



HAL
open science

SDN-based Mitigation of Synchronization Attacks on Distributed and Cooperative Controls in Microgrid

Aurélie Kpoze, Abdelkader Lahmadi, Isabelle Chrisment, Jules Degila

► **To cite this version:**

Aurélie Kpoze, Abdelkader Lahmadi, Isabelle Chrisment, Jules Degila. SDN-based Mitigation of Synchronization Attacks on Distributed and Cooperative Controls in Microgrid. NOMS 2024-2024 IEEE Network Operations and Management Symposium, May 2024, Seoul, France. pp.1-3, 10.1109/NOMS59830.2024.10575853 . hal-04703920

HAL Id: hal-04703920

<https://inria.hal.science/hal-04703920v1>

Submitted on 20 Sep 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

SDN-based Mitigation of Synchronization Attacks on Distributed and Cooperative Controls in Microgrid

Aurélie Kpoze* and Abdelkader Lahmadi† and Isabelle Chrisment† and Jules Degila*

*Université d'Abomey-Calavi, IMSP, Dangbo, Bénin

satou.kpoze@imsp-uac.org, jules.degila@imsp-uac.org

†Université de Lorraine, CNRS, Inria, LORIA, 54000 Nancy, France

abdelkader.lahmadi@loria.fr, isabelle.chrisment@inria.fr

Abstract—The power grid has recently evolved through the integration of Information and Communication Technologies (ICT), leading to the emergence of the smart grid. A key component of the smart grid is the microgrid, a small-scale electrical network made of Distributed Generators (DGs) that nowadays use distributed and cooperative control systems to ensure the reliability of its operations. However, the communication networks employed to control data exchange between DGs are subject to synchronization attacks that can disrupt grid operations. These existing communication infrastructures often lack the flexibility to deploy efficient mitigation and security measures against attacks. Software-Defined Networking (SDN) emerges as a promising solution, providing a dynamic and resilient approach to mitigate synchronization attacks. In this work, we build an SDN-enabled microgrid hardware platform comprising DGs, Open vSwitches (OVs) installed on Raspberry Pi devices, and a POX controller running on a laptop. In the demo, we will show two methods of mitigating Man-in-the-Middle (MitM) attacks to demonstrate the effectiveness of SDN in limiting their impact on the microgrid.

Index Terms—Microgrid, security, SDN, mitigation, MitM attack

I. INTRODUCTION

Smart grid emerged as a solution to meet the growing demand for energy and address the challenges associated with sustainable development goals [1]. Viewed as an evolution from the conventional power grid, the smart grid introduces new paradigms, including the adoption of microgrids. Microgrids are localized energy systems designed to serve a specific geographic area, relying on DGs, control systems, and communication networks for its operations. DGs are power generation sources dispersed throughout the microgrid's localized area. The control systems collect data and send control instructions through a communication network to ensure the microgrid runs reliably.

The communication network, crucial for data exchange between controllers and DGs, can be the target of MitM attacks [2]. In this scenario, an attacker intercepts and potentially modifies the data traffic between DGs. Specifically, our work focuses on a stealthy MitM attack known as "Measurement as Reference" (MaR), outlined in [3]. The attack consists of

substituting the reference signal with the measured data, a manipulation impacting the microgrid's synchronization.

Many new technologies, such as SDN, are under investigation to mitigate the consequences of successful attacks against ICS [4]. SDN's agile response mechanisms, such as network flow reconfiguration, mitigate security risks and ensure the network continues operating without interruption.

In this demo, we show the practical feasibility and the effectiveness of the SDN-based mitigation technique of MaR attack in a distributed cooperative control system with primary and secondary levels of control as described in [3].

II. THREAT MODEL AND EXPERIMENTAL SETUP

The microgrid under study relies on a distributed cooperative control system with primary and secondary control levels as proposed in [3]. The primary controller, a droop controller locally implemented at each DG unit, receives a reference signal through a synchronization process between neighboring nodes and voltage measurements from local meters. The secondary controller employs a centralized control structure to generate the voltage reference signal the primary controller needs in each DG unit [3]. The reference signal is sent to a leader DG unit, which shares this value with the other DGs through the communication network.

The simplified hardware platform built in [3] is extended to integrate SDN networking and OpenFlow switches. As described in [5], each DG unit comprises a Raspberry Pi and an Arduino Mega 2560 board, serving as the primary controller. It also includes two motors functioning as voltage generators and a light bulb acting as an electrical load. The platform consists of four DG units, each linked to an OVS [6], enabling their communication through the switches. As shown in Figure 1, the platform is extended with OVS installed on four Raspberry Pi devices; a POX controller [7] installed on a Linux Ubuntu 20.4 host with an Intel i7 processor and 8 GB of RAM.

We focus on mitigating the MaR attack realized using a MitM technique specified in [3]. The attacker uses the MitM technique to interpose between neighboring communicating DGs. The communications between the DGs are not encrypted

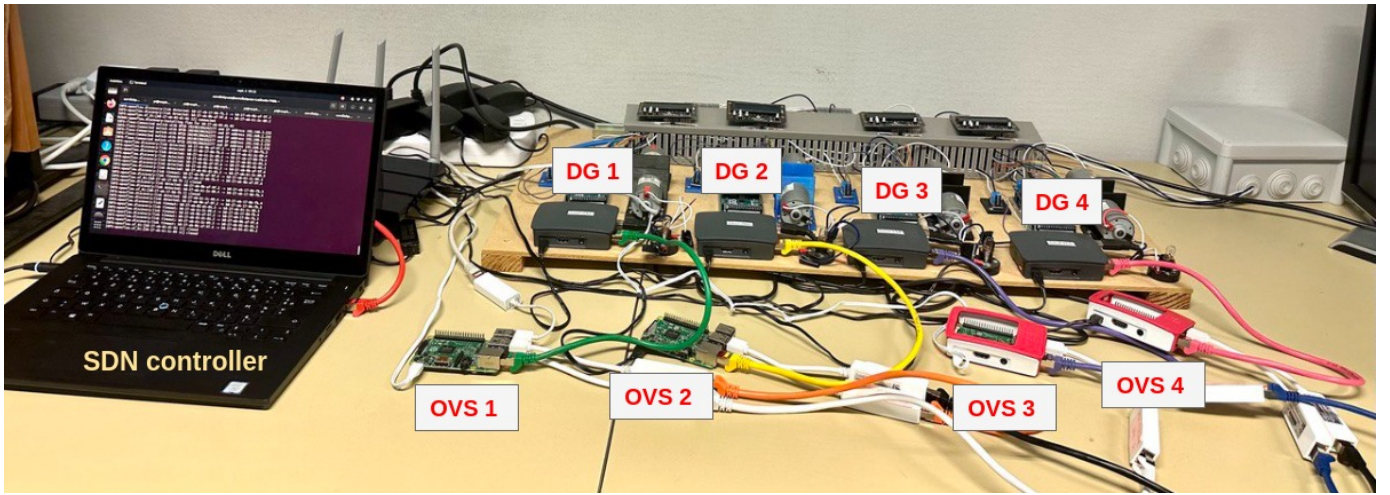


Fig. 1. Our testbed’s experimental configuration comprises the POX Controller (installed on the laptop), OVSs, and the microgrid platform with DG units.

and are based on the TCP protocol. Consequently, the attacker can impersonate both nodes, gaining access to the reference and measurement values the two nodes exchange and substituting the measurement with the reference. We assume the intruder has positioned itself between two OVSs since each DG is connected to one, and the traffic passes through these switches.

The network topology is modeled as an undirected graph $G = (V, E, A_G)$ with a nonempty finite set of N nodes $V = \{v_1, v_2, \dots, v_N\}$ and a set of edges $E \subseteq V \times V$. Each OVS and their corresponding communication links are considered as the nodes and edges of the communication graph. As depicted in Figure 2, the primary DG node (DG 1) acquires the reference voltage value V^* , and all remaining nodes synchronize their respective reference values with the leader node. For every DG Unit i , the necessary reference value $V_i^*(t)$ and voltage measurement $V_i^s(t)$ are transmitted through the communication links. We assume the MaR attack targets only one link at a time, concentrating on disrupting the connections between switches rather than individual nodes. In our scenario, multiple communication links are not compromised simultaneously, ensuring that a path can always be found to reach each DG unit.

III. SDN-BASED MITIGATION OF MAR ATTACK

A. Reconfiguration Process

In the demo, we will show the automated reconfiguration process of the voltage synchronization traffic between OVSs in response to the MaR attack described in section II. Based on the provided link information, the POX controller performs port forwarding by configuring OVSs to direct traffic from specific ports. This process involves the reconfiguration of the flow tables of the switches, allowing traffic to be rerouted through paths other than the compromised link. In the context of the distributed and collaborative microgrid control system, we assume that an existing spanning tree is required for nodes

to reach a consensus at the end of the voltage synchronization process [8]. We consider the OVS connected to the leader DG as the spanning tree’s root node.

Our mitigation process, implemented in the SDN controller, applies a modified version of Kruskal’s algorithm to compute the required spanning tree of the voltage synchronization while excluding the compromised edge. The computed Minimum Spanning Tree (MST) represents a subset of the graph’s edges that connects all nodes with the minimal possible total edge weight, ensuring the absence of cycles. The reconfiguration algorithm initiates with an empty MST and assigns a high weight to the compromised edge, effectively preventing its inclusion in the MST calculation. Additionally, we allocate random weights to all other edges in the graph, assuming other paths have slightly different costs to introduce variability and simulate real-world conditions where factors such as network congestion or traffic fluctuations can cause differences in path costs.

Subsequently, the algorithm proceeds to iteratively select edges with the smallest weights and ensure the absence of cycles during construction. This process ensures the formation of a tree that spans all nodes, including the root node. At this point, we demonstrate two modes of flow installation by the reconfiguration process on the OVSs. In the reactive mode, once the minimum spanning tree is calculated, flows are installed when a *packet-in* event is triggered on the switch, matching predefined criteria for packet processing. In the proactive mode, corresponding flows are installed instantaneously on each OVS. The videos of the demo are available in [9].

B. Reconfiguration time evaluation

We measure the network reconfiguration time for each reactive and proactive approach, which refers to the time between the leader DG issuing the voltage synchronization instruction to the first node and when the final node successfully receives and acknowledges the instruction. We repeat the reconfiguration process many times to evaluate the reconfiguration time

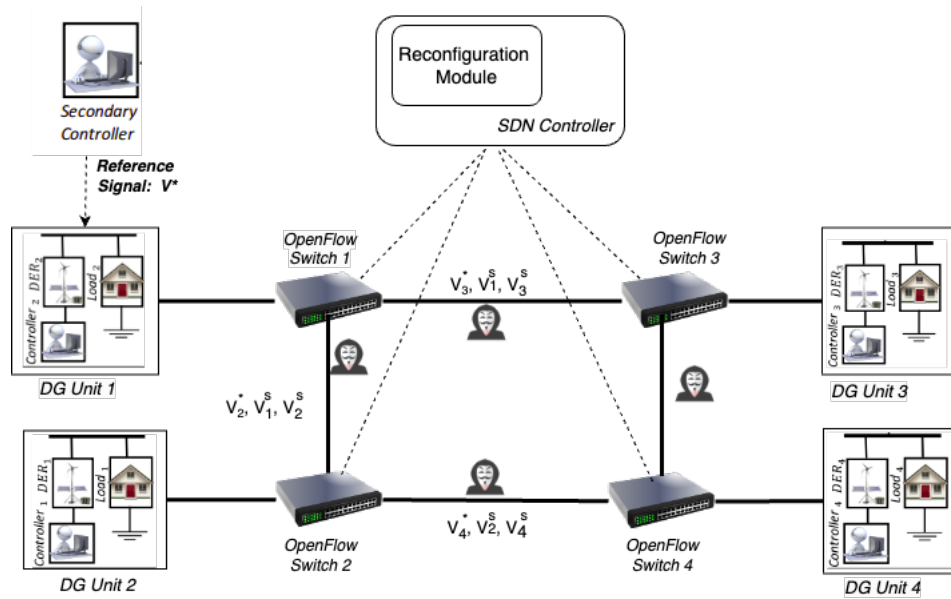


Fig. 2. A microgrid control system with primary and secondary controllers featuring SDN.

in each mode. As illustrated in Figure 3, the reconfiguration time significantly decreases when using the proactive approach compared to the reactive one. The Interquartile range (IQR) of the box plot for the proactive approach is smaller, indicating more consistent reconfiguration times because all flows are installed on the switches prior to the arrival of control packets. On the other hand, in the reactive approach, we have a larger IQR, indicating that the reconfiguration times vary widely due to the installation of flows triggered by specific *packet-in* events. In contrast, in the reactive mode, flows are installed only when necessary. This leads to less frequent flow installations and decreased communication between switches and the controller, which is advantageous for resource usage and scalability.

REFERENCES

- [1] M. I. Khalil, N. Jhanjhi, M. Humayun, S. Sivanesan, M. Masud, and M. S. Hossain, "Hybrid smart grid with sustainable energy efficient resources for smart cities," *sustainable energy technologies and assessments*, vol. 46, p. 101211, 2021.
- [2] P. Wlazlo, A. Sahu, Z. Mao, H. Huang, A. Goulart, K. Davis, and S. Zonouz, "Man-in-the-middle attacks and defense in a power system cyber-physical testbed," *IET Cyber-Physical Systems: Theory & Applications*, vol. 6, no. 3, pp. 164–177, 2021. [Online]. Available: <https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/cps2.12014>
- [3] M. Ma and A. Lahmadi, "On the impact of synchronization attacks on distributed and cooperative control in microgrid systems," in *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2018, pp. 1–6.
- [4] A. F. Murillo Piedrahita, V. Gaur, J. Giraldo, A. Cárdenas, and S. J. Rueda, "Leveraging software-defined networking for incident response in industrial control systems," *IEEE Software*, vol. 35, no. 1, pp. 44–50, 2018.
- [5] M. Ma, A. Lahmadi, and I. Chrisment, "Demonstration of synchronization attacks on distributed and cooperative control in microgrids," in *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, 2019, pp. 727–728.
- [6] "Ovs homepage," <https://www.openvswitch.org/>.
- [7] "Pox homepage," <https://github.com/noxrepo/pox>.
- [8] D. He, D. Shi, and R. Sharma, "Consensus-based distributed cooperative control for microgrid voltage regulation and reactive power sharing," in *IEEE PES Innovative Smart Grid Technologies, Europe*. IEEE, 2014, pp. 1–6.
- [9] A. Kpoze, A. Lahmadi, I. Chrisment, and J. Degila, "Sdn-based reconfiguration reactive and proactive scenarios videos," <https://drive.google.com/drive/folders/1NhtEhvStJsSmL46agOFGTyU11Sdv9Rp?usp=sharing>, 2023.

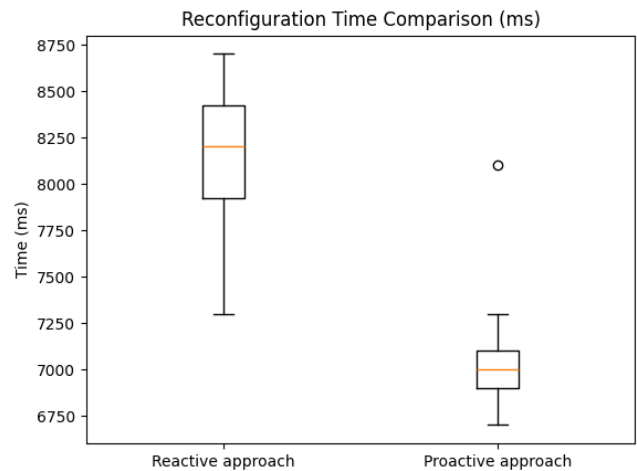


Fig. 3. Reconfiguration time for reactive and proactive scenarios.