Push-Sum-Enabled Resilient Microgrid Control

Pouya Babahajiani, *Graduate Student Member, IEEE*, Lizhi Wang, *Graduate Student Member, IEEE*, Ji Liu, *Member, IEEE*, and Peng Zhang, *Senior Member, IEEE*

***Abstract*—This letter devises a distributed microgrid control allowing for time-varying networks utilizing a continuous-time push-sum algorithm. The novelty of the push-sum-based approach lies in: 1) the ability to deal with unbalanced cyber network which represents unreliable communication among distributed energy resources (DERs); 2) the capability of switching among communication networks so as to provide non-interrupted operation; and 3) resiliency against cyber attacks. Case studies verify the efficacy of the new distributed microgrid control strategy and its capability of providing communication robustness while ensuring resilient frequency regulation and active power sharing.**

***Index Terms*—Push-sum, distributed microgrid control, frequency regulation, time-varying and unbalanced cyber network.**

I. Introduction

MICROGRIDS are prone to random link failures resulting in unbalanced communication networks. An unbalanced network may also occur when there is a need to prioritize traffic or mitigate adverse network conditions such as traffic congestion and packet drop. This makes the microgrid's Laplacian matrix no longer doubly stochastic, which invalidates the core assumption of existing distributed control methods and disastrously plagues distributed microgrid control based on averaged consensus [1].

Theoretically, traditional average consensus protocols cannot achieve the exact average under directed and time varying communication network [2]. Consequently, the stability of microgrids is jeopardized under unbalanced scenarios [3]. Existing attempts in the literature to address the unbalance issues [4], unfortunately, apply only to discrete-time systems. Their system dynamics are commonly assumed first order such that the agents need to only carry one state and they adopt time-varying stepsizes, making those algorithms unsuited for microgrid control.

To tackle the above challenges, a continuous-time push-sum algorithm is devised to enable resilient distributed control for microgrids. The new push-sum-enabled microgrid control can provably achieve average consensus at every node even under a time-varying, directed communication network. It enables flexible switching of communication topologies and thus leads to unprecedented cyber-physical resilience in microgrids.

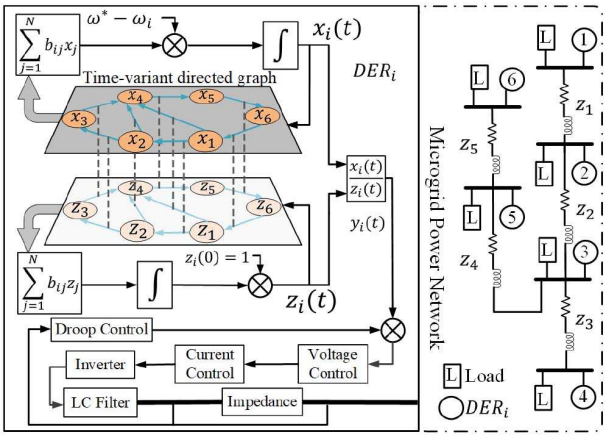

Fig. 1. Schematic diagram of the push-sum-enables microgrid control.

II. Push-Sum-Based Resilient Distributed Control

Recently, push-sum has been emerging to enhance the resilience of distributed averaging approaches for discrete-time systems [5], [6]. We extend the push-sum method [7] to continuous-time domain to devise a resilient distributed control scheme which is resilient against abrupt changes in communication topology and cyber-attack on communication links. The overarching goal is to enable unprecedented resilient control for real-life microgrids abstracted as time-varying graphs, which cannot be attained by conventional distributed control relying on the existence of spanning trees [8]. Here time-varying graphs means unreliable communications because of the unavoidable random failures in DER communications.

An islanded AC microgrid with inductive lines and inverter-interfaced DERs is considered, as shown in Fig. 1. Without loss of generality, a push-sum-enabled frequency controller is formulated as follows:

$$\begin{aligned} \omega_i &= \omega^* - n_i P_{e,i} + y_i, \\ \dot{x}_i &= \omega^* - \omega_i + \sum_{j=1}^{n} b_{ij} x_j, \\ \dot{z}_i &= \sum_{j=1}^{n} b_{ij} z_j, \quad z(0) = 1, \\ y_i &= \frac{x_i(t)}{z_i(t)}, \end{aligned} \tag{1}$$

Manuscript received May 24, 2020; revised September 23, 2020 and November 17, 2020; accepted February 4, 2021. Date of publication February 11, 2021; date of current version June 21, 2021. This work was supported in part by the National Science Foundation under Grant ECCS-1611095/2002897, Grant CNS-1647209/2006828, and Grant ECCS-1831811/2018492. Paper no. PESL-00169-2020. *(Corresponding author: Peng Zhang.)*

The authors are with the Department of Electrical and Computer Engineering, Stony Brook University, Stony Brook, NY 11794 USA (e-mail: pouya.babahajiani@stonybrook.edu; lizhi.wang@stonybrook.edu; ji.liu@stonybrook.edu; p.zhang@stonybrook.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2021.3058853.

Digital Object Identifier 10.1109/TSG.2021.3058853

where ω_i is the actual grid frequency, ω^* is the rated frequency, $P_{e,i}$ is the active power injection from DER inverter i, n_i is the droop coefficient and y_i is the secondary control signal.

In push-sum, the secondary control signal for microgrid DER i is determined by the cumulative estimate of the sum $x_i(t)$ and a weight $z_i(t)$. In other words, the push-sum algorithm solves the distributed averaging problem on networks with one additional variable per node such that nodes not only record a linear combination of other nodes, but also keep track of their relative importance in the system through the scaling factor "z" such that its magnitude is directly affected by the number of incoming links and inversely by the number of outgoing links. At the beginning, the weights are initialized as $z_i(0) = 1$. The algorithm also works for time-varying communication graphs. If a new node is added to the network or an existing node is removed, all z_i are again reset and initialized to 1.

The Laplacian matrix L for an underlaying time-variant directed graph $\mathcal{G}(t)$ is defined as $L = D_{in} - A$, where A and D_{in} are adjacency and in-degree matrices respectively. b_{ij} is the ij^{th} entry of $-L(t)$.

It can be shown that after communication network changes, $z_i(t) \to nv_i$ as $t \to \infty$ such that n is the number of DERs and the vector v is the normalized eigenvector of matrix e^{-Lt} associated with the simple eigenvalue 1 or the zero eigenvalue of $-L$. Fig. 1 illustrates the new control scheme where the communication network is modelled by a directed graph.

To formally prove the convergence of the push-sum-based method, the microgrid is assumed stable in the steady state. Since the DERs' frequency must be equal in steady state, we have $\omega_1 = \omega_2 = \cdots = \omega_n$ and thus $n_1P_{e,1} - y_1 = n_2P_{e,2} - y_2 = \cdots = n_nP_{e,n} - y_n$. This leads to

$$\begin{aligned}\dot{x}_i &= \omega^* - \omega_i + \sum_{j=1}^{n} b_{ij}x_j \\ &= n_iP_{e,i} - y_i + \sum_{j=1}^{n} b_{ij}x_j = 0. \end{aligned} \tag{2}$$

As each column-sum of the Laplacian matrix equals zero, i.e., $\sum_{i=1}^{n}\sum_{j=1}^{n} b_{ij}x_j = 0$, it can be found that

$$\sum_{i=1}^{n} \dot{x}_i = \sum_{i=1}^{n} \big(n_iP_{e,i} - y_i\big) = n\big(n_iP_{e,i} - y_i\big) = 0, \tag{3}$$

Consequently, $n_iP_{e,i} = y_i$. To study the convergence, we define

$$\bar{x}(t) \coloneqq \frac{1}{n}\sum_{i=1}^{n} x_i(t), \tag{4}$$

Substituting (3) to (4) yields

$$\dot{\bar{x}}(t) = \frac{1}{n}\sum_{i=1}^{n} \big(n_iP_{e,i} - y_i\big). \tag{5}$$

Let us construct a Lyapunov function $V(x) = \frac{1}{2}(x - x^*)^2$. Then we have

$$\begin{aligned}\dot{V}(\bar{x}(t)) &= \frac{1}{n}\sum_{i=1}^{n} \big(n_iP_{e,i} - y_i\big)\big(\bar{x}(t) - x^*\big) \\ &= \frac{1}{n}\sum_{i=1}^{n} \big(\omega^* - \omega_i\big)\big(\bar{x}(t) - x^*\big). \end{aligned} \tag{6}$$

To analyze the behavior of (6), suppose that system is in steady state and then experiences a power deficiency, e.g., a sudden step load or a loss of generation. At this instance, system's frequency drops as demand exceeds the generation. Hence, in order to compensate the power imbalance, DERs need to increase their generation and considering the power sharing, this results to a higher $n_iP_{e,i}$ which means the new equilibrium point will be a higher value. Therefore,

$$\omega^* - \omega_i > 0, \quad \bar{x}(t) - x^* < 0. \tag{7}$$

If the total active power produced outweighs the total demand, e.g., following a load reduction, system's frequency increases and the new equilibrium point will be a lower value, then

$$\omega^* - \omega_i < 0, \quad \bar{x}(t) - x^* > 0. \tag{8}$$

Considering (7) and (8), $\dot{V}(\bar{x}(t)) < 0$ and thus $\bar{x}(t) \to x^*$ as $t \to \infty$. It can be shown that $y_i(t)$ is an observer for $\bar{x}(t)$ and $\lim_{t\to\infty} \|y_i(t) - \bar{x}(t)\| = 0$ [7]. Therefore, eventually $n_iP_{e,i}$, y_i and $\bar{x}$ all converge to x^*, and ω_i converges to ω^*.

III. Case Studies

The performance of the push-sum-enabled distributed frequency control is tested on a microgrid with six inverter-interfaced DERs simulated in MATLAB/SIMPOWER environment (see Fig. 1). The nominal voltage and frequency are 380 V and 60 Hz respectively. Rated active powers for DERs 1/2, 3/4 and 5/6 are 100 kW, 80 kW and 116 kW respectively. Droop coefficients for DERs 1/2, 3/4 and 5/6 are 8×10^{-4}, 10^{-3} and 7×10^{-4} respectively. Line impedances are $Z_1(0.65\Omega, 1.3\text{ mH})$, $Z_2(0.5\Omega, 1\text{ mH})$, $Z_3(0.58\Omega, 1.2\text{ mH})$, $Z_4(0.6\Omega, 1\text{ mH})$ and $Z_5(0.55\Omega, 1.3\text{ mH})$.

A. Time-Varying Unbalanced Communication

This case verifies the performance of the push-sum scheme under unbalanced communication and switching topology (random graph). Initially the communication network operates as an undirected connected graph $\mathcal{G}_1$ [see Fig. 2(a)]. Then the cyber network is changed at t = 10s, t = 14s and t = 20s to directed unbalanced graphs $\mathcal{G}_2$, $\mathcal{G}_3$ and $\mathcal{G}_4$, respectively. Eventually a step load of 13 kW is applied at t = 30s.

As illustrated in Fig. 2(b), when the communication switches, the scaling factor z_i tracks the imbalances and prevents the secondary controller y_i from being disturbed and therefore, frequency remains intact.

B. Empowering Plug-and-Play

This case verifies the push-sum-based controller's feature of plug-and-play capability. This merit is investigated by detaching DER6 at t = 15s and plugging it in again at t = 22s. The exploited communication graph is shown in Fig. 3. As can be seen, if DERi is disconnected, the remaining graph is still strongly connected.

As depicted, after disconnection of DER6, the power deficiency reallocated among the remaining DERs and they manage to share the loads. As Fig. 3 shows, accurate active power sharing and frequency restoration are maintained during

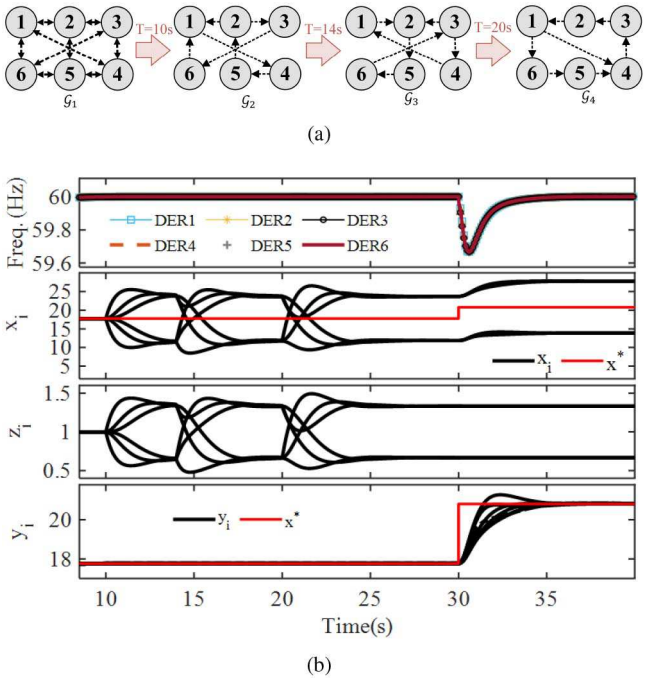

Fig. 2. (a) Time-varying unbalanced communications. (b) Microgrid's frequency and controller parameters under the condition of time varying unbalanced communications.

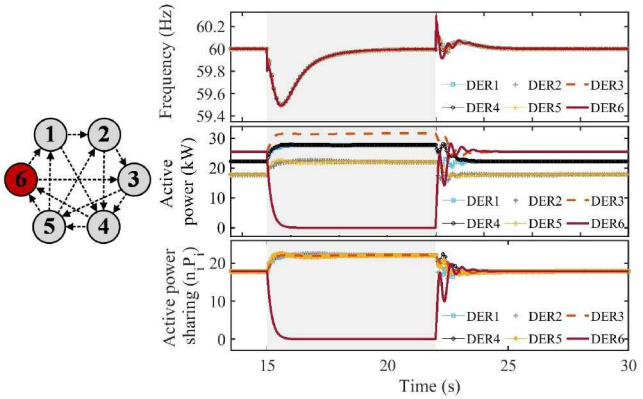

Fig. 3. Frequency and active power sharing after removal of DER6.

plug-and-play operation. The reason of small transient oscillations after reconnection of DER6 is that, no presynchronization is implemented ahead of reconnection.

C. Cyberattacks Immunity

Microgrid communication networks are exposed to potential cyber-attacks such as False-Data-Injection that would jeopardize the overall microgrid performance in terms of efficiency and stability. In this letter, the attack model assumed compromises the communication link between DERs. The attack model involves the following assumptions:

1) The attacker has knowledge of the microgrid and the topology $\mathcal{G}$.
2) The attacker is capable of relaying and altering the communications between two DERs.
3) The attacker is not able to predict the communication direction between DERs.

In case cyber attack on communication link happens, when topology switches, all DERs know where to send data and which adjacent DERs are supposed to send them data. Hence, if a received signal does not match with the switching pattern, that link is identified as a corrupted communication link. The attack is modeled as

$$\dot{x}_i = n_i P_{e,i} - y_i + b_{ii} x_i + \sum_{j=1,\, j\neq i}^{n} b_{ij}\big(x_j + \mu_j\big). \tag{9}$$

Suppose that, the malicious signal μ_j is injected into the information transferred from DER_j to DER_i. Summation over all $\dot{x}_i$s yields

$$\begin{aligned}\sum_{i=1}^{n}\dot{x}_i &= \sum_{i=1}^{n}\big(n_i P_{e,i} - y_i\big) \\ &\quad + \left[\sum_{i=1}^{n} b_{i,1}, \ldots, \sum_{i=1}^{n} b_{i,n}\right][x_1, \ldots, x_n]^T + b_{ij}\mu_j \\ &= \sum_{i=1}^{n}\big(n_i P_{e,i} - y_i\big) + \sum_{i=1}^{n}\sum_{j=1}^{n} b_{ij} x_j + b_{ij}\mu_j. \end{aligned} \tag{10}$$

Now, if the communication topology switches such that DER_j does not send information to DER_i, since DER_i knows all the incoming and outgoing links at each instant, the term $b_{ij}\mu_j$ in (10) will be disregarded, then

$$\sum_{i=1}^{n}\dot{x}_i = \sum_{i=1}^{n}\big(n_i P_{e,i} - y_i\big) + \sum_{i=1}^{n}\sum_{k=1,\, k\neq j}^{n} b_{ik} x_k. \tag{11}$$

Since the communication graph is still strongly connected and each column-sum of the Laplacian matrix equals zero,

$$\sum_{i=1}^{n}\sum_{k=1,\, k\neq j}^{n} b_{ik} x_k = \mathbf{1}Bx = 0, \tag{12}$$

where $\mathbf{1}$ is the vector whose entries all equal one, and

$$\sum_{i=1}^{n}\dot{x}_i = \sum_{i=1}^{n}\big(n_i P_{e,i} - y_i\big). \tag{13}$$

Comparing (13) and (3), it can be readily obtained that (2)-(8) can be followed to complete the proof of the system's stability as after attack elimination, the analyses are essentially the same.

Furthermore, since DER_i knows there is no information from DER_j but still receives $b_{ij}\mu_j$, the link from DER_j to DER_i is identified and isolated as a corrupted link. Therefore, after the communication topology switches, corrupted links (and consequently malicious signals) cannot jeopardize the convergence and stability as they are not parts of the communication graph anymore. This concept is also shown in Fig. 4(a).

As the third scenario, the communication networking starts from $\mathcal{G}_1$ in Fig. 4(a) and then links from DER2 to DER1 and DER4 to DER3 are attacked at t = 10s and t = 15s, respectively. A step load of 20 kW is also applied at t = 35s.

Fig. 4(b) shows the impacts of time-varying cyber-attacks on frequency and active power sharing, where the malicious signal μ_j is considered as Sine waves with an offset. Performance of the push-sum strategy against such

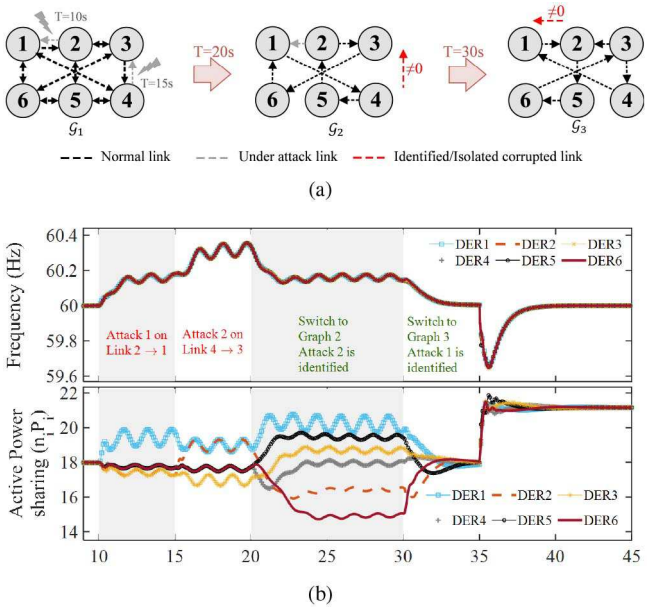

Fig. 4. (a) Attacked link identification/isolation procedure. (b) Impact of time-varying cyber-attack on frequency and active power sharing and the performance of the push-sum strategy.

cyber-attack is also demonstrated. After the attack, the communication topology switches at t = 20s and t = 30s.

It is worth noting that, speed of attack detection depends on the speed of topology switching and, in this scenario, the reason for choosing the switching and attack times are to better illustrate the impacts of attacks and performance of the push-sum enabled scheme.

According to the communication topology at t = 20s, there is no link from DER4 to DER3 and the data flow through this link is supposed to be zero which is not due to the attack. Hence, this link is identified as a corrupted link and it is isolated from the network. The same happens for the link from DER2 to DER1 at t = 30s. Consequently, the attacked links are identified and isolated, active power sharing is again synchronized among DERs and frequency is restored at the rated 60 Hz. The push-sum scheme thus guarantees ultra-resilience of microgrid operations and its speed of attack detection depends on the switching speed.

Regarding identification of cyberattack on communication links, there are some existing methods in the literature [9], [10]. To detect and isolate false data injections, [9] proposes a distributed cyber-attack control strategy for islanded MGs with distributed control systems, through turning on and off the communication links aperiodically. However, this action tangibly slows down the convergence.

To mitigate attacks on communication links, a trust/confidence-based control protocol is proposed in [10] such that each inverter monitors the information it receives from its neighbors, updates its local confidence factor, and sends to its neighbors. Data received at each inverter from neighbors is weighted by its trust factor. One shortcoming of this method is, the selection of the trust factor is done empirically, as it depends on several factors like network connectivity, speed of convergence of the consensus algorithm and other gains in the consensus algorithm. So if the communication topology changes, the trust factor needs to be reset accordingly and if anything happens to the system (e.g., inertia drop, communication noise, changes of network connectivity, etc.), there is no guarantee that the current trust factor does not jeopardize the system stability.

Compared to the above references, to identify attack on communication links, our developed method relaxes assumptions like constraints on the type of attack signals and empirical setting of trust factors that requires having knowledge about the network. With push-sum enabled scheme, corrupted link is identified if a received signal does not match with the topology switching pattern and rate of convergence depends on the network connectivity.

IV. Conclusion

This letter presents a push-sum-based microgrid control with guaranteed stable average consensus at every node. The practically nonrestrictive assumption of an unbalanced and time-varying communication network makes it ultra-resilient and robust. The new scheme enables timely detection and isolation of corrupted communication links in a distributed fashion without jeopardizing the microgrid normal operations. Push-sum, in conjunction with sparse data transmission and event-triggered methods, promises wide adoptions in power-electronic-enabled autonomic power systems where resilient high-speed communication is required and computation burden matters. Furthermore, generalizing the developed method to microgrids with resistive or non-negligible inductive lines will be a future research direction.

References

[1] P. Zhang, *Networked Microgrids*. Cambridge, U.K.: Cambridge University Press, 2021.

[2] T. Li and J.-F. Zhang, "Consensus conditions of multi-agent systems with time-varying topologies and stochastic communication noises," *IEEE Trans. Autom. Control*, vol. 55, no. 9, pp. 2043–2057, Sep. 2010.

[3] P. Rezaienia, B. Gharesifard, T. Linder, and B. Touri, "Push-sum on random graphs: Almost sure convergence and convergence rate," *IEEE Trans. Autom. Control*, vol. 65, no. 3, pp. 1295–1302, Mar. 2020.

[4] Q. Cao, Y.-D. Song, J. M. Guerrero, and S. Tian, "Coordinated control for flywheel energy storage matrix systems for wind farm based on charging/discharging ratio consensus algorithms," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1259–1267, May 2016.

[5] D. Kempe, A. Dobra, and J. Gehrke, "Gossip-based computation of aggregate information," in *Proc. 44th Annu. IEEE Symp. Found. Comput. Sci.*, Oct. 2003, pp. 482–491.

[6] B. Gerencsér and J. M. Hendrickx, "Push-sum with transmission failures," *IEEE Trans. Autom. Control*, vol. 64, no. 3, pp. 1019–1033, Mar. 2019.

[7] B. Touri and B. Gharesifard, "Continuous-time distributed convex optimization on time-varying directed networks," in *Proc. 54th IEEE Conf. Decis. Control*, Dec. 2015, pp. 724–729.

[8] S. Su and Z. Lin, "Distributed consensus control of multi-agent systems with higher order agent dynamics and dynamically changing directed interaction topologies," *IEEE Trans. Autom. Control*, vol. 61, no. 2, pp. 515–519, Feb. 2016.

[9] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "A cyber-attack resilient distributed control strategy in islanded microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3690–3701, Sep. 2020.

[10] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, "Synchrony in networked microgrids under attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6731–6741, Nov. 2018.