This is a preprint version of the paper entitled "False Data Injection Attacks against Low Voltage Distribution Systems". The paper was presented in 2022 IEEE GLOBECOM. The public version of the paper is available at the following link: https://ieeexplore.ieee.org/document/10000880

P. Radoglou-Grammatikis, C. Dalamagkas, T. Lagkas, M. Zafeiropoulou, M. Atanasove, P. Zlatev, A-A. Boulogeorgos, V. Argyriou, E. K. Markakis, I. Moscholios and P. Sarigiannidis "False Data Injection Attacks against Low Voltage Distribution Systems," GLOBECOM 2022 - 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 2022, pp. 1856-1861, doi: 10.1109/GLOBECOM48099.2022.10000880.

False Data Injection Attacks against Low Voltage Distribution Systems

Panagiotis Radoglou-Grammatikis[†], Christos Dalamagkas[‡], Thomas Lagkas[§], Magda Zafeiropoulou[¶], Maria Atanasova[¶], Pencho Zlatev[¶], Alexandros-Apostolos A. Boulogeorgos[†], Vasileios Argyriou[‖], Evangelos K. Markakis[**], Ioannis Moscholios[††] and Panagiotis Sarigiannidis[†]

***Abstract*—The transformation of the conventional electrical grid into a digital ecosystem brings significant benefits, such as two-way communication between energy consumers and utilities, self-monitoring and pervasive controls. However, the advent of the smart electrical grid raises severe cybersecurity and privacy concerns, given the presence of legacy systems and communications protocols. This paper focuses on False Data Injection (FDI) cyberattacks against a low-voltage distribution system, taking full advantage of Man In The Middle (MITM) actions. The first cyberattack targets the communication between a smart meter and an Active Distribution Management System (ADMS), while the second FDI cyberattack targets the communication between a smart inverter and ADMS. In both cases, the cyberattacks affect the operation of the distribution transformer, thus resulting in devastating consequences. Moreover, this paper provides an Artificial Intelligence (AI)-based Intrusion Detection System (IDS), detecting and mitigating the above cyberattacks in a timely manner. The evaluation results demonstrate the efficiency of the proposed IDS.**

***Index Terms*—Anomaly Detection, Cybersecurity, False Data Injection, Man In the Middle, Electrical Grid**

I. Introduction

The smart technologies play an important role in the digitisation of the conventional electrical grid into a new paradigm (usually called smart grid), providing multiple benefits, such as two-way communication, pervasive control and self-healing. However, this evolution brings also severe cybersecurity and privacy concerns due to the presence of legacy systems and new cyberthreats. In particular, legacy systems, such as Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA), use insecure communication protocols designed without comprising essential authentication and authorisation mechanisms [1]. In parallel, cyberattacks kits and malware are continuously evolving, resulting in devastating effects or even fatal accidents. A characteristic Advanced Persistent Threat (APT) [2] related to the energy sector was Indostroyer, generating a large-scale power outage in Ukraine.

In this paper, we focus our attention on False Data Injection (FDI) attacks. The 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. In particular, we investigate two FDI cyberattacks against a low-voltage distribution system. The first cyberattack targets the communication between a smart meter and the Active Distribution Management System (ADMS), while the second attack focuses on the communication between a smart inverter and ADMS. In both cases, the confidentiality is violated through a Man In The Middle (MITM) attack [3] against the Modbus/Transmission Control Protocol (TCP) [4], [5]. Finally, a relevant Intrusion Detection System (IDS) is presented. The proposed IDS utilises an autoencoder [6], (i.e., a kind of Deep Neural Network (DNNs)) capable of discriminating FDI-related network flows as oultiers/anomalies. Based on the aforementioned remarks, the contribution of this paper is twofold:

- **Modeling and Execution of FDI Cyberattacks against Low-Voltage Distribution Grid**: 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.
- **Detection of FDI Attacks**: An AI-based IDS is provided, recognising efficiently the aforementioned cyberattacks. The detection accuracy of the proposed IDS reaches 85%.

The rest of this paper is organised as follows. Section II presents some similar works related to FDI cyberattacks. Section III discusses the testbed utilised for the execution of the FDI cyberattacks. Section IV analyses further each FDI cyberattack, providing relevant technical details. Section V presents the proposed IDS. Finally, section VI discusses the experimental results, while section VII concludes this paper.

*This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833955.

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

[‡]C. Dalamagkas is with the Innovation Hub of Public Power Corporation S.A., Leontariou 9, Kantza, Attica 15351, Greece - E-mail: c.dalamagkas@dei.gr

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

[‖] 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

978-1-6654-3540-6/22 © 2022 IEEE

II. Related Work

Several works have investigated the security issues related to the smart electrical grid. Some of them are listed below [7]–[13]. In general, it is evident that the electrical grid suffers from a large number of cyberthreats. According to the goals of this paper, next, we summarise some works emphasising on FDI cyberattacks.

A survey on FDI attacks against active distribution systems is presented in [14]. The authors propose a taxonomy of FDI attacks based on the adversarial point of view. The threat categories examined are: end-user level, field devices, control centre and energy pricing and trading. The end-user level, which is the most relevant with respect to the attack scenarios studied in our work, includes FDI attacks targeting the energy management systems, such as energy storage, photovoltaic (PV) systems and Advanced Metering Infrastructures (AMIs).

The necessity for advanced detection methods against FDI attacks is highlighted in [15]. The authors identify significant challenges towards the development of efficient detection mechanisms that can recognise FDI cyberattacks, given the dynamic nature of the electrical grid, the uncertainty of electricity measurements, the data volume and factors that magnify the complexity of identifying patterns and understanding the FDI actions.

A MITM attack is demonstrated in [16] against a commercial solar PV inverter. A large-scale laboratory setup was employed, consisting of a Direct Current (DC) generator, an inverter, an artificial load, a control unit for ancillary services and the attacker. The attacker injects false measurements for the active and reactive power via the Local Area Network (LAN), causing the ancillary service-related controller to stop feeding the power grid, thus resulting in a regional blackout.

III. Testbed

The impact of each FDI cyberattack is investigated in a realistic testbed composed of commercial components to emulate an active low-voltage distribution grid. In this setup, the Modbus/TCP protocol is used by the ADMS to collect active and reactive power measurements from the underlying smart meters. Moreover, Modbus/TCP is also used by the ADMS to issue commands to the smart inverters, aiming to compensate the power factor by regulating the reactive power injection and avoiding reverse power flow conditions through curtailments (for limiting the active power generation of PV). The testbed architecture is depicted in Fig. 1. In particular, the following equipment is utilised.

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), which uses Modbus/TCP. This Modbus/TCP interface is utilised by the ADMS to monitor the active and reactive power of the PV inverter (P_{PV} and Q_{PV}). Moreover, the inverter accepts control commands through the same Modbus/TCP interface. Therefore, a 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.

Low-Voltage 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 (ADMS): The ADMS emulate the control centre of the operator. To this end, a server computer is utilised. The ADMS hosts an AMI-related technology, which receives all the measurements (P_{grid}, Q_{grid} from SM1, P_{Load}, Q_{Load} from SM2, P_{PV}, Q_{PV} from SM3) and stores them in a database. Based on the aforementioned measurements, two control schemes, namely (a) Power Factor Compensation Scheme and (b) Curtailment Control Scheme generate the control setpoints for the inverter every four seconds. The Power Factor Compensation Scheme aims to compensate the reactive power consumed by the load in order to achieve a unity power factor for the distribution grid. In particular, the reactive power setpoint (Q_{sp}) is generated by the control scheme to control the reactive power injection of the PV inverter. Thus, to achieve a $Qgrid$ near to zero, the power factor compensation scheme sets $Q_{sp} = Q_{Load}$. On the other hand, the Curtailment Scheme aims to prevent any intensive reverse power flow conditions. In such conditions, active power flows from the low-voltage side (consumers and prosumers) to the rest of the distribution grid. In order 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 by the loads. Consequently, the set-point for the upper limit of the inverter is set as $P_{max} = 1.1 \cdot P_{Load}$ in order to limit the generation according to the demand and therefore to limit the reverse power flow from the low-voltage distribution grid.

IV. False Data Injection Attacks

The low-voltage distribution grid is continuously monitored by smart meters responsible for sending measurements periodically to the ADMS. In turn, the ADMS processes those measurements in order to manage the inverters with respect to (a) power factor compensation and (b) curtailment. The MITM actions target (a) the communication between the smart meter and the ADMS and (b) the communication between the ADMS and the inverter. Both scenarios intend to violate the exchanged measurements or the coordination

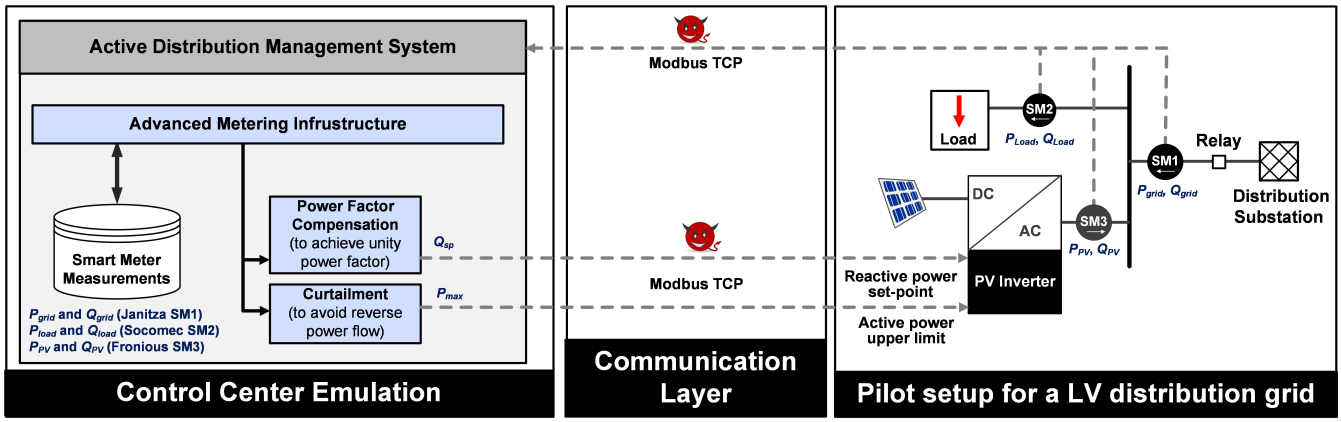

Fig. 1: Testbed - Execution of FDI Cyberattacks against a Low-Voltage Distribution Grid

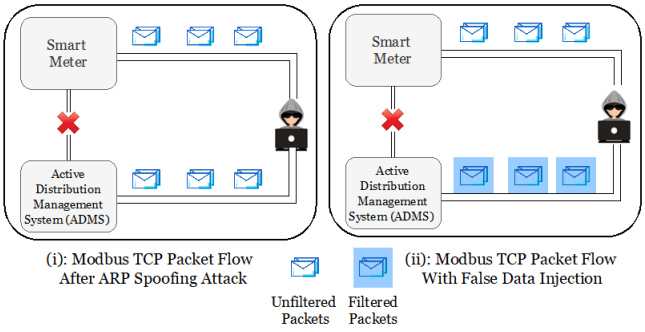

Fig. 2: Modbus/TCP Packet Flows Before and After the FDI Cyberattacks

setpoints, thereby resulting in critical effects, such as (a) loss of energy and (b) overloading. More information for each scenario is given below.

Attack Scenario A - Attacking Smart Meter Measurements: In this scenario, a malicious user attempts to malform the active and reactive power measurements of the load (P_{Load} and Q_{Load}) sent by the smart meter. Since the power factor compensation and the curtailment control scheme of the ADMS rely on the P_{Load} and Q_{Load} measurements, the overall operation of the distribution grid is threatened.

Attack Scenario B - Attacking Control Signals: The reactive power setpoint (Q_{sp}) and the active power limits ($Pmax$) coordination signals, (sent by the ADMS to the inverter), are targeted by the malicious actor. As a result, it is possible to alter the reactive power injection (Q_{PV}) and reduce the active power production (P_{PV}) of the PV inverter, thus affecting the overall operation of the distribution grid.

With respect to the MITM actions, they intend to violate the legitimate Modbus/TCP communication and alter the Modbus/TCP payloads. A significant assumption is that the attacker is part of the same LAN, thus monitoring and sniffing the Modbus/TCP traffic transmitted within the broadcast domain. The cyberattacker can be part of the targeted LAN by either accessing the network via a mobile computing system or a workstation or by remotely controlling a workstation that can access the LAN. In particular, during the first step of a MITM attack, the cyberattacker is placed between the smart meter and ADMS in order to capture the relevant network packets. To this end, Address Resolution Protocol (ARP) spoofing is used. The attacker broadcasts its Medium Access Control (MAC) address by sending forged ARP messages to the victim in order to associate the malicious MAC address with the legitimate one. For this purpose, `Ettercap` is used. The first stage of Fig. 2 illustrates this step. Thus, the cyberattacker is able to access the payload of the Modbus/TCP packets and identify the appropriate registers including the measurements that will be maliciously replaced. During this step, the cyberattacker has to investigate the underlying devices with respect to what Modbus/TCP function codes and registers are used. The final step refers to the FDI process. This step is implemented by custom `Ettercap` filters that replace the content of a Modbus/TCP register. The second part of Fig. 2 depicts also this process.

V. Proposed Intrusion Detection System

As illustrated in Fig. 3, the proposed IDS consists of four modules: (a) Network Traffic Monitoring Module, (b) Flow Extraction Module, (c) Analysis Engine and (d) Response Module. The first module is responsible for capturing the network traffic data on a periodical basis. For this purpose, `Tshark` is used. Next, the Flow Extraction Module receives the network traffic data and generates network flow statistics. The Analysis Engine undertakes to classify whether a network flow is normal or an FDI cyberattack. For this purpose, the Analysis Engine uses an autoencoder illustrated in Fig. 4. In particular, the autoencoder is composed of two complementary networks called encoder and decoder. Both consist of two layers with 62 and 34 nodes, respectively. In general, the encoder receives high-dimensional input data x and transforms it into a latent low-dimensional representation Z. On the other side, the decoder receives the output of the encoder Z and aims to reconstruct the initial data x'. However, in this paper, the proposed autoencoder is not used as an identity function,

but the training process aims to minimise the reconstruction error $L(x, x')$ between the initial input data x and the final outcome of the decoder x'. The reconstruction error $L(x, x')$ is compared to a threshold T, classifying all the data sample y with $L(y, y') > T$ as anomalies (i.e., FDI attacks). T is estimated in a heuristic manner based on the reconstruction error L related to the training data. Finally, the Response Module undertakes to inform the user about the presence of FDI attacks and generate relevant firewall rules.

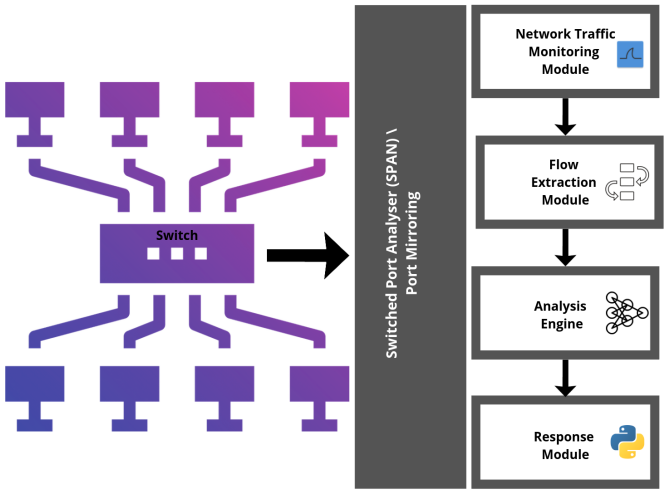

Fig. 3: Architecture of the Proposed IDS

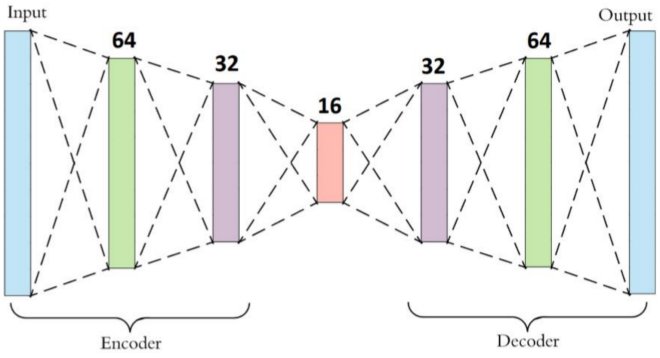

Fig. 4: Architecture of the Porposed Autoencoder

VI. Experimental Results

A. Attack Scenario A – Attack against the Smart Meter Measurements

In the first attack scenario, an FDI cyberattack is performed to alter the load measurements (P_{Load}, $QLoad$). As a result, the ADMS receives false information and the operator is misled about the load consumption of the consumer, leading to mistaken decisions regarding the power factor compensation or the curtailment control scheme, thus affecting the operation of the distribution grid in different ways. The results of this attack are illustrated in Fig. 5.

The execution of the first scenario is separated into two phases, namely (a) the normal operation phases (N1-N4) and (b) the attack phases (A1-A3). The main difference between the phases is that during the normal operation phases (N1-N4), the distribution grid operates under normal conditions without any anomalies. In contrast, during the attack phases (A1-A3), the FDI attacks are executed against the load measurements, thus violating the active and reactive power load. Each attack phase is further explained below.

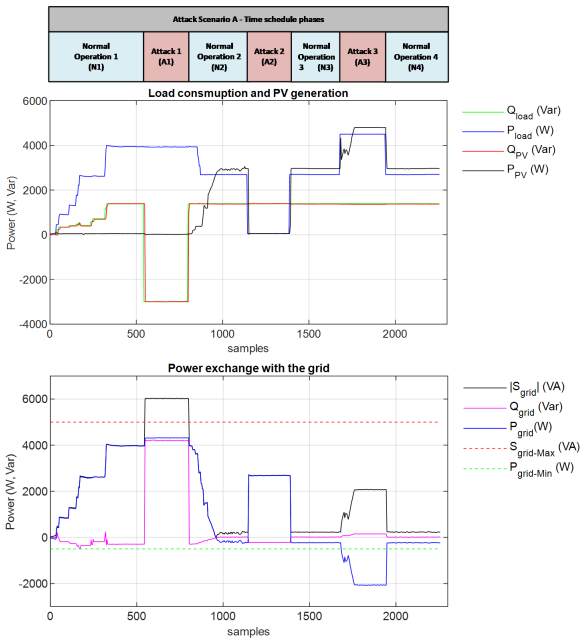

Fig. 5: Experimental Results of Attack Scenario A – Attack against the Smart Meter Measurements

Attack Phase 1 (A1) - $Q_{Load} = -3kVar$: In the first attack phase, the FDI attack alters the Q_{Load} from its actual value to -3 kVar. The power factor compensation controller uses this measurement to control the reactive power injection of the PV inverter in a way to balance the reactive power consumption of the load. As a result, the inverter is violated and injects -3000 Var (inductive) instead of 1380 Var (capacitive). Hence, during this attack, the reactive power exchange with the grid changes from near to 0 Var (during normal operation) to a high value (near to 4200 Var). Such a high reactive power consumption can cause a significant increase in the grid energy losses since it increases the current flow in the distribution lines. Furthermore, a high reactive power exchange with the grid in combination with the high net active power of the grid is able to create overloading conditions for the distribution grid. According to Fig. 5, during this attack, the apparent grid power (S_{grid}) is increased above 6 kVA, which is higher than the nominal power of the feeder (5 kVA). Such conditions can trip the protection relay of the distribution substation, resulting in a regional blackout for the LV distribution grid.

Attack Phase 2 (A2) - $P_{Load} = 50W$: In the second phase, the FDI attack alters the P_{Load} measurement from its actual

value to a close to zero value (i.e., 50 W). As a result, the billing of the consumer can be violated since the overall energy consumption is reduced by the attacker. Furthermore, since the curtailment control scheme limits the active power generation of PVs according to the real-time active power consumption (maximum PV power is equal to 110% of the load consumption) in order to prevent intense reverse power flow conditions, the overall operation of the distribution grid is also affected by this attack. As shown in Fig. 5, while the 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. In addition, the reduction of the PV generation increases the active power of the grid (P_{grid} and S_{grid}), which can potentially lead to overloading conditions under specific circumstances.

Attack Phase 3 (A3) - $P_{Load} = 4500W$: During the last attack phase, the FDI attack modifies the P_{Load} from its actual value to a higher value (i.e., 4500 W). As a result, the billing of the consumer can be violated since the overall energy consumption appears to be increased. Similarly, since the curtailment control scheme limits the active power generation of PVs according to the real-time active power consumption to prevent intense reverse power flow conditions, the overall operation of the distribution grid is also affected by this attack. As shown in Fig. 5, the attack (i.e., an increase of 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 ($P_{grid-Min}$) of the transformer (i.e., -500 W) and can lead to cascading events for the distribution grid.

B. Attack Scenario B – Attack against Control Signals

In the second scenario, an FDI attack is performed to modify the coordination signals sent by the ADMS to the PV inverter (P_{max}, Q_{sp}). This attack aims to damage the overall operation of the distribution grid. Moreover, the active and reactive power injection of a PV inverter can be affected. On the one hand, the attack related to the active power limitation of a PV inverter (P_{max}) can result in the loss of PV generation, increasing the apparent power of the grid. On the other hand, an attack related to the reactive power setpoint of the inverter (Q_{sp}) can vary the reactive power injection, leading to increased grid losses and potentially overloading conditions. The results of Attack Scenario B are demonstrated in Fig. 6.

Similarly to the first case, the second scenario is also separated into two main phases, namely the normal operation phases (N1-N3) and the attack phases (A1-A2). During normal operation phases, the distribution grid operates under normal conditions, while the attack phases (A1-A2) refer to an FDI attack against the active power limit and the reactive power setpoint of the inverter. Each attack phase is further explained below:

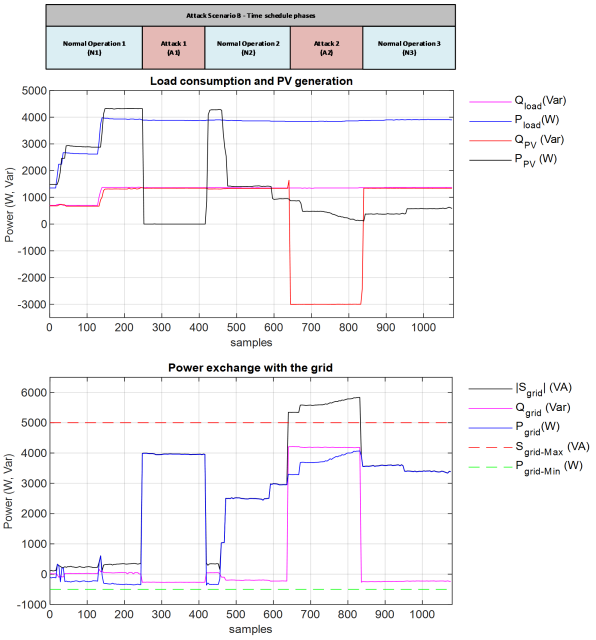

Fig. 6: Experimental Results of Attack Scenario B – Attack against Control Signals

Attack Phase 1 (A1) - $P_{max} = 0$: In this attack phase, the cyberattacker sets the upper active power limit of the PV inverter (P_{max}) to a zero value. As a result, the active power is limited to 0 W. The controller uses the active power to control the reactive power of the PV inverter. Therefore, an intense loss of the PV generation is observed, associated with an intense loss of profit for the prosumer. Furthermore, 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.

Attack Phase 2 (A2) - $Q_{sp} = -3000Var$: 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). Therefore, instead of compensating the reactive power consumption of the load according to the power factor compensation scheme, 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, as shown in Fig. 6. Such overloading conditions can trip the protection relays of the distribution transformer, leading to a regional blackout for the low-voltage distribution grid.

C. FDI Cyberattacks Detection

Before analysing the detection efficiency of the proposed IDS, we need to introduce first the relevant evaluation metrics. True Positives (TP) denotes the number of the correct classification with respect to the presence of the FDI attacks. Similarly, True Negatives (TN) indicates the number of the

correct classification regarding the normal network flows. 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.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

$$TPR = \frac{TP}{TP + FN} \tag{2}$$

$$FPR = \frac{FP}{FP + TN} \tag{3}$$

$$F1 = \frac{2 \times TP}{2 \times TP + FP + FN} \tag{4}$$

Table I summarises the evaluation results of the proposed autoencoder with other five outlier/novelty detection methods: (a) Isolation Forest, (b) Local Outlier Factor (LOF), (c) OneClassSVM, (d) Principal Component Analysis (PCA) and (e) Angle-base Outlier Detection (ABOD). Based on the evaluation results, the proposed autoencoder achieves the best performance where $Accuracy = 0.864$, $TPR = 0.776$, $FPR = 0.356$ and $F1 = 0.855$. On the other side, the worst efficiency is calculated by OneClassSVM where $Accuracy = 0.432$, $TPR = 0.280$, $FPR = 0.312$ and $F1 = 0.382$.

TABLE I: Evaluation Results of the Proposed Autoencoder with other Outlier/Novelty Detection Methods

AI Models	Accuracy	TPR	FPR	F1
Isolation Forest	0.549	0.421	0.217	0.549
LOF	0.502	0.336	0.217	0.458
OneClassSVM	0.432	0.280	0.312	0.382
Autoencoder	**0.864**	**0.776**	**0.356**	**0.855**
PCA	0.487	0.306	0.102	0.453
ABOD	0.534	0.393	0.102	0.549

VII. Conclusions

Although the smart technologies offer valuable services with respect to the typical electrical grid, severe cybersecurity and privacy issues arise due the insecure communication protocols and the presence of new cyberthreats and vulnerabilities. In this paper, we focus on FDI attacks against a low-voltage distribution grid. In particular, two attack scenarios are examined: (a) FDI attack between a smart meter and the ADMS and (b) FDI attack between an inverter and the ADMS. Both scenarios take full advantage of the Modbus/TCP protocol, which does not include any authentication and authorisation mechanisms. Thus, a cyberattacker can access and modify the Modbus/TCP packets. Moreover, a relevant IDS is presented, utilising an autoencoder, which can recognise the FDI-related network flows. The evaluation results demonstrate the efficiency of the proposed IDS.

VIII. Acknowledgement

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

References

[1] 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.

[2] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1851–1877, 2019.

[3] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.

[4] P. Huitsing, R. Chandia, M. Papa, and S. Shenoi, "Attack taxonomies for the modbus protocols," *International Journal of Critical Infrastructure Protection*, vol. 1, pp. 37–44, 2008.

[5] I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras, and P. Sarigiannidis, "A unified deep learning anomaly detection and classification approach for smart grid environments," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1137–1151, 2021.

[6] P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, P.-A. Karypidis, and A. Sarigiannidis, "Diderot: An intrusion detection and prevention system for dnp3-based scada systems," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 2020, pp. 1–8.

[7] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems," *IEEE Access*, vol. 7, pp. 46 595–46 620, 2019.

[8] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.

[9] A. Ghosal and M. Conti, "Key management systems for smart grid advanced metering infrastructure: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2831–2848, 2019.

[10] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart grid metering networks: A survey on security, privacy and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2886–2927, 2019.

[11] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[12] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renewable and Sustainable Energy Reviews*, vol. 57, pp. 302–318, 2016.

[13] P. Diamantoulakis, C. Dalamagkas, P. Radoglou-Grammatikis, P. Sarigiannidis, and G. Karagiannidis, "Game theoretic honeypot deployment in smart grid," *Sensors*, vol. 20, no. 15, p. 4199, 2020.

[14] M. A. Husnoo, A. Anwar, N. Hosseinzadeh, S. N. Islam, A. N. Mahmood, and R. Doss, "False Data Injection Threats in Active Distribution Systems: A Comprehensive Survey," *arXiv:2111.14251 [cs]*, Nov. 2021, arXiv: 2111.14251. [Online]. Available: http://arxiv.org/abs/2111.14251

[15] 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, May 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8887286/

[16] P. Zhuang and H. Liang, "False data injection attacks against state-of-charge estimation of battery energy storage systems in smart distribution networks," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2566–2577, May 2021. [Online]. Available: https://doi.org/10.1109/tsg.2020.3042926