Demonstration of Man in the Middle Attack on a Feeder Power Factor Correction Unit

Lenos Hadjidemetriou, Georgios Tertytchny, Hazem Karbouj,
Charalambos Charalambous and Maria K. Michael
KIOS Research and Innovation Center Of Excellence
Department of Electrical and Computer Engineering
University Of Cyprus, Nicosia, Cyprus
{*hadjidemetriou.lenos, tertytchny.georgios, karbouj.hazem,*
cchara63, mmichael}*@ucy.ac.cy*

Marios Sazos and Michail Maniatakos
Center for Cyber Security
New York University Abu Dhabi
Abu Dhabi, UAE
{*marios.sazos, mm6446*}*@nyu.edu*

***Abstract*—Cyber security of distribution power systems is of an increasing and pressing importance due to the fast modernisation of current systems. Cyber attacks on distribution power systems may aim to operate the system inefficiently, steal private smart meter data or cause intentional false tripping of few or all feeders. In this paper, a Man in The Middle (MiTM) attack on a power factor correction unit is implemented and demonstrated to overload a distribution feeder and cause an intentional false tripping of the entire feeder causing regional blackout. Experimental implementation of the attack is carried out in a laboratory-scale setup using commercial power equipment under different loading conditions to demonstrate the effectiveness of this attack.**

***Index Terms*—Cyber-physical attack, inverters, man in the middle attack, power factor correction, smart grid.**

I. Introduction

Transition of conventional power systems toward smart grids aims to improve reliability, efficiency, resilience and robustness of power grid operation. However, one of the major challenges to smart grid operation is cybersecurity. Recent cyber-attacks on smart grids reveal the risk and the scale of such attacks, such as the cyber-attack against Ukraine's smart grid [1], that lead to 225,000 customers being affected.

Typical smart grid architecture consists of three layers, communication, control and device layer [2]. A critical layer on which attacks might be launched from and affect the operation of smart grid security is the communication layer. Commercially available hardware (i.e., inverters, smart meters, etc.) use Industrial Internet of Things (IIoT) technology, to provide enhanced monitoring and control functionalities, usually through the use of open Internet Protocol (IP) based communication protocols. However, these aspects compromise the communication security and expose smart grids to inherent vulnerabilities and weaknesses of these protocols, allowing space for attacks such as IP spoofing, denial of service attacks, and Man in The Middle (MiTM) attacks [3]. A protocol that is widely used in smart grids is Modbus Transmission Control Protocol (TCP) [4]. Modbus TCP based attacks affecting the operation of smart grid are described in [5], [6].

One of the most common attacks on smart cyber-physical systems is MiTM attack [7], [8] or passive reconnaissance [9], where the attacker interrupts or sniffs the communication between a controller and the field devices or the Supervise Control and Data Acquisition (SCADA) system. MiTM attacks attacks could be deployed either to change the information exchanged at the Modbus TCP communication channel, or, in the passive reconnaissance scenario, to record and read the exchanged messages.

Countermeasures applied in order to secure the communication against such attacks are based on enhancing security features of the actual communication protocols. For instance, the authors in [10] improved Modbus protocol security by changing the packet format representation using encryption and checksum schemes such as SHA-2. Another security solution is the deployment of encrypted protocols for industrial control systems instead of open protocols that makes initiating such attacks a more challenging task. A protocol that is used to replace the traditional Modbus protocol is DNP3 secure authentication [11], designed not just to include encryption but also to enhance cyber security practises against well known intrusion methods. However, in the smart grids framework, there are several examples where these countermeasures have not been applied yet; Hence several smart IIoT enabled equipment (i.e., smart inverters supporting only modbus - Fronious, SMA, etc.) relies only on open protocols.

Significant research work has been carried out on cyber security of transmission power grids due to the powerful impact of cyber attacks on such grids and the possibility of cascading failure in worst case scenario [12]–[14]. However, cyber security of distribution power grids attracted less attention in literature as attacks on such systems do not pose a direct threat to system stability, despite the widespread of these grids and the possibility of targeted attacks against specific critical loads/feeders.

Cyber attacks on distribution power systems may target smart meters, demand side management systems [15], distributed generation control systems, etc. In [16], a false data injection attack (FDIA) is performed on a centralised voltage control system of a distribution system. The aim of the demonstrated attack was to cause an undesirable overvoltage or undervoltage in the distribution system. The authors of

[17] proposed a FDIA against state estimation of the distribution system. Such attacks, if not detected, may result in uneconomical operation of the system, operating the targeted distribution system out of the standard limits, or, tripping the distribution system in worst case scenario. An attack against smart metering infrastructure is proposed in [18] to mislead the Volt-VAr control system of a distribution system, aiming to cause overvoltage or undervoltage conditions in the system. An optimal Volt-VAr optimization system is proposed in [19] with capability of FDIAs mitigation. The authors in [20] proposed a neural network-based approach to detect FDIA on distribution system optimal power flow. The authors of [21], demonstrated several attacks on measurement devices and solar photovoltaic (PV) inverters in a simulation environment.

In this paper, MiTM attack on a reactive power compensation unit is exploited, aiming to overload the targeted feeder and cause an intentional false tripping of the feeder (regional blackout) without having a direct access to the feeder circuit breaker. In contrary to the theoretical studies in the literature, the specific attack is designed and implemented on actual devices in a laboratory-scale setup under two different loading conditions to demonstrate the effectiveness of the attack.

The rest of the paper is organized as follows. The targeted system is presented in Section II. The implemented MiTM attack is described in Section III and demonstrated on an experimental setup in Section IV. Finally, the paper is concluded in Section V.

II. System Description

Reactive power compensation devices are typically installed at feeder point of common coupling (PCC) in order to support the system voltage and reduce reactive power flow between the grid and the feeder. As a result, the energy losses are reduced and the utilization of existing grid capacity can be maximized [22]. Dynamic reactive power compensators such as DSTATCOM [23], have the advantage over fixed capacitors due to DSTATCOM capability of compensating reactive power dynamically, under various feeder loading and operation conditions. Similarly, inverter-interfaced distributed generatoion units, such as solar PV inverters, can play DSTATCOM role [24], due to the multi-functional capabilities of smart inverters [25].

DSTATCOM is operated in one of three control modes, reactive power control mode, voltage control mode and power factor control mode. In the first mode, DSTATCOM supplies/consumes a fixed desired reactive power set by distribution system operator (DSO). In the second mode, voltage control mode, DSTATCOM provide reactive power compensation ($Q_{C_{omp}}$) as a function of PCC voltage magnitude (V), typically with a linear relation between Q_{comp} and PCC voltage, i.e. $Q - V$ droop. In the third mode, power factor control mode, DSTATCOM is controlled to generate/consume reactive power such that a constant power factor is maintained at the feeder PCC. Unity power factor operation is a common control setting that ensures reactive power neutralization of the feeder, where DSTATCOM generate/consume reactive power equal in magnitude of the feeder consummation/generation of reactive power. Power factor control mode is used in this paper, with a unity power factor reference point. The DSTATCOM system is called power factor correction (PFC) unit in this paper as a similar attack can be performed on any inverter-interfaced compensator.

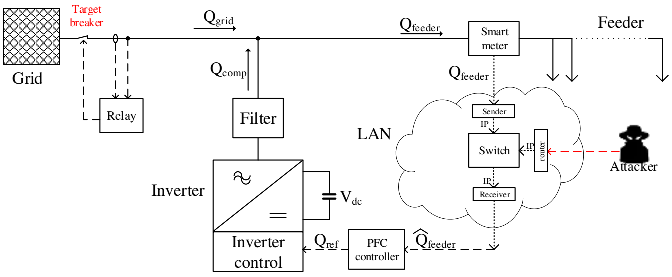

Fig. 1. Single line diagram of the attacked system

Typical power factor correction unit connected to a feeder PCC is shown in Fig. 1. A smart meter is used to measure the feeder reactive power, Q_{feeder}, which is communicated through communication network to the PFC controller. Reactive power reference Q_{ref} command is sent then from PFC controller to the inverter controller. The PFC is developed based on a simple Proportional (P) controller to ensure a unity power factor by compensating the feeder reactive power consumption considering the operational limits of the DSTATCOM inverter. This ensures that the reactive power flow from the grid, $Q_{grid} = Q_{comp} + Q_{feeder}$ approaches zero. The feeder is protected by a circuit breaker to trip the feeder under abnormal conditions such as overloading and short-circuits.

The communication of the measurements and the control set-points is performed through Local Area Network (LAN). Information is transmitted via Modbus TCP protocol, a client-server configuration between the smart meter and the PFC controller and between the PFC controller and the inverter controller. The PFC controller generates set-point commands for regulating the injection reactive power by the inverter. This is achieved through the inverter Modbus interface, where the PFC controller (a) specifies the corresponding Modbus holding register to activate the constant reactive power control mode for the inverter and (b) writes in every control loop the reference value for injecting the set-point reactive power to the corresponding Modbus holding register of the interface [26]. The common 502 port is used for the read and write commands, thus the packets exchanged in the network are reported in plain hexadecimal representation.

III. Implemented Attack

The threat model of this work considers that the attacker is allowed to take control of a workstation, that has direct access and it is located in the LAN of the grid setup. Moreover, an insider attack is considered, where attacker has knowledge of credentials and logins required for that workstation. Thus, the access can be either physically or remotely using Virtual Private Network (VPN) or other tools. Having access, on this

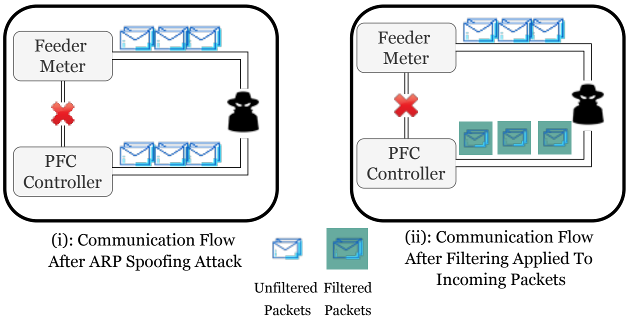
Feeder Meter
PFC Controller
(i): Communication Flow After ARP Spoofing Attack
Feeder Meter
PFC Controller
(ii): Communication Flow After Filtering Applied To Incoming Packets
Unfiltered Packets
Filtered Packets

Fig. 2. Attack Steps Diagram

workstation the attacker is able to scan and identify the IP addresses of the targeting hosts. Moreover, as the adversary will gain access to the LAN, it can perform the MiTM attack using tools like Ettercap, and through the packet analysis to identify the holding registers that are used in the information exchange between the smart meter and the PFC controller. As many of the industrial control systems are deployed with their simple default configurations and settings the attacker can then easily associate the holding register values with the values that are captured during the attack.

The aim of the implemented attack is to create an abnormal operating condition that can trip the feeder without having a cyber or physical access to the feeder circuit breaker. This is done by interfering the feeder reactive power measurement Q_{feeder} transmitted to the PFC controller and replaced by a false value $\hat{Q}_{feeder}$ such that the PFC inverter supplies/consumes reactive power Q_{comp}, which instead of compensating the feeder reactive power, it is actually amplifying the total reactive power. Thus, the PFC reactive power (Qcomp) creates along with the feeder actual load ($S_{feeder} = P_{feeder} + jQ_{feeder}$) an overloading condition of the feeder at PCC, which subsequently leads the feeder breaker to trip the feeder. The procedure of performing this particular attack on the communication layer is described as follows.

In order to perform the attack in the lab setup, two software tools are used, Wireshark [27] and Ettercap [28]. Wireshark is used for the first part of launching the MiTM attack, while Ettercap is a security tool for implementing MiTM in LAN using common Address Resolution Protocol (ARP) spoofing technique. The overall procedure of performing such an attack consists of three steps. In the first step, the aim of the attacker is to perform the ARP spoofing attack so that it can monitor the traffic exchanged between the feeder smart meter and the PFC controller, Fig. 1. As the attacker has access on the LAN, ARP spoofing can be performed, where the attacker sends (spoofed) ARP messages to both hosts, in order to associate MAC address of the target devices to the IP address of the attacker. This causes any traffic meant to be transmitted between sender and receiver to be sent to the attacker instead. In this work, this step is implemented via Ettercap and hence the channel between the smart meter and the PFC controller, is successfully interrupted. Data traffic is recorded by the attacker and passed to the controller without any modification on the actual content of it. The communication flow after the successful implementation of the spoofing attack is shown in Fig. 2(i).

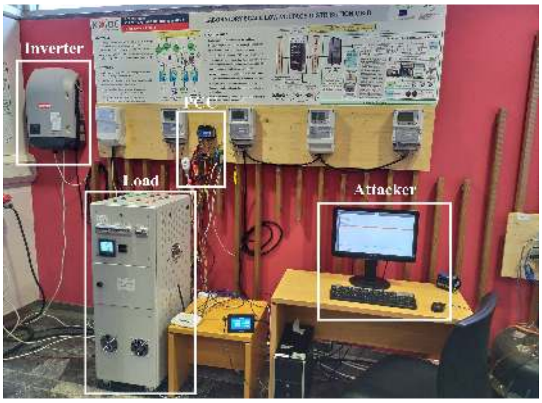

Fig. 3. Experimental Setup

In the second step, communicated packets are recorded and analysed by the attacker in order to derive the targeted measurement, which in this case represents the feeder reactive power Q_{feeder}. A Modbus TCP packet consists of the following fields: Transaction ID, Protocol ID, length, unit identifier, function code and data. Q_{feeder} measurement is part of the data field and thus analysis is focused on this part of the packet. For the specific smart meter used in this demonstration, the Modbus standard register that holds this value is register 7049. The main target of the attacker at this stage is not only to derive the hexadecimal representation of the targeted measurement but also to cover a range of possible values that these registers hold. Packet extraction and analysis for this part of the attack was implemented through Wireshark.

The final step of the attack, after recording and analysing the packets pattern, is to filter the packets generation, in which the packets are captured and manipulated to a specific false value $\hat{Q}_{feeder}$. Filter injection is part of Ettercap tool thus, an `attack.filter` file has been designed and generated by using `if, search, and replace commands` for replacing a range of values of the targeting measurement. By loading the compiled filter in Ettercap, all packets of read commands for Q_{feeder} register will be replaced with the non valid attacked value, $\hat{Q}_{feeder}$. During the attack, and when the filter is loaded to Ettercap, the measurement values are changed and thus, the controller will read interfered values, as shown in Fig. 2(ii).

IV. Results and Discussion

The laboratory scale experimental setup of Fig. 3 is used to demonstrate the implemented attack on a PFC unit. A three phase variable load is used to represent the feeder demand. A commercial 5 kVA three-phase inverter (Fronius Symo 5.0-3-M) is used as a feeder power factor correction unit where the maximum reactive power compensation has been limited to 3 kVAr. Lumel ND10 is used as a feeder smart meter to communicate Q_{feeder} through the laboratory local LAN network. The PFC controller is digitally implemented in a personal computer using a sample time of 2 sec. For the purpose of this

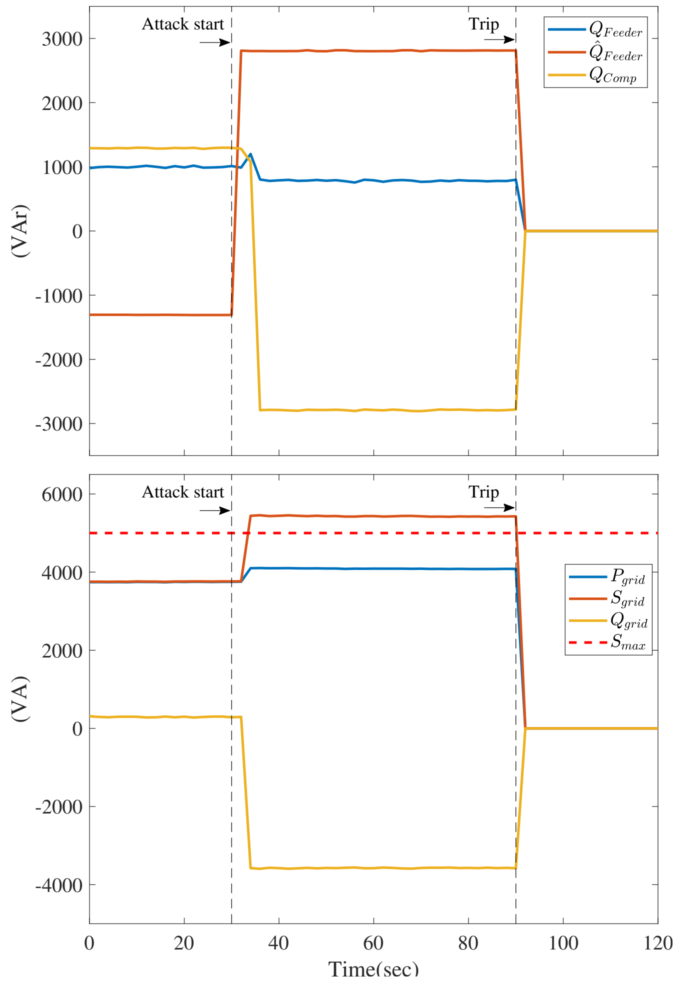

Fig. 4. Case 1: Successful attack

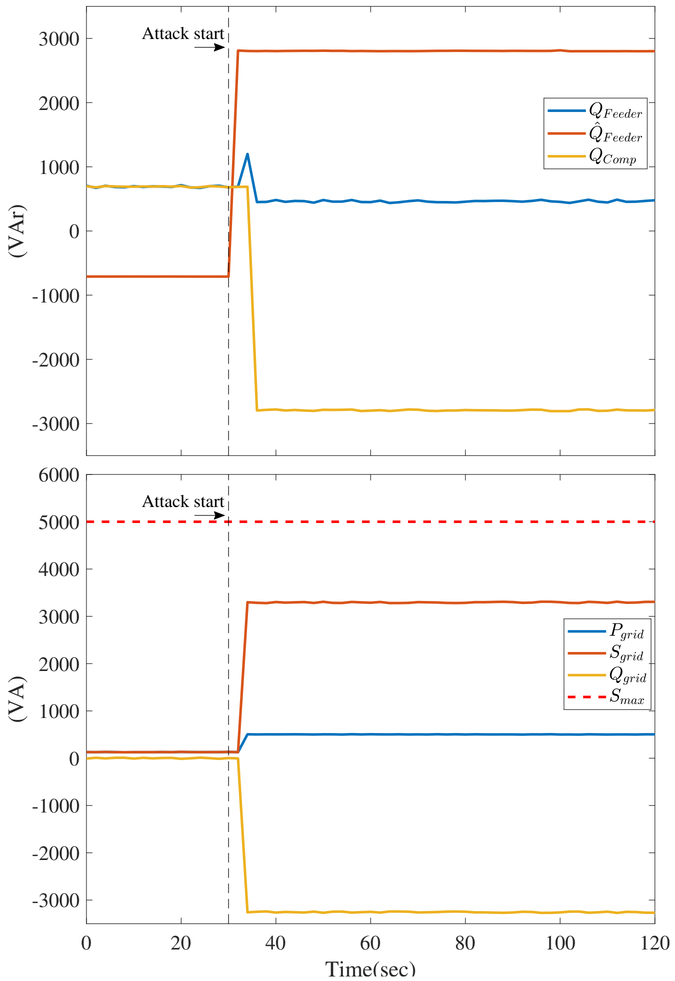

Fig. 5. Case 2: Unsuccessful attack

experiment, the grid power is measured by another three phase smart meter, Janitza UMG 604. The maximum capacity of the feeder is assumed to be 5 kVA. Exceeding this maximum limit for certain time will create overloading conditions that will trip the protection relay and isolate the feeder. It is noteworthy that the feeder circuit breaker in this case is not connected to the communication layer, which is the case in practice. The isolation of circuit breaker from the communication network provides an additional security to avoid direct attacks against the feeder. Two cases of successful and unsuccessful attacks are demonstrated in this section as follows.

A. Case 1: Successful attack

In this case, the feeder is loaded by 75% of maximum feeder capacity (S_{max}) before initiating the attack, as shown in Fig. 4. Moreover, before launching the attack, the reactive power consumed by the feeder, $Q_{feeder} = 1290\,\text{VAr}$, is compensated by the power factor compensation unit Q_{comp}, and the reactive power consumed from the grid, Q_{grid}, is close to zero.

At $t = 30\,\text{sec}$, the implemented attack is launched as explained in Section III. While the actual reactive power consumed by the feeder Q_{feeder} remained almost the same as before initiating the attack, the attacker falsely injected a false measurement reactive power $\hat{Q}_{feeder}$ through the communication network, as shown in Fig. 4. PFC controller responded to compensate the apparent change in reactive power and provided Q_{ref}. The inverter accordingly started consuming reactive power Q_{comp}, which is added to the feeder load.

It can be observed from Fig. 4 following the attack at $t = 30\,\text{sec}$ the apparent power withdrawn by the feeder is higher than the maximum capacity of the feeder S_{max}. Therefore, a tripping signal is initiated at $t = 90\,\text{sec}$, and the entire feeder is tripped. Hence, the attack results in the abnormal amplification (instead of compensation) of the reactive power of the feeder which indirectly causes overloading conditions to the feeder and this leads to a regional blackout of the feeder.

While the presented attack is implemented on a laboratory setup with a single inverter, realistic scenario may deploy a similar attack on multiple inverters in the feeder to create greater impact and increase the risk of taking the feeder out of service.

B. Case 2: Unsuccessful attack

In this case, the feeder is set to be lightly loaded as shown in Fig. 5. The reactive power consumed by the feeder is $Q_{feeder} = 700\,\text{VAr}$, which is compensated accordingly by the inverter before launching the attack at $t = 30\,\text{sec}$. Similarly to the attack performed in Case 1, the measured feeder reactive power is falsely replaced by a false reactive power signal $\hat{Q}_{feeder} = 2800\,\text{VAr}$, which caused the inverter to react by consuming similar amount of reactive power. Therefore, the feeder total apparent power is increased, however, less than the maximum limit of the feeder S_{max} due to the light loading condition of the feeder. Consequently, the feeder does not trip, as $S_{grid} < S_{max}$ and the attack is not successful since the attacked feeder is not overloaded.

It can be observed from Case 1 and Case 2 that two contributing factors can impact the effectiveness of the attack. The first factor is the loading conditions of the feeder, where heavily loaded feeder is more likely to be falsely tripped under this attack. The second factor is the capacity of the attacked PFC unit. A higher capacity of the PFC unit can make the developed attack more effective.

V. Conclusion

In this paper, a man in the middle attack on a feeder power factor correction unit is implemented and demonstrated in a laboratory-scale setup using a commercial inverter. The aim of the attack was to trip the targeted feeder indirectly (causing regional blackout) without having a remote access to the feeder circuit breaker. In the demonstrated attack, the attacker could take the advantage of communicating smart meter measurement through a local area network, interrupt this measurement and inject desired false measurement data instead. The demonstration of this attack on an experimental setup revealed the effectiveness and the damage that this attack may cause.

Defensive mechanisms against the presented attack may include encrypting the measurement communication protocol, strengthening the network security e.g. firewall, communication network segmentation, etc. The presented work, being implemented on a commercial setup, highlights the potential vulnerabilities in the current industrial practice and the importance of implementing such defensive mechanisms.

Future work may include increasing the scalability and impact of this attack and proposing intrusion detection schemes to avoid the false tripping of the feeder.

VI. Acknowledgement

This work is supported by the European Regional Development Fund and the Republic of Cyprus through the Research and Innovation Foundation (Project: INTEGRATED/0916/0035). It is also supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No 739551 (KIOS CoE) and from the Government of the Republic of Cyprus through the Directorate General for European Programmes, Coordination and Development.

References

[1] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," SANS Ind. Cont. Syst., Tech. Rep., 2016.

[2] Q. Zhu and T. Başar, "A hierarchical security architecture for smart grid," in *Smart Grid Communications and Networking*. Cambridge University Press, 2010, pp. 413–440.

[3] F. Aloul, A. Al-Ali, R. Al-Dalky, M. Al-Mardini, and W. El-Hajj, "Smart grid security: Threats, vulnerabilities and solutions," *Int. J. of Smart Grid and Clean Energy*, vol. 1, no. 1, pp. 1–6, 2012.

[4] A. Swales, "Open modbus/tcp specification," *Schneider Electric*, 1999.

[5] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2011.

[6] C. Konstantinou, M. Sazos, and M. Maniatakos, "FLEP-SGS 2: a Flexible and Low-cost Evaluation Platform for Smart Grid Systems Security," in *IEEE ISGT*, Washington, DC, USA, 2019.

[7] Z. Drias, A. Serhrouchni, and O. Vogel, "Taxonomy of attacks on industrial control protocols," in *Int. Conf. on Prot. Eng. (ICPE) and NTDS*, Paris, France, 2015, pp. 1–6.

[8] F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines, and J. Coble, "Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data," *IEEE Trans. Indust. Inform.*, vol. 15, no. 7, pp. 4362–4369, 2019.

[9] H. Sanghvi and M. Dahiya, "Cyber reconnaissance: an alarm before cyber attack," *Int. J. Comp. Applic.*, vol. 63, no. 6, 2013.

[10] I. N. Fovino, A. Carcano, M. Masera, and A. Trombetta, "Design and implementation of a secure modbus protocol," in *Int. conf. critical infrastructure protection*. Springer, 2009, pp. 83–96.

[11] C. Rosborough, C. Gordon, and B. Waldron, "All about eve: Coodparing dnp3 secure authentication with standard security technologies for scada communications," 2019.

[12] C. C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power and Energy magazine*, vol. 10, no. 1, pp. 58–66, 2012.

[13] H.-M. Chung, W.-T. Li *et al.*, "Local cyber-physical attack for masking line outage and topology attack in smart grid," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4577–4588, 2019.

[14] H. Karbouj and S. Maity, "On using TCBR against cyber switching attacks on smart grids," in *IEEE ISGT-Asia*, Melbourne, Australia, 2016, pp. 665–669.

[15] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[16] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi, "Detection of cyber attacks against voltage control in distribution power grids with PVs," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1824–1835, 2016.

[17] R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2871–2881, 2019.

[18] D. Choeum and D.-H. Choi, "OLTC-induced false data injection attack on Volt/VAR optimization in distribution systems," *IEEE Access*, vol. 7, pp. 34 508–34 520, 2019.

[19] A. Majumdar, Y. P. Agalgaonkar, B. C. Pal, and R. Gottschalg, "Centralized Volt–VAR optimization strategy considering malicious attack on distributed energy resources control," *IEEE Trans. Sustain. Energy*, vol. 9, no. 1, pp. 148–156, 2018.

[20] A. Ayad, "Cyber-physical security of power distribution systems," Master's thesis, University of Waterloo, 2019.

[21] A. Teymouri, A. Mehrizi-Sani, and C.-C. Liu, "Cyber security risk assessment of solar PV units with reactive power capability," in *44th Annual Conference of the IEEE Industrial Electronics Society (IECON)*, Washington, DC, USA, 2018, pp. 2872–2877.

[22] A. Charalambous, L. Hadjidemetriou *et al.*, "Phase balancing and reactive power support services for microgrids," *Applied Sciences*, vol. 9, no. 23, p. 5067, 2019.

[23] M. K. Mishra, A. Ghosh, and A. Joshi, "Operation of a DSTATCOM in voltage control mode," *IEEE Trans. Power Deliv.*, vol. 18, no. 1, pp. 258–264, 2003.

[24] S. Mishra and P. K. Ray, "Power quality improvement using photovoltaic fed DSTATCOM based on JAYA optimization," *IEEE Trans. Sustain. Energy*, vol. 7, no. 4, pp. 1672–1680, 2016.

[25] Z. Ali, N. Christofides *et al.*, "Diversifying the role of distributed generation grid-side converters for improving the power quality of distribution networks using advanced control techniques," *IEEE Trans. Indust. App.*, vol. 55, no. 4, pp. 4110–4123, 2019.

[26] [Online]. Available: https://www.fronius.com/downloads/Solar20Energy /Firmware/SE_FW_Fronius_Modbus_Card_Register_DE-EN.pdf

[27] U. Lamping, R. Sharpe, and E. Warnicke, "Wireshark user's guide," 2013.

[28] A. Ornaghi, M. Valleri, E. Escobar, E. Milam, G. Costamagna, and A. Koeppe, "The Ettercap project," 2015.