# Impact of cyber-attack on coordinated voltage control in low voltage grids

Farooq, Asma; Shahid, Kamal; Gui, Yonghao; Olsen, Rasmus Løvenstein

*Published in:*
IET Renewable Power Generation

*DOI (link to publication from Publisher):*
10.1049/rpg2.12571



*Publication date:*
2022

*Document Version*
Publisher's PDF, also known as Version of record

WILEY

# IET-Wiley Virtual Symposium on Renewable Energy 2022

Digital and flexible control and operation of transmission and distribution grids for renewable power systems.

**September 13 2022**

**Research conducted at institutions in Germany has led to exciting advances in the areas of renewable energy. This free virtual symposium supported by two of the IET's flagship open access journals *IET Renewable Power Generation (RPG)* and *IET Generation, Transmission & Distribution (GTD)* will be free to attend. It will provide a forum for researchers based in Germany to highlight their research and will celebrate the capacity for renewable energy research to engineer a better world.**

**Session Topics Include:**

- Power Flow Control for efficient Transmission Grids
- Digitalization of Power Systems
- Flexibility in Power Systems
- Smart Distribution Grids

**Register free today**

The Institution of Engineering and Technology

Received: 9 November 2021 | Revised: 27 June 2022 | Accepted: 29 July 2022

DOI: 10.1049/rpg2.12571

IET Renewable Power Generation

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

# Impact of cyber-attack on coordinated voltage control in low voltage grids

Asma Farooq[1] | Kamal Shahid[2] | Yonghao Gui[1] | Rasmus Løvenstein Olsen[1]

[1]Department of Electronic Systems, Aalborg University, Aalborg, Denmark

[2]Institute of Electrical, Electronics and Computer Engineering, University of the Punjab, Lahore, Pakistan

**Correspondence**
Asma Farooq, Department of Electronic Systems, Aalborg University, Aalborg, Denmark.
Email: asfa@es.aau.dk

**Funding information**
H2020 Energy, Grant/Award Number: 774145

**Abstract**

Power grid is facing several challenges such as voltage violation, power losses, and power quality issues due to the high integration of renewable energy sources such as solar and wind. One of the several strategies to overcome the voltage violation problem is the provision of reactive power from wind and solar power plants. Local controller of these plants coordinates with the controller to generate the reactive power. The coordinated controller performs its function based on the information obtained from the whole grid via communication network. Communication network infrastructure has high responsibility to ensure secure and stable services in order to provide reliable voltage control in distribution grids (DGs). Unstable or insecure communication networks can lead to several problems in the power system, such as increased power losses and in worse case blackouts. Therefore, this paper analyses the impact of cyber-attacks on the voltage quality control supported by the reactive power generation of PV plants in DGs. Two cyber-attack scenarios are demonstrated via a voltage coordination scenario based on a real distribution grid in Northern Denmark. Simulations are done in a Simulink model of Thy Mors Energi Grid, Denmark. A cyber control block is implemented within the coordinated controller in order to mitigate the effect of cyber-attack. Experimental results show that it is possible to detect and mitigate a cyber-attack such as denial of service and integrity attack before sending a control signal thus contributing towards a secure, stable, and resilient power grid.

## 1 | INTRODUCTION

Increased penetration of renewable energy sources (RES) in power grid and utilization of communication networks raises fundamental security challenges in terms of confidentiality, integrity, and availability, especially when the power grid is an essential part of a critical infrastructure [1]. Currently, around 3800 MW [2] of the wind power (WP) in Denmark is coming from onshore wind turbines, while the photovoltaic (PV) production of around 240 MW mainly consists of dispersed residential small units [3]. According to [4] the anticipated trend is that the increased share of installed renewable energy in Denmark will mainly be accomplished by integrating large concentrations of off-shore WP plants in the transmission system, onshore WPplant in the distribution system and large scale concentrated PV plants. This foreseen high penetration of such intermittent power sources, that is, wind and solar-based power sources into the Danish electricity supply will cause several problems, as discussed in [4] and [5]. These problems include grid congestion, power losses, voltage violations, low generation reserve and other issues that may lead to the degradation of the grid.

One of the solutions to address such issues is the provision of reactive power support from wind and solar power sources [6]. The provision of reactive power support from these power sources in the distribution grid will make it possible to down regulate the entire voltage profile in the distribution system and keep the voltage within the limits at the given nodes [4]. Thus, with the increasing number of such intermittent sources into the power grid, there is a strong need for coordination among the dispersed units in providing reactive power support and hence controlling voltage locally on a distribution grid. The

provision of reactive power support from wind and solar power plants and hence controlling voltage locally on a distribution grid imposes high responsibility on the ICT infrastructure. The authors of [7] present a bibliographic review on communication systems in distributed generation (DG) systems. The study identifies various communication technologies, standards, and protocols used in AC and DC-based DGs. Moreover, [7] contains the classification of different frameworks and methods involved. The methodology of different approaches and their likely combination are discussed for different types of communication networks. [7] also represents useful information for readers, thereby demonstrate the complete life-cycle of digital data in sensors/actuators, transmitter, receiver, filter, decoder for control of DG elements and identifies future challenges as well. While in [5], the authors have illustrated the use of the existing public network communication infrastructure and demonstrated the impact of imperfections in communication networks on the online voltage control coordination functionalities for wind and solar power plants in distributed grids. Similarly, the authors in [8] demonstrate the impact of cyber-attacks on online voltage control coordination from wind and solar power plants in a distribution grid scenario. The authors in [8] have evaluated various aspects related to the possible cyber-attack scenarios that may result in deviating voltage control performance in the distribution grid.

As described in [8], vulnerabilities associated with the use of communication networks may be exploited for financial or political motivation to delay, block, alter process related information (with fraudulent information) or even direct cyber-attacks against power generation plants, thereby preventing the control units from obtaining production metrics. All such cases will not only affect the integrity, confidentiality or availability of the ICT system [9] but can degrade the performance of the power system, which in worst case can lead to blackout. It is therefore, of the utmost importance to define strategies to cope with such risks, as failures in it could be catastrophic. Examples of such catastrophes include (1) the North American blackout of 2003. This was a 4-day event that triggered by a relatively small failure, which ended up costing the United States between $4 and $10 billion [10]. (2) the South Australian massive blackout of September 2016 [11], where a cascading failure impacted the entire state's power grid and affected close to 1.7 million residents. (3) December 2015 Ukrainian blackout being the first confirmed case of power loss directly attributed to the increasing incidence of cyber-attacks [12].

## 1.1 | State of the art

As an extension of the work presented in [5] and [8], this paper illustrates the impact of cyber-attack in terms of time-varying delays in communication and manipulation of the control messages caused by cyber-attacks on the system's performance. Since both the power distribution as well as communication networks are natural components of the critical infrastructure, security of power systems employing communication networks for control purposes has been addressed in several papers. For instance, authors in [13] present an OPNET based network model that is subjected to various Denial of Service (DoS) attacks to demonstrate cyber security aspect of an IEC-61850 based digital substations. The attack scenarios exhibit significant increases in the system delay and the prevention of messages from being transmitted within an acceptable time frame leading to malfunction of the devices such as unresponsiveness of IEDs, which could eventually lead to catastrophic scenarios under different fault conditions.

Authors of [14] propose an improvement in the estimation accuracy of an infected water cooling system in a combined cycle power plant system. This improvement is achieved by using an Interacting multiple model (IMM)-based fusion approach to consider the instant and time-varying nonlinear dynamics. At the local level, the IMM structure is supported by the subobserver-based estimation approach, which further computes the time-delay and cross-covariance between measurements to enhance the observability of the system. As a result, the proposed scheme is able to provide immunity to the system against the injected attacks. Similarly, the paper [15] proposes a multi-sensor track-level fusion-based model prediction in order to address the issue of injecting false synchrophasor measurements. The demonstration is based on a mature wide-area monitoring application that detects electromechanical oscillations by using Kalman-like particle filter (KLPF)-based smoother to extract the initial correlation information about attacked oscillation parameters. Performance evaluations in [15] are conducted using different data-injection scenarios in the IEEE New England 39 Bus system. Furthermore, [16] considers several cases of severe data-injections with high probabilities of information loss and proposes a Bayesian-based approximated filter to achieve an accurate supervision at each monitoring node using a distributed architecture. The performance of the proposed technique has been demonstrated in a mature synchrophasor application known as the oscillation detection. Two test cases have been generated to examine the immunity of the proposed estimation scheme in New Zealand and Oman power grids. The tests were conducted in the presence of harsh data-injection attacks and multiple system disturbances.

Authors in [17] present a survey of advances and state-of-the-art on smart grid cyber security by focusing on the entire grid instead of specific components. In [18], the authors analyze end-to-end security of the communication between DSO substation and distributed energy resources (DERs) over heterogeneous networks through TLS encryption and authentication in compliance with IEC 62351-3. Reference [19] describes an approach to use standardized technologies to provide secure communications for ancillary services with minimal configuration by administrators of corporate networks. Several organizations are involved with the development of security requirements for smart grids. For instance, Institute of Electrical and Electronics Engineering (IEEE), North American Electrical Reliability Corporation – Critical Infrastructure Protection (NERC CIP), International Society of Automation (ISA), National Infrastructure Protection Plan (NIPP), and National Institute of Standards and Technology (NIST) [20].

The authors in [19] also discuss the problems of integrating legacy devices. However, the authors in [19] do not focus on the voltage control coordination in particular considering the high penetration of wind and solar power plants in the power grid. Reference [9] focuses on medium voltage grids characterized by a high-level penetration of wind and solar power plants and examines the risks associated to the communication malfunctions of an ICT architecture implementing the voltage control function. Reference [9] is mainly based on the studies related to the Italian medium voltage grid without actually showing the impact of ICT malfunctioning on the grid implementation and voltages due to cyber-attacks. Whereas, in this paper the results are based on a Danish low voltage (LV) distribution grid, located in the Northern Denmark as a benchmark model to show the impact of cyber-attacks in terms of communication loss and manipulation of control commands. The benchmark power grid is present in a small town that consists of a secondary substation with a mixture of small industry, farms, supermarkets and households. It consists of 90 three-phase residential consumers supplied from a MV/LV power transformers via distribution boxes. 5 out of the 90 consumers of the LV network possess a three-phase PV system that can generate electricity and which, if it exceeds the local consumption, will be injected into the grid. Accordingly, those consumers would become electricity producers. It should be noted that each PV system is an in-house unit, connected to the main grid through the same smart meter as its associated residential consumer.

### 1.2 | Scope and purpose

Based on the coordinated voltage control algorithm implemented in [6] on the mentioned benchmark grid, this paper analyses the impact of cyber-attacks on the coordination of voltage control in the same low voltage distribution grid. As discussed in Section 1.1, several research methodologies have been proposed to concentrate on the protection of smart energy systems and networks from various attacks; however, these protection schemes are unable to guarantee proper security all the time. Consequently, the classification of cyber securities, cyber system's vulnerabilities identification, and the analysis of the system response to the attacks are highly crucial. To diagnose the vulnerabilities of the smart grid, several cyber assessment methods are proposed in the context of different subsystems [13]. These studies help to understand the attack scenarios and system response and thus provide the required information for designing cyber detection/protection systems [21]. Similarly, there is a emergent need to analyze existing threats in smart substation that involves data-fusion and signal processing of these devices providing measurements [13]. This also includes their effects on the operation, which defines the scope of this work.

The main contribution of this paper is to analyze Denial of Service (DoS) and Integrity attack on coordinated voltage controller of an LV grid located in northern Denmark. These attack scenarios are discussed in Section 2. The impact of these attacks on coordinated voltage control is then further demonstrated in 4.

The remainder of this paper is organized as follows: Section 2 explains the communication and cyber-attacks scenarios in low voltage distribution grids. Section 3 describes the problem formulation of our work and the implementation of cyber control block within coordinated controller. Furthermore, test cases for these cyber-attacks are explained in Section 4. Sections 5 and 6 show the simulation results, conclusion and future work, respectively.

## 2 | COMMUNICATION AND CYBER-ATTACK SCENARIOS IN LV GRID

The control of RES at remote geographical locations has urged the development of communication system in distributed power generation systems. Principally, the communication system is comprised of a communication infrastructure, communication network, and communication technologies. All these components contribute towards the control, monitoring and management of the DG system for a reliable delivery of energy to customers and industry end-users [7]. Different RES-based distributed generation can use different communication standards based on requirements, applications, as well as the available resources. As an example, the IEC61850-7-410 is a communication standard considered for monitoring and control using different logical nodes classes and data objects [7]. Several communication standards with their utilization and applications are summarized in [7]. According to [7], communication standards IEC 61850-7-410/420/500/510 cover communication for monitoring, control and logical nodes. Communication standards IEC 61850-90-1/2/3/4/5/6/7/8/9/10 look into communication between control centers, substations, object models etc. Communication standards IEC 61400-25-1/2/3/4/5/6 consider wind turbine and applications of information models, mapping, node/data classes etc. The details of these standards is out of scope of this work.

There are several kinds of cyber-attacks based on the types of adversary. For this work, two types of cyber-attack scenarios have been considered, namely, denial of service attack and integrity attack. Description of these attack scenarios is given in the following sections.

### 2.1 | Denial of service attacks

Integration of communication network infrastructure and other computing systems into the physical electric power grid has led to a real-time, complex heterogeneous environment [22]. In a cyber-attack, services provided by the infrastructure can be made completely unavailable for instance, power outages. Such type of attacks are called Distributed Denial of Service (DDoS) attacks or Denial of Service (DoS) attacks. DoS attackers can easily manipulate certain devices and effectively make them non-functional even if they don't have a full access to the control and communication network [23].

Power grids can be prone to DoS attacks on their communication network infrastructure potentially disrupting crucial

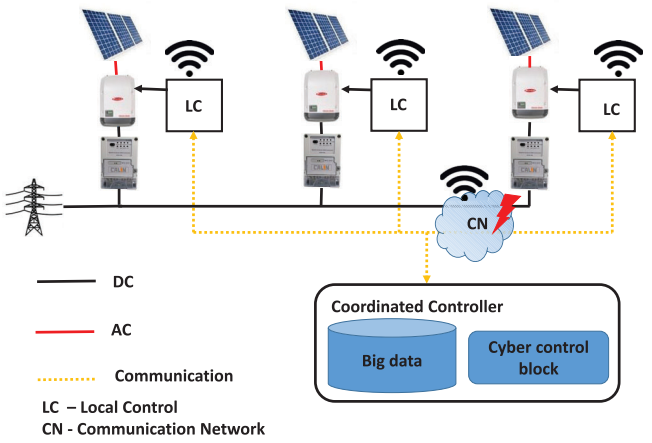



**FIGURE 1** Data flow and coordinated control in low voltage grid

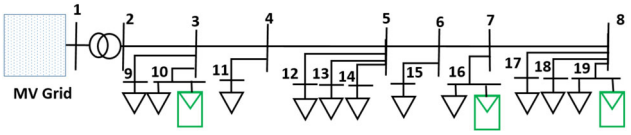



**FIGURE 2** Single line diagram of radial section of the grid

control commands. In such attacks, an attacker aims to flood some critical systems such as VPN entry point by sending useless requests to exhaust the network resources which ultimately suspends the exchange of control signals [24]. For a DDoS attacks, hundreds and thousands of requests per second originate from various sources and send to the target in order to completely shut down the system. Different researches have shown that components and protocols used in power control and communication network, are prone to various types of denial of service attacks [24-26].

For voltage control, local controllers need to coordinate with central or coordinated controller via communication network as shown in Figure 1. Communication networks experience delays, also known as latency, which effects the data processing of voltage controllers. Different studies have shown that these latencies have a diverse effect on the dynamic response of distributed energy resources (DERs) [27, 28]. Attackers exploit this latency effect by maliciously inserting delays into the communication network and thus suspend the exchange of messages carrying out between local controller and coordinated controller or in some cases completely switch off the controller.

## 2.2 | Integrity attacks

An attacker can indirectly influence the power grid even by taking control over a small subset of devices, for example, by manipulating set-points or sending forged commands to control room. Due to this false data injection, operators in control room may draw wrong conclusions and take steps for a non-existent problem [29, 30]. In an integrity attack, attacker maliciously manipulate the control signal in a current control loop so that the set-points send by the controller can differ from the true set-points. Integrity attacks on control signals require the adversary to have an extensive knowledge of the components and operation of the targeted system. SCADA software may able to detect such attacks through a bad data detection algorithm but it depends on the sophistication of the attacks [31]. Attacker can send arbitrary control signals to connected control systems if he has gained full access to the power control network which can disconnect entire power lines from the grid, potentially leading to a complete black out. For example, Ukraine attack in 2015, attacker got control of multiple substations and disconnected almost 225,000 consumers from the grid [32]. Hence, an attacker with enough resources may be able to disrupt and compromise any ICT structure.

According to [9], coordinated voltage control is crucial for the operation of power grids and it includes high level of communication network requirements for its ICT architecture. Therefore, communication between control centers and PV plants or any renewable generation plants is at high risk as compared to other parts of power system.

As discussed in Section 2.1, in voltage control scenarios, local controllers are generally distributed and are highly dependant on the centralized controller. Centralized controller usually send references which are followed by the local controllers. Thus, if an attacker manages to distort or alter the information received by local controller, it may have drastic effects on the output of the system. For this work, the above mentioned cyber-attacks are implemented in our system, which is explained in Section 3.

# 3 | PROBLEM FORMULATION

One of the main challenges in LV distribution grids is to keep the voltage within its specified limits, that is, ± 10% of its nominal value. Normally in Denmark, this is not a huge problem for now, but with the expected amount of electrical vehicles (EVs), heat pumps etc., voltage control is expected to become a challenge. Other countries may already see these issues, for example, Norway [33]. In case of an over-voltage situation, a coordinated control method can be used to update the set-points of local controller in order to bring the voltage back within the bounds. A coordinated controller calculates a correction signal which is reactive power, $Q_{cor}$, and sends this to each local PV inverter through a communication network as shown in Figure 1. In this paper, a cyber control block is introduced within the coordinated controller block with the aim to mitigate any cyber-attack on the droop value of coordinated controller. The selection of this parameter is due to the fact that even a slight change in droop value has a significant impact on the performance of voltage controller.

Figure 2 presents the single-line diagram of a part of the LV distribution grid explained in Section 1 to be used for testing and validation of the cyber-attack scenarios and its solution. The feeder shown in Figure 2 is based on a real Danish grid controlled by a DSO in Denmark named Thy-Mors Energi. It consists of 11 three-phase residential consumers (shown with

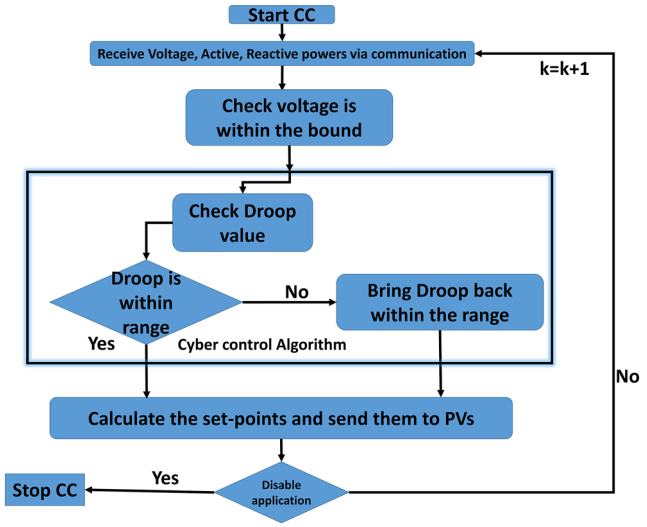



**FIGURE 3** Flowchart of cyber control algorithm

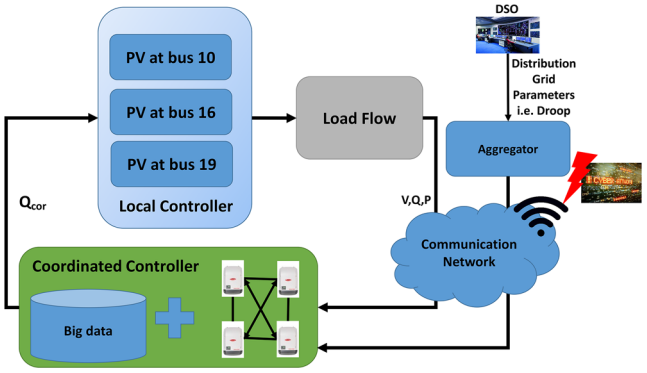



**FIGURE 4** Concept figure of the system including cyber-attack scenario

inverted triangles, labeled as 9, 10, 11, 12, 13, 14, 15, 16, 17, 18 and 19) supplied from a MV/LV power transformer via six distribution boxes labeled 3, 4, 5, 6, 7 and 8. The electric parameters of the constituent equipment of the LV distribution network are given in [34]. Three out of the 11 consumers of the LV network possess a three-phase PV system that can generate electricity and which, if it exceeds the local consumption, will be injected into the grid. Accordingly, those consumers would become electricity producers. The installed power and location of the PV systems are shown in Figure 2. It should be noted that each PV system is an in-house unit, connected to the main grid through the same smart meter as its associated residential consumer. The smart meters, one for each consumer, are not shown in Figure 2. Under normal conditions, voltage along the feeder always remains within the specified bound. Therefore, it was decided to add PVs to the last bus in order to create an over voltage situation, that is, PV systems at junction box 10, 16 and 19 were added where the voltages were highly sensitive to the active and reactive power inputs [6].

Figure 1 represents an adversary model which is studied in this paper. The inputs and outputs of the coordinated controller can be exploited by an adversary with the aim to destabilize the distribution grid. Figure 1 also shows that the connection of all the PV systems to the coordinated controller is through communication network. Therefore, the cyber security risk factor is associated with the use of these communication networks for the coordinated voltage control in low voltage grids as mentioned in Section 2. This scenario is further explained in next subsection with the help of a flow chart.

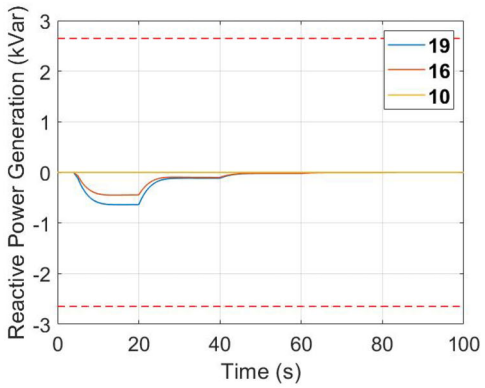
### 3.1 | Flowchart of cyber control algorithm

Figure 3 represents a flowchart of the overall scenario. Coordinated controller receives all the data information for example active power, reactive power and voltage values at each sampling instant denoted by k. The next step is to check whether the voltage is within a specified range. Before inserting cyber control block within the coordinated controller, system would always calculate the correction signal, $\mathcal{Q}_{cor}$, and send it to each PV inverter after checking the voltage bounds. In our scenario, system will always run the cyber control algorithm after the voltage check, in order to check the droop value. If droop value is not within the range, system will bring the value back within the range before calculating the correction signal, $\mathcal{Q}_{cor}$, and then, send it to each PV in order to bring the voltage back within the range in case of over voltage situation. Our algorithm will keep on running for the next time instants, that is, k=k+1 until the voltage values come back within a specified range.

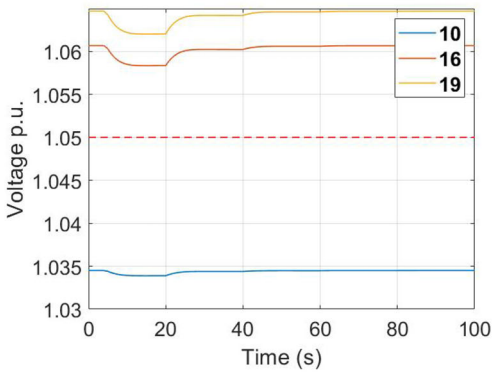
Detailed explanation of coordinated control scenario can be found in [35]. The scope of this study is to focus on the impact of cyber-attack on coordinated voltage control in distribution grids. Thus it was assumed that all the data sent to coordinated controller through a communication network. Since the focus is on cyber-attacks, all other communication characteristics such as packet losses, latencies, and network delays will not be considered in this study.

## 4 | SECURITY ATTACKS ON COORDINATED CONTROLLER IN LV GRID

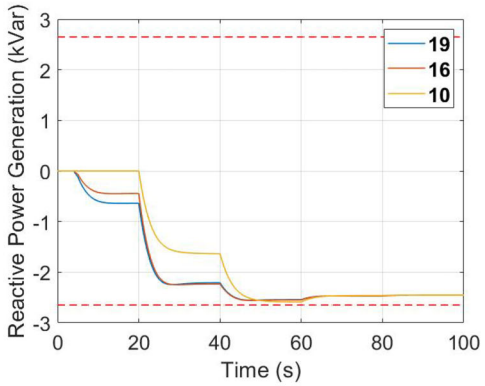
For the purpose of this work, we have considered the attack scenarios mentioned in Section 2 in our coordinated control system to replicate a real cyber-attack. Figure 4 shows the basic data flow in the coordinated control algorithm. Based on the voltage, active power and reactive power values, reactive power corrections are sent to PVs in order to bring back the over voltage. The system starts with an over-voltage situation due to PVs at bus 16 and 19. Before a certain time (i.e. 40s), local controller of PV system at bus 16 and 19 tries to bring back the voltage by generating reactive power. At 40s, coordinated controller starts and sends a correction signal, $\mathcal{Q}_{cor}$, also known as set-points, to the local controller of PV at bus 10. These new set-points make PV at bus 10 to contribute towards generating reactive power and bring the voltage at bus 16 and 19 back within the specified interval. Under normal circumstances, voltage comes back within



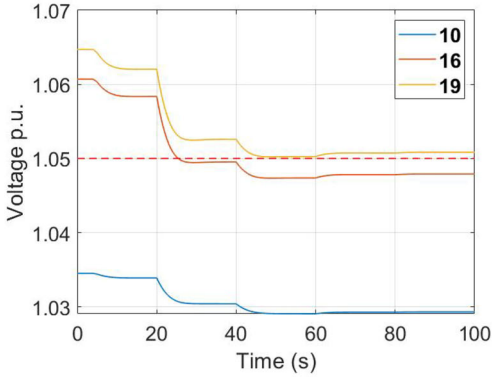

(a) Reactive Power for DDoS attack at the time when controller sends update




(b) Voltages for DDoS attack at the time when controller sends update




(c) Reactive Powers graphs when droop value is manipulated at 60s




(d) Voltages graph when droop value is manipulated at 60s

**FIGURE 5** Simulation Results for case 1 - DDoS attack and case 2 - Integrity attack

the limits after the contribution from the coordinated voltage controller. However, coordinated controller can react differently in case of cyber-attack, which will be analysed in this paper.

Coordinated controller requires information about the current power generation and voltage values from the entire grid in order to calculate set-points. Thus, manipulating this information may have drastic effects on the performance of coordinated controller. This paper considered cyber-attacks on the droop value of the system. Coordinated controller is getting droop information from the aggregator as an input, shown in Figure 4.

$$Droop(R) = Q_{max}/[V_a - V_b], \tag{1}$$

where $Q_{max}$ is initially 0.53 pu and $V_a$= 1.1 pu and $V_b$= 1.05 pu. Explanation of this equation is out of the scope of this work but can be found here [6].

Following are the two test cases considered in this work.

### 4.0.1 | Test case 1 - communication loss due to DoS attack

In this case, attacker manages to completely disconnect the droop value information coming from the aggregator. In real life, such attacks can be easily executed just by flooding the communication network by useless requests and suspend the exchange of messages between the aggregator and coordinated controller. Signals can be jammed if messages transfer is taking place via wireless channels otherwise wired communication can be blocked by cutting cables. Attackers can be bought by the adversary for a minute long attack as a service for as little as $5 [36]. Timing of attack can go even beyond minutes to hours when DDoS attack is done as a service. In this case, this paper analyses the effect of missing information or loss of communication from the grid on the working of coordinated controller.

### 4.0.2 | Test case 2 - manipulation of droop values due to integrity attack

In this case, intruder was able to manipulate the droop value of the system by changing $Q_{max}$ after the start of coordinated controller. As mentioned earlier, coordinated controller starts at 40s and sends set-points to the local controller. At 60s, the value of $Q_{max}$ is changed replicating a cyber-attack. For the purpose of this work, we have set a certain range for $Q_{max}$, that is, 0.53–0.63 pu. Within this range, all the values are acceptable for this algorithm. The reason for the selection of this range

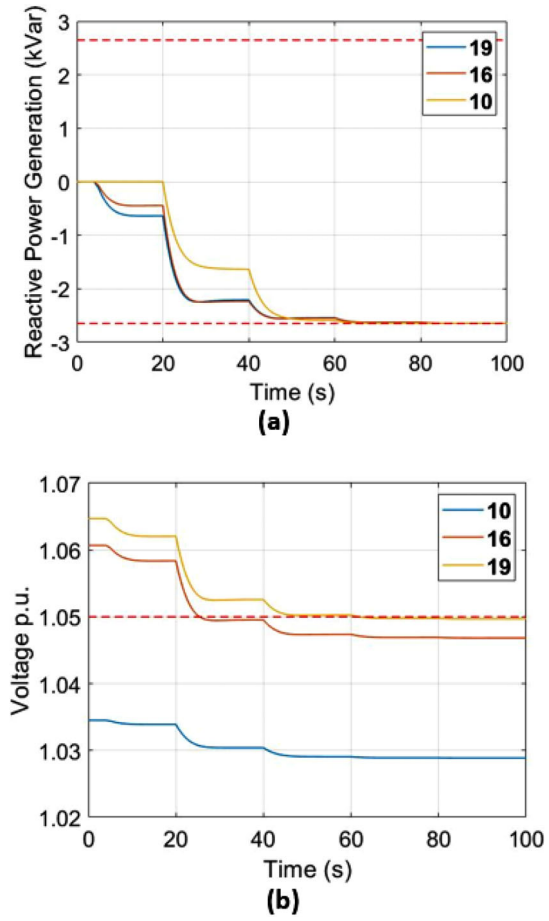



**FIGURE 6** Reactive power and voltage graphs in case of cyber control algorithm

is that, the minimum value of $Q_{max}$ for which voltage comes back within the specified range is 0.53 pu. If we increase this value, this would mean that coordinated controller is generating extra reactive power than the actual need, which is just a waste of resources and it is not desirable. So, we have selected a small range to work with. If attacker manages to change this value to a lower value than 0.53 pu, controller will not be able to bring back the voltages within voltage limits. Attacker can also increase this value to a certain high level. Although voltage would return for higher values of $Q_{max}$, but it would be waste of resources as mentioned earlier.

## 5 | SIMULATION RESULTS

Figure 5 shows the simulation results for the test cases. Figures 5a and 5b show the reactive power generation by PV at bus 10, 16 and 19 and voltages graphs, respectively. Due to loss of the communication, the coordinated control receives no voltage issues then it cannot work precisely. At 60s, reactive power generation graphs become zero showing total communication loss.

Figures 5c and 5d represent the results for the case in which the droop value has been manipulated. After coordinated control starts at 40s, PV at bus 10 starts to contribute in order to bring the voltage of bus 16 and 19 within the limits but at 60s, the droop value deviates from its original one. The voltage starts to go out of bound again and the PVs start to generate capacitive reactive power.

The results in Figure 5 show the impact of cyber-attack on the performance of coordinated voltage control. In first case, coordinated controller does not receive any voltage issue because attacker manages to disconnect the controller. Communication loss between controller and PV plants can lead to voltage fluctuations. In case of over voltage situation, controller will not react due to this loss of communication and voltage will remain out of bound for a longer period of time which is not desirable. In second case, droop value has been manipulated by the attacker which made the voltages at bus 16 and 19 to go out of the bound because coordinated controller calculated its set points based on a wrong droop value. Attacker manages to dodge the controller and thus, such attacks can have severe effects on the power grid such as increased power losses, and in worse case, shut down of power grid.

Figure 6 shows the results of both cases with cyber control algorithm. Cyber control algorithm block within the coordinated controller block checks for any loss of communication or droop value change before calculating new set-points. In case of communication loss, it utilizes the previously stored droop value and calculates set-points. If cyber control algorithm detects any change of value, it checks whether the new value is within the specified range. If the new value is within range, it keeps the same value otherwise it uses the previously stored droop value to calculate the set-points and brings the voltage back within the limits.

## 6 | CONCLUSION AND FUTURE WORK

In this paper, a cyber control algorithm within a coordinated controller for PV inverters is presented to not only keep the voltage within a specified limit but also check for any cyber-attacks on the coordinated controller in low voltage distribution grid. Based on the critical infrastructure of power systems, it is necessary to secure the grid against cyber-attacks. Particularly, cyber-attacks can have a diverse effect on the performance of the controller during the control actions taken by the controller. In this paper, we have considered two cyber-attack scenarios. Various other cyber threats should be taken into consideration specially for this voltage control system in order to obtain an ubiquitous power supply. Future work is planned to consider more sophisticated cyber-attacks and their impact on the voltage control algorithms. Furthermore, various smart algorithms to detect these cyber-attacks can be investigated. It is also planned to use machine learning algorithms to detect these kind of attacks in voltage control scenarios in low voltage distribution grids.

### ACKNOWLEDGEMENT

The research leading to these results has received funding from the European Union's Horizon 2020 Research and

Innovation Programme under Grant Agreement No 774145 for the Net2DG Project (www.net2dg.eu)

## CONFLICT OF INTEREST

The authors have declared no conflict of interest.

## ORCID

*Asma Farooq* https://orcid.org/0000-0003-0468-1838

## REFERENCES


1. Suciu, G., Sachian, M.A., Vulpe, A., Vochin, M., Farao, A., Koutroumpouchos, N., et al.: Sealedgrid: Secure and interoperable platform for smart grid applications. Sensors 21(16), 5448 (2021)
2. Energy islands in denmark. https://en.energinet.dk/
3. Overview of the danish power system and res integration. https://www.store-project.eu/documents/target-country-results/en_GB/energy-needs-in-denmark-executive-summary
4. Petersen, L., Iov, F., Hansen, A.D., Altin, M.: Voltage control support and coordination between renewable generation plants in mv distribution systems. In: 15th Wind Integration Workshop: International Workshop on Large-Scale Integration of Wind Power into Power Systems as well as on Transmission Networks for Offshore Wind Power Plants. Energynautics, Darmstadt, Germany (2016)
5. Shahid, K., Petersen, L., Iov, F., Olsen, R.L.: On the impact of using public network communication infrastructure for voltage control coordination in smart grid scenario. In: Smart Grid Inspired Future Technologies, pp. 3–14. Springer, Cham (2017)
6. Gui, Y., Bendtsen, J.D., Stoustrup, J.: Coordinated control of pv inverters in distribution grid using local and centralized control. In: IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society, pp. 1773–1778. IEEE, Piscataway (2020)
7. Rafique, Z., Khalid, H.M., Muyeen, S.M.: Communication systems in distributed generation: A bibliographical review and frameworks. IEEE Access 8, 207226–207239 (2020)
8. Shahid, K., Kidmose, E., Olsen, R.L., Petersen, L., Iov, F.: On the impact of cyberattacks on voltage control coordination by regen plants in smart grids. In: 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 480–485. IEEE, Piscataway (2017)
9. Dondossola, G., Terruggia, R.: Security of communications in voltage control for grids connecting der: impact analysis and anomalous behaviours. In: Cigré Session, pp. 24–29. Conseil International des Grands Re?seaux Electriques, Paris (2014)
10. Final report on the August 14, 2003 blackout in the us and canada: Causes and recommendations. https://www.energy.gov/oe/downloads/blackout-2003-final-report-august-14-2003-blackout-united-states-and-canada-causes-and
11. South australia blackout: Once in 50-year storm lashes state. https://www.smh.com.au/national/south-australia-blackout-once-in-50year-storm-lashes-state-20160928-grqpks.html
12. Cyber-attack against Ukrainian critical infrastructure. https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01
13. Ashraf, S., Shawon, M.H., Khalid, H.M., Muyeen, S.M.: Denial-of-service attack on iec 61850-based substation automation system: A crucial cyber threat towards smart substation pathways. Sensors 21(19), 6415 (2021). https://www.mdpi.com/1424-8220/21/19/6415
14. Khalid, H.M., Muyeen, S.M., Peng, J.C.H.: Cyber-attacks in a looped energy-water nexus: An inoculated sub-observer-based approach. IEEE Syst. J. 14(2), 2054–2065 (2020)
15. Khalid, H.M., Peng, J.C.H.: Immunity toward data-injection attacks using multisensor track fusion-based model prediction. IEEE Trans. Smart Grid 8(2), 697–707 (2017)
16. Khalid, H.M., Peng, J.C.H.: A bayesian algorithm to enhance the resilience of wams applications against cyber attacks. IEEE Trans. Smart Grid 7(4), 2026–2037 (2016)
17. Kotut, L., Wahsheh, L.A.: Survey of cyber security challenges and solutions in smart grids. In: 2016 Cybersecurity Symposium (CYBERSEC), pp. 32–37. IEEE, Piscataway (2016)
18. Terruggia, R., Dondossola, G.: Cyber security analysis of smart grid communications with a network simulator. In: DA-CH Conference on Energy Informatics, pp. 153–164. Springer, Berlin Heidelberg (2015)
19. Krebs, M., Röthlisberger, S., Gysel, P.: Secure communications for ancillary services. In: DA-CH Conference on Energy Informatics, pp. 141–152. Springer, Berlin Heidelberg (2015)
20. Liu, J., Xiao, Y., Li, S., Liang, W., Chen, C.P.: Cyber security and privacy issues in smart grids. IEEE Commun. Surveys Tutorials 14(4), 981–997 (2012)
21. Sun, C.C., Hahn, A., Liu, C.C.: Cyber security of a power grid: State-of-the-art. Int. J. Electr. Power Energy Syst. 99, 45–56 (2018). https://www.sciencedirect.com/science/article/pii/S0142061517328946
22. Kemal, M.S., Aoudi, W., Olsen, R.L., Almgren, M., Schwefel, H.P.: Model-free detection of cyberattacks on voltage control in distribution grids. In: 2019 15th European Dependable Computing Conference (EDCC), pp. 171–176. IEEE, Piscataway (2019)
23. Krause, T., Ernst, R., Klaer, B., Hacker, I., Henze, M.: Cybersecurity in power grids: Challenges and opportunities. arXiv preprint, arXiv:210500013 (2021)
24. Huseinović, A., Mrdović, S., Bicakci, K., Uludag, S.: A survey of denial-of-service attacks and solutions in the smart grid. IEEE Access 8, 177447–177470 (2020)
25. Radoglou.Grammatikis, P., Sarigiannidis, P., Giannoulakis, I., Kafetzakis, E., Panaousis, E.: Attacking iec-60870-5-104 scada systems. In: 2019 IEEE World Congress on Services (SERVICES), vol. 2642, pp. 41–46. IEEE, Piscataway (2019)
26. Jin, D., Nicol, D.M., Yan, G.: An event buffer flooding attack in dnp3 controlled scada systems. In: Proceedings of the 2011 Winter Simulation Conference (WSC), pp. 2614–2626. IEEE, Piscataway (2011)
27. Setiawan, M.A., Shahnia, F., Chandrasena, R.P., Ghosh, A.: Data communication network and its delay effect on the dynamic operation of distributed generation units in a microgrid. In: 2014 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), pp. 1–6. IEEE, Piscataway (2014)
28. Liu, S., Wang, X., Liu, P.X.: Impact of communication delays on secondary frequency control in an islanded microgrid. IEEE Trans. Indust. Electron. 62(4), 2021–2031 (2014)
29. Sridhar, S., Hahn, A., Govindarasu, M.: Cyber–physical system security for the electric power grid. Proc. IEEE 100(1), 210–224 (2011)
30. Hittini, H., Abdrabou, A., Zhang, L.: Fdipp: False data injection prevention protocol for smart grid distribution systems. Sensors 20(3), 679 (2020)
31. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Sec. (TISSEC) 14(1), 1–33 (2011)
32. Case, D.U.: Analysis of the Cyber Attack on the Ukrainian Power Grid. Electricity Information Sharing and Analysis Center (E-ISAC), Washington DC (2016)
33. Electric cars overload the norwegian electricity grid. https://ing.dk/artikel/elbiler-overbelaster-norske-elnet-206330
34. Ciontea, C.I., Iov, F.: A study of load imbalance influence on power quality assessment for distribution networks. Electricity 2, 77–90 (2021)
35. Net2dg deliverable 4. http://www.net2dg.eu/wafx_res/Files/Net2DG_D4.1_27.12.2019_final.pdf
36. Annual ddos threat. https://www.imperva.com/blog/2015-16-ddos-threat-landscape-report/


**How to cite this article:** Farooq, A., Shahid, K., Gui, Y., Olsen, R.L.: Impact of cyber-attack on coordinated voltage control in low voltage grids. IET Renew. Power Gener. 1–8 (2022). https://doi.org/10.1049/rpg2.12571