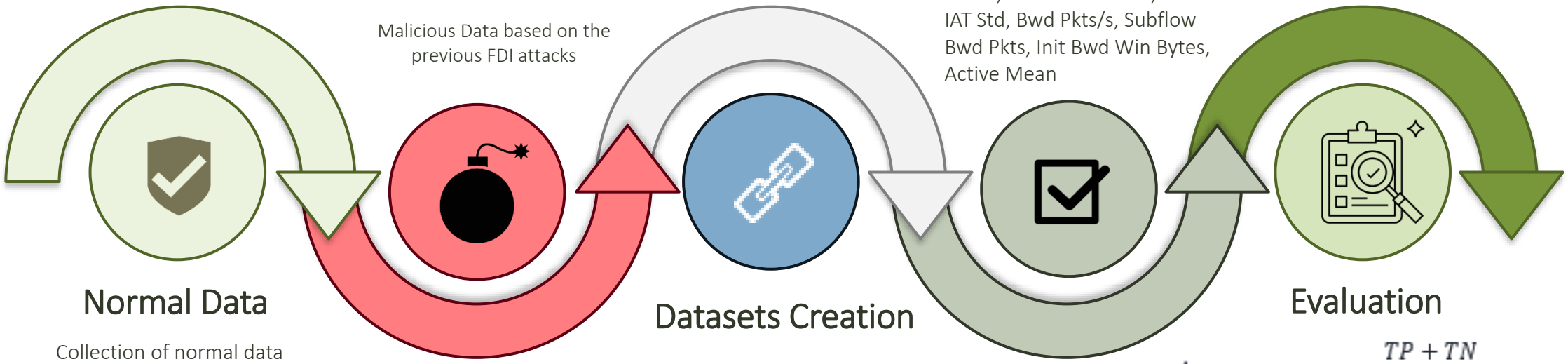
Detection of IEEE C37.118 FDI with Isolation Forest

- Isolation Forest is an unsupervised machine learning algorithm used for anomaly detection.
- It works by isolating anomalies as they are expected to be few and different from normal data points.
- The algorithm constructs a collection of binary trees, where each tree is grown by randomly selecting a feature and a random split value.
- Anomalies are expected to have shorter average path lengths in the tree structure compared to normal data points.
- Isolation Forest assigns anomaly scores to each data point based on the average path length in the trees.
- The anomaly score can be used to identify and rank potential anomalies in the dataset.
- Isolation Forest is efficient in terms of computation and memory usage, making it suitable for large datasets.

Evaluation Analysis

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

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

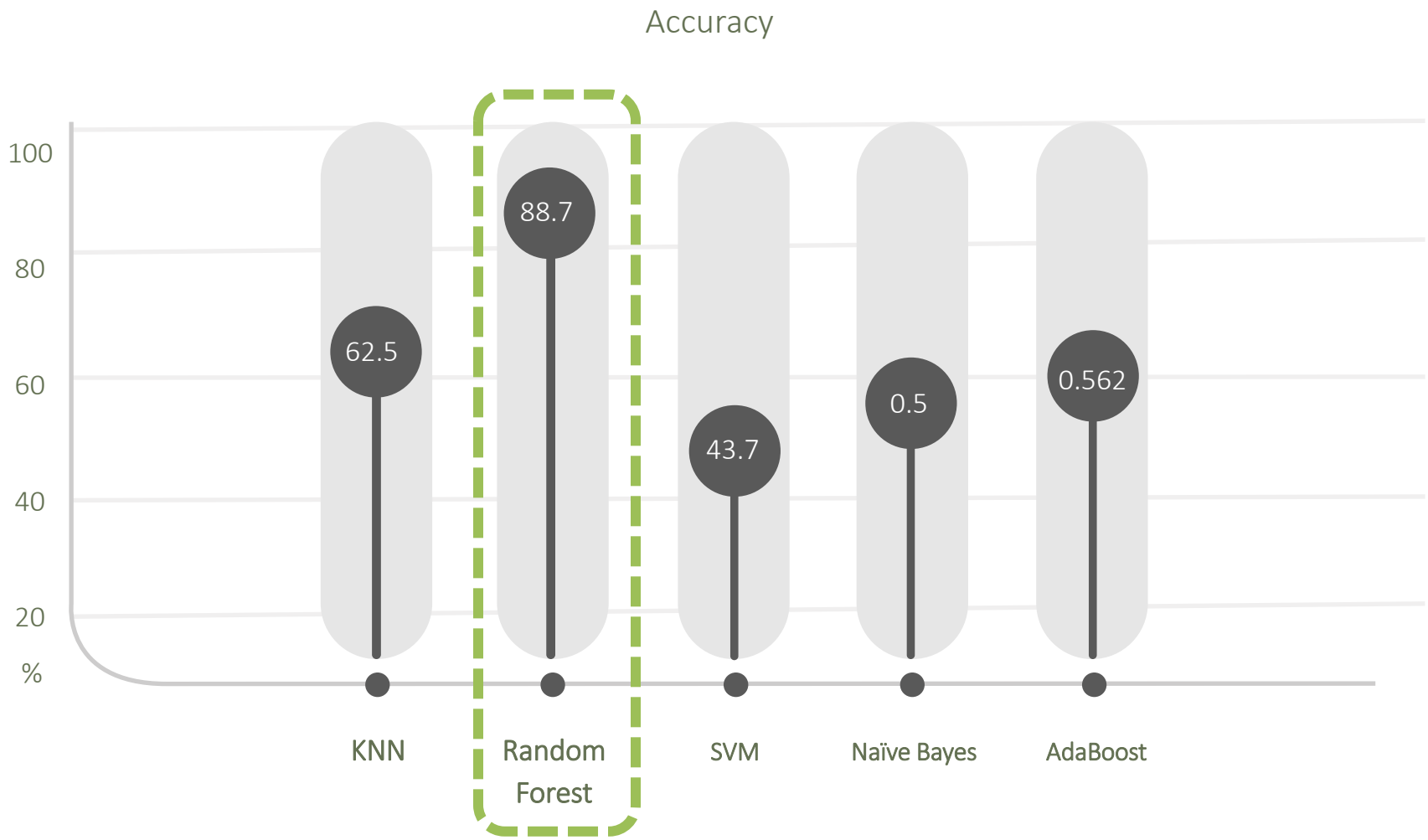
$$TPR = \frac{TP}{TP + FN}$$

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

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

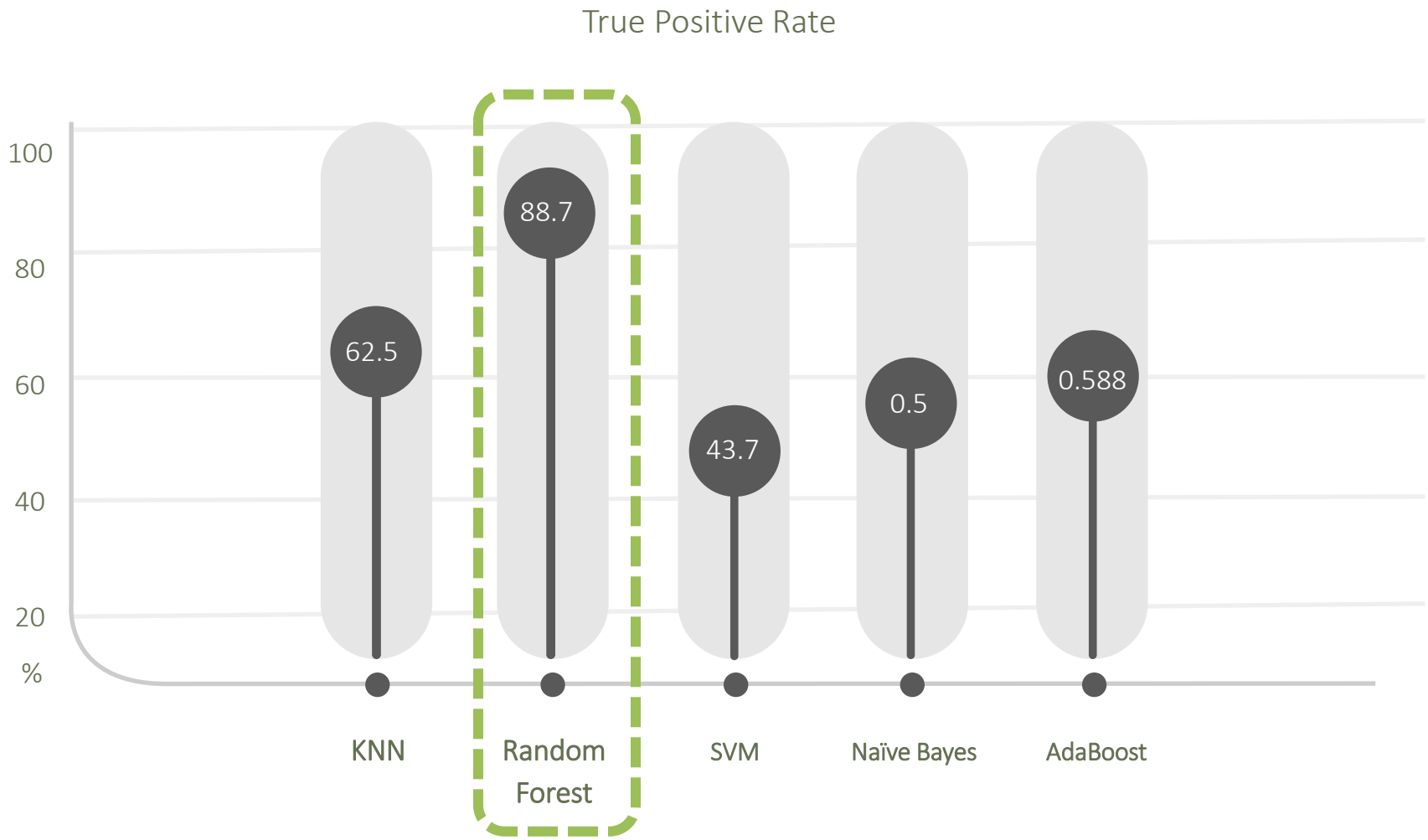
Evaluation Results

Detection of GPS Spoofing



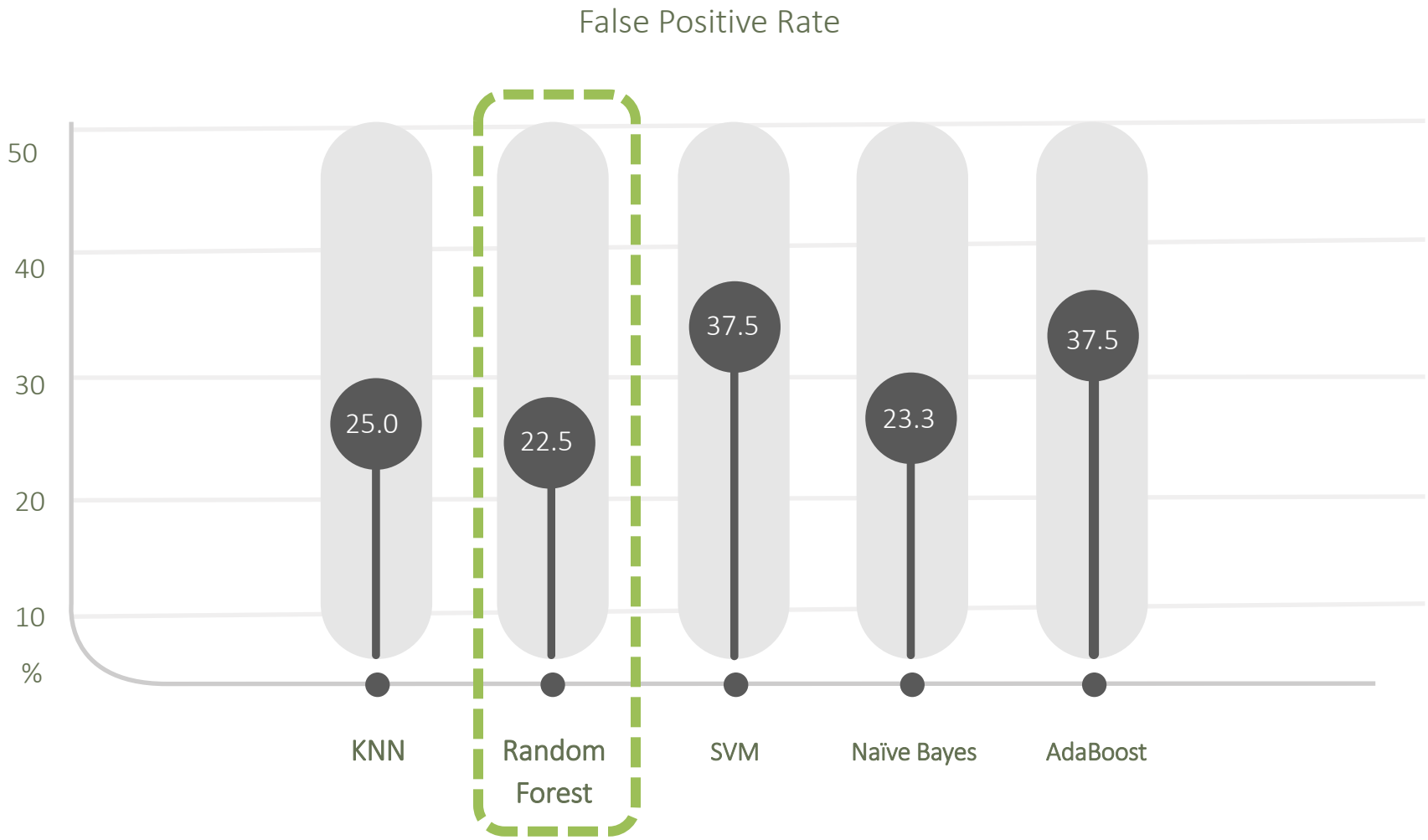
Evaluation Results

Detection of GPS Spoofing



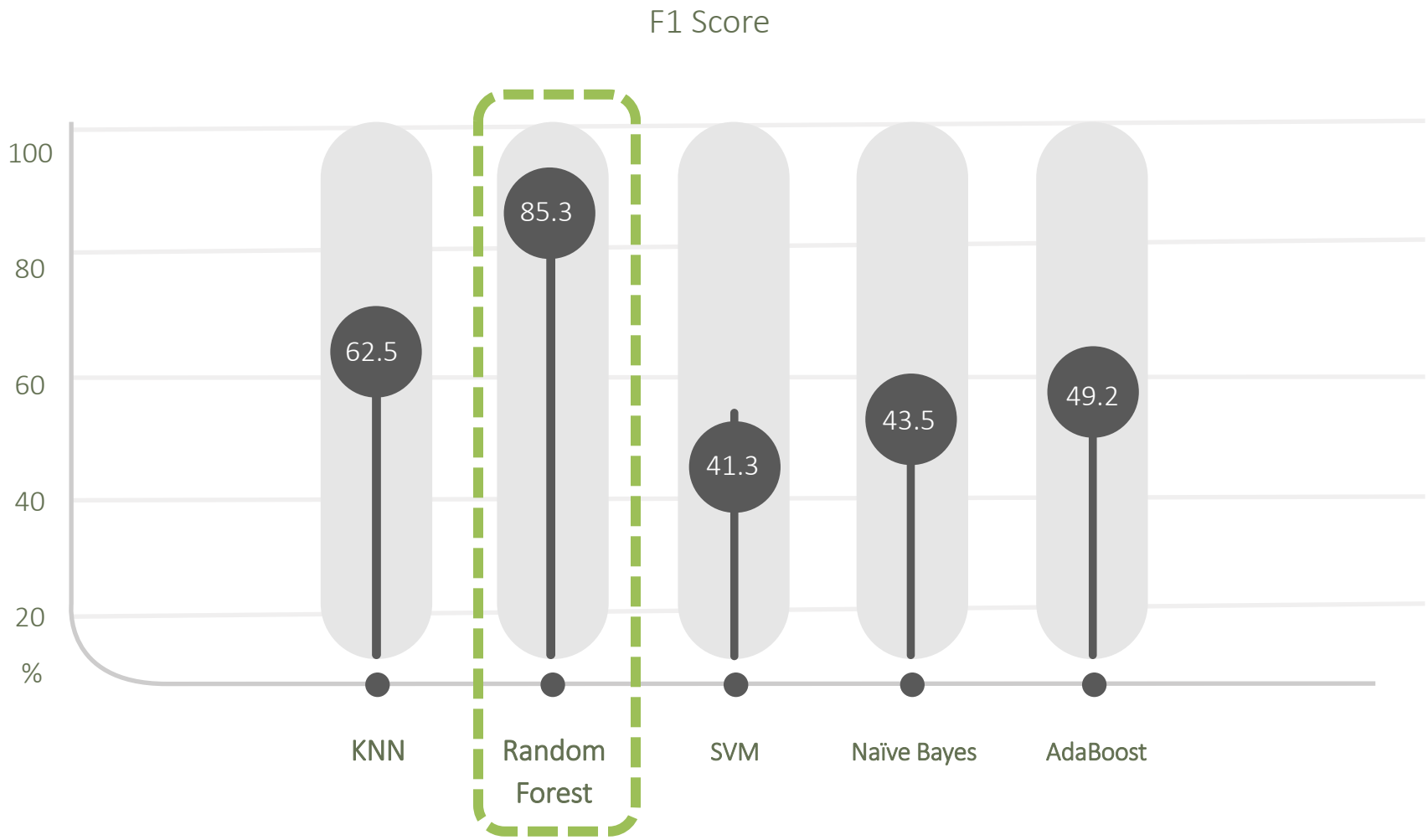
Evaluation Results

Detection of GPS Spoofing



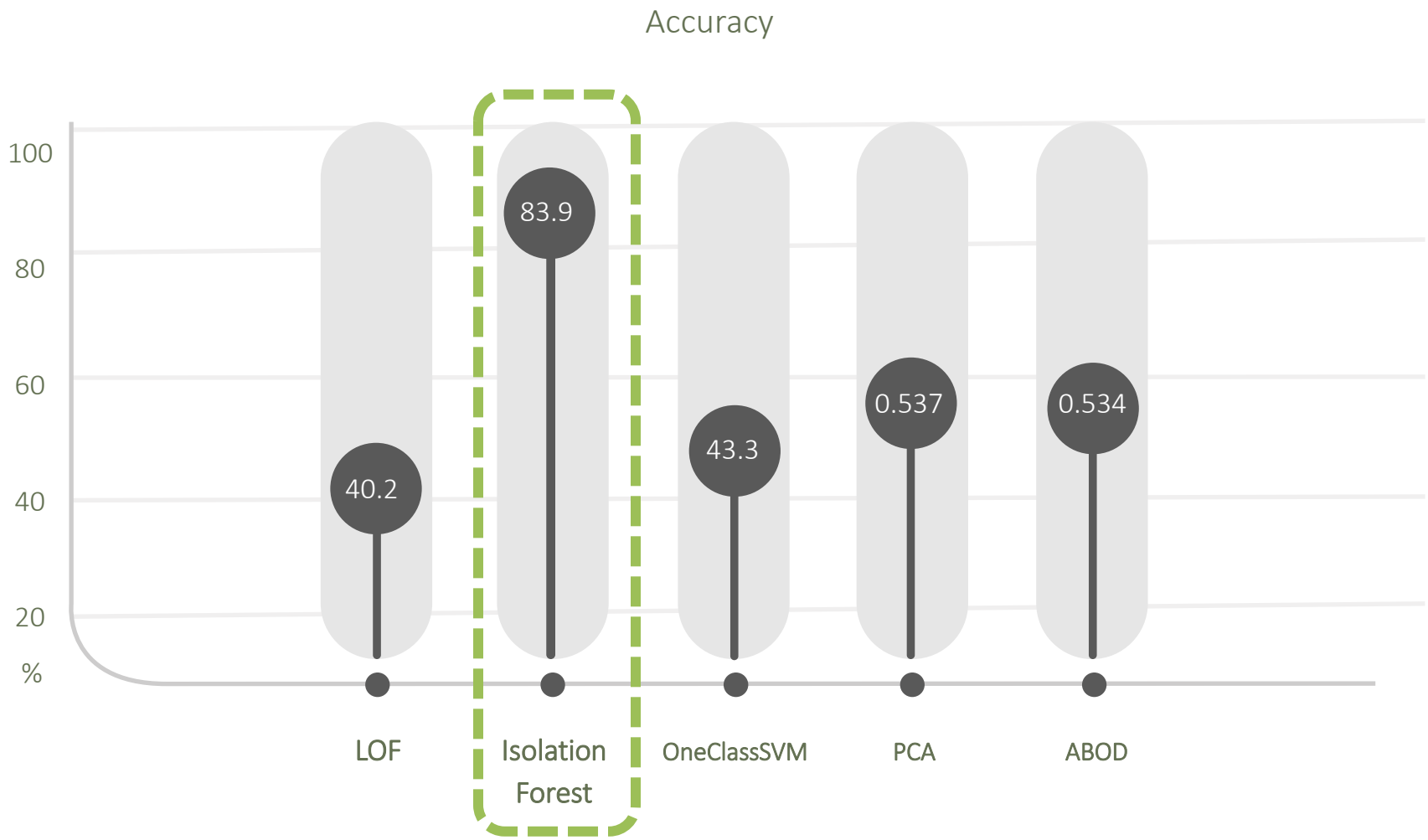
Evaluation Results

Detection of GPS Spoofing



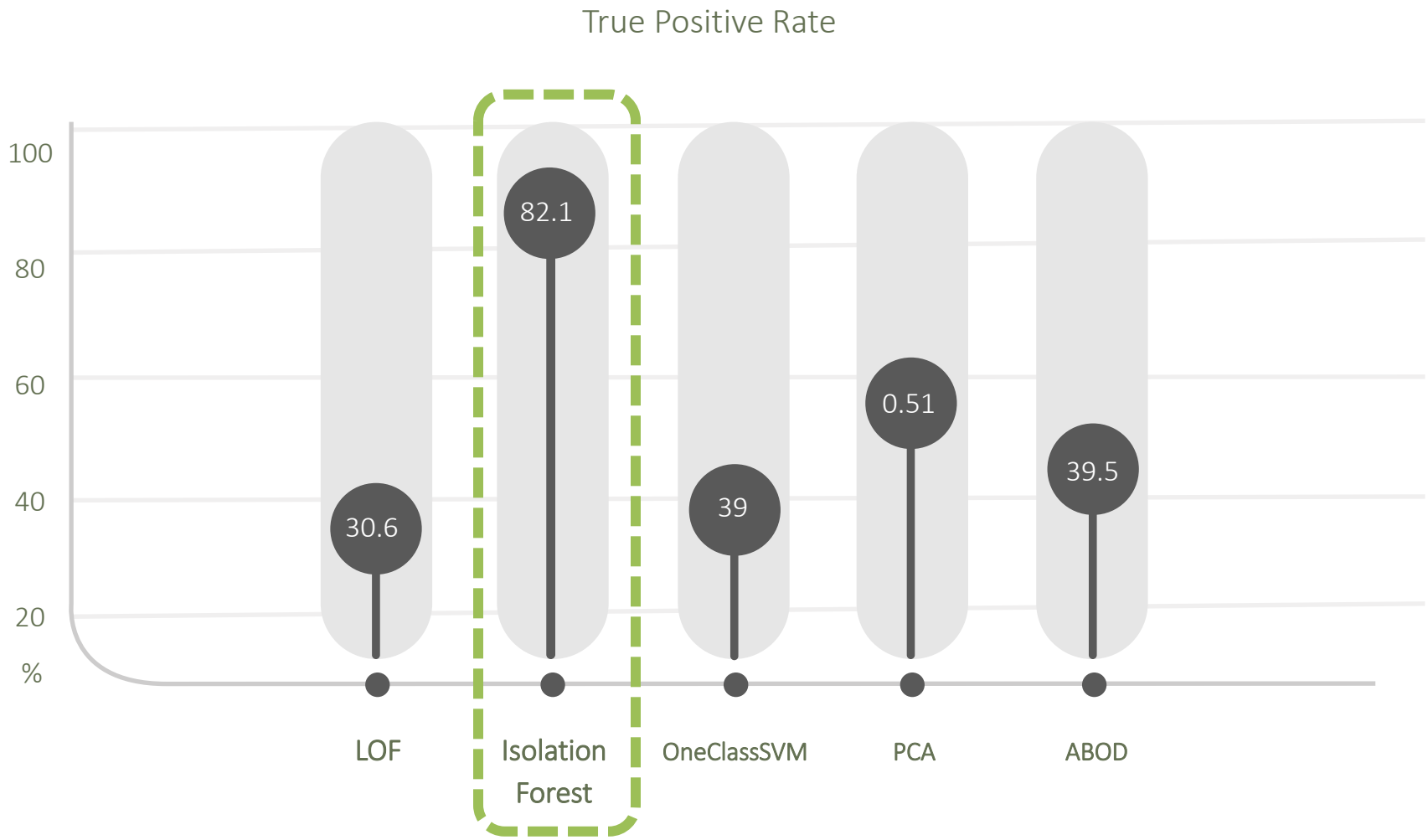
Evaluation Results

Detection of IEEE C37.118 FDI



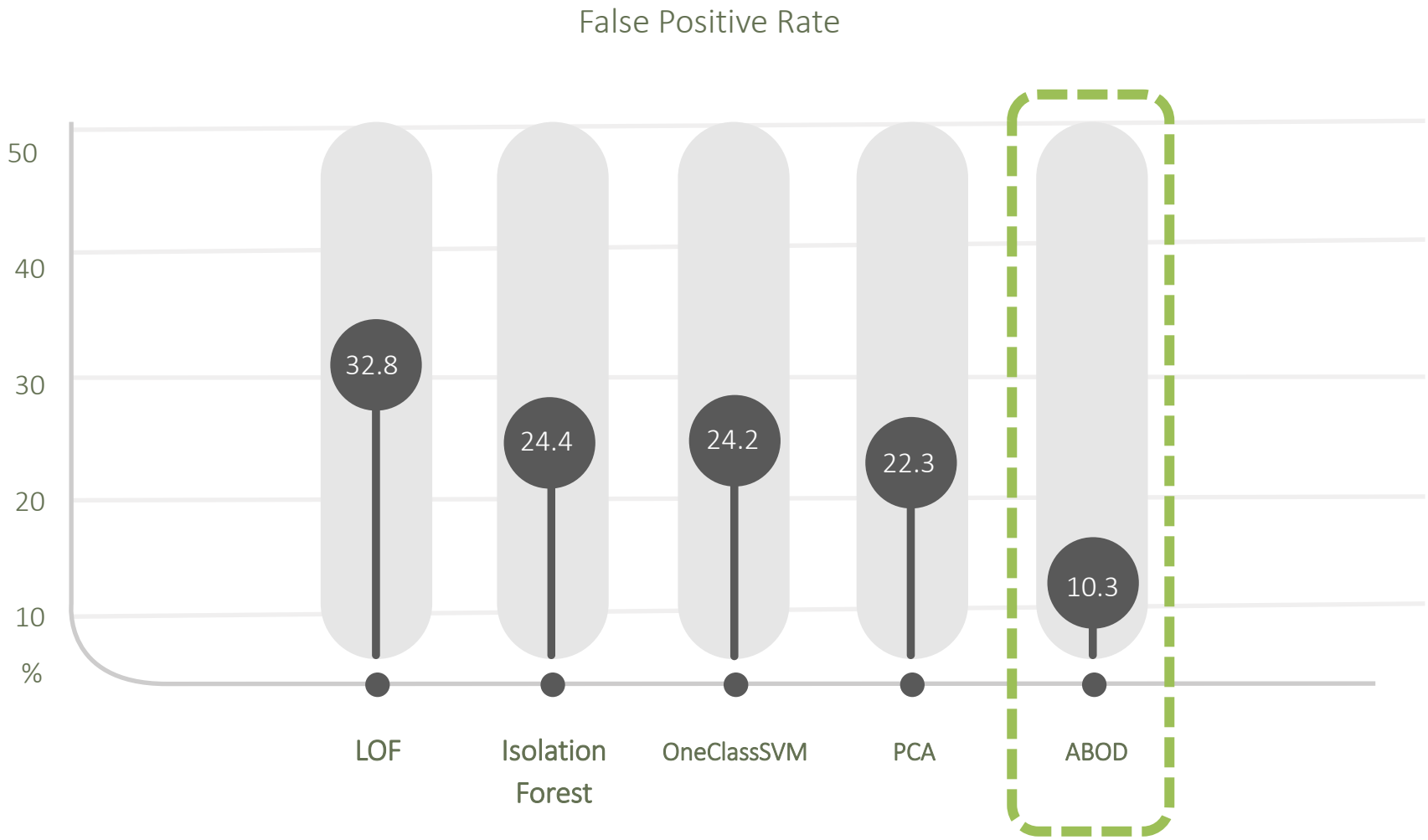
Evaluation Results

Detection of IEEE C37.118 FDI



Evaluation Results

Detection of IEEE C37.118 FDI



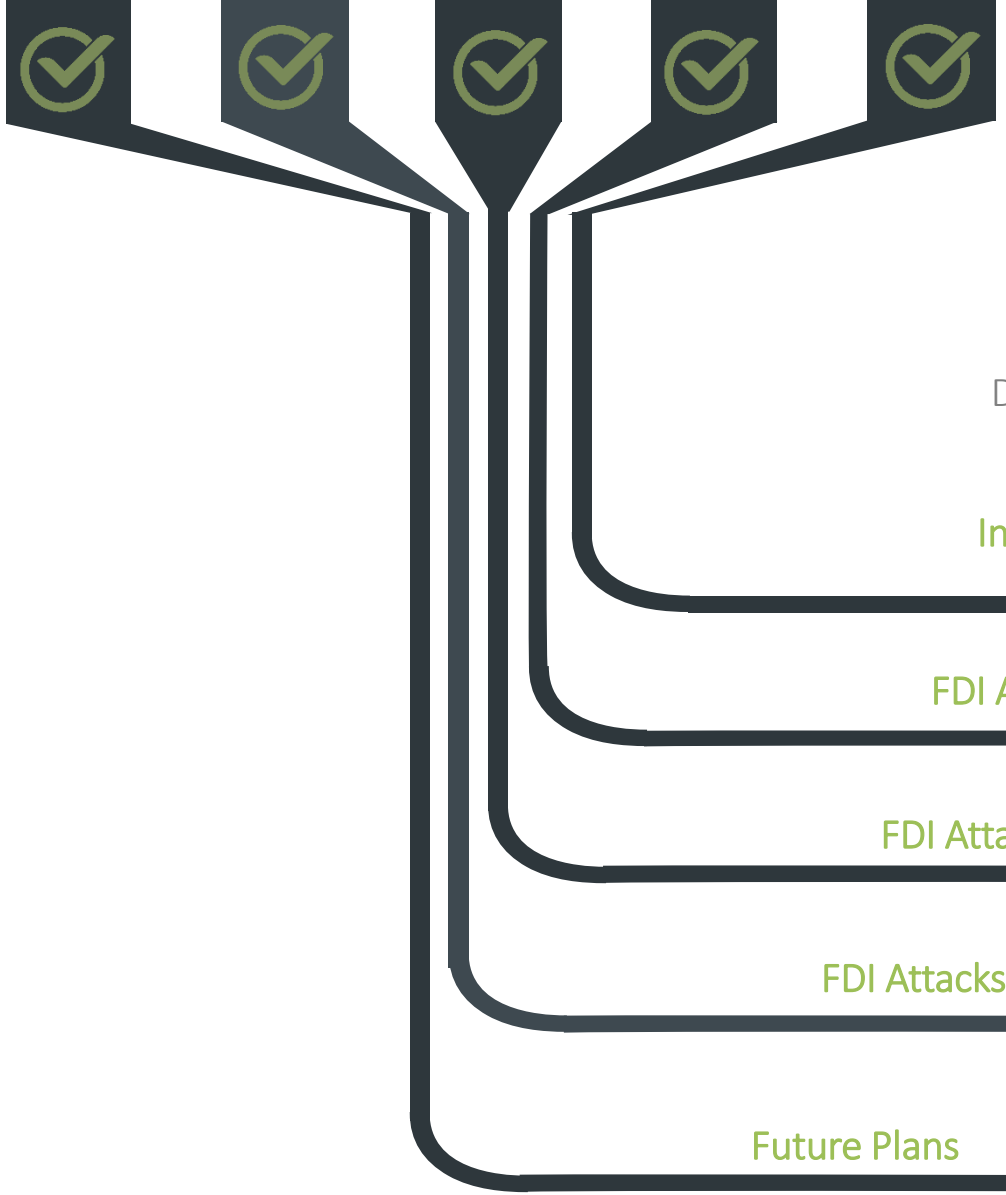
Evaluation Results

Detection of IEEE C37.118 FDI

Conclusions & Future Plans

Conclusions & Future Plans

Despite the smart technologies, severe security issues arise…



Introduction, Rationale & Objectives

1

Goal

Investigation of FDI attacks against HV Transmission Systems

FDI Attacks Modelling

2

Two FDI Attack Scenarios

(a) GPS Spoofing and (b) IEEE False Data Injection Attacks

FDI Attacks Implementation

3

Security Vulnerabilities

Both scenarios take full advantage of protocol vulnerabilities

FDI Attacks Detection

4

FDI Attacks Detection

Detecting successfully the previous cyberattacks through the ML methods: Random Forest and Isolation Forest

Future Plans

5

Future Plans

FDI attacks against Medium and Low Voltage Distribution Systems, Islanding Mechanisms

Thank You & Q/A

Contact us

ithaca (at) uowm (dot) gr

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

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

https://www.youtube.com/channel/UCl AuHbgmxirMxDy9zQt97Ew

Thank You

Q/A ?

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) .