Resilient Cooperative Voltage Control for Distribution Network with High Penetration Distributed Energy Resources

Azwirman Gusrialdi, Ying Xu, Zhihua Qu, and Marwan A. Simaan

***Abstract*— This paper considers the problem of designing a resilient distributed voltage control algorithm for distribution systems with high penetration of distributed energy resources in the presence of an unknown cyber-attack. The purpose of the attack is to force the system to violate the operating voltage limit by intercepting its communication channels and inserting exogenous signals to perturb and/or modify the information being exchanged. We first review the cooperative voltage control proposed in our previous work and provide a new stability analysis for it. Next, we present a resilient cooperative voltage control algorithm by introducing a virtual system interconnected with the original system such that the voltage can be maintained within the operational limit under unknown attacks. The resiliency of the proposed algorithm is demonstrated via simulations on the IEEE 8500-node system when subjected to an attack which consists of corrupting the data being exchanged in the communication network between two generation units.**

***Index Terms*— Voltage control, cooperative control, cyber attacks, resilient control, distribution network**

I. Introduction

The increasing number of controllable devices in high-penetration energy distribution networks and smart grids requires the application of distributed optimization and control algorithms in coordinating the operation of these devices. In contrast with centralized algorithms, where all data and computations are performed at a control center, computations in distributed algorithms are performed by agents locally and the resulting information is exchanged via a communication network to enable each agent to compute its own decisions variables. Distributed algorithms for optimization and control have several potential advantages over centralized algorithms including scalability to system's size, robustness with respect to failure of individual agents, robust state estimation, and preservation of data privacy [1]–[3]. In this paper, we focus on a distributed algorithm for optimization and control of voltage regulation in distribution energy networks. Distributed voltage control has attracted significant research interest in the literature (see for example the work in [4]–[10].

A. Gusrialdi is with Faculty of Engineering and Natural Sciences, Tampere University, Tampere 33014, Finland. Y. Xu, Z. Qu, and M. A. Simaan are with Department of Electrical and Computer Engineering, University of Central Florida, Orlando 32816, USA. Emails: *azwirman.gusrialdi@tuni.fi*, *ying.xu@ucf.edu*, *qu@ucf.edu*, and *simaan@ucf.edu*. This work is supported in part by US National Science Foundation under grants ECCS-1308928 and ECCS-1927994, by US Department of Energy's awards DE-EE0006340, DE-EE0007327 and DE-EE0007998, by US Department of Transportation's award DTRT13-G-UTC51, by Siemens Digital Grid and Building Technology grants, by Leidos contract P010161530, and by Texas Instruments grants.

The increased penetration of distributed energy resources (DERs) in energy systems over time provides an immense opportunity for improving the overall performance of the system. In particular, the potential significant role that reactive power produced by DERs plays in improving the voltage regulation's performance, increases the capacity of distribution networks for renewable energy resources.

While the information and communication technology (ICT) facilitates the implementation of distributed control algorithms, it is known that ICT is vulnerable to cyber-intrusions. A cyber attack on a power network may cause considerable damage due to the tight coupling between the physical and cyber (communication) layers. A real-world example of a cyber-attack on a power system is the most recent attack on the Ukraine power grid in December 2015. This attack was synchronized and coordinated causing a 6-hour blackout and affecting hundreds of thousands of customers [11]. Recent survey papers on different attack scenarios and defense strategies in smart power grids can be found in [12] and [13]. Cyber-attacks on voltage regulation may cause voltage violation, real power curtailments and economic losses. The analysis and impact of cyber-attacks on voltage regulation of future smart power distribution systems are investigated in [14]–[19]. Due to the impact that cyber-attacks can have on the operation of power systems, several papers have proposed methods to detect cyber attacks on voltage regulation in distribution system (see for example [20] and [21]). In all of these approaches, one issue that needs to be considered is that the stability of the system may already have been compromised before the attack is detected. Given that, in general, cyber-attacks cannot be foreseen in advance, it is therefore desirable to design distributed control algorithms so that the overall system becomes resilient against unknown attacks. Such algorithms which are capable of maintaining or restoring systems performance under unexpected events are commonly referred to as resilient control algorithms. The authors in [22] propose a trust-based resilient cooperative control (by removing/neglecting compromised data) to mitigate the adverse effects of attacks due to hijacking the communication links and controller in DC microgrids. However, the proposed method requires that the maximum number of converters and communication links being attacked be less than a certain threshold. Moreover, in [23] the authors propose an ad-hoc method of self-organizing communication architecture to mitigate the impact of denial-of-service attack on voltage control. In this paper, we first review the cooperative voltage control algorithm proposed in our previous work [5] and

present a new associated stability analysis. In comparison to the original analysis in [5], the new stability analysis does not require linearization and facilitates the design of resilient control algorithm. Next, we propose a resilient cooperative voltage control algorithm by introducing a virtual system interconnected with the original system such that the voltage can be maintained within the operational limit under unknown attacks. The virtual system can be realized using the software-defined networking technology. Furthermore, in comparison to the state-of-the-art, the algorithm proposed in this paper does not require any assumptions on the maximum number of communication links being attacked.

The paper is organized as follows. The cooperative voltage control problem proposed in our previous work is reviewed and reformulated in the presence of an unknown attack in Section II. A new stability proof that does not require linearization is presented in Section III. The proposed resilient cooperative voltage control algorithm is presented and discussed in Section IV and evaluated using the IEEE 8500-node system in Section V. Concluding remarks are presented in Section VI.

II. Problem Formulation

In this section, we first describe the models of distribution network together with distributed generations (DGs) and communication network topology. Next, we review the cooperative control algorithm developed in our previous work [5] and discuss a scenario in which the cooperative system is subjected to external (unknown) attacks.

A. Distribution Network, DGs and Their Communication

Consider a distribution network consisting of n number of distributed generations. The bus injection power flow equation in general is given as follows:

$$P_{g_i} - P_{d_i} = V_i \sum_k V_k (G_{ik} \cos\theta_{ik} - B_{ik} \sin\theta_{ik}), \quad (1a)$$

$$Q_{g_i} - Q_{d_i} = V_i \sum_k V_k (G_{ik} \sin\theta_{ik} + B_{ik} \cos\theta_{ik}), \quad (1b)$$

where P_{g_i} (resp. Q_{g_i}) and P_{d_i} (resp. Q_{d_i}) are real (resp. reactive) power generation and consumption on the ith node, respectively; $G_{ik} \geq$ and $B_{ik} \geq$ are real and imaginary parts of the system admittance matrix entries; V_i is the voltage at node i; and θ_{ik} is the phase difference between nodes i and k. A useful property of B_{ii} is $B_{ii} = -\sum_{k\neq i} B_{ik} < 0$. In addition, lets introduce the following property which holds in practice for power system and is used in the analysis of the proposed control.

Property 1: For an adequately designed power system, the following inequality holds: for $Q_i = Q_{g_i} - Q_{d_i}$,

$$Q_i < \frac{-V_i^2 B_{ii}}{3}. \quad (2)$$

Proof: In order to ensure both the system voltage and reactive power strength performance, the net power injection at bus i is always limited to be less than $1/3$ of the short circuit power S_{sc_i} as demanded by NERC regulations [24]. The short circuit power S_{sc_i} is defined as

$$S_{sc_i} = V_i^2 / Z_{Th_i},$$

where Z_{Th_i} is the Thevenin impedance. Given that $Q_i < S_{sc_i}/3$ and that the impedance satisfies the property of $1/Z_{Th_i} \leq -B_{ii}$, inequality (2) is obtained. ■

The power injection from the ith DG, i.e. P_{G_i} and Q_{G_i}, are generally determined by decoupled $d-q$ controls via phase locked loops. Since the active power control can be set by dispatch reference or certain curtailment strategy (which is not the focus of this work), the power injection P_{G_i} will be treated in this paper as a given reference. The reactive power generation Q_{g_i} is modeled by the following equations [25]:

$$Q_{g_i} = V_i I_{q_i}, \quad \dot{I}_{q_i} = u_i, \quad (3)$$

where

$$|Q_{g_i}| \leq \overline{Q}_{G_i}. \quad (4)$$

In the above, I_{q_i} is the output current in q-axis, u_i is the DG reactive power control input to be designed, S_{G_i} is its inverter capacity, and $\overline{Q}_{G_i} = \sqrt{S_{G_i}^2 - P_{g_i}^2} > 0$ is the maximum available reactive power at the DG. In practice, the dynamics (3) is very fast compared to cooperative control to be designed, and thus can be neglected in the subsequent analysis.

Finally, the communication network topology of the DGs can be modeled by a graph whose nodes represent the local controller of DGs and whose edges represent the communication links. Let $\mathcal{N}_i$ denote the neighboring set of node i. In other words, node $j \in \mathcal{N}_i$ if node i can receive information from node j. In this paper, it is assumed that the communication network topology is given by an *undirected* graph, that is $i \in \mathcal{N}_j \Leftrightarrow j \in \mathcal{N}_i$, see the example in Fig. 1. Moreover, the undirected graph is assumed to be *connected*, i.e., there is no isolated nodes in the network [26].

B. Cooperative voltage control and potential cyber-attacks

In this paper, we focus on the voltage control problem whose goal is to control the reactive power of DGs in a distributed manner such that the voltage deviation of all DG buses are well regulated within a certain limit, that is, V_i satisfies the operational constraint of

$$|1 - V_i| \leq 0.05 \; p.u. \quad (5)$$

in order to ensure power quality. To this end, we formulate the above objective as the following real-time optimization problem [5]:

$$\min_{Q_{g_1},\cdots,Q_{g_n}} F_v, \quad (6)$$

where F_v is defined as, for some $V_i^* \in (0.95,\ 1.05)$,

$$F_v = \sum_{i=1}^n f_{v_i} = \sum_{i=1}^n (V_i - V_i^*)^2. \quad (7)$$

Note that optimization (6) need only be performed for the buses with DGs due to two reasons. First, given that the initial operating condition (voltage) of power system is

within its limit, optimizing the voltages at the DG nodes also yields appropriate regulation of the voltages at the remaining nodes (without DGs). Second, the DGs can also be placed in a way so that the performance (voltage) of the overall system is within the limit given that (6) is optimized.

In addition to minimizing (7), we would like to see reactive power load sharing in the sense that all the DGs contribute equally. In other words, the so-called utilization ratio of reactive power, defined as state variable x_i as in [5],

$$x_i = Q_{g_i}/\overline{Q}_{G_i} \tag{8}$$

should reach a consensus. That is, our control objective is to achieve a fair (uniform) utilization ratio given by

$$x_1 = \cdots = x_n. \tag{9}$$

Given that the total maximum available reactive power of the DGs is sufficient to regulate the voltages, there exists a consensus solution (9), denoted by $x^* = [x_1^*, \cdots, x_n^*]^T = c^*\mathbf{1}$, to the optimization problem (7). As proposed in [5], an adaptive and distributed control solution can be chosen to be the following subgradient-based cooperative control:

$$\dot{x}_i = \sum_{j\in N_i} s_{ij}(x_j - x_i) - k_i g_i(x_i), \tag{10}$$

where $s_{ij} = 1$ if $j \in \mathcal{N}_i$ and $s_{ij} = 0$ if otherwise. Scalar $k_i > 0$ is a step size gain and g_i is the subgradient of f_{v_i} w.r.t. x_i, that is $g_i(x_i) = \partial f_{v_i}/\partial x_i$. Specifically, the subgradient g_i can be calculated from (7), (1b) and is given by [5]

$$g_i(x_i) = \frac{\partial f_{v_i}}{\partial V_i}\frac{\partial V_i}{\partial Q_{g_i}}\frac{\partial Q_{g_i}}{\partial x_i} = \frac{\overline{Q}_{g_i}(V_i - V_i^*)V_i}{Q_i - V_i^2 B_{ii}}. \tag{11}$$

The first term in (10) is designed so that x_i reach consensus for all DGs (i.e., satisfying (9)), and the second term is designed to minimize (7). It should be noted that V_i^* can be found distributively through a distributed optimal power flow solution similar to that in [4]; alternatively, we can choose $V_i^* = 1$ for simplicity and, in control implementation, set $k_i = 0$ once $|V_i - 1|$ becomes less than any chosen small threshold. Defining $x = [x_1, \cdots, x_n]^T$, $K = \text{diag}\{k_i\}$ and $g(x) = [g_1(x_1), \cdots, g_n(x_n)]^T$, we can write (10) for all the DGs in a compact form as

$$\dot{x} = -Lx - Kg, \tag{12}$$

where $L \geq 0$ is a Laplacian matrix whose entries are defined as $[L]_{ii} = \sum_{j\neq i} s_{ij}$ and $[L]_{ij} = -s_{ij}$. In addition, we have $L\mathbf{1}_n = 0$ where the vector $\mathbf{1}_n$ denotes a vector of length n whose entries are all ones. Hence, the eigenvalues of L are given by $0 = \lambda_1(L) < \lambda_2(L) \leq \cdots \leq \lambda_n(L)$.

Since it is not always possible to ensure that all communication networks/channels are secure, the system may be subject to attack. Specifically, in this paper we consider a cyber attack where the attacker distorts the communication channels by adding exogenous signals to modify the neighbors' information that a specific node receives, see Fig. 1. Hence, cooperative control (12) under potential attacks can then be written as

$$\dot{x} = -L(x - d) - Kg \tag{13}$$

where $d \in \mathbb{R}^n$ denotes the attack vector. Furthermore, it is assumed that the adversary inserts a bounded injection, that is, $\|d\|$ and $\|\dot{d}\|$ are both bounded, as considered in the literature, e.g., in [27]. This assumption is reasonable for the following two reasons. From the attacker's perspective, an intelligent attacker would aim at destabilizing the system (e.g., to steer its operating point away from the optimal value) with a limited change to avoid any detection. On the other hand, from the defender's perspective, an injection of unbounded magnitude can be easily rejected by a threshold check as discussed in [28]. Other than injections being bounded, there is no other assumption on injection d, including no restriction on the number of communication links that are attacked. There are many choices of d which make the voltages violate the operational constraints in (5), as will be demonstrated later in Section V-B. Therefore, the objective of this paper is to develop a network enabled defense mechanism for the cooperative system so that attacked system (13) remains to operate close to its optimal utilization ratio x^* under all possible attacks d.

Although the proposed cooperative voltage control contains a consensus term, the existing results on resilient consensus algorithms do not apply to system (13) since they are not designed to solve the optimization problem (7). Recently, distributed optimization under adversarial nodes is considered, where the mitigation of adversarial behavior is only guaranteed for the nonadversarial nodes under certain assumptions on network topology. In contrast to [29], the proposed design aims to guarantee resilient operation of all DG buses under unknown cyber attacks.

III. Cooperative Voltage Control: Revisited

It is shown in [5] that the state x in (12) converges to the optimal solution $x^* = c^*\mathbf{1}$. However, $V_i^* = 1$ for all i may not be realistic, and the proof in [5] is done using the eigenvalue analysis on the resulting linear dynamics from linearizing both subgradient term and power flow equation (1b). Furthermore, the previous analysis is performed for discrete-time system. In this section, we present an nonlinear proof which is based on Lyapunov stability analysis, does not involve any linearization, and in turn facilitates the analysis of resilient cooperative control in Section IV. To this end, the following result on convexity of f_{v_i} with respect to x_i is first introduced, and it plays an important role in concluding the stability analysis in the proof of theorem 1.

Lemma 1: For power systems satisfying Property 1, objective function f_{v_i} in (7) is strictly convex with respect to utilization ratio x_i, and $g_i(x_i)$ is uniformly bounded.

Proof: To prove that f_{v_i} is strictly convex with respect to x_i, we just need to show that $\partial^2 f_{v_i}/\partial x_i^2 > 0$. It follows that

$$\frac{\partial^2 f_{v_i}}{\partial x_i^2} = \frac{\partial g_i}{\partial x_i} = \frac{\partial g_i}{\partial V_i}\frac{\partial V_i}{\partial Q_{g_i}}\frac{\partial Q_{g_i}}{\partial x_i}.$$

It is clear that $\partial Q_{g_i}/\partial x_i > 0$. Next, we know from (2) that $|Q_i| < |V_i^2 B_{ii}|/3$ and thus $\partial V_i/\partial Q_{g_i} = V_i/(Q_i - V_i^2 B_{ii}) > 0$. Similarly, $\partial g_i/\partial V_i$ can also be evaluated as

$$\frac{\partial g_i}{\partial V_i} = \frac{\overline{Q}_{G_i}}{(Q_i - V_i^2 B_{ii})^2}[(2V_i - V_i^*)Q_i - V_i^2 B_{ii}].$$

When $0.95 \leq V_i < 1$ and since $|Q_i| < |V_i^2 B_{ii}|/3$ we have $(2V_i - V_i^*)Q_i - V_i^2 B_{ii} > 0$. Moreover, when $1 \leq V_i \leq 1.05$ and since $|Q_i| < |V_i^2 B_{ii}|/3$ we also have $(2V_i - V_i^*)Q_i - V_i^2 B_{ii} > 0$. Hence, it can be concluded that $g_i(x_i)$ defined in (11) is uniformly bounded and that $\partial^2 f_{v_i}/\partial x_i^2 = \partial g_i/\partial x_i > 0$ and thus function f_{v_i} is strictly convex with respect to x_i. ■

Theorem 1: The point $x^* = c^* \mathbf{1}_n$ is the unique equilibrium of (12) and is asymptotically stable.

Proof: It is well known [30] that for a strictly convex function $f : \mathbb{R}^N \to \mathbb{R}$, the following inequality holds for any $x, y \in \mathbb{R}^N$

$$(\nabla f(x) - \nabla f(y))^T (x - y) > 0 \tag{14}$$

where $\nabla f : \mathbb{R}^N \to \mathbb{R}^N$ denotes the gradient of f. Hence, we know from lemma 1 that

$$(g_i(x_i) - g_i(c^*))(x_i - c^*) > 0, \tag{15}$$

where c^* is the consensus equilibrium of x_i that yields solutions V_i^* to load flow equation (1b). Therefore, we know that subgradients have the property of $g_i(c^*) = 0$ and $g(x^*) = 0$. It follows from the property of Laplacian matrix $L\mathbf{1}_n = 0$ and from x^* being the optimal point that x^* is an equilibrium of (12), that is,

$$-L\mathbf{1}_n c^* - Kg(x^*) = 0.$$

Next, let us define the error state $\tilde{x} = x - x^*$. It follows that the error dynamics are

$$\dot{\tilde{x}} = -L\tilde{x} - K(g(x) - g(x^*)).$$

Taking the derivative of positive definite (p.d.) Lyapunov function $V = \|\tilde{x}\|^2/2$ results in

$$\begin{aligned}\dot{V} &= \tilde{x}^T(-L\tilde{x} - K(g(x) - g(x^*))) \\ &= -\tilde{x}^T L\tilde{x} - \sum_{i=1}^{n} \left[\underbrace{k_i(g_i(x_i) - g_i(x_i^*))(x_i - x_i^*)}_{\text{is p.d. from (15)}} \right] < 0\end{aligned}$$

Since $\dot{V} < 0$, then $\tilde{x} \to 0$ and thus $x \to x^*$, which completes the proof. ■

IV. Resilient Cooperative Voltage Control

In order to make cooperative voltage control (10) resilient against attacks, we adopt and extend the approach proposed in our previous work [28], [31], [32]. Specifically, a virtual system is introduced whose number of nodes is equal to n and interconnected with the cooperative control (i.e., local controller of the DGs) as illustrated in Fig. 1. The virtual system can be realized by using a cloud computing/communication in combination with software-defined networking [33], and its steady state is independent of the physical system during normal operations. The interconnection of cooperative system under potential attacks and the virtual system is given by:

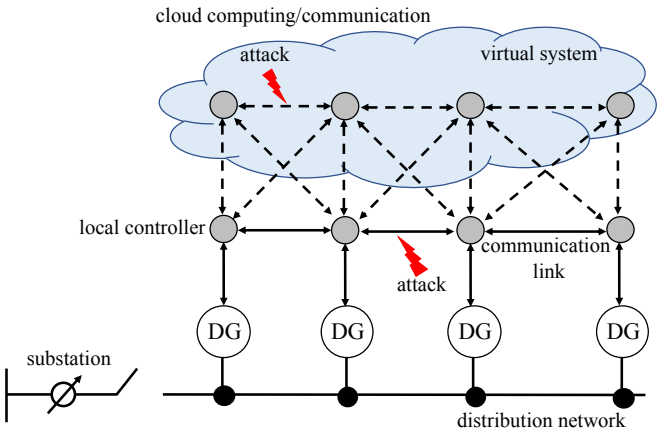

Fig. 1: Resilient cooperative control via a virtual network: dashed lines — auxiliary information flow within the virtual network; solid lines — information flow for the physical network.

$$\begin{aligned}\dot{x} &= -L(x - d) - \beta Kg + \beta Hz \\ \dot{z} &= -L_h z - \beta Gx\end{aligned} \tag{16}$$

where $z \in \mathbb{R}^n$ denotes the state of the virtual system, scalar $\beta > 0$ is the control gain, matrix L_h is the Laplacian matrix corresponding to the hidden network, and H and G are the interconnection matrices. Here, β, L_h, H, G will be designed such that stability of the overall system (16) is guaranteed, and state x converges to the neighborhood of x^* under unknown attack d, while virtual state z converges to its own equilibrium z^* or its neighborhood. Specifically, let us choose the matrices L_h, H, G in (16) as

$$L_h = H = G = P\Lambda^{\frac{1}{2}}P^T. \tag{17}$$

where $\Lambda = \text{diag}(0, \lambda_2(L), \cdots, \lambda_n(L))$, $P = [v_1, \cdots, v_n]$, and v_i denotes the eigenvector of L associated with eigenvalue $\lambda_i(L)$ (that is, $L = P\Lambda P^T$). Then, we have the following theorem.

Theorem 2: Let matrices L_h, H, G in (16) be chosen according to (17). For any sufficiently large value of $\beta > 0$, the state x in (16) asymptotically converges to a small neighborhood of $c\mathbf{1}$ under all bounded injection vectors of d. Furthermore, once x converges to $c\mathbf{1}$ for a sufficiently large $\beta > 0$, then $x \to x^*$.

Proof: First, it can be observed that L_h is a symmetric matrix and $L_h\mathbf{1}_n = 0$. Let us define the error states $\tilde{x} = x - x^e$, $\tilde{z} = z - z^e$, and $\tilde{d} = d - d^e$, where $x^e = [x_1^e, \cdots, x_n^e]^T$, z^e, and d^e denote the equilibria of system (16), respectively;

that is, the error system becomes

$$\begin{aligned}\dot{\tilde{x}} &= -L(\tilde{x}-\tilde{d}) - \beta K[g(x)-g(x^e)] + \beta L_h\tilde{z}\\ \dot{\tilde{z}} &= -L_h\tilde{z} - \beta L_h\tilde{x}.\end{aligned} \tag{18}$$

Next, consider the following Lyapunov function

$$V = \beta\|\tilde{x}\|^2 + \beta\|\tilde{z}\|^2 + 2\tilde{z}^T L_h\tilde{d}. \tag{19}$$

Taking the derivative of V along (18) and noting that $L_hL_h = L$ yield

$$\begin{aligned}\dot{V} &= -2\beta\tilde{x}^TL\tilde{x} + 2\beta\tilde{x}^TL\tilde{d} + 2\beta^2\tilde{x}^TL_h\tilde{z} - 2\beta\tilde{z}^TL_h\tilde{z}\\ &\quad -2\beta^2\tilde{x}^TK[g(x)-g(x^e)] - 2\beta^2\tilde{z}^TL_h\tilde{x}\\ &\quad +2\tilde{z}^TL_h\dot{\tilde{d}} - 2\tilde{z}^TL_hL_h\tilde{d} - 2\beta\tilde{x}^TL_hL_h\tilde{d}\\ &= -2\beta\tilde{x}^TL\tilde{x} + 2\beta\cancel{\tilde{x}^TL\tilde{d}} + 2\beta^2\cancel{\tilde{x}^TL_h\tilde{z}} - 2\beta\tilde{z}^TL_h\tilde{z}\\ &\quad -2\beta^2\sum_{i=1}^{n}[k_i(g_i(x_i)-g_i(x_i^e))(x_i-x_i^e)]\\ &\quad -2\beta^2\cancel{\tilde{z}^TL_h\tilde{x}} + 2\tilde{z}^TL_h\dot{\tilde{d}} - 2\tilde{z}^TL_hL_h\tilde{d}\\ &\quad -2\beta\cancel{\tilde{x}^TL\tilde{d}}.\end{aligned} \tag{20}$$

It follows from strict convexity that term $k_i(g_i(x_i) - g_i(x_i^e))(x_i - x_i^e) > 0$ when $x_i \neq x_i^e$ [30], hence the quadratic terms in $\dot{V}$ are negative definite with respect to $\tilde{x}$ and negative semi-definite with respect $\tilde{z}$. Moreover, term $-2\beta\tilde{z}^TL_h\tilde{z}$ is zero if and only if $\tilde{z} = \bar{c}\mathbf{1}$ which also implies the terms $2\tilde{z}^TL_h\dot{\tilde{d}}$ and $2\tilde{z}^TL_hL_h\tilde{d}$ are zero. Therefore, the above expression of $\dot{V}$ implies both $\tilde{x}$ and $\tilde{z}$ are uniformly bounded for any unknown but bounded injections d. Since the cross-product terms are independent of β, the ultimate bounds on $\tilde{x}$ and $\tilde{z}$ become small as β increases.

The next step is to prove that x^e converges to $c\mathbf{1}$ as the value of β increases. At the steady state of (16), we have

$$\begin{aligned}0 &= -L(x^e-d^e) - \beta Kg(x^e) + \beta L_hz^e,\\ 0 &= -L_hz^e - \beta L_hx^e.\end{aligned}$$

Eliminating L_hz^e yields

$$(L_h + \beta^2 I)L_hx^e = Ld^e - \beta Kg(x^e), \tag{21}$$

which yields

$$L_hx^e = (L_h+\beta^2I)^{-1}[Ld^e - \beta Kg(x^e)].$$

Recalling from lemma 1 that $g(\cdot)$ is uniformly bounded, we know from the above equation that $L_hx^e \to 0$ or equivalently $x^e \to c\mathbf{1}$ as β increases.

The final step shows that, if $x^e = c\mathbf{1}$ for sufficiently large $\beta > 0$, then $x^e = x^*$. This can be seen from (21) since, if $x^e = c\mathbf{1}$,

$$g(x^e) = -\frac{1}{\beta}K^{-1}Ld^e,$$

which yields $c \to c^*$ or $x^e \to x^*$ due to the unique optimum under strict convexity. This completes the proof. ∎

As its name suggests, the virtual nodes are not physical and the state of the virtual system has no physical meaning which makes it less meaningful to an attacker or difficult for the attacker to associate the information flow with measurements of physical variables exchanged among the DGs. While the addition of such a virtual system incurs an additional cost of increased communication, such a burden is manageable and the corresponding computational is minimal since both the communication and computation are performed distributively and using one of the standard network technologies.

Next, we consider the case that the virtual system is also subject to attacks. In this case, the interconnected system with matrices L_h, H, G chosen as in (17) is expressed as

$$\begin{aligned}\dot{x} &= -L(x-d) - \beta Kg + \beta L_hz,\\ \dot{z} &= -L_h(z-d') - \beta L_hx,\end{aligned} \tag{22}$$

where $\|d'\|, \|\dot{d'}\|$ are also uniformly bounded.The following theorem provides the stability result.

Theorem 3: Consider (22) in which matrices L_h, H, G are chosen according to (17). For any positive value of β, the state x in (22) is unformly bounded under all bounded injections d and d'.

Proof: Analogous to the proof of theorem 2, the error dynamics of interconnected system (22) can be written as

$$\begin{aligned}\dot{\tilde{x}} &= -L(\tilde{x}-\tilde{d}) - \beta K[g(x)-g(x^e)] + \beta L_h\tilde{z},\\ \dot{\tilde{z}} &= -L_h(\tilde{z}-\tilde{d'}) - \beta L_h\tilde{x}.\end{aligned} \tag{23}$$

where $\tilde{d'} = d' - d'^e$. Choosing Lyapunov function (19), we know from (20) that the time derivative of V along (23) is

$$\begin{aligned}\dot{V} &= -2\beta\tilde{x}^TL\tilde{x} - 2\beta\tilde{z}^TL_h\tilde{z} - 2\beta^2\underbrace{\tilde{x}^TK[g(x)-g(x^e)]}_{\text{p.d. w.r.t. }\tilde{x}}\\ &\quad +2\tilde{z}^TL_h\dot{\tilde{d}} - 2\tilde{z}^TL_hL_h\tilde{d} + 2\tilde{d}^TL_hL_h\tilde{d'}\\ &\quad +\beta\tilde{z}^TL_h\tilde{d'}.\end{aligned} \tag{24}$$

It is clear that the quadratic terms are negative definite with respect to $\tilde{x}$ and $L_h\tilde{z}$ and that all cross-product terms involving $\tilde{z}$ vanish if $L_h\tilde{z} = 0$. Therefore, we know that all the state variables are uniformly bounded no matter what d and d' are, as long as the attack vectors are uniformly bounded. This completes the proof. ∎

The result in theorem 3 is much weaker than those in theorem 2, and this is due to the fact that, in (24), the last cross-product term is proportional to β. In order to recover the result in theorem 2 for the case that the one-layer virtual network may be comprised, we can introduce and activate additional layer(s) of virtual networks. As did in theorem 2, asymptotic convergence to a small neighborhood of the optimal solution can be shown for multi-layer virtual networks so long as one or more layers of the network is free of attacks. That is, *deep virtual networks* provide an effective way to design resilient cooperative controls and achieve robustification of cooperative systems.

V. Simulation

The proposed resilient cooperative voltage control is demonstrated and evaluated using IEEE 8500-node system, with 100% penetration distributed evenly among 10 PVs at two branches: group 1 contains 7 PVs and group 2 contains 3

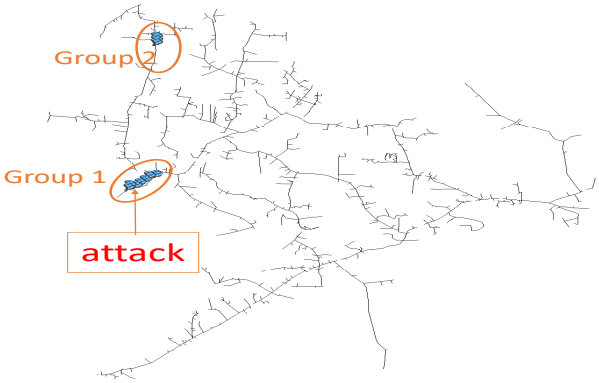

Fig. 2: IEEE 8500 system utilized in the simulation

PVs as shown in Fig. 2. We assume that only DGs in group 1 are being attacked, that is the attacker manipulates data being exchanged between the DGs over the communication network. The Laplacian matrix of the DGs in group 1 which represents the communication network topology is given by

$$L = \begin{bmatrix} 3 & -1 & 0 & 0 & 0 & -1 & -1 \\ -1 & 3 & -1 & 0 & 0 & 0 & -1 \\ 0 & -1 & 3 & -1 & 0 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ -1 & 0 & 0 & 0 & -1 & 3 & -1 \\ -1 & -1 & -1 & 0 & 0 & -1 & 4 \end{bmatrix}.$$

In order to demonstrate efficacy of the proposed strategy, we investigate the following three cases: (i) the baseline case, that is the cooperative control (12) without attacks; (ii) cooperative control under attacks given by (13); (iii) cooperative control interconnected with hidden network in the presence of attacks, as given by (16).

A. Case 1: cooperative voltage control without attacks

We set the gain K in (12) to

$$K = \text{diag}\{[0.05 \quad 0.05 \quad 0.05 \quad 0.05 \quad 0.05 \quad 0.05 \quad 0.05]\}.$$

The voltage profile and reactive power utilization ratios under (12) are shown in Fig. 3a and Fig. 3b, respectively. The results show that the system voltages are well maintained within the limit (5) using cooperative voltage control (12). Moreover, the utilization ratios of the DGs reach a consensus, that is each DG contributes equally to the voltage regulation.

B. Case 2: cooperative control under attacks but without protection

Next, we simulate a scenario where cooperative voltage control in group 1 is being attacked. The attack vector in (13) in group 1 is given by

$$d = [0,\ 0,\ 0,\ 0,\ 0,\ 0.5,\ 0]^T,$$

that is node 6 sends compromised information over local communication network to its neighbors. The Voltage profile of the DGs under such attack is shown in Fig. 4a. It can be observed that the attack yields an overvoltage problem (i.e., the voltages violate the limit in (5)) for the DGs in groups 1 and 2. Moreover, the utilization ratios of the DGs fail to reach a consensus as can be seen from Fig. 4b.

C. Case 3: resilient cooperative control in the presence of attacks

Finally, we interconnect the cooperative control with a virtual system whose overall system under potential attacks is given by (16). To this end, we set L_h, G, and H according to (17), and also we set the control gain $\beta = 8$. As can be seen from Fig. 5, by interconnecting the cooperative system with the virtual network, the voltages of the DGs can still be regulated within the limit (5) even though some of the communication links are being compromised. Moreover, utilization ratios of the DGs almost reach a consensus (i.e., close to each other).

VI. Conclusions and Future Work

In this paper, we present a resilient cooperative voltage algorithm for distribution network to ensure the voltage of the system are within the operational limit in the presence of unknown attacks. To this end, the paper considers distributed voltage control problem for distribution network with high penetration distributed energy resources in the presence of unknown attacks. The resilient cooperative voltage control algorithm is realized by introducing a virtual system (virtual network) interconnected with the cooperative system in a way such that the overall system is stable under unknown attacks. In addition, we also present a new stability proof of the cooperative voltage control proposed in our previous work. Simulations on IEEE 8500-node system verify the efficacy of the proposed algorithm to maintain the voltages within the operational limit under attacks. In the future, we aim to apply the proposed framework to other security problems in power system including the problem of frequency stability in the presence of cyber-attacks.

References

[1] D. K. Molzahn, F. Dörfler, H. Sandberg, S. H. Low, S. Chakrabarti, R. Baldick, and J. Lavaei, "A survey of distributed optimization and control algorithms for electric power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2941–2962, 2017.

[2] T. Shinohara, T. Namerikawa, and Z. Qu, "Resilient reinforcement in secure state estimation against sensor attacks with a priori information," *IEEE Transactions on Automatic Control*, p. to appear, 2019.

[3] K. E. Antoniadou-Plytaria, I. N. Kouveliotis-Lysikatos, P. S. Georgilakis, and N. D. Hatziargyriou, "Distributed and decentralized voltage control of smart distribution networks: models, methods, and future research," *IEEE Transactions on smart grid*, vol. 8, no. 6, pp. 2999–3008, 2017.

[4] Y. Liu, Z. Qu, H. Xin, and D. Gan, "Distributed real-time optimal power flow control in smart grid," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 3403–3414, 2017.

[5] A. Maknouninejad and Z. Qu, "Realizing unified microgrid voltage profile and loss minimization: A cooperative distributed optimization and control approach," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1621–1630, 2014.

[6] M. H. J. Bollen and A. Sannino, "Voltage control with inverter-based distributed generation," *IEEE Transactions on Power Delivery*, vol. 20, pp. 519–520, Jan 2005.

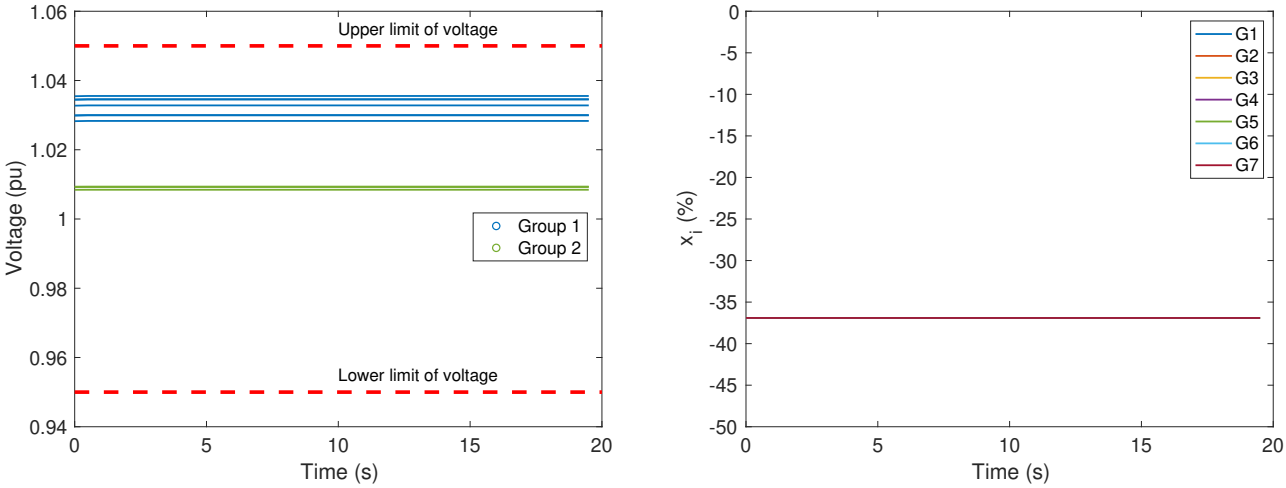

Fig. 3: Case 1: cooperative voltage control (12) without attacks. (a) Voltage profile; (b) utilization ratio x_i of DGs in Group 1.

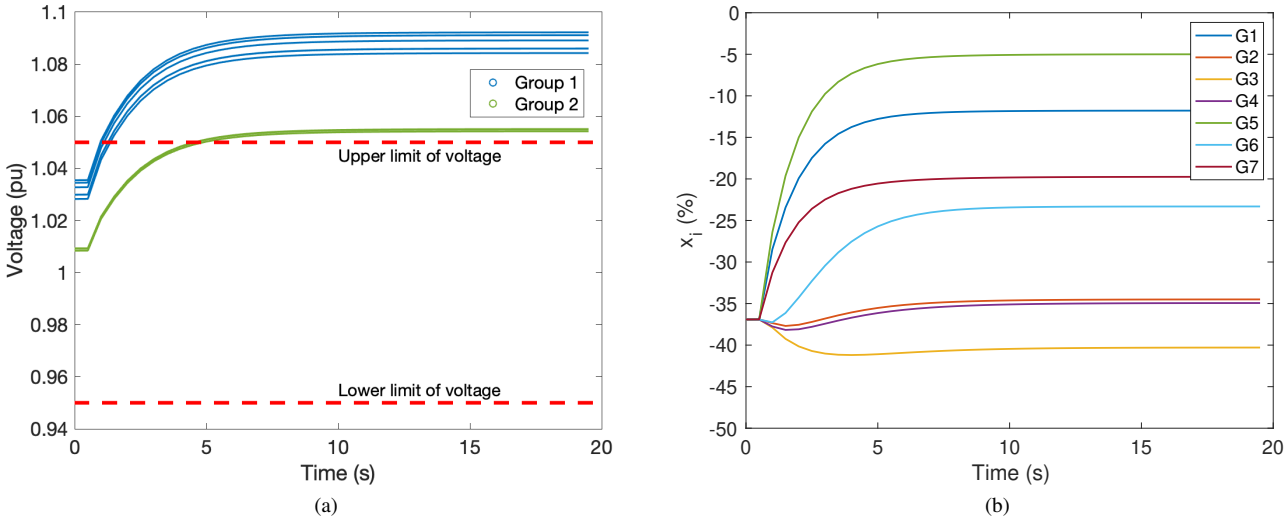

Fig. 4: Case 2: cooperative control under attacks. (a) Voltage profile; (b) utilization ratios x_i of DGs in Group 1.

[7] J. W. Simpson-Porco, Q. Shafiee, F. Dörfler, J. C. Vasquez, J. M. Guerrero, and F. Bullo, "Secondary frequency and voltage control of islanded microgrids via distributed averaging," *IEEE Transactions on Industrial Electronics*, vol. 62, pp. 7025–7038, Nov 2015.

[8] J. Schiffer, T. Seel, J. Raisch, and T. Sezi, "Voltage stability and reactive power sharing in inverter-based microgrids with consensus-based distributed voltage control," *IEEE Transactions on Control Systems Technology*, vol. 24, pp. 96–109, Jan 2016.

[9] H. Xin, Z. Qu, J. Seuss, and A. Maknouninejad, "A self organizing strategy for power flow control of photovoltaic generators in a distribution network," *IEEE Transactions on Power Systems*, vol. 26, no. 3, pp. 1462–1473, 2011.

[10] H. Li, F. Li, Y. Xu, D. T. Rizy, and J. D. Kueck, "Adaptive voltage control with distributed energy resources: Algorithm, theoretical analysis, simulation, and field test verification," *IEEE Transactions on Power Systems*, vol. 25, pp. 1638–1647, Aug 2010.

[11] T. Pultarova, "Cyber security - ukraine grid hack is wake-up call for network operators [news briefing]," *Engineering Technology*, vol. 11, pp. 12–13, February 2016.

[12] A. Gusrialdi and Z. Qu, "Smart grid security: Attacks and defenses," in *Smart Grid Control: An Overview and Research Opportunities* (J. Stoustrup, A. Annaswamy, A. Chakrabortty, and Z. Qu, eds.), pp. 199–223, Springer Verlag, 2019.

[13] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016.

[14] A. Teymouri, A. Mehrizi-Sani, and C. Liu, "Cyber security risk assessment of solar PV units with reactive power capability," in *44th Annual Conference of the IEEE Industrial Electronics Society*, pp. 2872–2877, Oct 2018.

[15] M. Ma and A. Lahmadi, "On the Impact of Synchronization Attacks on Distributed and Cooperative Control in Microgrid Systems," in *IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids*, (Aalborg, Denmark), Oct. 2018.

[16] A. Teixeira, G. Dán, H. Sandberg, R. Berthier, R. B. Bobba, and A. Valdes, "Security of smart distribution grids: Data integrity attacks on integrated volt/var control and countermeasures," in *Proceedings of American Control Conference*, pp. 4372–4378, 2014.

[17] A. Teixeira, K. Paridari, H. Sandberg, and K. H. Johansson, "Voltage control for interconnected microgrids under adversarial actions," in *IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*, pp. 1–8, 2015.

[18] Y. Liu, H. Xin, Z. Qu, and D. Gan, "An attack-resilient cooperative

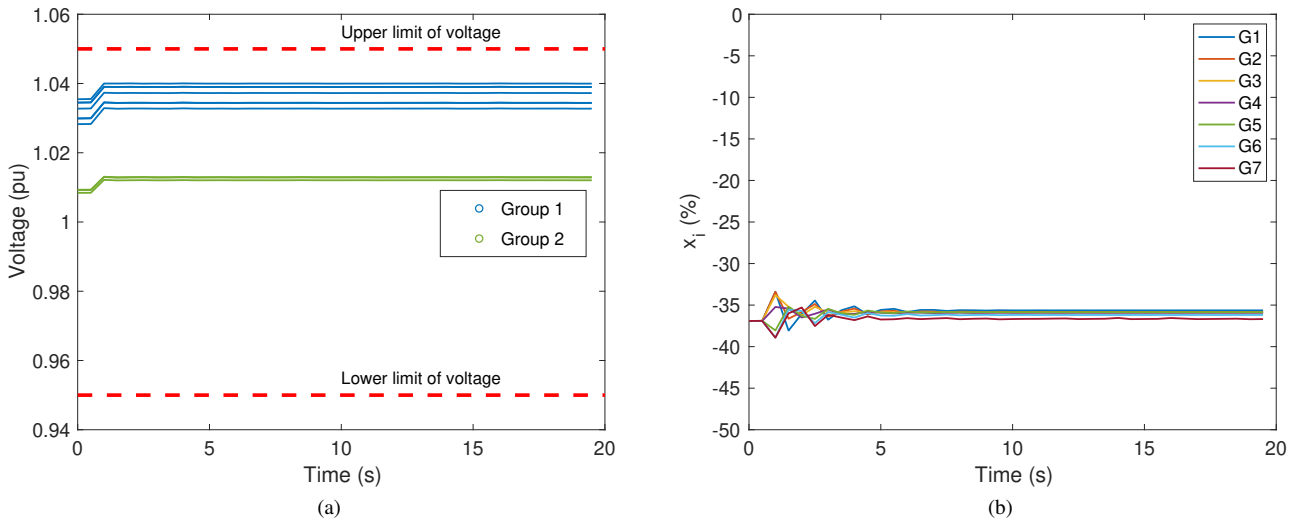

Fig. 5: Case 3: resilient cooperative voltage control against attacks. (a) Voltage profile; (b) utilization ratios x_i of DGs in Group 1.

control strategy of multiple distributed generators in distribution networks," *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2923–2932, 2016.

[19] M. Ma, A. M. Teixeira, J. van den Berg, and P. Palensky, "Voltage control in distributed generation under measurement falsification attacks," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 8379–8384, 2017.

[20] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi, "Detection of cyber attacks against voltage control in distribution power grids with PVs," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1824–1835, 2016.

[21] A. M. Kosek, "Contextual anomaly detection for cyber-physical security in smart grids based on an artificial neural network model," in *2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG)*, pp. 1–6, IEEE, 2016.

[22] S. Abhinav, H. Modares, F. L. Lewis, and A. Davoudi, "Resilient cooperative control of dc microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 1083–1085, 2019.

[23] C. Cameron, C. Patsios, P. Taylor, and Z. Pourmirza, "Using self-organizing architectures to mitigate the impacts of denial-of-service attacks on voltage control schemes," *IEEE Transactions on Smart Grid*, 2018.

[24] NERC, *Essential Reliability Services Task Force Measures Framework Report*. `https://www.nerc.com/comm/other/essntlrlbltysrvcstskfrcdl/erstf\%20framework\%20report\%20-\%20final.pdf`, November, 2015.

[25] H. Xin, Z. Lu, Z. Qu, D. Gan, and D. Qi, "Cooperative control strategy for multiple photovoltaic generators in distribution networks," *IET control theory & applications*, vol. 5, no. 14, pp. 1617–1629, 2011.

[26] Z. Qu, *Cooperative Control of Dynamical Systems*. London, U.K.: Springer, 2009.

[27] G. D. L. Torre and T. Yucelen, "Adaptive architectures for resilient control of networked multiagent systems in the presence of misbehaving agents," *International Journal of Control*, pp. 1–13, 2017.

[28] A. Gusrialdi, Z. Qu, and M. A. Simaan, "Competitive interaction design of cooperative systems against attacks," *IEEE Transactions on Automatic Control*, vol. 63, no. 9, pp. 3159–3166, 2018.

[29] S. Sundaram and B. Gharesifard, "Distributed optimization under adversarial nodes," *IEEE Transactions on Automatic Control*, vol. 64, no. 3, pp. 1063–1076, 2019.

[30] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge university press, 2004.

[31] A. Gusrialdi, Z. Qu, and M. Simaan, "Robust design of cooperative systems against attacks," in *Proceedings of American Control Conference*, pp. 1456–1462, Portland, OR, June 4-6, 2014.

[32] A. Gusrialdi, Z. Qu, and M. A. Simaan, "Game theoretical designs of resilient cooperative systems," in *Proceedings of European Control Conference*, pp. 1705–1711, 2015.

[33] D. Kreutz, F. M. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2015.