Volt/VAR Optimization in the Presence of Attacks
A Real-Time Co-Simulation Study

Aftab, Mohd Asim; Chawla, Astha; Vergara, Pedro P.; Ahmed, Shehab; Konstantinou, Charalambos

DOI
10.1109/SmartGridComm57358.2023.10333952

Publication date
2023

Document Version
Final published version

Published in
2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, SmartGridComm 2023 - Proceedings

2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) | 978-1-6654-5556-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/SmartGridComm57358.2023.10333952

Volt/VAR Optimization in the Presence of Attacks: A Real-Time Co-Simulation Study

Mohd Asim Aftab*, **Astha Chawla**†, **Pedro P. Vergara**‡, **Shehab Ahmed***, **Charalambos Konstantinou***
*CEMSE Division, King Abdullah University of Science and Technology (KAUST)
†Siemens, India
‡Intelligent Electrical Power Grids, Delft University of Technology (TU Delft)
E-mail: {mohammad.aftab, shehab.ahmed, charalambos.konstantinou}@kaust.edu.sa,
astha.chawla@siemens.com, p.p.vergarabarrios@tudelft.nl

***Abstract*—Traditionally, Volt/VAR optimization (VVO) is performed in distribution networks through legacy devices such as on-load tap changers (OLTCs), voltage regulators (VRs), and capacitor banks. With the amendment in IEEE 1547 standard, distributed energy resources (DERs) can now provide reactive power support to the grid. For this, renewable energy-based DERs, such as PV, are interfaced with the distribution networks through smart inverters (SIs). Due to the intermittent nature of such resources, VVO transforms into a dynamic problem that requires extensive communication between the VVO controller and devices performing the VVO scheme. This communication, however, can be potentially tampered with by an adversary rendering the VVO ineffective. In this regard, it is important to assess the impact of cyberattacks on the VVO scheme. This paper develops a real-time co-simulation setup to assess the effect of cyberattacks on VVO. The setup consists of a real-time power system simulator, a communication network emulator, and a master controller in a system-in-the-loop (SITL) setup. The DNP3 communication protocol is adopted for the underlying communication infrastructure. The results show that corrupted communication messages can lead to violation of voltage limits, increased number of setpoint updates of VRs, and economic loss.**

***Index Terms*—Volt/VAR optimization (VVO), conservation voltage reduction (CVR), distributed network protocol (DNP3), cybersecurity, co-simulation setup, cyberattacks.**

I. Introduction

Electric power distribution systems currently adopt Volt/VAR optimization (VVO) as a method to increase energy and operational efficiency as well as reduce power losses through voltage control. Specifically, the distribution network experiences a voltage drop as one moves from the substation to the remote feeder end. This problem is typically resolved by employing VVO algorithms in the distribution network to realize voltage regulation as well as loss reduction. VVO can provide setpoints to on-load tap changers (OLTCs), voltage regulators (VRs), and shunted capacitor banks to achieve desired voltage profiles. These components are scheduled to maintain voltage within the specified limits through day-ahead scheduling based on load forecasting. The main objective of VVO is to achieve conservation voltage reduction (CVR). CVR, which has received significant attention in recent literature [1], is a technique at the distribution system operator (DSO) level to deliberately reduce the feeder voltage and maximize energy savings. The voltage is maintained within the lower bounds of ANSI standard C84.1-2011 (0.95-1.05 per unit (p.u.)) [2]. Annual energy savings by implementing CVR are in the range of 0.5% to 4% [3].

In recent years, increased attention towards environment-friendly energy generation led to the penetration of renewable energy resources (RES) in distribution networks. RES-based distributed energy resources (DERs), such as rooftop solar PV, are interfaced with the distribution networks through inverters which are responsible for the DC/AC conversion with a unity power factor. However, the revised IEEE 1547-2018 standard allows DERs to participate in grid support functions such as Volt/VAR and Volt/Watt control [4]. Thus, in modern distribution networks, DERs are paired with smart inverters (SIs) to support relevant functionalities per the recommendation of IEEE 1574-2018 standard.

Due to the intermittent nature of renewable-based DERs, the VVO problem transforms into a dynamic problem in modern distribution networks. Its solution requires coordinated operation among OLTCs, VRs, shunted capacitor banks, and SIs, which are collectively termed VVO actors. The VVO actors extensively communicate with the controller to realize the VVO scheme. Measurements from smart meters and micro-PMUs (phasor measurement units) are acquired and transmitted to the VVO controller to compute optimized setpoints for VVO actors to maintain system voltage. To support this operation, extensive communication is required to achieve VVO in modern distribution networks. As a result, such schemes can be susceptible to cybersecurity effects due to the reliance on information and communication technologies [5]. The potential vulnerability to cyberattacks could lead to power quality issues in distribution networks as well as under/overvoltage conditions and even voltage instability events.

The relevant literature indicates that attacks on the communication infrastructure of energy systems can lead to disastrous consequences [6], [7]. Considering malicious attacks on DERs and their supporting ecosystem [8], several strategies for mitigating the effects on VVO are reported in the literature. In [9], the detection of bad data in critical measurements of PV inverters which can lead to erroneous VVO is reported. For the mitigation of cyberattacks, solutions based on local measurements and historical data are proposed. A tri-level defender-attacker-defender optimization model is proposed in

978-1-6654-5556-5/23/$31.00 ©2023 IEEE

[10] to mitigate cyberattacks against VVO. In [11], the authors present a secure autonomously coordinated VVO scheme in the presence of high DER penetration to avoid grid oscillations and unintended switching operations of voltage regulators. In [12], an adaptive scheme is proposed to mitigate cyberattacks on a number of SIs in the distribution network. The presented technique adjusts the setpoints of non-attacked SIs to maintain system-wide voltage stability.

It is evident that existing literature is primarily focused on mitigating and defending against cyberattacks in distribution networks. However, the research is limited on analyzing such attacks on VVO schemes in real-time co-simulation testbeds and how vulnerabilities in the communication medium can be exploited to launch these attacks. Hence, to fill this gap, this paper develops a real-time co-simulation setup for an advanced distribution management system (ADMS) to assess cyberattack impacts on the VVO scheme. The system-in-the-loop (SITL) setup comprises of real-time power system simulator, a network emulator, and a master controller to emulate a DNP3 client and run the VVO algorithm. The setup allows to test the actual control code, control hardware, and communication infrastructure realistically as they would be utilized in the field, representing an accurate representation of the actual system, and providing insights on the severity assessment of cyberattacks in ADMS.

The paper is organized as follows. Section II presents the formulation of the VVO problem to achieve CVR. Section III explains the development of the real-time co-simulation setup for ADMS and the threat model of cyberattacks on VVO scheme. Finally, Section IV provides the results of the impact assessment, while Section V concludes the paper.

II. VVO Problem Formulation for CVR

The VVO is a multi-objective nonlinear optimization problem aimed at maintaining the distribution network voltage profile. The objectives of VVO considered in this paper are the minimization of distribution network losses and energy savings using CVR. The VVO algorithm is solved using the alternating direction method of multipliers-based scheme (ADMM) [13]. The VVO algorithm computes the updated setpoints for VVO actors. The VVO formulation, in this paper, considers VRs, capacitor banks, and photovoltaic smart inverters (PVSIs). The objective function is formulated as the minimization of Eq. (1):

$$F = Min\left[C_{loss,t_k} + C_{VR,t_k} + C_{CB,t_k} + C_{PVSI,t_k}\right] \quad (1)$$

where F is the objective function, C_{loss,t_k} is the grid loss cost, and C_{VR,t_k}, C_{CB,t_k}, C_{PVSI,t_k} are operating costs of VRs, capacitor banks, and SIs, respectively.

The cost of power loss in the distribution network is computed as the product of the cost of energy and power loss in line resistance as shown below:

$$C_{loss,t_k} = C_E * i_{i,j}^2 r_{i,j} \quad (2)$$

where C_E is the cost of energy, and $i_{i,j}^2 r_{i,j}$ is the power loss between i_{th} and j_{th} node. Considering R as the number of VRs, and B as the number of capacitor banks in the distribution network, the cost of VRs is computed as the product of the cost incurred for VRs operation per step, C_{r,t_k}, and the modulus of change in the number of steps of VRs, ΔX_{VR}, as per Eq. (3). Similarly, the cost of the capacitor banks is computed as per Eq. (4):

$$C_{VR,t_k} = \sum_{i=1}^{R} C_{r,t_k} * |\Delta X_{VR}| \quad (3)$$

$$C_{CB,t_k} = \sum_{i=1}^{B} C_{b,t_k} * |\Delta X_{CB}| \quad (4)$$

In our problem, DERs are represented by PV power plants interfaced with the distribution network through SIs. Consumers with PVSI facilities participate in VVO. The SI is operated in Volt/VAR mode to provide reactive power support to the distribution network. The cost of PVSI operation is computed as the incentives provided to PVSI owners per unit of reactive power supplied, Q_{PVSI}^i, based upon the cost of grid power at that specific time instant, C_{grid,t_k}, as follows:

$$C_{PVSI,t_k} = \sum_{i=1}^{P} C_{grid,t_k} * Q_{PVSI}^i \quad (5)$$

The objective function of Eq. (1) is solved with certain constraints presented in Eqs. (6)-(10). The voltage limits on the feeder must be maintained within limits as specified in [14]. The operational constraint for every i_{th} bus is given as:

$$0.95\ pu \leq V_i \leq 1.05\ pu \quad (6)$$

The VRs in substations are equipped with taps to participate in voltage control. However, they are limited by the tap's operational limits as per Eq. (7):

$$0.9\ pu \leq Tap_{i,VR} \leq 1.1\ pu \quad (7)$$

SIs can contribute to VVO by modulating their reactive power output as a function of voltage measured at the point of common coupling (PCC) [15]. In order to fully utilize their capability of reactive power support, the SIs apparent power rating is designed to be more than the active power rating. In this way, each SI can provide reactive power support even if its active power output is dispatched at maximum value [16]. The PVSI must balance the relation between active and reactive power as per Eq. (8). To follow the industry best practices, the PVSI is limited to delivering 60% of its total rated capacity as per Eqs. (9)-(10).

$$S_{PVSI}^2 = P_{PVSI}^2 + Q_{PVSI}^2 \quad (8)$$

$$Q_{PVSI,t}^i = \beta_{PVSI} * S_{PVSI,t}^i \quad (9)$$

$$0 \leq \beta_{PVSI} \leq 0.6 \quad (10)$$

where S_{PVSI}, P_{PVSI}, and Q_{PVSI} are the apparent, active, and reactive power of SI, respectively.

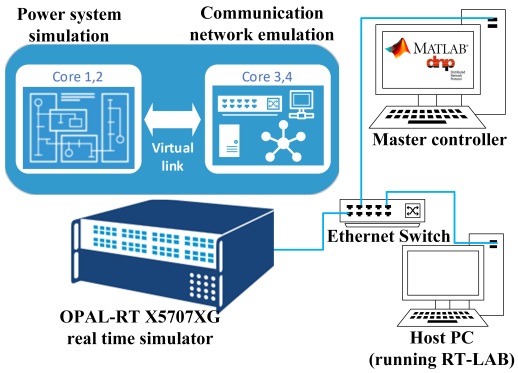

Fig. 1: Overview of the developed advanced distribution management system-in-the-loop (SITL) co-simulation setup.

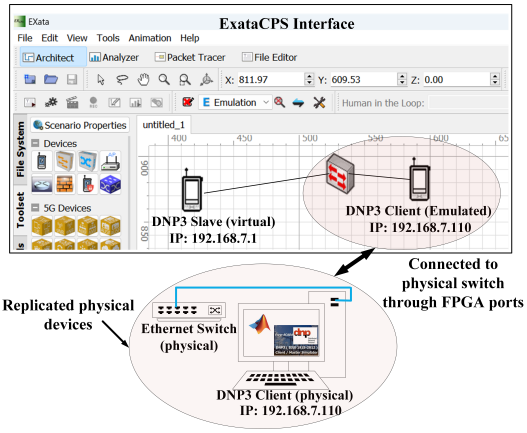

Fig. 2: EXATACPS interface with the master controller.

In addition, the power flow equations for active and reactive power must be satisfied as presented in [17]. For assessing the energy savings through CVR, the loads in the distribution network are modeled using the ZIP load model. This model expresses the correlation between voltage magnitude and power through a polynomial equation that incorporates constant impedance (Z), current (I), and power (P) components. The VVO aims to reduce the grid's loss as well as operational expenses, taking into account network limitations at each quasi real-time phase. The VVO algorithm as in Eq. (1) is executed subject to Eqs. (6)-(10) and setpoints for VRs, CBs and PVSIs are obtained. These setpoints change with the load profile of the feeder and with variations in solar irradiance. The VVO is performed every 15 minutes, and new settings are communicated to the VVO actors to maintain the voltage profile of the feeder and maximize energy savings for the DSO.

III. REAL-TIME CO-SIMULATION SETUP FOR ADMS

The assessment of cyberattacks on ADMS in a real-time setup provides a realistic and controlled environment to evaluate different scenarios, identify vulnerabilities, and validate the effectiveness of security measures. It also ensures the reproducibility of results. For these reasons, a real time co-simulation setup employing both a real time simulator and a network emulator is utilized in this paper.

A. Overview of the Co-Simulation Setup

The real-time co-simulation setup for the ADMS consists of a real-time power system simulator (OPAL-RT OP5707XG), a communication network emulator (EXATACPS), and a master controller for monitoring and control. The setup is implemented over the DNP3 TCP/IP-based protocol, typically employed in distribution networks in North America. DNP3 is a client-server layer 2 communication protocol. It also defines generic data types employed for supervisory control and data applications. An overview of the ADMS SITL setup is shown in Fig. 1. Different components of the setup are explained below.

The distribution network is modeled in a *real-time power system simulator*, the OPAL-RT simulator (OP5707XG), which is an FPGA-based hardware. It can mimic the operation of power systems in real-time, ensuring that all iterations of the model are completed in a prescribed amount of time at each time-step.

A *communication network emulator* is used to replicate the behavior of the communication network with high accuracy. EXATACPS network emulator is employed for modeling the network of the distribution system. EXATACPS runs by reserving one of the FPGA cores on OPAL-RT and interacts with the power system simulation running on RT-LAB through a virtual link as shown in Fig. 1. This is advantageous compared to other communication network emulators, which run in local machines and interact with real-time power system simulators through network interface cards (NICs). In such setups, the simulation time-step of the power system in a dedicated real-time simulator and the communication network emulation in the local machine are different. This issue is resolved by running EXATACPS on one of the cores of OPAL-RT with the exact same time-step.

The *master controller* is a PC running the DNP3 client software and VVO code in MATLAB. The DNP3 client simulator from FREYRSCADA is employed as the DNP3 client software. It sets up a DNP3 master connection through TCP/IP to the DNP3 slave running as a virtual device inside the EXATACPS emulation. The DNP3 analog input messages are saved in `.csv` format within MATLAB. An ADMM-based VVO code is used to run the optimization program and compute new setpoints for VRs and the Volt/VAR curve for the SI [13]. The DNP3 master sends analog output point commands to set the new values in the distribution network simulation through EXATACPS interface. The DNP3 client is an emulated intelligent electronic device (IED) that communicates to a virtual slave inside EXATACPS as shown in Fig. 2.

B. Threat Model and Attack Scenarios

In order to assess the impact of cyberattacks on VVO in the developed setup, the threat model and attack scenarios are described below. The load measurements through smart meters located on nodes of the distribution network are periodically updated and transferred to the VVO controller. The VVO

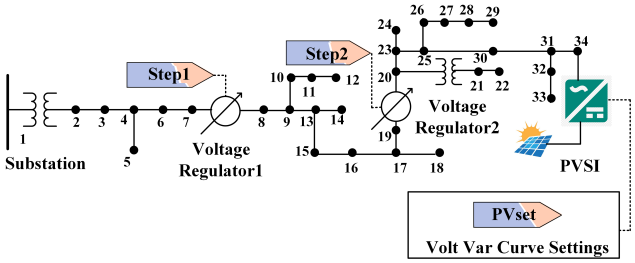

Fig. 3: Schematic representation of modified IEEE 34-bus system.

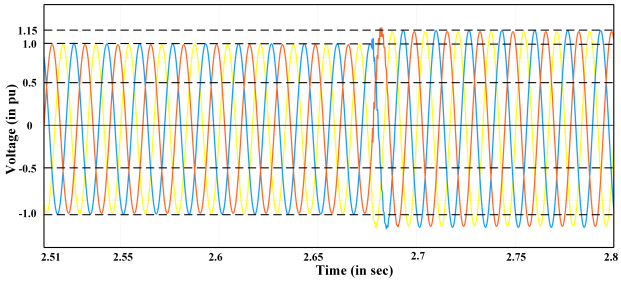

Fig. 4: Voltage variation from 1.0 p.u. to 1.15 p.u. in distribution feeder at node 8 due to the packet modification attack ①.

controller computes new setpoints for voltage control. With the inclusion of DERs through SIs, the DER owners also participate in the VVO scheme. These SIs are connected through public networks of DER owners who are not fully aware of cyber-threats and related potential vulnerabilities. Thus, adversaries can gain access control through DER units and launch cyberattacks. The primary goal of such attackers is to stealthily change the voltage level of the distribution feeder.

In this work, we consider that the cyberattacks on VVO are realized via a data integrity modification [18], [19]. We consider malicious adversaries accessing and replacing real measurements y in the system with fake information $\hat{y}$. This can be modeled as an optimization problem, where the adversary aims to minimize the detection of the attack while maximizing the damage caused, i.e., minimize $[f(\hat{y}) + \lambda \cdot g(\hat{y}, y)]$, where $f(\hat{y})$ represents a cost function that quantifies the damage caused by the attack, and $g(\hat{y}, y)$ represents a measure of the similarity between the tampered measurements $\hat{y}$ and the original measurements y. The parameter λ controls the trade-off between causing damage and avoiding detection. To perform the attack, the adversary manipulates the measurements by adding a perturbation vector d to the real measurements, i.e., $\hat{y} = y + d$. Specifically, we assume that an attacker is able to tamper DNP3 communication messages and modify exchange packets, i.e., *modify packets (MODP)*, on the DNP3 client node. Data packet modification can be performed by adding on the offset, inverting data bits, multiplying each field with a value, replacing bits with random values, or even completely interrupt the communication (i.e., denial-of-service (DoS)). The DNP3 frame has a header and data section and the maximum frame length can be 292 bytes. For launching the MODP attack in EXATACPS, the starting byte, i.e., the byte at which the DNP3 payload begins, needs to be specified so that the attack produces "correct" results.

In our experiments, the *MODP attack is realized under three categories in terms of the considered VVO application* [20]:
① *Tampering VVO setpoints*: The setpoints for VVO actors are communicated through DNP3 direct operate messages. These setpoints can be deliberately tampered via MODP by an attacker. As a result, conditions could arise related to *(i)* under/overvoltage violations in the operating feeder, *(ii)* exceeding operating voltage limits as per the ANSI standard C84.1-2011, and *(iii)* economic loss to the DSO.

② *Tampering smart meter measurements*: In this scenario, tampering with active and reactive power measurements through a smart meter is considered. The primary goal of the attacker is to render the VVO scheme ineffective due to the corrupted measurements. For this, a DoS attack can be launched by an attacker (e.g., cancel via a MODP perturbation vector d the real measurements y, so that $\hat{y}$ is nullified) which can result in the failure of communication infrastructure.
③ *Modifying SI Volt/VAR curve setpoints*: The attacker can modify the Volt/VAR curve of the SI either by changing its slope or by changing the voltage dead band [20]. As a result, unwanted oscillations could arise in the distribution feeder. Under this attack scenario, and in order to maintain the voltage within limits, there can be an increased number of setpoint updates of VR's, leading to economic loss and even sometimes failure of the VVO controller to produce optimized setpoints, and hence rendering VVO ineffective.

IV. Results and Discussion

In order to investigate the impact of cyberattacks on the VVO scheme, the IEEE 34-bus radial system is considered in this paper. The 34-bus system has an operating voltage of 4.16 kV. The system is modified to include VRs between nodes 7-8 and 19-20 as well as a PVSI on node 34, which is one of the optimal locations for DER placement in this benchmark [21]. The SI is implemented through the SI toolbox of OPAL-RT to enable Volt/VAR control. Moreover, the nodes of the feeder are monitored using smart meters which communicate voltages as well as active and reactive power to the master controller through DNP3 messages. The VVO is performed every 15 mins and changes in setpoints are updated. The modified network is modeled in RT-LAB and smart meters communicate through DNP3 slaves to EXATACPS through the OPOUTPUT block of the RT-LAB library. The DNP3 master is a physically emulated IED running on a PC in the SITL setup, as shown in Fig. 1. With the initial measurements, the VVO code computes the setpoints of VRs and the Volt/VAR curve of SI. These are written to the slave through direct operate messages by the master. Finally, the setpoints are received inside the simulation through the OPINPUT block of the RT-LAB library. A schematic representation of the modified 34-bus system with the OPINPUT and OPOUTPUT blocks is shown

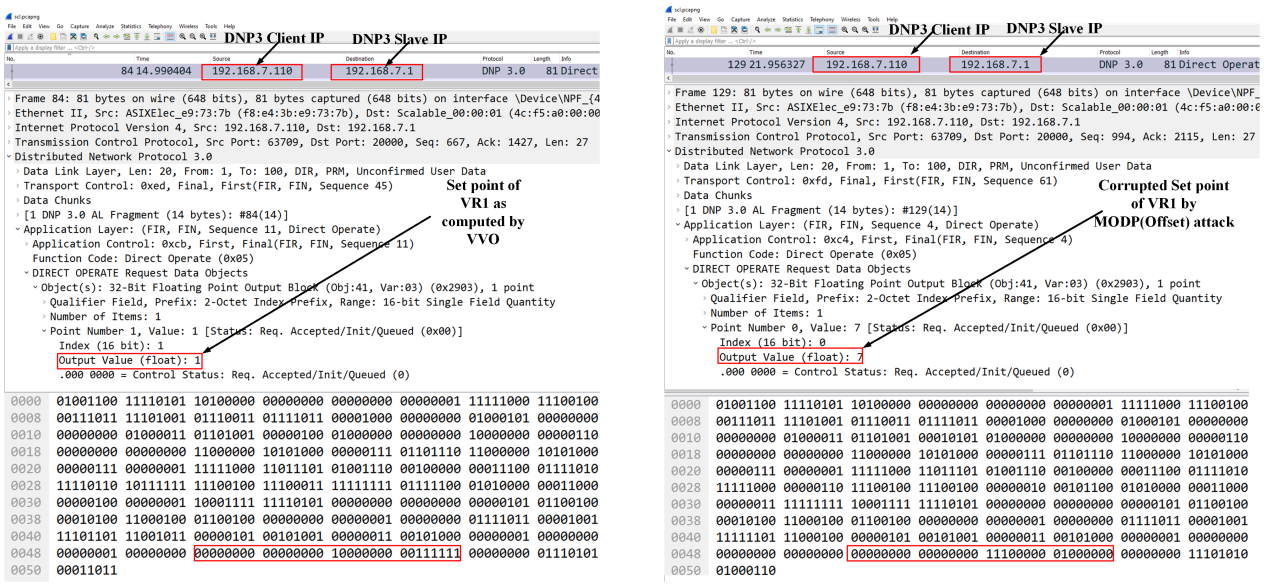

Fig. 5: Wireshark capture of direct operate DNP3 message to set step value in VR1: (a) before, and (b) after, the add offset attack ①.

in Fig. 3. The results of the impact of cyberattacks on the VVO scheme in the developed setup are presented in two parts, one focusing on the analysis affecting the ADMS operation and the second focusing specifically in the effects on the CVR part.

A. *Impact Analysis on ADMS Operation*

To illustrate the impact of attack category ①, we consider tampering the setpoint of VR1 during a load change operation. Let us assume a load change of 25% on a balanced RL load with a capacity of 0.1 MW and 0.6 MVar at node 8 of the modified IEEE 34-bus system. In this scenario, the master controller sends a request to the DNP3 slave to retrieve values stored in the read buffer. The DNP3 slave acknowledges the master's request and sends a read response message, which includes measurement data of the load obtained from a smart meter. This information is then used to update the load change in the VVO algorithm and calculate optimized setpoints for VR1. Since the voltage remains within operational limits, the load increase does not require any voltage level adjustments. As a result, the setpoints of VR1 remain unchanged. Consequently, the DNP3 master sets the setpoint value of VR1 to 1, reflecting the previous value of the VR1 step. However, in this scenario, the DNP3 client inside EXATACPS is subjected to a *MODP* add offset attack, which modifies the payload of the DNP3 stream by adding an offset of $+6$. This alteration causes the communicated value to the DNP3 slave to increase by 6 points, resulting in a corrupted setpoint for VR1 of 7 instead of the intended 1. As a consequence, an undesired voltage increase is observed in the feeder near node 8, as illustrated in Fig. 4. This voltage rise exceeds the operating voltage range defined by the ANSI standard, reaching 1.15 p.u. To further analyze the impact of the attack, we examine the Wireshark captures of the DNP3 message both before and after the cyberattack, as shown in Fig. 5. It is evident that the MODP attack corrupts the setpoint of VR1, leading to an unintended change in voltage within the distribution feeder, as depicted in Fig. 4.

The effect of attack category ②, i.e., cause the meter measurements not to be available for performing VVO, is demonstrated by launching a DoS attack on the DNP3 client in the EXATACPS interface. DoS attack works by flooding the victim node with excessive traffic thereby making it inoperative. Once the attack is launched, the DNP3 client simulator displays a connection lost status. As a result, the previously updated values of measurement messages are available with the master controller to run VVO for the next cycle, which in turn results in failure to compute updated setpoints for VVO, thereby rendering VVO ineffective, as depicted in Fig. 6.

The SIs provide reactive power support to the distribution network as per the generalized Volt/VAR curve regulated by IEEE 1547-2018 standard. In the case which the Volt/VAR curve setpoints of SI are modified under the attack ③ scenario, the slope of the curve can be increased or decreased by an attacker resulting in a steep or shallow Volt/VAR curve, respectively, as shown in Fig. 7. In EXATACPS, a MODP attack with a multiply option is selected to modify the slope of the Volt/VAR curve. The Volt/VAR curve setpoints are stored in an array and are updated in the secondary control block under the reactive power mask of the SI through RT-LAB. The node voltage at the PVSI node is monitored during the attack. Corrupted Volt/VAR curve settings lead to increased voltage transients as shown in Fig. 8, and hence, this creates issues with the load, DER units, and switchgear components.

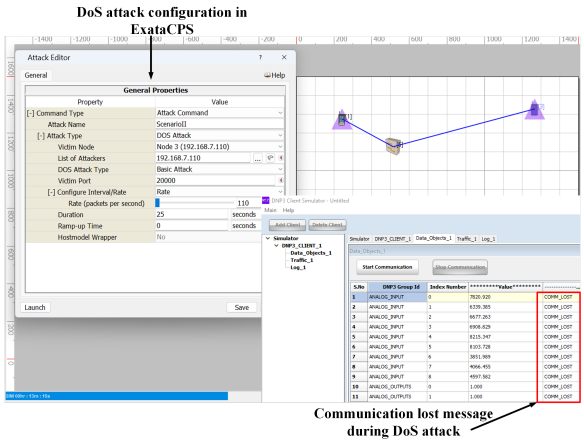

Fig. 6: Once the DoS attack (2) is launched, the communication is lost to the DNP3 client.

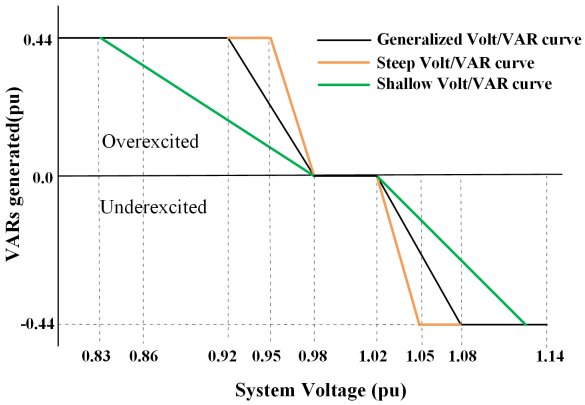

Fig. 7: Modification of Volt/VAR curve during attack (3) on SI.

B. Impact Analysis on CVR

In order to illustrate the impact of the attack scenarios on CVR, we run the simulation for a 24-hour period in which the MODP attack realization is launched using EXATACPS library. During the simulation, the changes in the number of setpoints in VRs and Volt/VAR curve are measured. Using this information, the energy savings achieved through CVR are calculated. Subsequently, the results are compared with the energy savings achieved in the absence of an attack.

The load demand profile for a day is considered for the simulation as in [17]. It is observed that the load consumption is lower during the night and early morning compared to the daytime. Thus, the load profile is divided into two stages: a lightly loaded and a heavily loaded period. The average electricity purchase rate, denoted as C_{E,t_k}, is considered as \$0.20 per kWh for a day [22]. The operating cost of VR is considered as \$0.05 per tap change [23]. The CVR factor, which represents the ratio of percentage energy saved to percentage reduction in voltage achieved through CVR, is computed for each attack following the method in [3]. A higher value of CVR factor indicates higher savings and vice-versa.

Table I presents the total number of updates in setpoints for the VRs under the different attack categories. Under *tampering*

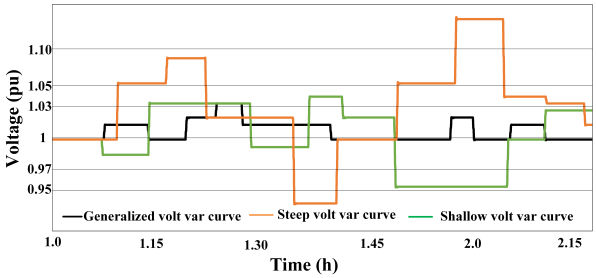

Fig. 8: Voltage variations in voltage at node 34 due to modification in slope of Volt/VAR curve during attack (3) on SI.

VVO setpoint attack (1), increased number of setpoint updates in VRs occurs as compared to normal operation. When a DoS attack is launched under *tampering smart meter measurements* attack (2), communication between VVO controller and VRs is lost and hence no changes in setpoint of VRs are observed. Therefore, results for this attack are not included in Table I. In the case of *modifying SI Volt/VAR curve* attack (3), when the slope of the Volt/VAR curve is reduced resulting in a shallow curve, increased number of setpoint updates for VRs occurs. A reduced number of setpoint updates for VRs is observed under steep Volt/VAR curve, however, this leads to an increased number of voltage limit violations as shown in Fig. 8.

Table II presents the cost analysis and CVR factor for the attack categories. The procedure for calculating the cost terms in Table II is as follows. The average electrical energy supplied from the substation in the modified IEEE 34-bus system is measured in RT-LAB. This is then multiplied by the average electricity purchase rate to obtain the energy purchase cost. The operating cost of the VRs is calculated by multiplying the number of setpoints updates in Table I with the cost per tap change. The total active power loss is computed using the modified ADMM algorithm, and then used to calculate energy loss cost. The total operational cost, which includes energy cost, losses, and the operating cost of the VRs, is compared to a baseline case in which CVR is not implemented and no attack occurs. This serves as the reference point for evaluating the percentage cost savings. The first two columns of Table II correspond to values when VVO is implemented without and with CVR, respectively. The other columns correspond to cost values for attack categories (1) and (3), respectively. As for attack (2), due to a successful DoS attack, communication was lost, and thus, no outcomes could be obtained. Based on the presented results in Table II, it can be concluded that implementing CVR with VVO and without any attack being realized yields cost savings of 3.17% and 1.44% during light load and heavy load conditions, respectively. The cost savings as well as the CVR factor deteriorate under the effect of attacks. It is worthwhile to mention that although under Volt/VAR curve with steep slope attack, cost savings are better as compared to other attack categories, this scenario leads to a higher number of violations in voltage limits as per the ANSI standard C84.1-2011 (Fig. 8).

TABLE I: Number of setpoint updates in VRs during the simulation.

Operating Devices	Normal operation		① Tampering VVO setpoints		③ Modifying SI Volt/VAR curve setpoints			
	Light load	Heavy load	Light load	Heavy load	Shallow Curve		Steep Curve	
					Light load	Heavy load	Light load	Heavy load
VR1	4	7	16	24	5	10	3	5
VR2	9	12	21	17	11	16	8	9

TABLE II: Cost analysis and CVR under the different attack scenarios.

Cost terms	VVO without CVR		VVO with CVR		① Tampering VVO setpoints		③ Modifying SI Volt/VAR Curve Setpoints			
	Light load	Heavy load	Light load	Heavy load	Light load	Heavy load	Shallow Curve		Steep Curve	
							Light load	Heavy load	Light load	Heavy load
Energy purchased ($)	7288	12776	6873	12478	7117	12506	7137	12601	7208	12253
VR operating costs ($)	–	–	0.65	0.95	1.85	2.05	0.8	1.3	0.55	0.7
Cost of Energy loss ($)	97	161	63	113	91	179	79	153	76	152
% Energy saved	–	–	3.17	1.44	1.07	0.6	0.9	0.1	1.41	2.8
CVR factor	–	–	0.8	0.57	0.36	0.3	0.23	0.46	0.23	0.46

V. Conclusion

This paper investigates the impact of cyberattacks on the VVO scheme using a real-time co-simulation setup. A detailed discussion of the setup considered for this study is provided. The developed co-simulation setup is flexible and can be seamlessly adapted to other industrial communication protocols used in electric utilities such as IEC 61850, OpenADR, IEEE 2030.5 etc. The results demonstrate that the number of setpoint updates of VRs increases under influence of cyberattacks. Moreover, cyberattacks on modifications of VVO device setpoints lead to an increased number of voltage limit violations on the distribution feeder. CVR factor also reduces under the influence of the attacks. The benefit of the developed real-time co-simulation setup is that it can be employed to assess the impacts of different attack scenarios and to test mitigation strategies before field deployment.

References

[1] H. Mataifa, S. Krishnamurthy, and C. Kriger, "Volt/var optimization: A survey of classical and heuristic optimization methods," *IEEE Access*, vol. 10, pp. 13 379–13 399, 2022.

[2] Z. Wang and J. Wang, "Review on implementation and assessment of conservation voltage reduction," *IEEE Transactions on Power Systems*, vol. 29, no. 3, pp. 1306–1315, 2014.

[3] ——, "Time-varying stochastic assessment of conservation voltage reduction based on load modeling," *IEEE Transactions on Power Systems*, vol. 29, no. 5, pp. 2321–2328, 2014.

[4] IEEE Std 1547, "IEEE Guide for Using IEEE Std 1547 for Interconnection of Energy Storage Distributed Energy Resources with Electric Power Systems," *IEEE Std 1547.9-2022*, pp. 1–87, 2022.

[5] I. Zografopoulos *et al.*, "Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies," *IEEE Access*, vol. 9, pp. 29 775–29 818, 2021.

[6] C. Konstantinou *et al.*, "Gps spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment," *IET Cyber-Physical Systems: Theory & Applications*, vol. 2, no. 4, pp. 180–187, 2017.

[7] C. Peng *et al.*, "A survey on security communication and control for smart grids under malicious cyber attacks," *IEEE Trans. on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1554–1569, 2019.

[8] I. Zografopoulos, C. Konstantinou, and N. D. Hatziargyriou, "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations," *IEEE Systems Journal*, pp. 1–15, 2023.

[9] A. Majumdar *et al.*, "Centralized volt–var optimization strategy considering malicious attack on distributed energy resources control," *IEEE Transactions on Sustainable Energy*, vol. 9, no. 1, pp. 148–156, 2018.

[10] D. Choeum and D.-H. Choi, "Trilevel smart meter hardening strategy for mitigating cyber attacks against volt/var optimization in smart power distribution systems," *Applied Energy*, vol. 304, p. 117710, 2021.

[11] A. Joseph, K. Smedley, and S. Mehraeen, "Secure high der penetration power distribution via autonomously coordinated volt/var control," *IEEE Transactions on Power Delivery*, vol. 35, no. 5, pp. 2272–2284, 2020.

[12] D. Arnold *et al.*, "Adaptive control of distributed energy resources for distribution grid voltage stability," *IEEE Transactions on Power Systems*, vol. 38, no. 1, pp. 129–141, 2023.

[13] A. Alburidy and L. Fan, "An alternating direction method of multipliers-based approach to solve mixed-integer nonlinear volt/var optimization problems in distribution systems," *International Transactions on Electrical Energy Systems*, vol. 31, no. 3, p. e12795, 2021.

[14] S. Singh, V. B. Pamshetti, and S. Singh, "Time horizon-based model predictive volt/var optimization for smart grid enabled cvr in the presence of electric vehicle charging loads," *IEEE Transactions on Industry Applications*, vol. 55, no. 6, pp. 5502–5513, 2019.

[15] A. Singhal *et al.*, "Real-time local volt/var control under external disturbances with high pv penetration," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3849–3859, 2019.

[16] T. Basso, "IEEE 1547 and 2030 Standards for Distributed Energy Resources Interconnection and Interoperability with the Electricity Grid," National Renewable Energy Laboratory, Tech. Rep., 12 2014.

[17] S. Singh *et al.*, "Event-driven predictive approach for real-time volt/var control with cvr in solar pv rich active distribution network," *IEEE Transactions on Power Systems*, vol. 36, no. 5, pp. 3849–3864, 2021.

[18] I. Zografopoulos *et al.*, "Security assessment and impact analysis of cyberattacks in integrated t&d power systems," in *Proceedings of the 9th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, 2021, pp. 1–7.

[19] A. Intriago *et al.*, "Residual-based detection of attacks in cyber-physical inverter-based microgrids," *IEEE Transactions on Power Systems*, 2023.

[20] A. Joseph, K. Smedley, and S. Mehraeen, "Secure power distribution against reactive power control malfunction in der units," *IEEE Transactions on Power Delivery*, vol. 36, no. 3, pp. 1552–1561, 2021.

[21] S. Dharmasena, T. O. Olowu, and A. I. Sarwat, "Algorithmic formulation for network resilience enhancement by optimal der hosting and placement," *IEEE Access*, vol. 10, pp. 23 477–23 488, 2022.

[22] M. S. Hossan and B. Chowdhury, "Integrated cvr and demand response framework for advanced distribution management systems," *IEEE Transactions on Sustainable Energy*, vol. 11, no. 1, pp. 534–544, 2020.

[23] M. Manbachi *et al.*, "Impact of ev penetration on volt–var optimization of distribution networks using real-time co-simulation monitoring platform," *Applied Energy*, vol. 169, pp. 28–39, 2016.