Preprint of the manuscript.
Full text available at: https://ieeexplore.ieee.org/abstract/document/9770160
Cite as: P. S. Sarker, N. Patari, B. Ha, S. Majumder and A. K. Srivastava, "Cyber-Power Testbed for Analyzing Distributed Control Performance during Cyber-Events," 2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES), 2022.

Cyber-Power Testbed for Analyzing Distributed Control Performance during Cyber-Events

Partha S. Sarker, *Student Member, IEEE,* Niloy Patari, *Student Member, IEEE,* Brian Ha, Subir Majumder, *Member, IEEE,* Anurag K. Srivastava *Fellow, IEEE*

***Abstract*—In recent years, increasing attention over distributed control or optimization applications necessitated a unified environment to validate their performance. The proposed cyber-power co-simulation test-bed provides a realistic environment to facilitate such performance analysis, where the quasi-static power network is modeled using OpenDSS, and a realistic cyber network is modeled using Mininet. A distributed coordination algorithm using network communication has been developed to aid distributed applications such as distributed Volt-VAR control to determine the connectivity of distributed controllers. The entire co-simulation test-bed is integrated together using a wrapper developed using python. Two cyber-attack scenarios, namely, the Man in the Middle and the Denial-of-Service, have been appropriately modeled to test the performance of the considered control/optimization algorithm. We have shown the efficacy of our test-bed while simultaneously analyzing the performance of the distributed control algorithm utilizing an IEEE 13-node 3-ϕ unbalanced distribution network, with a feedback-based Volt-VAR optimization algorithm as a use-case.**

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

I. Introduction

With the increasing penetration of small-scale inverter-based behind-the-meter and front-of-meter distributed energy resources (DERs), typical control center-based centralized approaches pose significant coordination and scalability challenges. The need to aggregate sensor data at a centralized location creates privacy concerns in the operation of these resources. Increasing use of information and communication technologies (ICTs) and the supporting communication topology to satisfy centralized control center-based architecture poses significant vulnerabilities given single-point of failure (with backup) in operation and exposes the system to various cyber-attacks. Furthermore, the control-center-based approaches are not very scalable with increasing penetration of renewable-based resources. Alternatives, such as local control, while being less reliant on the ICTs, do not guarantee optimality in the decision-making. This calls for alternative architecture in the control application, such as distributed control, that does not rely on all sensor data to be communicated to the control center while guaranteeing optimality in a limited scope.

While, over the years, a multitude of distributed control/optimization strategies have been developed in the academic literature (see [1] for a recent review), other than increased computation time in the distributed control, the resulting solution is shown to be on-par with control center-based solution. However, simplification of the utilized ICTs, an essential component for the real-world implementation of any distributed control strategies, often projects an optimistic solution compared with other control/optimization architectures. Here, considering our previously developed distributed VAR control/optimization algorithm as a use-case, we have developed a cyber-power test-bed to analyze the performance of the voltage control approach under a much more realistic environment.

The development of co-simulation platforms involving power and communication networks is not new. In this regard, development of co-simulation platform for centralized VAR optimization using IEC 61850 [2], centralized DERs VAR control using IEEE 2030.5 [3], distributed microgrid control using Gridlab-D – HELICS platform [4], distributed Remedial Action Scheme (DRAS) algorithm with RTDS-PMUs along with CISCO FOG using Resilient Information Architecture Platform for Smart Grid [5], distributed VAR optimization in the SYSLAB facility utilizing ZeroMQ for TCP transport to facilitate reliable data delivery among physical network and controller [6], modular distributed infrastructure facilitating various power system simulators integrated with (MQTT) protocol and REST server, various load and generator emulator along with physical devices and control algorithm [7], centralized system with digital simulator, Common Open Research Emulator (CORE) for emulation with TCP/IP based interface for microgrid control [8], distributed multi-model multi-energy system [9] are few among recently available literature. While the developed co-simulation platform facilitating cyber communication are plenty, capable of analyzing the impact of communication network on the performance of the controller objective and the cyber-attacks are very limited. Furthermore, none of these available works facilitate distributed application running capability and performance analysis of the distributed controllers at any power system node under actual cyber-attacks on the communication network.

We present a realistic Python-based co-simulation platform by utilizing OpenDSS as the power distribution system and Mininet as the communication network emulator. The contribution of our paper is twofold:

(i) A cyber-power co-simulation platform, emulating realistic power as-well-as communication networks facilitating distributed optimization-based applications, has been developed in this paper. Each power system node is equipped with a cyber host, capable of running multiple application instances while communicating with other hosts representing other power system nodes. Here, the focus is more on developing a realistic cyber network

Partha S. Sarker, 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).

Niloy Patari was with the Washington State University (WSU) and now working with the National Grid, Waltham, MA. Brian Ha was with WSU. We would like to acknowledge Jonathan and Sanjita. This material is partially supported by the US Department of Energy UI-ASSIST project #DE-IA0000025, and NSF CPS aDoption 1932574.

in Mininet in a virtualized environment, where inter-host communication is implemented using socket communication. A distributed coordination algorithm has been developed to identify paths for inter-controller for the distributed control application, which gains significant importance if the power network and its corresponding cyber network suffer from outages or are reconfigured. The utility of the developed test-bed has been demonstrated using a distributed VAR application, where the application utilizes the hosts identified by the distributed coordination algorithm for control.

(ii) Two cyber-attack scenarios, namely, the Man in the Middle and the Denial-of-Service, have been developed with the capability of attacking multiple hosts in the communication layer has been developed. Considering distributed VAR algorithm as a use-case, we demonstrate the impact of the said cyber-attacks on the performance of the distributed control.

Cyber-power test-bed for distributed optimization and control along with distributed coordination algorithm has been presented in Section II. The use-case distributed feedback-based VAR control optimization algorithm is presented in Section III. Section IV details the performance of the optimization algorithm tested in the developed test-bed under cyber-attacks. Section V concludes this paper.

II. Cyber-Power Test-Bed with Distributed Coordination for Distributed Control

To enable requisite rapid and frequent communication among participating computing nodes, the focus is laid on a very detailed cyber network modeling, facilitating testing of any distributed control/optimization algorithm in a realistic environment. Typical 3-ϕ unbalanced power distribution system modeling is considered a physical network model. The test-bed also facilitates requisite coordination among computing nodes and provision of imposing cyber-attacks during any communication, which are necessary to analyze the real-world performance testing of distributed control algorithms.

The cyber-power co-simulation platform is comprised of three layers: (i) power system layer, (ii) cyber layer, and (iii) application layer. We have utilized OpenDSS to model the power system layer. Mininet has been used for networking, and Python programming language has been used to build all the applications (in the application layer). Note that the proposed test-bed has the plug-and-play capability, facilitating performance analysis of any distributed control application, with distributed coordination application suitably updated to facilitate data exchange among requisite computing nodes. Finally, the overall test-bed integration has been carried out utilizing a wrapper developed with Python. The overview of the developed test-bed architecture is shown in Fig. 1 while each sub-components are explained below.

A. Power System Layer

The power system layer is built around OpenDSS as a realistic tool for 3-ϕ unbalanced distribution system modeling, assuming the system's dynamics are slow enough that the overall control process can be represented as a quasi-static process. Co-simulation capabilities and support of the communication interface (COM) of OpenDSS have been utilized here to simulate a time-varying system. Here, the measurement from OpenDSS is fetched through the COM interface into the other layers for generating the control signal. Subsequently, a new set of control signals are deployed to OpenDSS again through the COM interface. Afterward, OpenDSS solves the power flow to generate measurement for the next time step. A set of wrappers coordinates this entire sequential process.

While the use of a quasi-static process to represent power system dynamics has an immediate advantage in avoiding time-synchronization among multiple layers of co-simulation platform. However, to alleviate the overall disadvantages of modeling power systems as a slow dynamical system can be alleviated by using an appropriate off-line real-time simulator and integrating in this testbed.

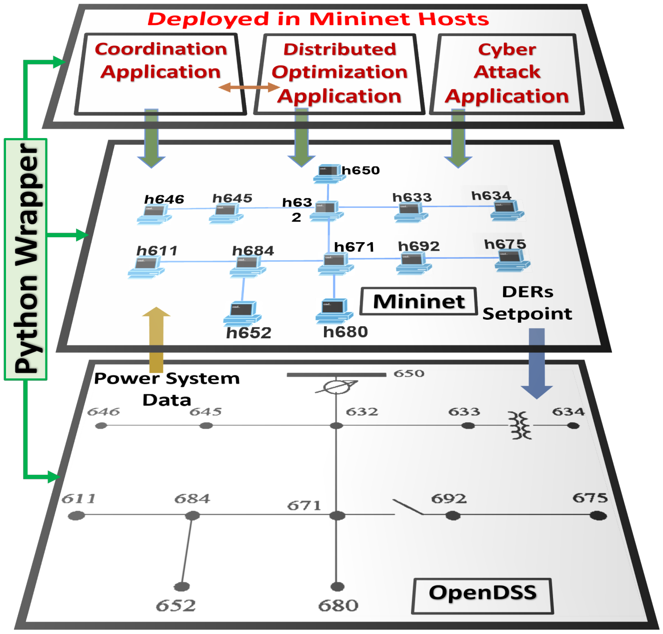

Fig. 1: Test-bed architecture.

B. Cyber Layer

Mininet is a network emulator that can create a virtual network with hosts, switches, controllers, and links [10] and work on a single Linux kernel. To enable communication among DER controllers in a distributed fashion, every power system node in the power system layer is represented by a Mininet host in the cyber layer. The hosts are emulated as bash processes, and each host will have its own private network and can only see its own processes. As a result, the host can run any application without the interference of other hosts. This perfectly mimics the real-world scenario where each power system node runs a distributed control algorithm in its own computing device, which is represented as a Mininet host. Mininet host gets its corresponding power system node data whenever required, which, as already discussed, is achieved through the python wrapper facilitated by the COM interface of OpenDSS. Then when it comes to data exchange among different power system nodes via communication network, the mininet hosts of those corresponding nodes use the mininet network. We rely on interprocess communication for message passing among hosts, given hosts in Mininet are emulated as bash processes. We have used sockets for this communication as it allows us to create custom network packets. This customization is necessary for distributed control applications as the necessary data can be easily exchanged among the participating hosts as network packet payloads through socket communication.

In this work, we have assumed that communication network utilizes power line communication and used Mininet Python API to create the cyber network of the given power system network from its graph network topology with a one-to-one mapping between both networks as done in other testbed [11]. This one-to-one mapping is essential to facilitate any distributed control application in the corresponding cyber layer of each power system node. Also, this has made the implementation of a cyber network scalable for any large distribution system while maintaining the geographical sparsity attribute of each distribution system node. The communication topology can vary based on the communication infrastructure utilized, but the host needs to have one-to-one mapping to its power system node to run any application.

C. Application Layer

Here, the application layer has three applications that can run in the individual host as required, as discussed in the Cyber Layer model. Considering the distributed VAR control application as a use-case, the distributed coordination application is suitably updated to facilitate communication among neighboring DERs. Description of the distributed VAR-control use-case is detailed in Section III. Distributed coordination and cyber-attack applications are described below:

1) Distributed Coordination: Any distributed control application requires a coordination algorithm to identify necessary controllers to communicate with as the power network frequently suffers from outages, reconfiguration, etc. Our developed distributed coordination application takes input from the distributed control application about its requirement of coordination topology and some of the measurements from the power system layer to determine the needed inter-host communication topology. This provides the test-bed a plug-and-play facility as any distributed control application can be deployed here without providing inter-controller communication topology each time whenever there is a change in the system. In our case-case, the requirement is to find out nodes with DER and their neighbor list in terms of DER presence in the power system layer. The application in each host access its host-specific power system node attributes available in JSON format. An example attributes for node 684 in the power system layer (see Fig. 1) is given below:

$$\{Node\ ID: 684, Voltage: 1pu, DER: Yes,$$
$$Neighbour\ Node\ IDs: 611, 652, 671\}$$

Then each host runs the algorithm given in Fig. 2 to determine its eligibility for running the use-case control application and control coordination topology. We utilize the Mininet communication network to implement this algorithm with multicast. It is important to note that a distributed variant of this algorithm based on recursion is also possible and is a work-in-progress.

The application runs on-demand if triggered by a change in the power system network or the cyber network host becomes offline due to any cyber attack or device malfunction.

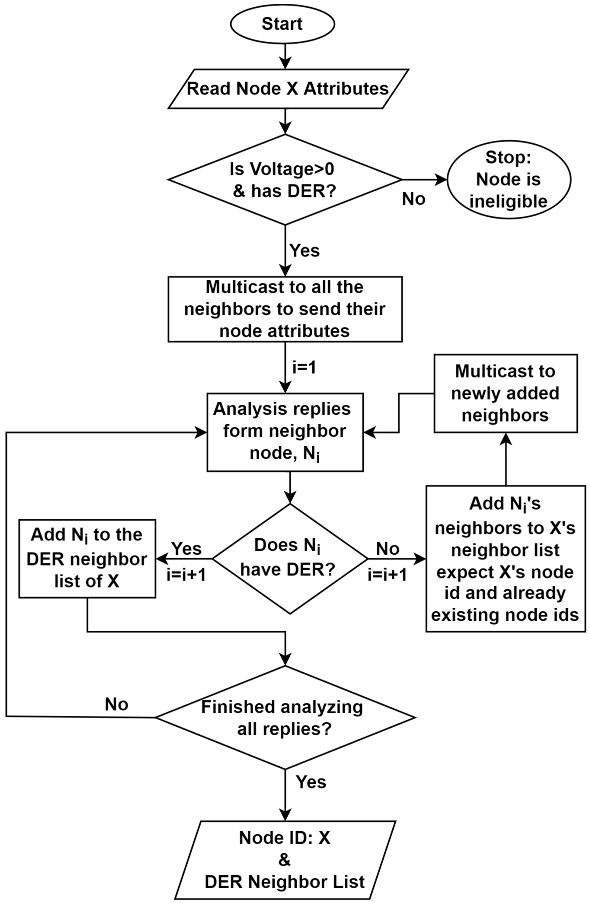
Start
Read Node X Attributes
Is Voltage>0 & has DER?
No
Stop: Node is ineligible
Yes
Multicast to all the neighbors to send their node attributes
i=1
Analysis replies form neighbor node, N_i
Multicast to newly added neighbors
Add N_i to the DER neighbor list of X
Yes
i=i+1
Does N_i have DER?
No
i=i+1
Add N_i's neighbors to X's neighbor list expect X's node id and already existing node ids
No
Finished analyzing all replies?
Yes
Node ID: X & DER Neighbor List

Fig. 2: Distributed Coordination Algorithm.

2) Cyber-Attacks: In this work, we have implemented two cyber attacks as described below:

- Man in the Middle (MitM): MitM attack is a cyber-attack that occurs when an attacker intercepts communication between 2 parties. The attacker may steal the information or modify the information in transit. For our work, the attack application introduces a rouge host with server and client capabilities in the Mininet network within the same local area network. For simplicity, we have placed this rouge host between links associated with the host under attack and assumed it has packet intercepting and modification capability. As a result, all communications of the host under attack go through the rouge host, and the rouge host alters the original data going via that communication channel.
- Denial-of-Service (DoS): DoS attack is a cyber-attack that occurs when an attacker prevents real users from accessing a network resource, usually in the form of flooding a network server with traffic. This will cause the server to be overwhelmed as it tries to authenticate each request that it receives. Here, we used the ‘hping3’ tool in the attack application to perform the DoS attack. This has allowed the attack application to send manipulated packets, specifically, control the size, quantity, and rate of the packets to the Mininet host under attack.

As a part of our test-bed, once the distributed coordination application provides the requisite node-ids (using the Mininet as a communication interface) to communicate with, the use-case distributed algorithm takes over. The use-case distributed application fetches data from the power system layer and shares data over the other hosts identified already through Mininet to generate suitable set-points. Finally, the set-point is sent to the OpenDSS for the next step simulation of the power system. All of these processes are coordinated by the Python wrapper.

III. Distributed Volt-VAR Control

The feedback-based distributed Volt-VAR control algorithm, utilized as a use-case to test the efficacy of the proposed test-bed, based on one of our earlier research [12], is briefly discussed in this section for completeness.

A. Power Flow Model for Three Phase Unbalanced Distribution Network

Consider a $N+1$-node multi-phase radial distribution grid with the set of nodes be denoted as $\mathcal{N} = \{0, 1...., N\}$. Given the radiality of the network, the total number of branches will be N, and the set of branches will be $\mathcal{E} \in \mathcal{N} \times \mathcal{N}$. All electrically connected neighbor nodes are included in the set $\mathcal{N}_j$ which includes node j and excludes the substation node.

In this work, branch flow models have been utilized for calculating power flow within the distribution system and are generally preferred over node injection models due to their inherent mathematical simplicity [13], [14]. While the use of Linearized Dist-Flow model for radial distribution systems has been utilized here to generate the control signal, an earlier research work presented in [15], shows that the discussed model is a good approximation on the original non-convex power flow equations for multiphase radial distribution systems. The assumptions included for linearization will be: (a) neglecting line losses and (b) node voltages are considered to be balanced (phase voltage angles being 120 electrical degrees apart).

The Linearized Dist-Flow model for multiphase distribution systems, as discussed in [12], is briefly discussed here. Suppose, the voltage vector for the network be: $\widetilde{\boldsymbol{v}} = [v_1.....v_N]^T$ with $v_j = \left[\left|V_j^a\right|^2, \left|V_j^b\right|^2, \left|V_j^c\right|^2\right]^T, \forall j \in \mathcal{N}$, network-wide power injection vector 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 network-wide reactive power injection vector be: $\widetilde{\boldsymbol{Q}} = [q_1.....q_N]^T$ where $q_j = \left[q_j^a, q_j^b, q_j^c\right]^T, \forall j \in \mathcal{N}$. With the linear approximations discussed above, power flow through the branches will be linear sum of the node injections. Consequently, as discussed in [16], the voltage vector $(\widetilde{\boldsymbol{v}})$ will be dependent purely on power injection vectors $(\widetilde{\boldsymbol{P}}, \widetilde{\boldsymbol{Q}})$ and substation end voltage (v_0), and the associated expression is given in (1).

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

$\bar{Z}^P$ and $\bar{Z}^Q$ in the voltage calculation expression will be 3-ϕ impedance matrix representing the distribution network.

B. Problem Formulation

The expression shown in (1) indicates that voltage control can be achieved by the control of either active power or reactive power (VAR) injection, and the degree of controllability relies on impedance matrices. In this work, network-wide voltage control is primarily achieved by providing VAR injection set-points to DERs. In this regard, suppose, the network VAR injection vector $(\widetilde{\boldsymbol{Q}})$ can be decomposed in such a way that $\widetilde{\boldsymbol{Q}} = \widetilde{\boldsymbol{Q}}^{\boldsymbol{c}} + \widetilde{\boldsymbol{Q}}^{\boldsymbol{unc}}$, where $\widetilde{\boldsymbol{Q}}^{\boldsymbol{c}}$ is the VAR injections from controllable DERs and $\widetilde{\boldsymbol{Q}}^{\boldsymbol{unc}}$ is the VAR injection vector comprising of the demand of all types of loads present within the system. Therefore, (1) can now be simplified as (2a)-(2b). Here, $\widetilde{\boldsymbol{v}}^{\boldsymbol{unc}}$ represents the voltage vector dependent on uncontrollable reactive power and active power injections throughout the network.

$$\widetilde{\boldsymbol{v}} = \bar{Z}^Q \widetilde{\boldsymbol{Q}}^{\boldsymbol{c}} + \widetilde{\boldsymbol{v}}^{\boldsymbol{unc}} \tag{2a}$$

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

C. Feedback Based Control Approach

$\widetilde{\boldsymbol{v}}^{\boldsymbol{unc}}$ in the earlier expression relies on network-wide system-parameters, which although can be directly measurable, is not intended as a part of the distributed approach. To circumvent this issue, we utilize a feedback-based control approach, where, $\widetilde{\boldsymbol{v}}^{\boldsymbol{unc}}$ is indirectly measured from the system itself. This approach serves two important benefits: (i) each nodes can independently estimate $\widetilde{\boldsymbol{v}}^{\boldsymbol{unc}}$ from the system itself, allowing us to develop a distributed controller, and (ii) imperfection in the calculated voltages with the use of linearized controller gets compensated. Let us rewrite (2a) for the time instant, t, with voltage vector be $\widetilde{\boldsymbol{v}}\,(\boldsymbol{t})$, and controllable VAR injection vector $\widetilde{\boldsymbol{Q}}\,(\boldsymbol{t})$.

$$\widetilde{\boldsymbol{v}}\,(\boldsymbol{t}) = \bar{Z}^Q \widetilde{\boldsymbol{Q}}\,(\boldsymbol{t}) + \widetilde{\boldsymbol{v}}^{\boldsymbol{unc}}\,(\boldsymbol{t}) \tag{3}$$

As a part of feedback-based control approach, the controller at j^{th} node generates optimal VAR injection vector $q_j\,(t+1)$ for the next time instant $(\forall j \in \mathcal{N})$, based on the local voltage measurement $v_j(t)$. Each of the controllers, communicates and shares $\Omega_{ji}(t)$ with it's neighboring controllers to generate $q_j\,(t+1)$. In this case, while each of the nodes in the power distribution system is equipped with a controller, the controller needs to only communicate with the neighboring controller with DERs, as determined in the distributed coordination algorithm developed in Section II. A detailed description of the shared variables is explained in Section III-D.

D. Distributed Optimization for Voltage Control

Here, auxiliary variable vectors $\hat{q}_j, \xi_j, \overline{\lambda}_j, \underline{\lambda}_j$ are utilized for every node j, to facilitate calculation of the VAR-injection set-points. Given that the number of available phases at each bus can be different, with $\sigma(\Phi_j)$ number of available phases in the node j, each of the auxiliary variable vectors will be comprised of $\sigma(\Phi_j)$ elements. Detailed implementation steps of OPTDIST-VC algorithm, which is inherently distributed, as shown in [12] are presented herein for completeness.

OPTDIST-VC: At time t, each controller connected at node j $(j \in \mathcal{N})$ follows the following four implementation steps.

Step 1 (Measurement): Local voltages at all the available phases $v_j(t)$ at time instant (t) is measured.

Step 2 (Calculation of algorithm primal and auxiliary variables): The primal variable, $\hat{q}_j(t+1)$, and auxiliary variables, $\xi_j(t+1), \bar{\lambda}_j(t+1), \underline{\lambda}_j(t+1)$, are calculated as follows:

$$\hat{q}_j(t+1) = \hat{q}_j(t) - \alpha \Bigg\{ \bar{\lambda}_j(t) - \underline{\lambda}_j(t) + d\hat{q}_j(t) + \sum_{i \in \mathcal{N}_j} [\bar{Z}^Q]^{-1}_{ji} \Big[f'_i(\hat{q}_i(t)) + \mathrm{ST}^{c\bar{q}_i}_{c\underline{q}_i}(\xi_i(t) + c\hat{q}_i(t)) \Big] \Bigg\} \tag{4a}$$

$$\xi_j(t+1) = \xi_j(t) + \beta \frac{\mathrm{ST}^{c\bar{q}_j}_{c\underline{q}_j}(\xi_j(t) + c\hat{q}_j(t)) - \xi_j}{c} \tag{4b}$$

$$\bar{\lambda}_j(t+1) = [\bar{\lambda}_j(t) + \gamma(v_j(t) - \bar{v}_j)]^+ \tag{4c}$$

$$\underline{\lambda}_j(t+1) = [\underline{\lambda}_j(t) + \gamma(\underline{v}_j - v_j(t))]^+ \tag{4d}$$

here, $\mathcal{N}_j$ is the set of all neighbor nodes connected to node j ($\forall j \in \mathcal{N}$); $[\cdot]^+$ indicates projection onto the nonnegative orthant; and, α, β, γ and c are suitably tuned positive scalar hyper-parameters used in this algorithm. For any $e_1 < e_2$, the soft-thresholding function, $\mathrm{ST}^{e_2}_{e_1}(\cdot)$, can be defined as, $\mathrm{ST}^{e_2}_{e_1}(z) = \max(\min(z - e_1, 0), z - e_2)$. The matrix $[\bar{Z}^Q]^{-1}_{ji}$, is inherently block-sparse for three-phase distribution systems. Furthermore, since the matrix $[\bar{Z}^Q]^{-1}_{ji}$ possess non-zero values only for all self nodes and neighbor nodes in the radial power distribution network, VAR set-point calculation relies only on the measurement available at the neighbouring nodes. Furthermore, additional improvements made in this algorithm ensure that only the neighbouring controllers with DERs need to communicate (and the proposed distributed coordination algorithm facilitates the same). Thusly, the algorithm is distributed in nature where computation of local VAR injections at node j is dependent only on local variables and measurements, and shared variables from neighbor nodes.

Step 3 (Injection of Reactive Power): The reactive power injection at time $t+1$ as

$$q_j(t+1) = [\hat{q}_j(t+1)]^{q^u_j}_{q^l_j} \tag{5}$$

here, $[\cdot]^{q^u_j}_{q^l_j}$ indicates a projection operator onto the set $[q^l_j, q^u_j]$. Also, $[q^l_j, q^u_j]$ are the limits identifies VAR-injection capability at node j.

Step 4 (Communication): Values $f'_j(\hat{q}_j(t+1)) + \mathrm{ST}^{cq^u_j}_{cq^l_j}(\xi_j(t+1) + c\hat{q}_j(t+1))$ are sent to neighbor nodes in set $\mathcal{N}_j$. □

To summarize, following accumulation of local three phase voltage vector $(v_j(t))$ at each DER controller in **Step 1**, in **Step 2**, the DER controllers uses received $(\Omega_{ij}(t) = f'_i(\hat{q}_i) + \mathrm{ST}^{cq^u_i}_{cq^l_i}(\xi_i(t) + c\hat{q}_i(t)))$ from DER controller in node i $(\forall i \in \mathcal{N}_j)$ to compute primal variables $\hat{q}_j(t+1)$. The node j controller then computes auxiliary variables $\xi_j(t+1), \bar{\lambda}_j(t+1), \underline{\lambda}_j t+1)$. Subsequently, in **Step 3**, VAR injection (the primal variable), $\hat{q}_j(t+1)$, is projected onto the set $[q^l_j, q^u_j]$. In **Step 4**, controller in node j shares variable $(\Omega_{ji}(t+1))$ to DER controllers i $(\forall i \in \mathcal{N}_j)$. This entire process then repeats indefinitely.

IV. Test Cases and Results

A modified IEEE 13-node radial distribution system is considered as a physical layer to test the capability of the proposed cyber-power co-simulation test-bed. As we have already indicated, the cyber-layer, modeled in Mininet, also constitutes of 13 different hosts, each of which is connected to the physical nodes (e.g., cyber-layer host h692 is corresponding to physical node 692 as shown in Fig. 1). The communication network topology for the cyber-layer is given, and in this paper, it is assumed that communication network topology mimics physical network graph topology. As for the power network, we assume that the switch between nodes 671 and 692 is normally closed. Furthermore, voltage controllers like regulators and line capacitors are disconnected from the test network.

As indicated in Section II, the physical network is modeled in OpenDSS to run power-flow analysis. It provides our OPTDIST-VC algorithm with true AC voltage measurements against provided VAR-injection set-points. The performance characteristics of the algorithm is measured against static loading conditions, with all nodes are subjected to 100% loading. The simulation set-up implies that certain node voltages can fall well below the recommended lower threshold of 0.95 *pu*. The algorithm is expected to provide optimal VAR-injection set-points from DERs to maintain nodal voltages within 0.95 *pu*-1.05 *pu*. In this example case, DERs are connected at nodes 671, 684, 675, and 634.

The reactive power limits for all nodes are considered to be 0.2 *pu* ($\bar{q}_k = 0.2$, $\underline{q}_k = -0.2$) with base VA of 3000 kVA. The upper and lower nodal voltage limits are set to be 0.95 *pu* and 1.05 *pu* respectively ($\bar{v}_i = 1.05^2$, $\underline{v}_i = 0.95^2$). Parameters d, α, β and γ are set to be 1, 0.00001, 0.5 and 20 respectively. The objective is $f_i(q_i) = \frac{\eta}{s^{max}_i} q^2_i$ where $\eta = 10$ and s^{max}_i are values randomly taken between 0.5 and 1.

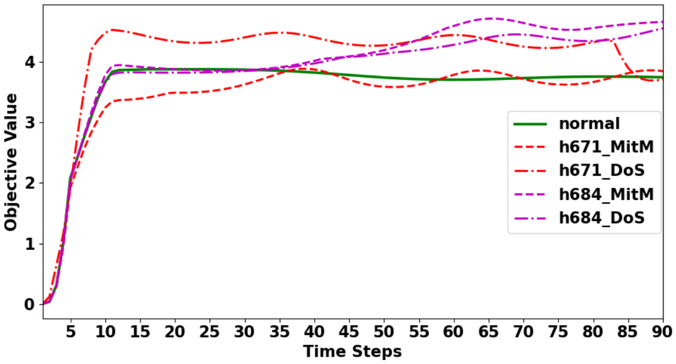

Fig. 3: Objective function during different scenarios.

Cyber-attacks like MitM and DoS are considered to study the algorithm performance under cyber vulnerabilities. Given that the attacks are generally performed in the communication layer, Mininet is used to incorporate these attacks. Given that the OPTDIST-VC algorithm relies on information obtained from neighboring DERs, cyber-attacks are performed in Step 4 (Communication round) of the use-case algorithm. Given the objective of minimizing the squared sum of VAR injections while ensuring voltages remain within limits, in a system that is heavily loaded, the objective function value quickly stabilizes to its desired value within 50-60 time steps, as is shown in Fig. 3.

In our example case, there are four scenarios: MitM in the controller at node 671, DoS in the controller at node 671, MitM in the controller at node 684, and DoS in the controller

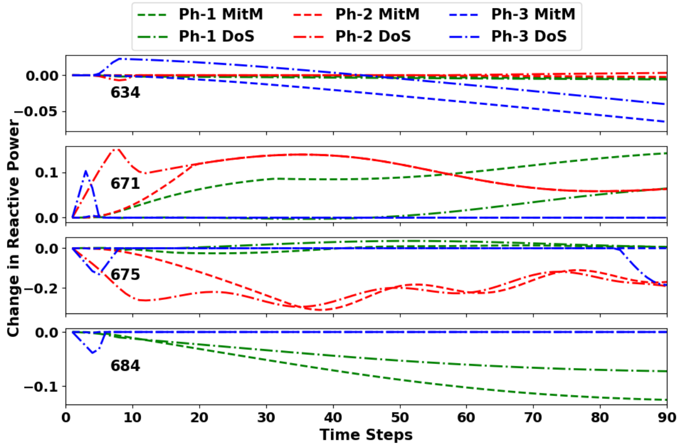

Fig. 4: Change in reactive power injection in DER nodes during different attacks at h671.

at node 684, have been considered. Out of these scenarios, deviation in VAR injections for each DERs under MitM and DoS in controller 671 are shown in Fig. 4. All the reactive power deviations are presented relative to the normal scenario or when no attack is performed. As shown in the figure, the reliance of the control algorithm on shared variables from neighboring DER controllers negatively impacts the performance of the distributed controller during cyber-attacks. Given the objective of the DoS attack to flood a host with unwanted packets, the capability of the DER controller connected to that host is significantly impeded. As shown in Figs. 3 and 4, the objective function oscillates around a new operating point. Since the MiTM attack hijacks the communication channels to a given host, the attacker can manipulate data packets; the reliance of the controller on neighbors' information for setpoint determination would not let the objective function reach the desired steady state. Needlessly, further investigation is needed to analyze observed deviation in the VAR injection in the presence of these attacks and analyze the impact at the nodal and at the system level.

V. Conclusions

This work presents a cyber-power co-simulation test-bed utilizing OpenDSS as a power network and Mininet as a cyber network, integrated with distributed coordination and cyber-attack modeling. The developed test-bed is capable of analyzing distributed control/optimization application performance during cyber-attacks and a feedback-based Volt-VAR optimization algorithm is utilized as a use-case. The test-bed fetches measurements from the power layer using COM-interface and passes the relevant data to each host running the controller using a python wrapper. Socket communication has been utilized to relay information among the hosts for coordination and solving distributed control/optimization problems. First, the distributed coordination application identifies the nodes among which the information needs to be routed, and the control/optimization application utilizes the said information for generating an appropriate signal. Once the control signal is generated, the revised control signal is routed to the power layer using the COM interface. Subsequently, the power network solves a three-phase power flow algorithm to generate the next set of measurements for the distributed control/optimization, making the test-bed quasi-static. Two cyber-attack scenarios, MitM, and DoS, have been modeled to analyze the performance of the utilized use-case. While our text examples show that the algorithm is unable to maintain the reactive power profile in the event of an attack, the possibility of dividing the network into subsystems in the event of an attack and disabling VAR injection from the controller at the infected host would ensure better performance than a centralized controller. Furthermore, the test-bed can be utilized to analyze the robustness of any distributed control/optimization algorithms in the event of cyber-attacks and how it performs compared to the centralized control.

References

[1] 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.

[2] M. Manbachi, A. Sadu, H. Farhangi, A. Monti, A. Palizban, F. Ponci, and S. Arzanpour, "Real-time co-simulation platform for smart grid volt-var optimization using iec 61850," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 4, pp. 1392–1402, 2016.

[3] 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.

[4] R. Sadnan, N. Gray, A. Dubey, and A. Bose, "Distributed optimization for power distribution systems with cyber-physical co-simulation," in *2021 IEEE Power Energy Society General Meeting (PESGM)*, 2021, pp. 1–5.

[5] V. V. G. Krishnan, S. Gopal, Z. Nie, and A. Srivastava, "Cyber-power testbed for distributed monitoring and control," in *2018 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, 2018, pp. 1–6.

[6] L. Ortmann, A. Prostejovsky, K. Heussen, and S. Bolognani, "Fully distributed peer-to-peer optimal voltage control with minimal model requirements," *Electric Power Systems Research*, vol. 189, p. 106717, 2020.

[7] L. Bottaccioli, A. Estebsari, E. Pons, E. Bompard, E. Macii, E. Patti, and A. Acquaviva, "A flexible distributed infrastructure for real-time cosimulations in smart grids," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3265–3274, 2017.

[8] 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.

[9] D. S. Schiera, L. Barbierato, A. Lanzini, R. Borchiellini, E. Pons, E. Bompard, E. Patti, E. Macii, and L. Bottaccioli, "A distributed multimodel platform to cosimulate multienergy systems in smart buildings," *IEEE Transactions on Industry Applications*, vol. 57, no. 5, pp. 4428–4440, 2021.

[10] B. Lantz and B. O'Connor, "A mininet-based virtual testbed for distributed sdn development," *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 4, pp. 365–366, 2015.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.