Preprint of the manuscript.
Full text available later
Cite as: P. S. Sarker, S. Majumder, M. F. Rafy, and A. K. Srivastava, "Impact analysis of cyber-events on distributed voltage control with active power curtailment," in Power Electronics, Drives and Energy Systems (PEDES), IEEE, Dec. 2022.

Impact Analysis of Cyber-Events on Distributed Voltage Control with Active Power Curtailment

Partha S. Sarker, *Student Member, IEEE,* Subir Majumder, *Member, IEEE,*
Md Fazley Rafy, *Student Member, IEEE,* Anurag K. Srivastava *Fellow, IEEE*

***Abstract*—Advanced distributed control algorithms can assist in efficiently operating the power distribution systems with Distributed Energy Resources (DERs), while ensuring resiliency during critical events like cyber-attacks. In this work, we assess the resiliency of the developed distributed feedback-based Volt-Watt controller. In this regard, a Cyber-Physical System (CPS) test-bed, which uses OpenDSS for power system simulation and Mininet for communication network emulation and simulated various attack scenarios, has been utilized. Multiple attacks, including Denial of Service (DOS), Man in the Middle (MitM), and replay attacks, were modeled and deployed in the Mininet emulation. We observe that simulated attacks impact depends on the system configuration, system dynamics, attack type, embedded control, and supporting cyber systems.**

***Index Terms*—Cyber-Power Systems, DERs, Co-Simulation, Test-bed, Mininet, Distributed Optimization, Cyber-attacks.**

I. Introduction

ANSI C84.1-2020 standard advocates maintaining voltage profile within $\pm 5\%$ in the low-voltage distribution grid [1]. Voltage control are usually accomplished using tap operation of the transformers, series voltage regulators, and capacitor banks for the legacy distribution system. However, with increasing participation of distributed energy resources (DERs) into the distribution network, especially during the lightly loaded condition, the network may frequently suffer from over-voltage conditions and high uncertainty to maintain voltage. Enabled by the IEEE-1548 standard [2], DERs are able to contribute to control distribution network-wide voltage profile, one of the possible monetizable value-streams for grid-integration of DERs [3]. This could be facilitated by satisfying the reactive power demand of the loads locally (during heavily loaded conditions) or through VAR absorption (during the lightly loaded condition, with increased generation from these DERs). Contrary to the transmission network, the R/X ratio of the distribution network is non-negligible, and the voltage profile could also be controlled by active power [4]. If VAR absorption is unable to control voltage within the bound, active power curtailment would be needed, which is usually classified as "Volt-Watt" control.

Requisite communication infrastructure within a control-center-based voltage control framework with a multitude of small-scale inverter-interfaced DERs introduces scalability challenges and increases the cyber attack surface. Given a direct correlation between DER profitability and active power curtailment, the financial consequence for non-optimal operations and/or cyber-attacks could be enormous. In this regard, methodologies, such as local approaches, do not guarantee optimality. And therefore, an optimization methodology that avoids data aggregation at a centralized location guarantees optimality and reorganizes itself during cyber or physical threats gains immense significance. As given in [5], multiple distributed control/optimization strategies for the power distribution system can be found in the recent academic literature. Voltage optimization and control are often used synonymously in the existing literature, and we will continue to do so in this article.

Like volt-var optimization, volt-watt optimization has been thoroughly studied in the recent literature. Typically, the optimizers are expected to solve an optimal power flow (OPF) problem with an expected bound on a network-wide voltage profile. Traditional 'droop' based local approaches are extremely popular, and one such approach has been demonstrated using Hardware-in-the-Loop (HIL) test platform [2]. A combined alternative direction multiplier method (ADMM) and branch and bound method for distributed volt-var and volt-watt control is shown in [6]. Given increasing cyber and physical vulnerabilities, the controllers may suffer from instabilities, the effect of which is studied in [7]. However, these methods generally assume the availability of a detailed mathematical model representing the system and associated disturbance.

Furthermore, impact analysis (both cyber and physical) of the distributed algorithm requires a realistic co-simulation platform. In this regard, the RTDS and network simulator-3 (NS-3) based simulation test-bed [8], NS-3 coupled HELICS based co-simulated test-bed [9] implementation of 2030.5 protocol for resiliency analysis [10], federated test-bed combining performances of RTDS and OPAL-RT [11] have been developed to analyze controller performance under cyber attacks. However, not all kinds of cyber-attacks are practicable from the distribution network operational point of view. Cyber-attacks, such as denial of service (DOS), man-in-the-middle (MitM), and replay attacks, are quite popular in analyzing controller performance integrated with the power distribution network. Resiliency against DOS attack in Simulink and OPNET-based co-simulation model has been developed in [12]. Impact of cyber-attacks on micro-grids also was demonstrated utilizing the Common Open Research Emulator (CORE) based model in [13]. Notably, test-bed models as an alternative to the actual power system gain immense significance especially during cyber events [14].

The primary focus of this paper would be to analyze the

Partha S. Sarker, Md Fazley Rafy, Subir Majumder and Anurag K. Srivastava are with the Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, West Virginia 26506. (E-mail: anurag.srivastava@mail.wvu.edu).

This material is partially supported by the US Department of Energy UI-ASSIST project #DE-IA0000025, and NSF CPS aDoption 1932574.

performance of the proposed feedback-based distributed volt-watt control approach in the presence of cyber-attacks. Our previously developed test-bed [15] would facilitate testing the efficacy and performance of the control algorithm in the presence of cyber-attacks. The contributions of our paper would therefore be two-fold:

(i) A distributed feedback-based volt-watt controller that guarantees asymptotic convergence of voltage-related constraints has been proposed in this paper. Our objective would be to minimize the cost of active power curtailment. Given the DERs are expected to operate at their maximum power point, the associated impact on the controller design has been considered. The controller consists of multiple edge-based computing nodes, and the proposed approach limits controller communication to the neighboring control nodes. This provides advantages such as limited communication requirements. A taxonomy of the proposed control approach aiming to provide a performance evaluation of the controller is also included.

(ii) Three cyber-attack scenarios, namely, the MitM, DOS, and the Replay Attack, have been developed in the communication layer. These malicious hosts are capable of attacking multiple DER hosts. The performance impacts of these cyber-attacks on the proposed distributed Volt-Watt algorithm have been evaluated.

The proposed distributed volt-watt control algorithm is discussed in Section II. A brief cyber-power co-simulation test-bed description and cyber-attack models for simulation is presented in Section III. Algorithmic performance against the simulated cyber-attacks is detailed in Section IV. Section V concludes this paper.

II. Volt-Watt Control with DERs

Renewable energy resources must be operated at the maximum power point. With the increasing penetration of renewable energy resources, VAR control may not be sufficient to ensure that the voltages remain within limits, necessitating the curtailment of active power. In this work, we utilize a feedback-based distributed control for the unbalanced system proposed in an earlier research [16], which has the following form:

$$\min_{\mathbf{x}} \sum_{\forall i} f_i(x_i) \tag{1a}$$

$$\text{s.t.} \quad \underline{y}_i \leq y_i(x_i) \leq \overline{y}_i \tag{1b}$$

$$\underline{x}_i \leq x_i \leq \overline{x_i} \tag{1c}$$

Here, the objective function ($f_i : \mathbb{R} \to \mathbb{R}$) is required to be μ-strongly convex and l-smooth. As shown, the proposed problem is fully decomposable in terms of x_i, and these variables are only interconnected by function y_i, which can be inherently non-linear. We identify a linear relationship among x_i and y_i for updating the primal variables to solve the optimization problem. We utilized the plant itself for determining $y_i(x_i)$, which will be further utilized for updating the dual variables, making our approach feedback-based, or, dynamic [17]. The use of this feedback-based approach iteratively eliminates the model inaccuracy due to the use of this approximated relationship. Here, through the volt-watt control application, we see that the proposed method in [16] for solving (1) can be sufficiently generalized for other control applications.

Linear approximation of the power flow equations for the distribution network is described in following subsections:

A. 3-ϕ Linearized Unbalanced Power Flow Equations

We consider a three-phase unbalanced $N+1$-node radial distribution network with the set of nodes being $\mathcal{N} = \{0, 1...., N\}$. As given in an earlier research [18], we utilized branch flow models for calculating the linear approximate for its approximation accuracy, and inherent mathematical simplicity [19], [20]. This linearized model ignores line losses and assumes that the node voltages are balanced. The discussed linear approximation of the power flow equations will be given by:

$$\widetilde{\boldsymbol{v}} = \bar{Z}^P \widetilde{\boldsymbol{P}} + \bar{Z}^Q \widetilde{\boldsymbol{Q}} + v_0 1_{3N} \tag{2}$$

Here, the voltage vector for the network will be given by $\widetilde{\boldsymbol{v}} = [v_1.....v_N]^T$ with $v_j = \left[\left|V_j^a\right|^2, \left|V_j^b\right|^2, \left|V_j^c\right|^2\right]^T, \forall j \in \mathcal{N}$. The active power injection vector will be: $\widetilde{\boldsymbol{P}} = [p_1.....p_N]^T$ where $p_j = \left[p_j^a, p_j^b, p_j^c\right]^T, \forall j \in \mathcal{N}$, and the reactive power injections will be $\widetilde{\boldsymbol{Q}} = [q_1.....q_N]^T$ where $q_j = \left[q_j^a, q_j^b, q_j^c\right]^T, \forall j \in \mathcal{N}$. Furthermore, $v_0 1_{3N}$ will be the substation end voltages. Also, as discussed in [21], $\bar{Z}^P$ and $\bar{Z}^Q$ will be $3-\phi$ matrices, that are equivalent to resistances and reactances of the distribution network.

B. Utilized Feedback-Based Approach

Active power injection in (2) can be separable into curtailable and fixed components, $\widetilde{P}^C$ and $\widetilde{P}^F$ respectively, where, $\widetilde{P} = \widetilde{P}^F + \widetilde{P}^C$. Let, $\widetilde{\boldsymbol{v}}^{\boldsymbol{unc}}$ be a factor dependent on $\widetilde{P}^F$ and $\widetilde{\boldsymbol{Q}}$ respectively, the network-wide voltage profile will be given by,

$$\widetilde{\boldsymbol{v}}(\widetilde{P}^F) = \bar{Z}^P \widetilde{\boldsymbol{P}}^{\boldsymbol{C}} + \widetilde{\boldsymbol{v}}^{\boldsymbol{unc}} \tag{3a}$$

$$\widetilde{\boldsymbol{v}}^{\boldsymbol{unc}} = \bar{Z}^P \widetilde{\boldsymbol{P}}^{\boldsymbol{F}} + \bar{Z}^Q \widetilde{\boldsymbol{Q}} + v_0 \mathbf{1}_{3N} \tag{3b}$$

We stress on $\widetilde{\boldsymbol{v}}(\widetilde{P}^F)$ to highlight input-output relationship among active power curtailment and voltage profile throughout the network. At a given time t, if the active power curtailment vector throughout the network is given by $\widetilde{P}^F(t)$, and following its deployment if the measured voltage is $\boldsymbol{v}(t)$, the resulting lagrangian multiplier in would dictate the control action $\widetilde{P}^F(t+1)$.

C. Distributed Optimization

The lagrangian multiplier of the optimization problem (1) can be written as:

$$\mathcal{L}(\hat{\boldsymbol{p}}, \xi, \lambda) = \sum_{\forall i} f_i(\hat{p}) + \underline{\lambda}^T \left(\underline{\boldsymbol{v}} - \boldsymbol{v}(\hat{p})\right) + \bar{\lambda}^T \left(\boldsymbol{v}(\hat{p}) - \bar{\boldsymbol{v}}\right) + \sum_{\forall i} K_i(\hat{p}_i, \xi_i) \tag{4}$$

Here, $K_i(\hat{\boldsymbol{p}}_{\boldsymbol{i}}, \xi_i)$ is a quadratic penalty function that actively helps the objective function to converge faster. Without loss of generality, here, $\hat{p}$ represents requisite active power curtailment.

$$K_i(\hat{p}_i, \xi_i) = \begin{cases} \xi_i \left(\hat{p}_i - \underline{p}\right) + \frac{c}{2}\left(\hat{p}_i - \underline{p}\right)^2 & \hat{p}_i + \frac{\xi_i}{c} < \underline{p} \\ -\frac{\xi_i^2}{2c} & \bar{p} \leq \hat{p}_i + \frac{\xi_i}{c} \leq \underline{p} \\ \xi_i \left(\hat{p}_i - \bar{p}\right) + \frac{c}{2}\left(\hat{p}_i - \bar{p}\right)^2 & \bar{p} < \hat{p}_i + \frac{\xi_i}{c} \end{cases} \tag{5}$$

Following standard primal-dual algorithm, primal updates will be:

$$\hat{p_i}(t+1) = \hat{p_i}(t) - \alpha \left\{ \left(\overline{\lambda_i} - \underline{\lambda_i}\right) + \sum_{\forall j \in \mathcal{N}} \left[\bar{Z}^P\right]^{-1} \left[f_i'(x_i) + \mathrm{ST}_{c\underline{p_i}}^{c\overline{p_i}}\left(\xi_i + c\hat{p_i}\right)\right] \right\} \tag{6}$$

In (6), for any $e_1 < e_2$, the soft-thresholding function, $\mathrm{ST}_{e_1}^{e_2}(\cdot)$, is defined by, $\mathrm{ST}_{e_1}^{e_2}(z) = \max(\min(z - e_1, 0), z - e_2)$. Inherent sparsity of $\left[\bar{Z}^P\right]^{-1}$ with DER penetration at limited number of nodes is presented in [16], and its block-sparse form is derived for 3-ϕ case in [22]. Notably, scaling of the gradient for updating the primal variable by $\left[\bar{Z}^P\right]^{-1}$ leads to the overall distributed nature of the proposed method. However, with increasing modeling accuracy, $\left[\bar{Z}^P\right]^{-1}$ may not remain positive semi-definite, an essential criterion to guarantee asymptotic convergence. This led us to use the linearized 3-Φ network with no cross-coupling among phase resistances and reactances.

Similarly, the dual updates will be given by:

$$\xi_i(t+1) = \xi_i(t) + \beta \frac{\mathrm{ST}_{c\underline{p_i}}^{c\overline{p_i}}\left(\xi_i + c\hat{p_i}\right) - \xi_i(t)}{c} \tag{7}$$

$$\overline{\lambda}_i(t+1) = \overline{\lambda}_i(t) + \gamma \left[\left(v_i^{meas}(t) - \overline{v_i}\right)\right]^+ \tag{8}$$

$$\underline{\lambda}_i(t+1) = \underline{\lambda}_i(t) + \gamma \left[\left(\underline{v_i} - v_i^{meas}(t)\right)\right]^+ \tag{9}$$

Here, $[\cdot]^+$ is a projection operator that symbolizes the associated variable projected onto the non-negative orthrant. Notably, the use of voltage measurements $v_i^{meas}(t)$ alleviates the need to calculate $\widetilde{\boldsymbol{v}}^{\boldsymbol{unc}}$, which is a function of system-wide loading condition, and inherent non-linearity of AC power flow equations. Furthermore, the tuple $\left[\underline{p_i}, \overline{p_i}\right]$ would be non-zero only for the DER nodes. If the maximum active power injection capability of the DER node i is given by P_i^{DER}, active power control set-points to be provided to the DER inverter would be:

$$p_i^{inj}(t+1) = P_i^{DER}(t) + \left[\hat{p_i}(t+1)\right]_{\underline{p_i}}^{\overline{p_i}} \tag{10}$$

Both maximum power point and curtailable part together are needed to calculate set-point for each DERs. Here, $[\cdot]_{\underline{p_i}}^{\overline{p_i}}$ indicates projection onto set $[\underline{p_i}, \overline{p_i}]$. However, given the majority of the DERs are renewable energy interfaced, and at any point of time, t, these DERs are expected to operate at their maximum power point level, $p_i^{mpp}(t)$. However, the maximum power point level at the next time-step is not known before computation, which necessitates active power injection set-points to be updated as follows:

$$p_i^{inj}(t+1) = \left[p_i^{mpp}(t+1) + \left[\hat{p_i}(t+1)\right]_{-p_i^{mpp}(t)}^{0}\right]_{0}^{p_i^{mpp}(t+1)} \tag{11}$$

Also, intermediate primal and dual variable will be updated using, $p_i^{mpp}(t)$. With suitable limits, storage devices could also be suitably incorporated in this framework. However, given the focus of this paper is to understand the impact of cyber attacks on the controller dynamics, we assume that $p_i^{mpp}(t)$ stays at a constant level.

D. Volt-Watt Control Algorithm

We extend the algorithm proposed in [16], which is further updated for the unbalanced distribution system in [22], to develop optimal distributed volt-watt control algorithm (OPTDIST-VWC). It can be envisaged that both OPTDIST-VC in [22] and the proposed OPTDIST-VWC operate alongside each other for an optimal voltage control. The proposed algorithm facilitates the plug-and-play capability of the DERs through the distributed coordinator application developed in [15]. As discussed, the proposed algorithm requires communication only among the neighboring DER nodes, and the distributed coordinator application facilitates the same upon discovering a change in network topology. It can be seen that updating only primal variables (see (6)) require communication among neighboring nodes, and each of the DER nodes communicate $f_i'(\hat{p_j}) + \mathrm{ST}_{c\underline{p_i}}^{c\overline{p_i}}\left(\xi_i + c\hat{p_i}\right)$. Updating dual variables is independent of measurement at neighboring nodes. This alleviates the exchange of voltage and MPPs among the DER nodes.

Primal auxiliary variable $\hat{p_i}$, and dual auxiliary variables $\xi_i, \overline{\lambda_i}, \underline{\lambda_i}$ (each of these variables for a given node are vectors for all three phases) are utilized for calculating the controller set-points. Voltage controllers are assumed to be present in all the phases[1]. At a given time t, voltages at the DER nodes, $v_i^{meas}(t)$, and active power capability based on MPP, $p_i^{mpp}(t)$, are measured. Given available $\hat{p_i}(t), \xi_i(t), \overline{\lambda_i}(t), \underline{\lambda_i}(t)$, and exchanged information from neighboring DERs, the auxiliary variables are updated. Active power injection set-points, $p_i^{inj}(t+1)$, are subsequently calculated, and locally deployed.
OPTDIST-VWC: Each DER controller for a given node j ($j \in \mathcal{N}$) follows four different steps at time t:

Step 1 (Measurement): Measure local phase voltages at all available phases $v_j(t)$.

Step 2 (Calculating): Calculate, $\hat{p}_j(t+1), \xi_j(t+1), \bar{\lambda}_j(t+1), \underline{\lambda}_j(t+1)$, using the following equations:

$$\hat{p}_j(t+1) = \hat{p}_j(t) - \alpha \left\{ \left(\overline{\lambda}_j(t) - \underline{\lambda}_j(t)\right) + \sum_{\forall i \in \mathcal{N}_j} \left[\bar{Z}^P\right]_{ji}^{-1} \left[f_i'(\hat{p}_i(t)) + \mathrm{ST}_{-cp_j^{mpp}(t)}^{0}\left(\xi_i(t) + c\hat{p}_i(t)\right)\right] \right\} \tag{12a}$$

$$\xi_j(t+1) = \xi_j(t) + \beta \frac{\mathrm{ST}_{-cp_i^{mpp}(t)}^{0}\left(\xi_j(t) + c\hat{p}_j(t)\right) - \xi_j(t)}{c} \tag{12b}$$

$$\overline{\lambda}_j(t+1) = \overline{\lambda}_j(t) + \gamma \left[\left(v_j^{meas}(t) - \overline{v_j}\right)\right]^+ \tag{12c}$$

[1]If DERs are not present in all the phases, it will be represented through suitable bounds.

$$\underline{\lambda}_j(t+1) = \underline{\lambda}_j(t) + \gamma \left[\left(\underline{v_j} - v_j^{meas}(t) \right) \right]^+ \quad (12d)$$

here, $\mathcal{N}_j$ is the set of all neighbor nodes of node j ($\forall j \in \mathcal{N}$). **Step 3 (Active Power Set-Point Deployment):** Maximum power point for DER is calculated $p_j^{mpp}(t+1)$. Active power injection set-point at time $t+1$ is calculated as

$$p_j^{inj}(t+1) = \left[p_j^{mpp}(t+1) + [\hat{p}_j(t+1)]_{-p_j^{mpp}(t)}^{0} \right]_0^{p_j^{mpp}(t+1)} \quad (13)$$

Step 4 (Communication): Values $f_j'(\hat{p}_j(t+1)) + \text{ST}_{-cp_j^{mpp}(t+1)}^{0}(\xi_j(t+1) + c\hat{p}_j(t+1))$ are communicated to neighboring DER nodes. □

III. Test-Bed for Performance Analysis

The overall architecture of the test-bed to facilitate demonstration of the proposed approach is briefly described here, and [15] could be refereed for details:

A. Power System Layer

OpenDSS, a power distribution simulator, has been utilized to mimic an exact 3-ϕ unbalanced power system. A quasi-static model of the system has been considered to reduce the time synchronization complexities while facilitating the analysis of a dynamical system. The communication port (COM) of OpenDSS has been used to fetch the system voltage measurements from and deploy the generated control signals. The wrapper, built around Python, ensures coordinated data flow among different layers of the model.

B. Cyber Layer

Each power system node is equipped with an independent host in a virtual communication network implemented using Mininet facilitating server-less peer-to-peer (P2P) control. It is a software-defined network (SDN) emulator that utilizes OpenFlow protocol for resilient custom routing, which can be used to run applications in a real-time environment. Mininet can be used to prototype SDN in such a manner that developers can create multiple hosts, switches, and topologies according to the project requirement. We preferred using mininet to other network simulators, as it can be extensively modeled to configure the virtual network and adjust the parameters, such as bandwidth, delay, etc., as required. The hosts in our virtual network communicate – exchange data – and acknowledge the presence of neighbor hosts using socket communication. Since each host can function independently, the controllers and coordinators running power system applications can communicate exclusively using the SDN. A wrapper developed in Python has been used to interface data exchange between the power and cyber layer.

An adversary can hijack a controller/coordinators node through the corresponding host in the SDN, and the specifics of the cyber-attacks are detailed as follows:

- **MitM:** The general concept behind this kind of attack is that an adversary takes control of the existing host or assigns a malicious one inside the network. Further deterioration is ensured by manipulating the shared measurements between two hosts in different ways. Here, as shown in Fig. 1, the perpetrator impersonates the compromised hosts to intercept and later modify the packets being sent. For example, the attacker has the certificate of the compromised node and thus is able to send altered packets to other hosts without suspicion. Given that the attacker has no access to the certificate of the non-compromised nodes received, respective data-packets will remain unaltered.

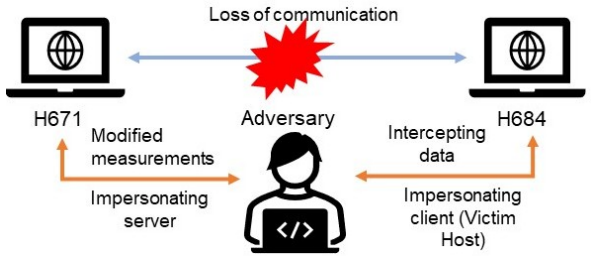

Fig. 1. MitM attack

- **DOS:** DOS occurs when legitimate users are denied accessing information from a specific user due to the intervention of a malicious threat actor. In the DOS attack, the perpetrator floods the communication channel of the designated host with unwanted network traffic flow, causing it to be incapable of maintaining communication. As shown in Fig. 2, we used hping3 tool to generate a large number of malformed UDP network traffic packets to overwhelm the victim node. Using the tool, we can trigger volumetric DOS attacks using different control sizes, quantities, and packet delivery rates.

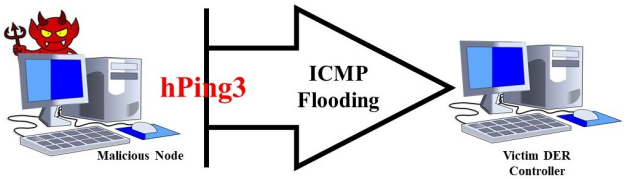

Fig. 2. DOS attack

- **Replay attack:** As shown in Fig. 3, a replay attack is a kind of MitM attack where the malicious entity secretly eavesdrops and records the data-exchange from the compromised host to its neighbors, only to send it later down the line. The perpetrator modifies the sending packets given the availability of the certificate of the compromised node. Here, the attacker can easily pass the firewall, as the data being communicated will hardly raise the deauthentication flag. Furthermore, the malagent can perform multiple data transmissions and flood the receiving end with unwanted data. In this case, the cyber threat actor allows normal data packet transmission from the target host for a certain period of time and, at the same time, stores a copy of the transmitted packets for future reference. After that certain period of time, the threat actor replaces the packet data of real-time communication with the past prerecorded ones.

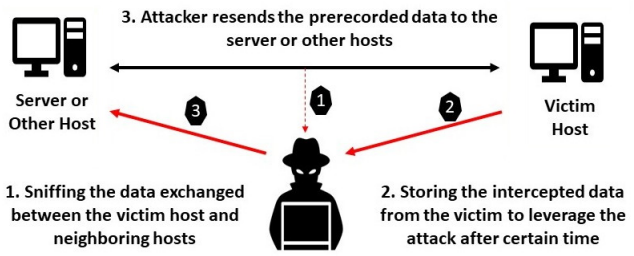

Fig. 3. Replay attack

C. Control and Computing

The control and computing layer sits between the cyber and power infrastructure layer and executes the desirable application. As for the distributed application, the controllers coordinate with each other to determine the control action and identify whom to communicate with. This facilitates a plug-and-play capability while implementing the algorithm developed in Section II.

IV. Case Study and Results

In this work, a modified IEEE 13-node radial distribution system (see [15]) has been used to demonstrate the efficacy of the proposed OptDist-VWC and study the effects of cyber-attacks on the control application. Considering power line communication (PLC), we assume that the topology of the communication network is similar to the power network topology. Highlighting the research work present in [17], the taxonomy of the control approach is given in Fig. 4. Notably, this taxonomy encompasses the fast time-scale operation of the controller, which is also the primary focus of this case study. Time-decomposability aspects in the overall operation could be exploited to incorporate the requisite coordination aspect for overall performance evaluation of the controller.

	Power Domain		Cyber Domain		Decision-Making	
	System Model	Application Type	Implementation Type	Communication	Iterative Data Exchange	Algorithm type
Distributed Method	Relaxed Three-Phase Branch Flow	Voltage Profile Improvement (Volt-Watt Control)	P2P Serverless Control	Frequent	Dynamic Method	Distributed-Dual Method (Primal-Dual Method)

Fig. 4. Taxonomy of the OptDist-VWC Algorithm

DERs are supposedly connected at nodes 634, 671, 675, and 684 of the distribution system, and corresponding Mininet hosts are running the control application. The upper and lower bounds for the nodal voltages are set to be 0.95 *pu* and 1.05 *pu* respectively. Given the curtailment will be needed in the excess generation scenario, we consider the case that all DERs are injecting real power of 0.8 *pu* with an apparent base power of 3000 kVA. Parameters d, α, β and γ are set at 0.00001, 0.01, 20, and 250 respectively. The objective is to minimize $f_i(p_i) = a_i p_i^2$ where a_i corresponding to DER nodes are randomly chosen to be as follows: node 634 $\rightarrow$ [20 20 22], node 671 $\rightarrow$ [25 30 22], node 675 $\rightarrow$ [18 19 21], node 684 $\rightarrow$ [23 24].

MitM, DOS, and replay attacks have been simulated along with normal operating conditions to validate the resiliency of the developed voltage control algorithm. Fig. 5 illustrates the overall performance of the controller under different attack cases. Performance analysis of the controller under different parameters d, α, β, and γ were also carried out but are not shown here for brevity. As shown in the figure, the objective function is able to converge within 22-time steps under the DOS attack. The objective function suffers from minor transients during the Replay attack during 50 to 60-time steps. The controller is unable to converge during a MitM attack. The associated impact on the active power set points is shown in Fig. 6.

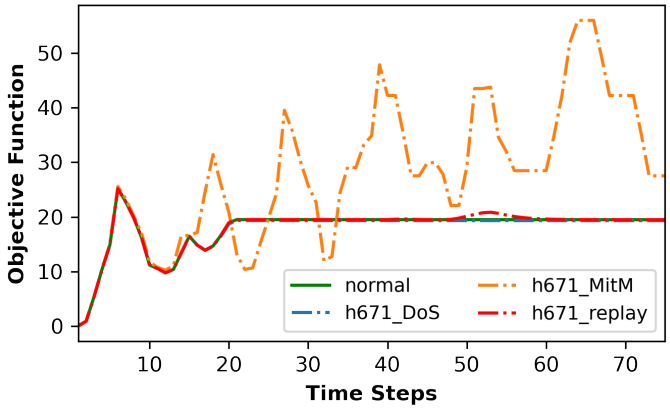

Fig. 5. Objective function during simulated cyber events

As for the implementation, during a DOS attack, the attacker severely limits communication with the node being communicated. During MitM, the attacker uses a prespecified multiplier for the desired communication. In a replay attack, the previous data points are recorded, only to be communicated later. Therefore, during a DOS attack, it can be envisaged that although the attacker is able to disable all communication to a particular node, and by doing so, it is dividing the controller into multiple clusters, where each cluster can act on its own. Therefore, we observe a minimal impact on the controller performance. As for the MitM, the multiplier used has a severe impact on the controller performance. With a chosen multiplier of 0.2, we observe that the controller cannot converge within the simulation window. However, for the differently chosen multiplier (not shown here for brevity), the controller performance is actually improved. We can theorize that the said multiplier provides a type of positive/negative feedback to the overall controller performance. As for the replay attack, although the algorithm can re-stabilize itself, this may not always be the case for a different network, associated parameters, etc.

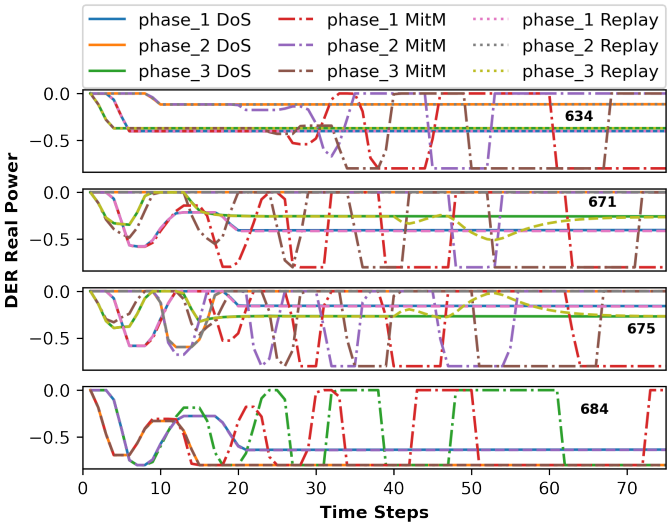

Fig. 6. DER Real Power curtailment in different DER nodes during different simulated attacks at node h671

V. Conclusions

In this work, the performance of the proposed feedback-based distributed Volt-Watt control application has been analyzed utilizing a Cyber-Physical co-simulation test-bed for the power distribution system. Three different cyber attacks, namely, Man in the Middle (MitM), Denial of Service (DOS), and Replay attacks, have been simulated. We observe that, due to distributed communication of controller nodes and limited local voltage measurements, the DOS attack has minimal impact with the implemented OptDist-VWC algorithm. In contrast, the performance of replay attacks can significantly change with a different system, different attack windows, etc. In MitM, the attacker can positively/negatively impact the controller's performance. We are also working to extend our work to develop the test-bed further to facilitate executing multiple control applications simultaneously to show performance analysis under different cyber vulnerabilities. Future work will be to analyze the impact in a larger system through additional practical cyber-attack models and utilize the understanding of the analysis to develop more cyber-resilient control algorithms.

References

[1] "American national standard voltage ratings for electric power systems and equipment (60 Hz)," *American National Standards Institute*, 2020.

[2] "IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces," *IEEE Std 1547-2018*, 2018.

[3] S. Majumder and A. Srivastava, "Resilience-driven integration of distributed energy resource (der): Holistic value analysis," *IEEE Smart Grid eBulletin*, Sep. 2022.

[4] S. Majumder and S. A. Khaparde, "Revenue and ancillary benefit maximisation of multiple non-collocated wind power producers considering uncertainties," *IET Generation, Transmission & Distribution*, vol. 10, no. 3, pp. 789–797, 2016.

[5] N. Patari, V. Venkataramanan, A. Srivastava, D. K. Molzahn, N. Li, and A. Annaswamy, "Distributed optimization in distribution systems: Use cases, limitations, and research needs," *IEEE Transactions on Power Systems*, pp. 1–1, 2021.

[6] Y. Liu, L. Guo, C. Lu, Y. Chai, S. Gao, and B. Xu, "A fully distributed voltage optimization method for distribution networks considering integer constraints of step voltage regulators," *IEEE Access*, vol. 7, pp. 60 055–60 066, 2019.

[7] D. Arnold, S. S. Saha, S.-T. Ngo, C. Roberts, A. Scaglione, N. G. Johnson, S. Peisert, and D. Pinney, "Adaptive control of distributed energy resources for distribution grid voltage stability," *IEEE Transactions on Power Systems*, pp. 1–1, 2022.

[8] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2444–2453, 2015.

[9] H. M. Mustafa, D. Wang, K. S. Sajan, E. N. Pilli, R. Huang, A. K. Srivastava, J. Lian, and Z. Huang, "Cyber-power co-simulation for end-to-end synchrophasor network analysis and applications," in *2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2021, pp. 164–169.

[10] P. S. Sarker, V. Venkataramanan, D. S. Cardenas, A. Srivastava, A. Hahn, and B. Miller, "Cyber-physical security and resiliency analysis testbed for critical microgrids with ieee 2030.5," in *2020 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, 2020, pp. 1–6.

[11] V. Venkataramanan, P. S. Sarker, K. S. Sajan, A. Srivastava, and A. Hahn, "Real-time federated cyber-transmission-distribution testbed architecture for the resiliency analysis," *IEEE Transactions on Industry Applications*, vol. 56, no. 6, pp. 7121–7131, 2020.

[12] M. A. H. Sadi, M. H. Ali, D. Dasgupta, R. K. Abercrombie, and S. Kher, "Co-simulation platform for characterizing cyber attacks in cyber physical systems," in *2015 IEEE Symposium Series on Computational Intelligence*, 2015, pp. 1244–1251.

[13] V. Venkataramanan, A. Srivastava, and A. Hahn, "Real-time co-simulation testbed for microgrid cyber-physical analysis," in *2016 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, 2016, pp. 1–6.

[14] H. M. Mustafa, M. Bariya, K. S. Sajan, A. Chhokra, A. Srivastava, A. Dubey, A. von Meier, and G. Biswas, "Rt-meter: A real-time, multi-layer cyber-power testbed for resiliency analysis," in *Proceedings of the 9th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, ser. MSCPES '21. New York, NY, USA: Association for Computing Machinery, 2021.

[15] P. S. Sarker, N. Patari, B. Ha, S. Majumder, and A. K. Srivastava, "Cyber-power testbed for analyzing distributed control performance during cyber-events," in *Proceedings of the 9th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, ser. MSCPES '22, 2022.

[16] G. Qu and N. Li, "Optimal distributed feedback voltage control under limited reactive power," *IEEE Transactions on Power Systems*, vol. 35, no. 1, pp. 315–331, 2019.

[17] S. Majumder, N. Patari, A. K. Srivasava, P. Srivasava, and A. M. Annaswamy, "Epistemology of voltage control in der-rich power system," *Elec. Pow. Syst. Res.*, 2023 (in Press).

[18] L. Gan and S. H. Low, "Convex relaxations and linear approximation for optimal power flow in multiphase radial networks," in *2014 Power Systems Computation Conference*. IEEE, 2014, pp. 1–9.

[19] M. E. Baran and F. F. Wu, "Optimal capacitor placement on radial distribution systems," *IEEE Transactions on power Delivery*, vol. 4, no. 1, pp. 725–734, 1989.

[20] M. Farivar and S. H. Low, "Branch flow model: Relaxations and convexification—part i," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 2554–2564, 2013.

[21] V. Kekatos, L. Zhang, G. B. Giannakis, and R. Baldick, "Voltage regulation algorithms for multiphase power distribution grids," *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3913–3923, 2015.

[22] N. Patari, A. K. Srivastava, G. Qu, and N. Li, "Distributed voltage control for three-phase unbalanced distribution systems with ders and practical constraints," *IEEE Transactions on Industry Applications*, vol. 57, no. 6, pp. 6622–6633, 2021.