This is a preprint version of the paper entitled "False Data Injection Attacks Against High Voltage Transmission Systems". The published version is available in IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/10257248
Citation: P. Radoglou-Grammatikis, M. Zafeiropoulou, M. Atanasova, P. Zlatev, S. Giannakidou, T. Lagkas, V. Argyriou, E. K. Markakis, I. Moscholios, P. Sarigiannidis, "False Data Injection Attacks Against High Voltage Transmission Systems," 2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT), Pafos, Cyprus, 2023, pp. 324-329, doi: 10.1109/DCOSS-IoT58021.2023.00060.

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[†]

***Abstract*—The digitisation of the smart electrical grid provides several advantages and valuable services, such as self-monitoring, pervasive control and smart healing. However, despite the benefits of this progression, critical cybersecurity and privacy issues are raised due to the vulnerabilities of legacy Electrical Power and Energy Systems (EPES) and the evolution of stealthy cyberthreats and malware. In this paper, we give emphasis to False Data Injection Attacks (FDIAs) that can affect the EPES State Estimation (SE). In particular, we investigate two FDIA categories, namely: (a) Global Positioning System (GPS) Spoofing Attacks and (b) IEEE C37.118 FDIAs against an actual testbed emulating a high-voltage IEEE 9-Bus transmission grid. Finally, we provide a relevant Intrusion Detection System (IDS) capable of detecting the aforementioned FDIAs. The evaluation analysis demonstrates the impact of the above FDIAs and the efficiency of the proposed IDS.**

***Index Terms*—False Data Injection Attacks, GPS Spoofing, High Voltage Transmission Grid, IEEE C37.118, Intrusion Detection**

I. Introduction

The smart technologies play a significant role in the digital era of the Electrical Power and Energy Systems (EPES) [1]. Despite the fact that they offer valuable services and benefits, such as (a) the two-way communication between the energy utilities and consumers, (b) self-monitoring and (c) pervasive control, they also raise severe cybersecurity and privacy issues due to the rapid evolution of stealthy cyberthreats and malware and the presence of legacy systems. In particular, both legacy and smart systems use insecure industrial protocols that do not incorporate essential authentication and authorisation mechanisms, thus allowing the execution of various cyberattacks. A special category of them against the EPES monitoring systems is the False Data Injection Attacks (FDIAs) that can access and manipulate the State Estimation (SE), compromising the relevant communications and systems. SE refers to an essential process of estimating unknown state variables based on electricity measurements and the grid topology. FDIAs can bypass the SE mechanisms, such as Bad Data Detection (BDD) methods, resulting in devastating effects.

In this paper, we focus our attention on FDIAs against a high voltage IEEE 9-Bus transmission system. In particular, we investigate the impact of two FDIA categories: (a) Global Positioning System (GPS) Spoofing Attacks and (b) IEEE C37.118 FDIAs. Both attacks aim to access and manipulate the measurements of Phasor Measurement Unit (PMUs). The first category uses GPS spoofing techniques in order to affect the time synchronisation of the PMUs and modify the voltage and current phasor measurements. On the other hand, the IEEE C37.188 FDIAs rely on Man in the Middle (MiTM) activities, targeting the communication between PMUs and the Phasor Data Concentrator (PDC). Finally, we introduce an Artificial Intelligence (AI)-based Intrusion Detection System (IDS) capable of detecting the aforementioned cyberattacks. Therefore, based on the aforementioned remarks, the contribution of this paper is twofold:

- **Modeling and Execution of FDIAs against a High-Voltage Transmission Testbed**: The impact of two FDIAs are investigated: (a) GPS spoofing attacks and IEEE C37.118 attacks against a testbed emulating a high-voltage IEEE 9-Bus transmission grid.
- **Detection of FDIAs**: We provide an efficient IDS capable of detecting the above cyberattacks.

The rest of this paper is organised as follows. Section II discusses other similar works in this area, highlighting the contribution of this paper. Next, section III introduces the IEEE 9-Bus transmission grid testbed used for the execution of the FDIAs. Section IV provides an overview of the GPS spoofing attacks and the IEEE C37.118 FDIAs. Section V presents the proposed IDS. Finally, section VI is devoted to the evaluation results, showing the impact of the FDIAs and the detection efficiency of the proposed IDS.

II. Related Work

Several papers have already investigated the security issues of the EPES and the impact of the FDIAs on them. Some of them are listed in [2]–[4]. In particular, in [3], G. Lian

*This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021936.

[†]P. Radoglou-Grammatikis and P. Sarigiannidis are with the Department of Electrical and Computer Engineering, University of Western Macedonia, Kozani 50100, Greece - E-Mail: {pradoglou,psarigiannidis}@uowm.gr

[¶] M. Zafeiropolou, M. Atanasova and P. Zlatev are with Innovative Energy and Information Technologies LTD (IEIT), BIC-IZOT, office 615 Boulevard Tsarigradsko shose, No 133, Sofia 1784, Bulgaria - E-Mail: {magda.zafiropoulou,m.atanasova,p.zlatev}@ieit.eu

[‡]S. Giannakidou is with K3Y Ltd, Dobrotitsa Despot 41, Lagera Region, 1612, Sofia, Bulgaria - E-mail: sgiannakidou@k3y.bg

[§] T. Lagkas is with the Department of Computer Science, International Hellenic University, Kavala Campus, 65404, Greece - E-Mail: tlagkas@cs.ihu.gr

[‖] V. Argyriou is with the Department of Networks and Digital Media, Kingston University London, Penrhyn Road, Kingston upon Thames, Surrey KT1 2EE, UK - E-Mail: vasileios.argyriou@kingston.ac.uk

[‡‡] E. K. Markakis is with the Department of Electrical and Computer Engineering, Hellenic Mediterranean University, 71004 Crete, Greece - E-Mail: emarkakis@hmu.gr

[††] I. Moscholios is with the Department of Informatics & Telecommunications, University of Peloponnese, 22100 Tripolis, Greece - E-Mail: idm@uop.gr

et al. present a detailed review of the FDIAs against modern power systems. In [2], M. Ahmed and A. K. Pathan provide an overview of the FDIAs and a set of evaluation metrics with respect to relevant countermeasures. In [5], A. S. Musleh et al. focus on detecting FDIAs against EPES. Finally, in [4], S. Ali et al. present a survey of Machine Learning (ML) methods for detecting FDIAs. Next, we investigate further some particular works related to FDIAs and discuss the contribution of our work.

In [6], G. Chaojung et al. present a novel detection method to detect FDIAs by tracking the dynamics of measurement variations, calculating distance indices between the adjacent steps. The new detection-based method addresses the limitations of existing methods and is based on the Kullback-Leibler distance (KLD), which calculates the distance between two distributions, p and q. The authors utilise the measurement variation from the historical data to derive the q. For every time step, p is derived from the measurement variation between the current time step and the previous time step. Based on the evaluation analysis, when there are no false data injection attacks, the KLD is quite small. When false data is injected, the KLD. The proposed method was tested, using different attack scenarios, showing that most of the attack scenarios can be detected successfully. Finally, it is worth mentioning that the proposed method does not work very well for continuous small-scale cyberattacks and continuous replay attacks.

In [7], J. Zhang et al. focus on the presence of FDIAs in the local and communicated estimated voltage within distributed dc microgrids. Based on the authors, this is a new form of intelligent attack, and it is referred to as a concurrent attack. A concurrent attack is designed to mask itself as a communication link attack, misleading the operators from taking appropriate actions. Such an attack can pose challenges that are promptly resolved by model-based detection. Therefore, the authors propose a novel nonparametric detection based on an Ensemble Empirical Mode Decomposition (EEMD). The presence of FDIAs is identified from the energy relationship of neighbouring agents, which operates on the decomposed Intrinsic Mode Functions (IMFs) of the EEMD method. A differentiation criterion is further used to classify the type of attack after detection, i.e., whether the attack is a concurrent attack or a communication link attack, based on the voltage correction terms generated by the voltage observer in the secondary controllers. Finally, an event-driven mitigation approach is proposed, reconstructing a trustworthy signal using the authenticated inputs from the proposed detection strategy. According to the classification of the attacked quantity, the reconstructed trustworthy signal replaces the attacked signal and eliminates all the risks associated with the attack. The performance of the proposed resilient control scheme has been validated under load changes, faults, converter outages and communication failures.

In [8], C. Chen et al. propose a data-driven FDIA-resilient Automatic Generation Control (AGC) scheme. The main advantages of this design include the reduced complexity of learning models and the preservation of existing control structures. The proposed FDIA-resilient AGC scheme is model-free and appealing to real-life complex power systems. The regression models studied can be characterised by two types of FDIA signals, where the sequence to-one regression model is adopted for the estimation and non-constant ones where the Long Short-Term Memory (LSTM) network powered sequence-to-sequence regression model is used to predict future non-constant FDIA signals. The authors also propose a compensation-based reconfigured mechanism using quantitative information of FDIA signals, to attenuate the impact of the FDIAs on the system frequency control performance. The effectiveness of the proposed method is validated via a benchmark power system. Based on the experimental results, the main advantage of the proposed scheme is the engineering feasibility. This is because it does not change the basic structure of the controller and outperforms the model-based controllers for large-scale power systems.

Undoubtedly, the previous works provide useful methods and results. However, it is worth mentioning that none of them focuses on the actual impact of the FDIAs against a high voltage transmission system through experimental results. Consequently, in this paper, we study two FDIA categories, namely (a) GPS Spoofing Attacks and (b) IEEE C37.118 FDI Attacks against a high-voltage transmission testbed. The impact of each category is discussed based on the false measurements injected in each case. Next, we provide a relevant IDS, which can recognise timely the aforementioned FDIAs. The evaluation results demonstrate the efficiency of the proposed IDS.

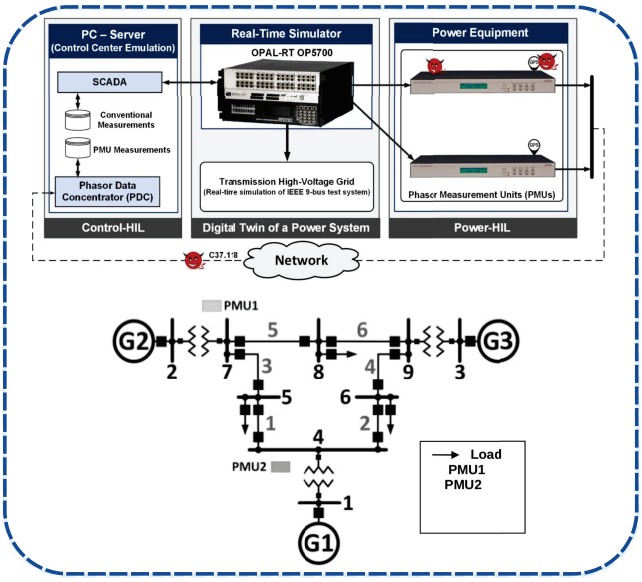

Fig. 1: Testbed

III. Testbed

As illustrated in Fig. 1, the proposed testbed consists of three generators and nine buses based on the IEEE 9-bus transmission grid model. Two Phasor Measurement Units (PMUs) (i.e, PMU1 and PMU2) have been deployed at two buses (i.e.,

bus 7 and bus4), respectively. The PMUs are integrated into the Power-Hardware In the Loop (HIL) setup, which provides measurements received from the Real-Time Simulator (OPAL-RT OP5700) to the Phasor Data Concentrator (PDC). The measurements are used to monitor the high voltage IEEE 9-bus transmission grid emulated by the Real-Time Simulator. 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. The first PMU (i.e., PMU1) is responsible for monitoring the voltage and current phasors of bus 7, while the second PMU (i.e., PMU2) monitors the voltage and current phasors of bus 4. The PDC undertakes to align the PMU measurements according to their GPS timestamps and stores them in a database at the control center. In particular, the PMU measurements include: (a) the PMU identifier, (b) timestamp, (c) the positive sequence voltage phasor measurements, (d) the positive sequence current phasor measurements and (e) the frequency measurements. The PMU measurements can be used by a Wide Area Measurement System (WAM) in order to monitor the dynamic behaviour of the grid. The PMU measurements and the analysis of WAM can be used for damping inter and local oscillations after disturbances. Moreover, apart from the PMU measurements, a set of conventional measurements (real/reactive power injection and flow) are provided by the Real-Time Simulator asynchronously within 5-30 seconds. The conventional measurements include: (a) the voltage magnitude of each bus, real and reactive power flow of each line and real and reactive power injection of each load. The conventional measurements are provided by the Real-Time Simulator in a slower sate than the PMU measurements in an asynchronous manner within 5-30 seconds.

IV. False Data Injection Attacks

As mentioned earlier, two FDIA categories are investigated in this paper, namely (a) GPS Spoofing Attacks and (b) IEEE C37.18 FDIAs. Both attacks target the PMU measurements. Each of them is further analysed in the following subsections, respectively.

A. GPS Spoofing Attacks

The GPS spoofing attacks rely on GPS spoofing techniques in order to modify the time synchronisation of the PMUs. Next, a relevant error is added to the voltage and current measurements. In particular, the attacker aims to violate the GPS signal received by the PMUs that are connected to the Real-time Simulator. The GPS spoofing attacks can modify the measurements of the voltage angle, which significantly impacts the grid monitoring and the control capacity of the control centre. Consequently, inaccurate monitoring might trigger unnecessary remedial control actions. In general, a higher difference with respect to the voltage angle between two buses can present a larger power flow between them. It is also worth mentioning that such a difference can result in inaccurate loading conditions of the lines.

B. IEEE C37.118 False Data Injection Attacks

Regarding the IEEE C37.18 FDIAs, the IEEE C37.118 communication between the PMUs and PDC is targeted. The PMU measurements are transmitted to the PDC through IEEE C37.118 data frames. In particular, an IEEE C37.118 data frame can include: (a) the magnitude and angle of phasors in a rectangular or polar format, (b) frequency and (c) the Rate of Change of Frequency (ROCOF). Thus, the goal of the cyberattacker is to intercept the IEEE C37.118 messages and inject false measurements. For this purpose, a Man In the Middle (MITM) attacks is executed between the PMU and PDC, taking full advantage of the Address Resolution Protocol (ARP) weaknesses. The ARP cache of the PMUs and PDCs is poisoned in order to forward their network traffic data to the cyberattacker before the packets reach their original destination. `NetfilterQueue` is used to process the IEEE C37.118 packets, while `Scapy` is used to alter their content. False PMU measurements stored in a PDC can lead the system operator to perform mistaken actions with devastating effects. The IEEE C37.118 protocol is prone to FDIAs and integrity attacks since the relevant Cyclic Redundancy Check (CRC) can be easily violated. In particular, the cyberattacker can inject false measurements when the 16-bit CRC is re-calculated. Next, since CRC is valid, the false PMU measurements are accepted normally by PDC.

V. Proposed Intrusion Detection System

The proposed IDS is composed of four modules: (a) Data Collection Module (DCM), (b) Network Flow Extraction Module (NFEM), (c) Analysis Engine and (d) Response Module (RM). The DCM receives the various PMU measurements, such as the positive sequence voltage magnitude and angle. Moreover, DCM can monitor continuously the network traffic data of PMUs, through a Switched Port Analyser (SAPN) and `Tcpdump`. Next, the NFEM receives the aforementioned data from DCM and generates bidirectional network flow statistics. Next, the Analysis Engine receives both kinds of data (i.e., (a) PMU measurements and (b) network flow statistics), preprocesses them and detects potential FDIAs. The PMU measurements are used to detect the GPS spoofing attacks, while the network flow statistics are utilised for the detection of the IEEE C37.118 FDIAs. With respect to the detection process, the Analysis Engine relies on an autoencoder. Finally, the RM receives the detection outcomes and generates security events based on the AlienVault OSSIM format [9].

VI. Evaluation Analysis

A. Experimental Results - GPS Spoofing Attack

Based on the Positioning, Navigation and Timing (PNT) services of GPS, the PMUs use GPS signals in order to provide timestamped measurements like voltage and current phasors, frequency and ROCOF. In a GPS spoofing attack, the PMUs synchronisation is compromised, thus affecting the measurements transmitted. A GPS spoofing attack is performed through a particular device called GPS spoofer, which transmits satellite signals manipulating the actual GPS

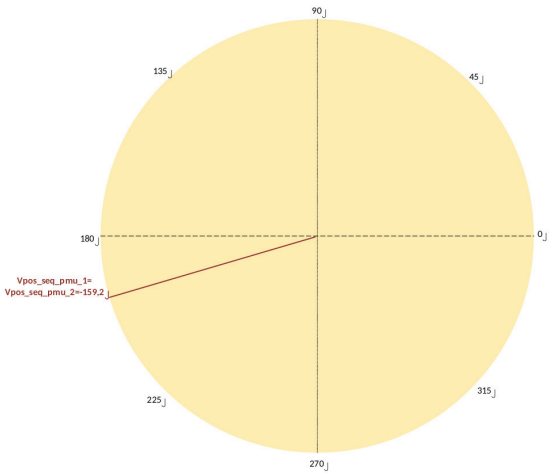

Fig. 2: Phasor Measurement at Bus 4 from PMU1 and PMU2 before the GPS Spoofing Attack

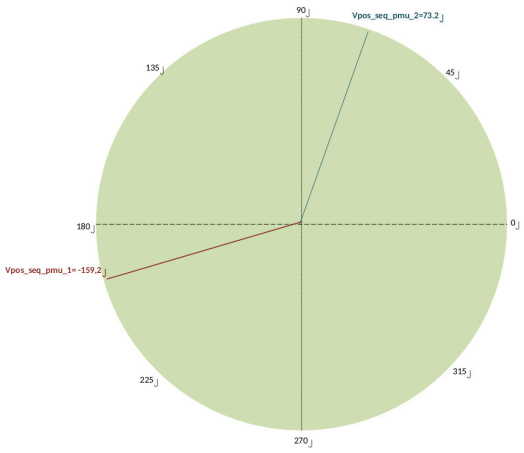

Fig. 3: Phasor Measurement at Bus 4 from PMU1 and PMU2 after the GPS Spoofing Attack

signal, thus leading the GPS receiver of a PMU to perceive an erroneous clock offset. Based on an f-Hz signal, the phase measurement error e is calculated by Equation 1.

$$e = [f \times (\tilde{t_\delta} - t_\delta) \times 360^o] \mod 360^p \quad (1)$$

where $\tilde{t_\delta}$ indicates the receiver clock offset (post-attack), t_δ is the pre-attack value and finally f denotes the frequency.

The GPS spoofing attack was executed against the PMU2 located at bus 4. In order to verify that the GPS spoofing attack is successful, PMU1 is also placed on bus 4, receiving the actual GPS signal (not the manipulated one). Fig. 2 shows the voltage phasor measurements of PMU1 and PMU2 before the attack, while Fig. 3 shows the voltage phasor measurements after the attack. During the GPS spoofing attack, a receiver clock offset error of 7.05 ms is injected into the actual GPS signal. This time offset between the real and the manipulated GPS signal generates an error with respect to the voltage angle by 126.9^o. Such a variance is adequate to impact significantly the grid monitoring and control mechanisms. Moreover, as illustrated in Table I, other clock offset errors were tested, resulting in the corresponding voltage phasor angles.

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

B. Experimental Results - IEEE C37.18 FDI Attacks

Regarding the IEEE C371.118 FDIAs, several malicious activities are performed during five attack phases. For the PMU1-Bus 7, the following attack phases are executed, as illustrated in Fig. 4.

- **A1 (465s-525s) - Lines 7-2**: Current magnitude and angle attack
- **A2 (1100s-1160s) - Lines 7-2**: Voltage magnitude attack and current magnitude attack
- **A3 (2085s-2145s) - Lines 7-5**: Current magnitude attack
- **A4 (2905s-2965s) - Lines 7-5**: Current angle attack
- **A5 (3710s-3770s)**: Voltage magnitude and angle attack at Bus 7

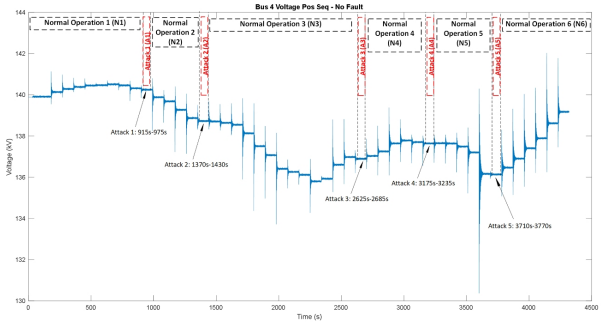

Fig. 4: Summary of IEEE C371.118 FDI attacks against PMU1 - Bus 7

In a similar manner, as depicted in Fig. 5, the following attack phases are executed against PMU2 - Bus 4.

- **A1 (915s-975s)**: Voltage magnitude attack at Bus 4
- **A2 (1370s-1430s) - Lines 4-1**: Current magnitude attack
- **A3 (2625s-2685s)**: Voltage angle attack at Bus 4
- **A4 (3175s-3235s) Lines 4-1**: Current angle attack
- **A5 (3710s-3770s)**: Frequency attack

During the angle-related attacks, the phase angle is set to 90^o. On the other hand, with respect to the magnitude-related attacks, the phasor's magnitude is increased by 50%. In addition, a ramp attack is executed when the frequency measurement is modified. More specifically, the attacker slowly decays the value of frequency to 49 Hz and then increases it back to 50 Hz. Figs. 6-10 show how the various measurements are affected during the various IEEE C37.118 FDIAs. In particular, Fig. 6 shows that the magnitude of the positive

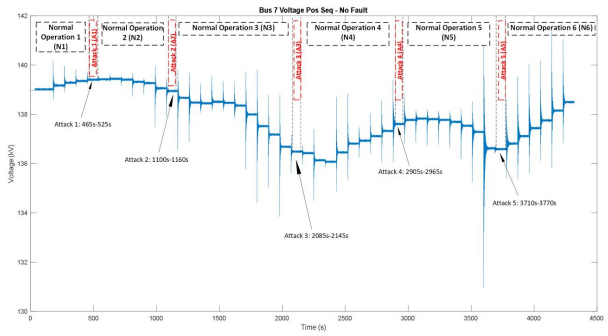

Fig. 5: Summary of IEEE C371.118 FDI attacks against PMU1 - Bus 4

sequence voltage is increased by 50% of its nominal value in the 915_{th} second. Fig. 7 illustrates an angle-related FDIA, where the phase angle is set to 90^o. Next, Fig. 8 and Fig. 9 show the FDIAs related to (a) the positive sequence current magnitude and (b) the angle. The magnitude is increased by 50% of its nominal value, and the angle is set to 90^o. Finally, Fig. 10 depicts the frequency-related FDIA where the frequency is reduced to 49 Hz and then it is increased to 49.8 Hz.

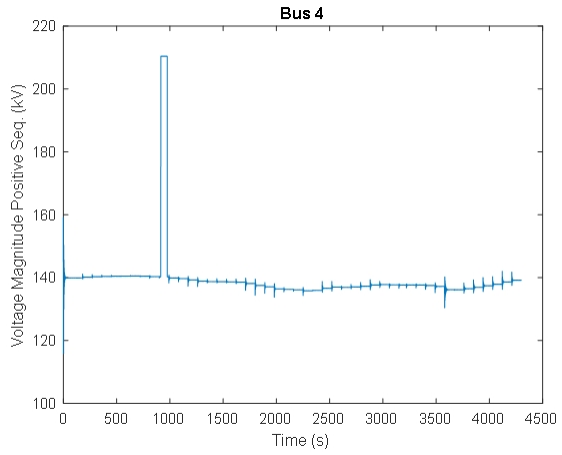

Fig. 6: IEEE C37.118 FDI Attack against PMU2 - Bus 4 // Positive Sequence Voltage Magnitude

C. FDIA Detection

Before discussing the detection performance of the proposed IDS, we have to introduce first the necessary terms. Thus, True Positives (TP) denotes the number of the correct classification with respect to the presence of FDIAs. Similarly, True Negatives (TN) implies the number of the correct classification regarding the normal instances. On the other side, False Negatives (FN) and False Positives (FP) implies the mistaken classification related to the FDI attacks. Thus, based on the aforementioned terms, the following evaluation metrics are used.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (2)$$

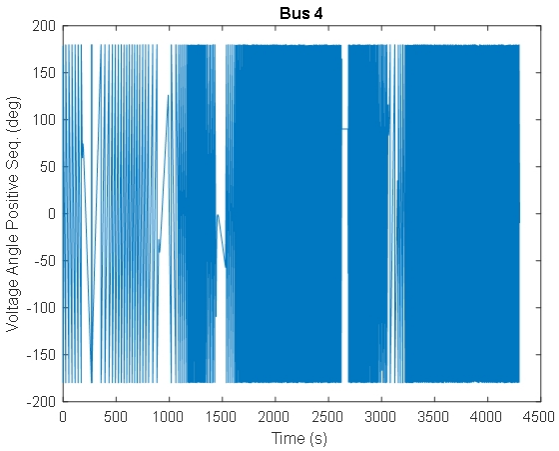

Fig. 7: IEEE C37.118 FDI Attack against PMU2 - Bus 4 // Positive Sequence Voltage Angle

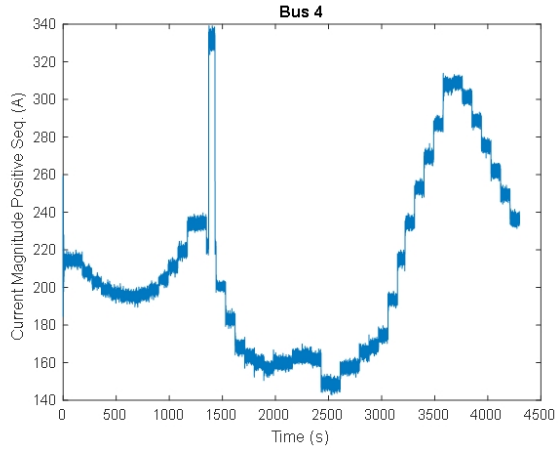

Fig. 8: IEEE C37.118 FDI Attack against PMU2 - Bus 4 // Positive Sequence Currrent Magnitude - Line 4-1

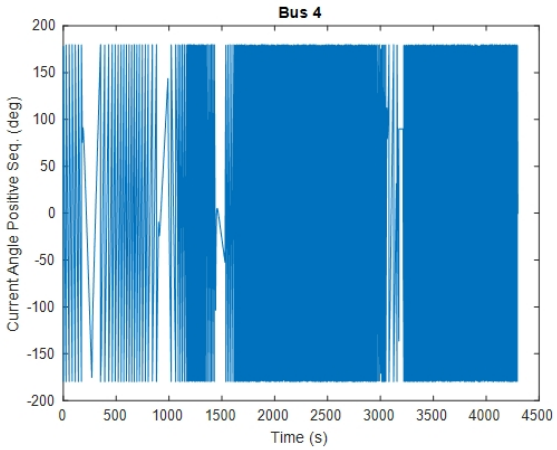

Fig. 9: IEEE C37.118 FDI Attack against PMU2 - Bus 4 // Positive Sequence Current Angle - Line 4-1

$$TPR = \frac{TP}{TP + FN} \quad (3)$$

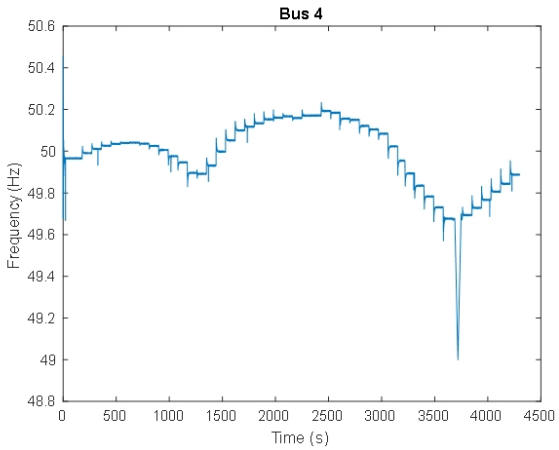

Fig. 10: IEEE C37.118 FDI Attack against PMU2 - Bus 4 // Frequency

$$FPR = \frac{FP}{FP + TN} \tag{4}$$

$$F1 = \frac{2 \times TP}{2 \times TP + FP + FN} \tag{5}$$

Table II shows evaluation results regarding the detection efficiency of GPS spoofing attacks. In particular, five outlier/novelty detection methods are utilised and evaluated with each other: (a) Local Outiler Factor (LOF), (b) Isolation Forest, (c) OneClassSVM, (d) Principal Component Analysis (PCA) and (d) Angle Based Outlier Detection (ABOD). The best performance is accomplished by Isolation Forest where $Accuracy = 0.839$, $TPR = 0.821$, $FPR = 0.244$ and $F1 = 0.823$. Table III summarises the evaluation results with respect to detecting IEEE C37.118 FDIAs. In particular, five AI model were used and evaluated with each other: (a) K-Nearest Neighbour (KNN), (b) Random Forest, (c) Support Vector Machine (SVM), (d) Naive Bayes and (e) Adaboost. Based on the evaluation results, Random Forest achieves the best performance where $Accuracy = 0.887$, $TPR = 0.887$, $FPR = 0.225$ and $F1 = 0.853$.

TABLE II: Evaluation Results: Detection of GPS Spoofing Attacks

AI Model	Accuracy	TPR	FPR	F1
KNN	0.625	0.625	0.250	0.625
Random Forest	**0.887**	**0.887**	**0.225**	**0.853**
SVM	0.437	0.443	0.375	0.413
Naive Bayes	0.500	0.500	0.233	0.435
Adaboost	0.562	0.588	0.375	0.492

TABLE III: Evaluation Results: Detection of IEEE C371.118 FDIAs

AI Model	Accuracy	TPR	FPR	F1
LOF	0.402	0.306	0.328	0.401
Isolation Forest	**0.839**	**0.821**	**0.244**	**0.823**
OneClassSVM	0.433	0.390	0.242	0.421
PCA	0.537	0.512	0.223	0.522
ABOD	0.534	0.395	0.133	0.529

VII. Conclusions

It is evident that the digitisation of the EPES raises severe cybersecurity and privacy risks with disastrous effects. For instance, Indostroyer was a characteristic Advanced Persistent Threat (APT), leading to a large-scale power outage in 2015 for more than 220,000 people in Ukraine. In this paper, we focus our attention on FDIAs against high-voltage transmission grid systems. In particular, we investigate two FDIA categories: (a) GPS Spoofing Attacks and (b) IEEE C37.118 FDIAs based on a real testbed emulating a high-voltage IEEE 9-Bus transmission grid. Both categories intend to violate the PMU measurements determining the SE of the grid. The impact of each attack is investigated with respect to the various PMU measurements. Finally, we provide an IDS capable of recognising the above FDIAs. The evaluation results demonstrate the impact of the FDIAs and the detection performance of the proposed IDS.

VIII. Acknowledgement

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936.

References

[1] P. R. Grammatikis, P. Sarigiannidis, C. Dalamagkas, Y. Spyridis, T. Lagkas, G. Efstathopoulos, A. Sesis, I. L. Pavon, R. T. Burgos, R. Diaz *et al.*, "Sdn-based resilient smart grid: The sdn-microsense architecture," *Digital*, vol. 1, no. 4, pp. 173–187, 2021.

[2] M. Ahmed and A.-S. K. Pathan, "False data injection attack (fdia): an overview and new metrics for fair evaluation of its countermeasure," *Complex Adaptive Systems Modeling*, vol. 8, no. 1, pp. 1–14, 2020.

[3] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2016.

[4] 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," *IET Smart Grid*, vol. 3, no. 5, pp. 581–595, 2020.

[5] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2218–2234, 2019.

[6] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in ac state estimation," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2476–2483, 2015.

[7] J. Zhang, S. Sahoo, J. C.-H. Peng, and F. Blaabjerg, "Mitigating concurrent false data injection attacks in cooperative dc microgrids," *IEEE Transactions on Power Electronics*, vol. 36, no. 8, pp. 9637–9647, 2021.

[8] C. Chen, Y. Chen, J. Zhao, K. Zhang, M. Ni, and B. Ren, "Data-driven resilient automatic generation control against false data injection attacks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 12, pp. 8092–8101, 2021.

[9] P. Radoglou-Grammatikis, P. Sarigiannidis, E. Iturbe, E. Rios, S. Martinez, A. Sarigiannidis, G. Eftathopoulos, Y. Spyridis, A. Sesis, N. Vakakis *et al.*, "Spear siem: A security information and event management system for the smart grid," *Computer Networks*, vol. 193, p. 108008, 2021.