Demonstration of Man in the Middle Attack on a Commercial Photovoltaic Inverter Providing Ancillary Services

Georgios Tertytchny, Hazem Karbouj, Lenos Hadjidemetriou, Charalampos Charalambous and Maria K. Michael
KIOS Research and Innovation Center Of Excellence
Department of Electrical and Computer Engineering
University Of Cyprus, Nicosia, Cyprus
{tertytchny.georgios, karbouj.hazem, hadjidemetriou.lenos, 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—Rapid modernisation of distribution power systems aims to improve system efficiency and reliability while increasing photovoltaic (PV) penetration levels. However, ensuring the cyber security of such smart distribution grids has emerged as major challenge. Cyber-attacks on key equipment of distribution power systems may lead to inefficient operation of the grid, breach private smart meter data or cause intentional false tripping of feeders. In this paper, a man in the middle attack on a commercial solar PV inverter, which provides ancillary services to the grid, is demonstrated to cause an intentional false tripping of the entire feeder leading to a regional blackout. The successful experimental implementation of the attack reveals the effectiveness and the risk of this attack. Detailed risk analysis is conducted to assess the influence of different factors, such as feeder loading and PV inverter capacity, on the effectiveness of the proposed attack.

Index Terms—Cyber-physical attack, man in the middle attack, solar PV inverter, smart grid.

I. INTRODUCTION

Integration of inverter-interfaced distributed generation (DG), such as solar photovoltaic (PV) inverters, is shaping the future of distribution power systems. Various technical challenges accompany the rapid transition of distribution systems from a consuming to a prosuming (production and consumption) entity, such as, reverse power flow and lack of reactive power reserve. To avoid installing additional infrastructure, solar PV inverters can provide essential ancillary services to mitigate such pressing challenges at high penetration of DG [1], [2].

Ancillary services from solar PV inverters are services provided beyond mandatory grid code requirements aiming to operate distribution power systems in more efficient and stable way. Furthermore, ancillary services from DG are not limited to support distribution systems. Transmission systems can also benefit from such services when proper coordination system and market coordination are in place [3].

To achieve efficient and dynamic operation in an ancillary service system, wider adoption of communication technologies and protocols is required. However, existing commercially available protocols and hardware, can expose a power system to inherent vulnerabilities and weaknesses. A widely used communication protocol, initially implemented for industrial control purposes, is Modbus [4]. Modbus is also widely used by various devices in smart grids, such as inverters and smart meters, to communicate measurements and command signals. The communication is performed in a client/server manner using the Modbus Transmission Control Protocol (TCP). However, Modbus can expose a smart grid to typical examples of cyber attacks such as Internet Protocol (IP) Spoofing, Address Resolution Protocol (ARP) poisoning, Denial of Service (DoS) and Man In The Middle (MiTM) attacks [5]. Possible Modbus TCP based attacks affecting the operation of smart grid are described in [6], [7]. In [8], a cyber attack is demonstrated on a voltage control system aiming to cause voltage limit violation in the distribution system. In [9] a MiTM is demonstrated on a distribution reactive power compensation system by exploiting vulnerabilities in the Modbus protocol which is used to communicate measurement information to the compensation control system. Several attacks on measurement devices and solar PV inverters are demonstrated using a simulation platform in [10]. An optimal Volt-VAr optimisation system is proposed in [11], with capability of False Data Injection Attacks (FDIA) mitigation.

Security countermeasures that aim to provide protection against Modbus TCP-based attacks are focus on the enhancement of its security features. This is done by re-configuring the protocol to enable capturing security mechanisms. For example, as it is proposed by authors in [12], Modbus TCP is improved by changing its packet format representation using encryption and checksum schemes. Such schemes provide the minimum requirements for a secure protocol in terms of integrity, authenticity and non repudiation. Moreover, Modbus TCP-based attacks can be eliminated with the replacement of
such protocols with newer and more secured ones that encapsulate security features such as authentication and encryption by design. An example of such protocol is DNPSec [13]. This protocol enables confidentiality, integrity, and authenticity security features by altering the format of packets in the data link layer and is an extension of the DNP3 protocol, which is not secured by design. Despite these security countermeasures there is a large amount of legacy devices placed in smart grid systems configured with the unsecured Modbus TCP with no security enhancement features. Thus, in this work we focus on demonstrating the attack in such framework where the majority of devices use non secured Modbus TCP protocol for their communication.

This paper demonstrates a MiTM attack on a solar PV inverter that provides ancillary service to a feeder for reactive power compensation and reverse power flow mitigation. The aim of the proposed attack is to affect the operation of the particular feeder and cause a mistripping of the feeder by targeting the measurement system of solar PV inverters. The attack is demonstrated successfully on an experimental setup with a commercial solar PV inverter. The attack risk is further assessed under different solar PV penetration levels in the feeder. The rest of the paper is organised as follows. The targeted system is presented in Section II. The proposed attack is described in Section III. Risk analysis of the proposed attack is presented in Section IV. An experimental demonstration of the proposed attack is presented in Section V. Finally, the paper is concluded in Section VI.

II. SYSTEM DESCRIPTION

The rapid integration of solar PV inverters has resulted in various challenges for reliable and stable operation of distribution power system. These challenges include reverse power flow and lack of voltage control resources. Reverse power flow occurs when the net generated power from the feeder DGs is higher than the feeder net demand. High reverse power flow may result in maloperation of control and protection relays and voltage rise [14], [15]. On the other hand, excessive import/export of reactive power from high voltage network increases system energy losses and affects system voltage quality.

In order to overcome these issues, DGs across distribution feeder, including solar PV inverters, can provide mitigating solutions by utilising the multi-functional capabilities of smart inverters [16]. Fig. 1, shows a representative example of a solar PV inverter, installed at the feeder terminal and providing such services. In Fig. 1, a centralised smart meter, installed at the feeder output (at the substation level), measures the grid active and reactive power ($P_{\text{grid}}, Q_{\text{grid}}$) and communicates these measurements to the ancillary service controller through Modbus TCP. The ancillary service controller is responsible for the provision of ancillary services by coordinating the operation of solar PV inverters installed within the feeder through Modbus TCP as well. For reverse power flow mitigation, the ancillary service controller compares the active power at the feeder ($\hat{P}_{\text{grid}}$) with the generated power from the solar PV inverter ($P_{\text{inv}}$). The controllers acts only when there is a reversed power flow by reducing the maximum generated power ($P_{\text{max}}$) of the inverter to bring the reversed power flow of the grid to 0. On the other hand, for reactive power compensation, the ancillary service controller compares the grid reactive power ($\hat{Q}_{\text{grid}}$) with the reactive power generated by the inverter ($Q_{\text{inv}}$) and coordinates the reactive power command ($Q_{\text{ref}}$) to achieve zero reactive power flow. As a result, it minimises the energy losses. In both ancillary services, a simple proportional P controller is used to generate the reference signals and maintain the proper operation of the distribution feeder. Then, the inverter controller (embedded

![Fig. 1: Single line diagram of the attacked system](image)
within the PV inverter) receives the coordination signals \((P_{\text{max}}\text{ and } Q_{\text{ref}})\) and regulates the inverter to extract maximum power by PV panels without exceeding the \(P_{\text{max}}\) limit. This is also used for injection of reactive power according to reference signal \(Q_{\text{ref}}\). In other words, the ancillary service controller limits the inverter active power \(P_{\text{inv}}\) and controls the inverter reactive power \(Q_{\text{inv}}\) with the objective of minimizing the grid power flow \((P_{\text{grid}}, Q_{\text{grid}})\) through the neutralisation of the feeder power consumption \((P_{\text{feeder}}, Q_{\text{feeder}})\).

The smart meter (sender) and the ancillary service controller (receiver) are located in the same network and communicate using Modbus TCP. The devices share the same subnet mask and communicate by sharing their IP addresses. The communication is performed in constant periods of time where read commands are exchanged between controller and smart meter. The controller sends read requests to the smart meter for reading the values stored in Modbus holding registers regarding the active and reactive power flow measurements \((P_{\text{grid}}\text{ and } Q_{\text{grid}})\). The packets formed for both read commands and replies are in plain text in Modbus.

III. PROPOSED ATTACK

The threat model considered in this work allows the attacker to gain access to a workstation with administrative credentials placed inside the Local Area Network (LAN) of the sender and receiver. Similarly, the attacker could use his own computer as this workstation inside the LAN. Having access to a workstation with access on the LAN, the attacker could install any operating system and tools required to perform the attack. For example, the attacker can install Kali Linux, a Debian-derived Linux distribution designed for penetration testing, which can be used for the successful implementation of various cyber attacks including MiTM. Having access to the network through the workstation the attacker is allowed to identify, scan and monitor the IP addresses of all participants in the network. In this way the attacker obtains IP addresses of its victims for the proposed attack. Scanning and monitoring is feasible through the use of open source software tools, such as Fing [17]. Finally, the attacker can sniff and analyse packets exchanged in the network by using tools like Ettercap [18]. Such analysis is important for the successful implementation of the proposed attack as an important step involves the successful association of the holding registers value with packets exchanged. This allows the attacker to replace the values in the targeting devices by simple following the manual of such legacy devices, which are configured to operate in their default configuration settings as provided by the manufacturer.

The proposed attack aims to overload the feeder operating conditions by manipulating the response of the ancillary service controller to trip the overcurrent protection relay. As a result, a regional blackout occurs without having a remote/direct access to the relay. The proposed attack interferes the communication channel between the smart meter and the ancillary service controller, as shown in Fig. 1, and injects false measurements \((P_{\text{grid}}, Q_{\text{grid}})\) instead of the actual measurements \((P_{\text{grid}}, Q_{\text{grid}})\), respectively. In order to maximise the impact of the attack, the manipulated active power measurement \(P_{\text{grid}}\) is set to a negative value, which indicates a reverse power flow, i.e., excess of active power generation over consumption. The ancillary service controller is expected in this case to keep decreasing \(P_{\text{max}}\) until \(P_{\text{grid}}\) is back to positive. Eventually, \(P_{\text{max}}\) reaches to 0 under the attack. Therefore, the feeder is overloaded with the entire demand with zero active power production by the solar PV inverter. Furthermore, the manipulated reactive power measurement \(Q_{\text{grid}}\) is set to a high capacity value to indicate a sudden increase in reactive power in the feeder. The ancillary service controller in this case is expected to start consuming reactive power \(Q_{\text{inv}}\), which is added to the actual feeder reactive power demand \(Q_{\text{feeder}}\). Hence, the feeder is overloaded at the circuit breaker point (substation level), which in turn leads to overloading conditions and tripping of the feeder.

The procedure of performing the proposed attack on the communication layer is described next.

The overall attack plan is given in subsequent phases that aim to: (i) identify the targeted devices (smart meter and controller) and disrupt their communication by receiving all the traffic exchanged between them (passive MiTM), (ii) record the packets, after successful implementation of the attack (iii) analyse the content of the packets in order to derive the necessary text that will be used for the false data injection, (iv) inject false data to all captured packets of the communication between the smart meter and the controller. Each phase is described below, with emphasis on the tools that are used in each phase.

In the first phase, the attacker considers identifying the targeted devices (sender and receiver) over which the MiTM attack will be performed. Thus, running the Fing tool [17], we can derive a list of the devices that are located in the network. From the extracted list, the IP addresses of the victim devices can be derived. Having the IP addresses of the targeting hosts, the MiTM can be performed by using the ARP (Address Resolution Protocol) spoofing attack. During this spoofing procedure an attacker can advertise its MAC address by sending (spoofed) ARP messages to victim nodes multiple times. This causes any traffic meant to be transmitted between the sender and the receiver to be sent to the attacker instead. This step can be performed through the use of Ettercap
Fig. 3: Risk and impact analysis of the proposed attack tool [18]. Having access to the traffic being exchanged between the smart meter and the ancillary service controller Fig. 2(i) the attacker is able to monitor and analyse all the traffic that is exchanged, completing the second phase of the attack. The monitoring and analysis of the packets can be done through Wireshark [19]. During this analysis the attacker aims to find the useful part of the plain text of the packets which describe the values that are stored in the holding registers for $P_{\text{grid}}$ and $Q_{\text{grid}}$. This is achieved by considering the configuration of the smart meter based on the standard registers used by Modbus. In this step, the attacker aims not only to find the actual values of $P_{\text{grid}}$ and $Q_{\text{grid}}$ but also to derive a range for these values. After completing the third phase of the attack, the attacker is able to perform the false data injection to all the packets captured (phase iv). For this phase, we utilised the widget that is part of Ettercap tool.

False data injection phase is implemented through specific filters. In this case, an attackall.filter file is designed by using if, search, and replace commands that allows the replacement of the two range values for $P_{\text{grid}}$ and $Q_{\text{grid}}$ registers, by a constant falsely value. A single filter for both measurements is generated, that after compilation using the etterfilter compiler is loaded as an .ef file to Ettercap. By loading the compiled filter in Ettercap, all the packets, whose measurement fall in the range of captured values are replaced the false values, $\hat{P}_{\text{grid}}$ and $\hat{Q}_{\text{grid}}$, respectively. By having the compiled filter loaded in Ettercap all the packets, whose measurement fall in the range of captured values are
replaced by the faulty measurements and as a result the controller reads the interfered values for both registers. This is also presented in Fig. 2(ii).

IV. RISK ANALYSIS OF THE PROPOSED ATTACK

In this section, the risk and impact of achieving the goal of the attack, tripping the targeted feeder, is assessed assuming that the communication layer security is compromised and the attacker has gained the access to the local communication network as described in Section III.

As the main aim of the proposed attack is to manipulate the measurements received by the ancillary service controller to overload the feeder leading it to trip. We compute the maximum overloading factor (MOLF) by (1):

\[
MOLF = \frac{\sqrt{(P_{\text{feeder}})^2 + (Q_{\text{feeder}} + Q_{\text{max}})^2}}{S_n}
\]

where \(Q_{\text{max}}\) is the maximum reactive power that can be provided by the solar PV inverter, \(Q_{\text{max}} \leq S_{\text{inv}}\) and \(S_n\) is the rated power capacity of the feeder. A successful attack requires a MOLF higher than 1 in order to cause the tripping of the feeder. The risk increases when MOLF is higher as it is demonstrated in Fig. 3(a). According to Fig. 3(a), the risk of the attack success (visualised through MOLF) increases when the inverter capacity is higher and when the feeder demand consumption \(P_{\text{feeder}}\) and \(Q_{\text{feeder}}\) increases.

The impact of this attack is to cause overloading conditions and trip the feeder. To evaluate this impact, the formulated MOLF is translate to a tangible factor (tripping time) through the inverse time tripping characteristic of the feeder over-current relay, as shown in Fig. 4. Therefore, the tripping time is calculated for every point of the risk surface as shown in Fig. 3(b), demonstrating how many seconds are required to cause regional blackout under any operating conditions and under any inverter rating power. Three cross sections of the tripping surface are presented in Fig. 3(c)-(e). It can be observed from Fig. 3(b) that the feeder can be tripped instantaneously by the attacker if the solar PV inverter has sufficient capacity under feeder high reactive power demand, while the attacker may not be able to perform a successful attack at low reactive demand and low penetration of solar PV. Moreover, it can be observed from Figs. 3(c)-(e) that the feeder active power demand has less impact on the attack compared to the feeder reactive power demand as the solar PV inverter is capable to generate and consume reactive power. This can be aligned with the feeder reactive power consumption while in case of active power the inverter is only capable to limit its active power generation.

V. RESULTS AND DISCUSSION

A laboratory-scale experimental setup shown in Fig. 5 for the system described in Fig 1, is used to demonstrate the effectiveness of the proposed attack. The experimental setup consists of a solar emulator to emulate the behaviour of solar PV panel, a commercial three phase solar PV inverter (Fronius Symo 5.0-3-M) with rated 5 kVA capacity, a three phase resistive and inductive load bank that mimics feeder demand, and a smart meter connected to the laboratory LAN. A personal computer, connected to the same LAN, is used to lunch the proposed attack. The ancillary service controller is digitally implemented in a common personal computer using a sample time of 5 s. The rated capacity of the feeder is assumed to be 5kVA. If the demand exceeds this threshold for certain time, the breaker (associated with the over-current protection relay) will trip causing a regional blackout for the feeder.

Fig. 6 shows the experimental results of the proposed attack. Before initiating the attack, the load is set to 4 kVA, i.e. 80% of maximum feeder capacity (\(S_{\text{max}}\)). Prior launching the attack, the inverter works in MPPT mode with a total active power (\(P_{\text{inv}}\)) close to 2870 W, which brings the active power consumed from the grid \(P_{\text{grid}}\) to approximately 980 W. The reactive power consumed by the feeder is compensated by solar PV inverter \(Q_{\text{inv}}\), and the reactive power consumed from the grid, \(Q_{\text{grid}}\), is close to zero.

The proposed attack is lunched at \(t = 30\) sec. It can be observed from Fig. 6 that while active and reactive power consumed by the feeder did not change compared to the state before initiating the attack, the attacker was able to inject
a false measurement for active and reactive power $\hat{P}_{\text{feeder}}$, $\hat{Q}_{\text{feeder}}$ through the communication network. $\hat{P}_{\text{feeder}}$ is set to a negative value to indicate a false reverse power flow condition and $\hat{Q}_{\text{feeder}}$ is set to a capacitive value to indicate a false over compensation downstream the feeder. The ancillary service controller responded to these false measurements by setting the maximum active power generated by the inverter $P_{\text{max}}$ to 0, hence not generating any active power, and by consuming more reactive power in order to counter the feeder capacitive reactive power which is added to the actual feeder demand $Q_{\text{feeder}}$. This had an amplification effect as the power consumed by the inverter and feeder aligned in the same direction and the power at the grid point exceeded the rated power $S_{\text{max}}$, which eventually resulted in achieving the attack goal and tripping the feeder at $t = 90\text{sec}$ (60 seconds after launching the attack).

VI. CONCLUSION

In this paper a man in the middle attack is proposed and demonstrated on a commercial solar PV inverter that provides ancillary services to the grid. The attack lead to a mis-operation of the ancillary services controller leading to overloading conditions which trip the feeder breaker and cause a regional blackout without having a cyber access to the actual breaker. Risk analysis of the proposed attack revealed that feeders with high reactive power production and consumption are less immune against the proposed attack compared to unity power factor loading condition of the feeder. This is due to higher reactive power loading of the feeder before launching the attack, and therefore, tighter loading margin of the feeder which gives the attacker the opportunity to overload the feeder with less available inverter capacity. Moreover, the risk analysis revealed that the effectiveness of the attack increases significantly when higher solar PV inverter capacity is involved in the attack.

VII. ACKNOWLEDGEMENT

This work is funded by the European Union’s Horizon 2020 research and innovation programme under grant agreement No 739551 (KIOS CoE) and from the Republic of Cyprus through the Directorate General for European Programmes, Coordination and Development.

REFERENCES

[1] A. Cagnano, F. Torelli, F. Alfonzetti, and E. De Tuglie, “Can pv plants provide a reactive power ancillary service? a treat offered by an on-line controller,” Renewable Energy, vol. 36, no. 3, pp. 1047–1052, 2011.
[2] K. Heussen, D. E. M. Bondy, J. Hu, O. Gehrke, and L. H. Hansen, “A clearinghouse concept for distribution-level flexibility services,” in IEEE PES ISGT Europe 2013, 2013, pp. 1–5.
[3] G. De Zotti, S. A. P. Kani, J. M. Morales, H. Madsen, and N. K. Poulsen, “A control-based method to meet tso and dso ancillary services needs by flexible end-users,” IEEE Trans. Power Sys., 2019.
[4] A. Swales et al., “Open modbus/tcp specification,” Schneider Electric, 1999.
[5] 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.
[6] 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.

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

[8] 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.

[9] L. Hadjidemetriou, G. Tertychny *et al.*, “Demonstration of man in the middle attack on a feeder power factor correction unit,” in *IEEE Innovative Smart Grid Technologies-Europe (ISGT-Europe)*, The Hague, The Netherlands, 2020, pp. 1–5.

[10] 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.

[11] A. Majumdar, Y. P. Agulgaonkar, 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.

[12] 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.

[13] M. Majdalawieh, F. Parisi-Presicce, and D. Wijesekera, “Dnpsec: Distributed network protocol version 3 (dnp3) security framework,” in *Advances in Computer, Information, and Systems Sciences, and Engineering*. Springer, 2007, pp. 227–234.

[14] G. De Carne, G. Buticchi, Z. Zou, and M. Liserre, “Reverse power flow control in a st-fed distribution grid,” *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3811–3819, 2017.

[15] K. I. Jennett, C. D. Booth, F. Coffele, and A. J. Roscoe, “Investigation of the sympathetic tripping problem in power systems with large penetrations of distributed generation,” *IET Generation, Transmission & Distribution*, vol. 9, no. 4, pp. 379–385, 2014.

[16] Z. Ali, N. Christofides, L. Hadjidemetriou, and E. Kyriakides, “Diversifying the role of distributed generation grid-side converters for improving the power quality of distribution networks using advanced control techniques,” *IEEE Trans. Ind. Appl.*, vol. 55, no. 4, pp. 4110–4123, 2019.

[17] [Online]. Available: https://www.fing.com/products/fing-desktop

[18] A. Ornaghi, M. Valleri, E. Escobar, E. Milam, G. Costamagna, and A. Koepp, “The Ettercap project,” 2015.

[19] U. Lamping, R. Sharpe, and E. Warnicke, “Wireshark user’s guide,” 2013.