Demonstration of Synchronization Attacks on Distributed and Cooperative Control in Microgrids

Mingxiao Ma, Abdelkader Lahmadi, Isabelle Chrisment
Université de Lorraine, CNRS, Inria, Loria, F-54000 Nancy, France
Email: {firstname.lastname}@loria.fr

***Abstract*—Microgrid platforms are experiencing an increasing integration of distributed and cooperative control coupled with communication links to guarantee safe and reliable operations of their distributed power generators (DG). However, they are subject to several threats and attacks because of the widely use of communication networks in their control layers. In this demo paper, we demonstrate the practical feasibility and the impact of a novel attack, named measurement as reference attack (MaR), on the distributed control mechanism of a microgrid, where an attacker replaces the reference values with measurements during its synchronization operations. We build in this work a hardware platform modelled after a simplified microgrid with DG units based on Raspberry Pi and Arduino boards, DC motors for power generation and light bulbs as electrical loads. We study two variations of the MaR attack using man-in-the-middle (MITM) and malware techniques to demonstrate and validate its impact on the microgrid synchronization and its voltage stability which affect end user's electrical devices.**

I. Introduction

Modern power distribution systems relying on microgrids will have an increasingly high integration of distributed power generators (DG). A microgrid is a cluster of DG units that coordinates the inter-connected DGs by interfacing them through power electronic devices such as the voltage sourced inverter (VSI) [1]. To ensure safe and reliable operations of microgrids, a hierarchical control structure using supervisory control and data acquisition (SCADA) systems is applied [2] to collect data from remote facilities and send back control instructions to those facilities. In these systems, communication networks play an important role to transmit data between their distributed controllers and generators [3].

However, using communication networks at the different control layers of microgrids introduces challenges regarding their security where they become targets of cyber attacks. The well-known power blackout caused by the malware *BlackEnergy* in Ukraine during 2015 has proved that cyber attacks could cause a major blackout. Thus, it is of great importance to study potential vulnerabilities and attacks of these systems and design mitigation or detection schemes against the high-risk threats [4]. In a previous work [5], we have designed a novel attack, named Measurement as Reference attack (MaR), where an attacker is able to affect the voltage stability of the microgrid by replacing the reference voltage values with the measurement value while they are exchanged between distributed and cooperative controllers. In the previous work, we have only studied its impact through theoretical analysis and Matlab based simulations. In this paper, we demonstrate the practical feasibility and the impact of the MaR attack using a hardware platform modeled after a simplified microgrid.

978-3-903176-15-7

II. Attack Model and Experimental Setup

In our previous work [5], we proposed a distributed and cooperative control structure for a microgrid system. Specifically, we use quadratic droop control as the primary control layer and cooperative control as the secondary control layer. Simulation results have proved that this design is more realistic and reliable than traditional control schemes as proposed in [4] and [6]. In this work, and for experimental reasons, we simplify the microgrid model presented in [5] and build a hardware platform to validate attacks on communication network used by the control layers. As shown in Figure 1, the simplified microgrid consists of N DG units and a sparse communication network.

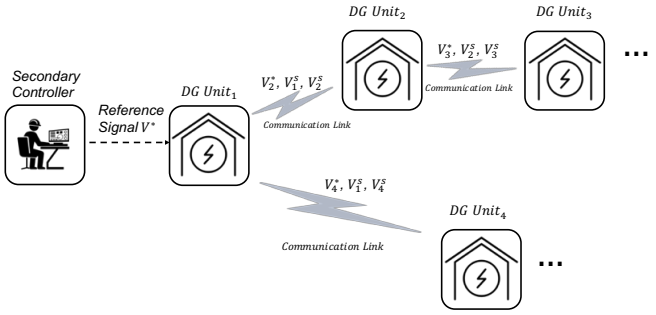

Fig. 1. A microgrid control platform consisting of primary and secondary controllers. Neighbouring DG units can exchange data through sparse communication networks, e.g., transmitting reference signals and voltage measurements (denoted by the superscript s).

In this microgrid platform, we characterize the network topology by a directed graph (digraph) $\mathcal{G} = (\mathcal{V}, \mathcal{E}, A_G)$ with a nonempty finite set of N nodes $\mathcal{V} = \{v_1, v_2, \ldots, v_N\}$, a set of edges $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$, and the associated adjacency matrix A_G. Specifically, DG units and their corresponding communication links are considered as the nodes and edges of the communication graph. As shown in Figure 1, only one leader node (DG Unit$_1$) gets access to the the reference V^* and all other nodes will synchronize their corresponding reference values with the leader node while communicating with their neighbouring nodes.

For each DG Unit$_i$, the required reference value $V_i^*(t)$ and voltage measurement $V_i^s(t)$ are transmitted through the

communications links. As shown in Figure 2, each DG is composed of of Raspberry Pi and Arduino Mega 2560 board acting as the primary controller, two motors A and B acting as a voltage generator, and one light bud acting as an electrical load. The Raspberry Pi is the main control center of the DG unit which sends commands to the Arduino board through USB port to control the voltage generator by using a PI algorithm. The generated voltage will power the light bulb, and its fluctuation affects the level of brightness.

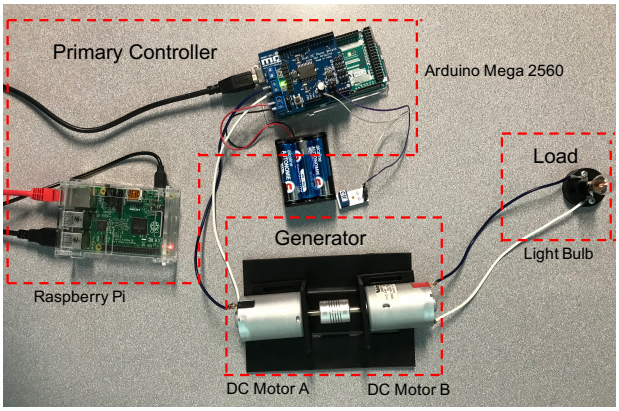

Fig. 2. Each DG unit is composed of one Raspberry Pi, one Arduino board, two motors and one light bulb to demonstrate the effect of voltage instability on the level of brightness.

For the system described in Figure 1 and the experimental setup depicted in Figure 2, we implement our MaR (Measurement as Reference) attack that affects the voltage stability and reference signal synchronization as we studied it theoretically in [5]. We assume that the attacker has knowledge about the distributed and cooperative control structure where it targets the communication links between DG units or the controller station to maliciously replaces the reference signal with the measurement of the previous node. This attack is "naturally stealthy" because usually the reference value and the voltage measurement are close enough and it would be difficult for traditional threshold based detectors to identify malicious data replacement without causing false alarms.

Without loss of generality, the MaR attack targets the communication link between DG units i and $i+1$, where the attacker accesses and manipulates the exchanged data by replacing the reference signal $V^*_{i+1}(t)$ for DG unit $i+1$ with the voltage measurement $V^s_i(t)$ of DG unit i , witten as: $V^*_{i+1}(t) = V^s_i(t)$.

III. MaR attack Demonstration

In this section, we demonstrate two types of attack techniques, man-in-the-middle attack (MITM) and malware, to implement the MaR attack as described in Section II.

A. MaR with a man-in-the-middle attack

In this scenario, we demonstrate the MaR attack when the attacker uses a MITM technique to introduce itself between two communicating DGs neighbours. We assume, in this scenario, that the communications between DGs are not encrypted

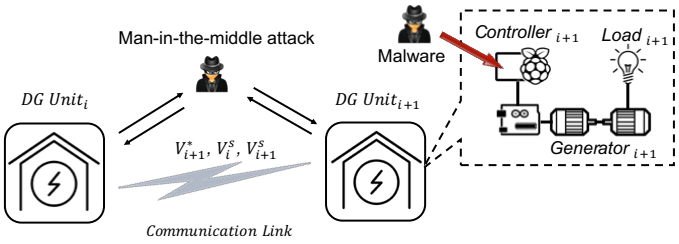

Fig. 3. MaR attack implementations using either MITM or malware techniques.

and using the TCP protocol. As shown in Figure 3, only neighbouring nodes exchange data through the communication link between them. The attacker can introduce itself into a conversation between two DG units and acts as relay/proxy, impersonates both nodes and gets access to the reference and measurements values that the two nodes are sending to each other.

B. MaR with a malware based attack

In the second scenario, we demonstrate the MaR attack by using a malware technique to infect a DG, as shown in Figure 3. In this demonstration, we craft a malware that installs itself on the network hosting the DGs nodes. It scans the network looking for open SSH or Telnet ports on the DGs devices. When it founds an open port on one of them, it uses a dictionary of credentials to brute-force the access to the device. After success, it installs itself and replaces the control program with a new version that replaces the reference value with the measurement. In this scenario, we mainly show the feasibility of the MaR attack by infecting a DG when the communications between DGs are encrypted.

Acknowledgment

This work has been funded by the French Government under grant FUI 23 PACLIDO (Protocoles et Algorithmes Cryptographiques Légers pour l'Internet Des Objets).

References

[1] F. Katiraei, M. R. Iravani, and P. W. Lehn, "Micro-grid autonomous operation during and subsequent to islanding process," *IEEE Transactions on power delivery*, vol. 20, no. 1, pp. 248–257, 2005.

[2] M. E. Khodayar, M. Barati, and M. Shahidehpour, "Integration of high reliability distribution system in microgrid operation," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1997–2006, 2012.

[3] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi, "On detection of cyber attacks against voltage control in distribution power grids," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2014, pp. 842–847.

[4] A. Teixeira, K. Paridari, H. Sandberg, and K. Johansson, "Voltage control for interconnected microgrids under adversarial actions," in *IEEE Emerging Technologies & Factory Automation (ETFA)*, 2015, pp. 1–8.

[5] M. Ma and A. Lahmadi, "On the Impact of Synchronization Attacks on Distributed and Cooperative Control in Microgrid Systems," in *IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids*, Aalborg, Denmark, Oct. 2018. [Online]. Available: https://hal.inria.fr/hal-01870771

[6] M. Ma, A. Teixeira, J. van den Berg, and P. Palensky, "Voltage control in distributed generation under measurement falsification attacks," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 8379–8384, 2017.