2024 European Control Conference (ECC)
June 25-28, 2024. Stockholm, Sweden

Secure control for a microgrid of VSMs with Virtual Friction

Florian Reißner, Michelle S Chong

Abstract— **Electric grids with a high share of inverter-interfaced power sources require novel control approaches like the popular virtual synchronous machine (VSM) to ensure stable operation. Such power systems are increasingly relying on real time communications between individual machines to achieve control objectives. Signals sent over a communication network include power set points, configuration parameters and machine health data. A novel damping mechanism for VSMs, virtual friction (VF), makes use of this communication infrastructure to provide damping for the machines with low impact on the output powers of the inverters during frequency deviations from the nominal. We investigate in this paper, how this system can be secured when the communication channels are compromised by malicious actors. We analyze a microgrid with several VSMs employing VF in the presence of manipulated signals, and a secure control scheme is proposed that is able to maintain strong damping during attacks. The efficacy of the proposed secure control scheme is validated using a high fidelity simulation model.**

I. Introduction

The increasing share of inverter-interfaced power sources in electric grids requires such inverters to implement grid support functions usually proper to synchronous generators. A well known approach to provide such capabilities is the virtual synchronous machine (VSM): an inverter controlled by an algorithm that emulates inertia, frequency- and voltage-droop similar to the characteristics of a synchronous generator [1]. In order to operate power systems with many VSMs in a stable manner, damping methods have to be implemented (e.g. PLL-damping, virtual damper windings, high frequency droop) [2]. A more recent method is virtual friction (VF) [3], [4], [5], a damping torque applied to the swing equation of the VSM, acting in proportion to the deviation of the virtual rotor frequency from the center of inertia (COI)-frequency of the microgrid. The advantage of VF compared to frequency droop is its lower impact on the output power of the VSM, which is important for power sources where the output power is regulated to yield a maximum amount of energy from the connected primary energy source (e.g. wind, sun). [6] indicates further that VF increases the region of attraction of the stable operating point of a microgrid, potentially improving system stability compared to other damping methods.

In this paper, we address the vulnerability of the communication channels between the VSMs and the central controller (CC) with respect to cyber attacks. Possible scenarios for such attacks are denial of service (DoS) attacks or false data injection attacks, where the data sent over the communication channels has been manipulated with malicious intent, see [7] and the references therein. Of course, the communication channels themselves may be secured by encryption or watermarking [8], [9]. However, these techniques require high computational power at each VSM, which may not be practical. We present here a redesign of the control algorithm executed at the CC (centralized) and at each of the VSMs (distributed) by implementing two mechanisms: (i) a *centralized* secure state estimator (adapted from [10]) in the CC to mitigate the potentially manipulated measurements received by the CC, and (ii) a *distributed* attack detector/corrector at each VSM which uses only local data as a countermeasure for potentially manipulated COI-frequencies.

The secure state estimator employs the architecture developed in [10], by choosing a state estimate from a bank of robust observers. Due to the uncertainty of the grid parameters, we need to design robust observers with state estimation errors that remain bounded in the presence of parameter mismatch. Moreover, we design the observer gain and parameter matrices such that the estimated output (angular frequencies) of a subset of the VSMs converges asymptotically to the corruption free measured output (angular frequencies) of the same subset of the VSMs. We hypothesize that this will be the key in ensuring that the VSMs synchronize just as in the nominal case presented in [4]. Crucially, we guarantee that the state estimation error is independent of the false data injection attack on the measured data, provided that at least half of the communication channels have not been compromised (the attacker has no access).

In addressing the potentially corrupted COI-frequency received at each VSM, we are limited to using only local data. Hence, we propose an attack detection/correction mechanism, that uses local data to estimate the COI-frequency. This estimate is compared to the COI-frequency received from the CC and a decision is made on whether the estimate or the received COI-frequency is used to stabilize the grid. We remark that existing methods, e.g. [11] are not applicable as individual machines do not communicate with each other and have no knowledge about the grid-architecture.

The contributions of this paper are:

1) A *centralized* secure state estimation algorithm which is robust with respect to parameter uncertainty and an estimation error that is independent of the additive attacks on the measurements, when at least half of the

This research was co-funded by the European Union's Horizon 2020 research and innovation program under the Marie Sklodowska-Curie grant agreement no. 861398 and supported by the ERA-Net Smart Energy Systems (project RESili8, grant agreement No 883973). F. Reißner is with the School of Electrical Engineering, Tel Aviv University, Ramat Aviv 69978, Israel. Michelle S. Chong is with the Department of Mechanical Engineering, Eindhoven University of Technology, the Netherlands (e-mail: reissner@tauex.tau.ac.il, m.s.t.chong@tue.nl)

communication channels are uncompromised.

2) A *distributed* attack detection and correction mechanism which uses only local data.
3) A validation of the proposed mechanisms using a high fidelity simulation model of a microgrid consisting of three interconnected VSMs.

All relevant proofs can be found in the Appendix.

Notation

Let $\mathbb{C}$ be the set of complex numbers, $\mathbb{R} = (-\infty, \infty)$, $\mathbb{R}_{\geq 0} = [0, \infty)$, $\mathbb{R}_{>0} = (0, \infty)$, $\mathbb{N}_{[i,i+k]} = \{i, i+1, i+2, \dots, i+k\}$, $\mathbb{N}_{\geq i} := \{i, i+1, \dots, \}$ and $\mathbb{T} := (-\pi, \pi]$ (modulo 2π). The number of k-element subsets of an n-element set is denoted $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. A block diagonal matrix with square matrices $D_i \in \mathbb{R}^{n\times n}$, $i \in \mathbb{N}_{[1,n]}$ is denoted by $\mathrm{diag}(D_1, D_2, \dots, D_n)$. $\mathbf{0}^{(\mathbf{N}\times\mathbf{M})}$ denotes an $N \times M$ matrix of zeros, $\mathbf{1}^{(\mathbf{N}\times\mathbf{M})}$ denotes an $N \times M$ matrix of ones and $\mathbf{I}^{(\mathbf{N})}$ denotes an $N \times N$ identity matrix. The Euclidean norm of a vector $x \in \mathbb{R}^n$, is denoted $|x|$ and for a matrix $A \in \mathbb{R}^{n\times n}$, its induced norm is $|A|$. Given a point $x \in \mathbb{R}^n$, the closed ball with radius Δ around x is denoted as $\mathbb{B}_{x,\Delta} = \{z \in \mathbb{R}^n \,|\, |z-x| \leq \Delta\}$. When x is the origin, we use $\mathbb{B}_\Delta$. The step function is denoted by $\mu_\tau(t) = \begin{cases} 0, & \text{if } t < \tau, \\ 1, & \text{else.} \end{cases}$

II. Problem formulation

We consider a microgrid with $N \in \mathbb{N}_{>0}$ interconnected VSMs which communicate with a CC through communication channels as shown in Fig. 1. In Sect. II-A, we describe the friction enhanced power system (FEPS) model used to represent the electrical dynamics of the grid and the VSMs and show the modeling of the vulnerability of the communication channels. We then outline a mitigation strategy in Sect. II-B.

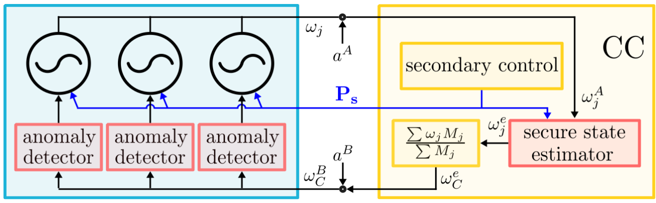


Fig. 1: Secure control scheme for a microgrid with several VSMs.

A. Model of a microgrid under attack

We use the FEPS model proposed in [4], where for $j \in \mathbb{N}_{[1,N]}$, each j-th VSM is described by

$$M_j\dot{\omega}_j = P_{s,j} - P_{e,j} + \omega_n[D_j(\omega_n - \omega_j) + F_j(\omega_{C,j} - \omega_j)], \quad (1)$$

where $(M_j, D_j, F_j) \in \mathbb{R}^3_{\geq 0}$ are model parameters, $P_{s,j} \in \mathbb{R}$ is a power term, $\omega_{C,j} \in \mathbb{R}_{\geq 0}$ is the COI-frequency given in (4), ω_n is the nominal grid frequency and $P_{e,j} \in \mathbb{R}$ is the electric power output of the j-th generator defined by

$$P_{e,j} := \sum_{k\in\mathbb{N}_{[1,N]}} \alpha_{jk} \sin(\delta_j - \delta_k - \varphi_{jk}), \quad (2)$$

with model parameters $\alpha_{jk} \in \mathbb{R}_{\geq 0}$, $\varphi_{jk} \in \mathbb{T}$ and $\delta_j := \theta_j - \theta_1$ where $\theta_j \in \mathbb{T}$ is the rotor angle of the j-th VSM. For a detailed explanation of all model parameters and conditions for synchronization in the absence of attacks, the reader is referred to [4].

We assume that every VSM communicates with the CC via its own communication channel. In other words, there are N independent communication channels between the microgrid and the CC. An attacker may have gained access to the communication channels between the VSMs and the CC, with the ability to manipulate the data. We model such false data injection attacks by potentially unbounded additive signals a^A and a^B. Malicious actors may target frequency data ω_j sent from each VSM towards the CC by corrupting it with a_j^A. We model the signals between VSM $j \in \mathbb{N}_{[1,N]}$ and the CC as

$$\omega_j^A = \omega_j + a_j^A, \quad (3)$$

where $a_j^A : \mathbb{R} \to \mathbb{R}$ is unknown to the operator and ω_j is the angular frequency of the j-th VSM from (1)-(2).

The COI-frequency $\omega_{C,j}$ of the grid is transmitted back to each j-th VSM for the VF-damping term. The transmitted COI-frequency $\omega_{C,j}$ might also be subjected to attacks. This is also modelled as an additive and unknown signal a^B such that the COI-frequency received by each VSM $k \in \mathbb{N}_{[1,N]}$ is

$$\omega_{C,k} := \omega_C^{\mathrm{n}} + \frac{\sum_{j\in\mathbb{N}_{[1,N]}} M_j a_j^A}{\sum_{j\in\mathbb{N}_{[1,N]}} M_j} + a_k^B, \quad (4)$$

where $\omega_C^{\mathrm{n}} = \frac{\sum_{j\in\mathbb{N}_{[1,N]}} M_j\omega_j}{\sum_{j\in\mathbb{N}_{[1,N]}} M_j}$ is the nominal COI-frequency in the absence of attacks a_j^A and a_k^B. Further, we assume that at least half of the communication channels cannot be accessed by the attacker for all $t \in \mathbb{R}_{\geq 0}$. This assumption is crucial for securely estimating the states of the VSMs at the CC, which we state formally as follows.

Assumption 1 (At least half of the channels are secure): Let $\mathcal{I} \subseteq \mathbb{N}_{[1,N]}$ be the index set of attacked channels with cardinality $|\mathcal{I}| = Q < \frac{N}{2}$, which remains constant over all time $t \in \mathbb{R}_{\geq 0}$. The attack vectors $a^A := (a_1^A, a_2^A, \dots, a_N^A)^T$ and $a^B := (a_1^B, a_2^B, \dots, a_N^B)^T$ satisfy $(a^A, a^B) \in \mathcal{A}_\mathcal{I}$, where $\mathcal{A}_\mathcal{I} := \{(a^A \times a^B) \in \mathbb{R}^N \times \mathbb{R}^N : a_j^A(t) = 0, a_j^B(t) = 0, \forall t \in \mathbb{R}_{\geq 0}, \forall j \in \mathcal{I}\}$.

Under the ideal scenario when there are no attacks, i.e., $a^A = 0$ and $a^B = 0$, prior work [4, Theorem 1] provides algebraic conditions based on the model parameters to achieve synchronization. We recall the synchronization conditions for the model (1), (2) and (4) in the absence of attacks below.

Lemma 1 (Theorem 1 of [4]): Consider the microgrid model (1)-(4) when there are no attacks, i.e., $a^A = 0$ and $a^B = 0$. Then, there exists $\Delta_\gamma \in \mathbb{R}_{\geq 0}$ such that for any $\Delta_\delta = \Delta_\delta(\Delta_\gamma) \in \mathbb{R}_{>0}$ and $\Delta_\omega \in \mathbb{R}_{>0}$, there exists $\epsilon^* \in \mathbb{R}_{>0}$ such that if for all $j \in \mathbb{N}_{[1,N]}$,

- the microgrid parameters D_j, F_j and M_j satisfy $\frac{M_j^2}{(D_j+F_j)^2} \in (0, \epsilon^*)$, and
- the power input is constant, i.e., $P_{s,j}(t) = P_j^*$, for all $t \in \mathbb{R}_{\geq 0}$, where $P_j^* \in \mathbb{R}$, and

- $\delta(0) \in \mathbb{B}_{\Delta_\delta}$ and $\omega(0) \in \mathbb{B}_{\Delta_\omega}$,

then there exist $(\delta^*, \omega^*) \in \mathbb{R}^{N-1} \times \mathbb{R}^N$ such that $\lim_{t\to\infty} \delta(t) = \delta^*$ and $\lim_{t\to\infty} \omega(t) = \omega^*$.

The synchronization point (δ^*, ω^*) is given in Theorem 1 of [4]. We will be exploiting this result in the design of our attack mitigation mechanisms. The presence of false data injection attacks a^A and a^B may disrupt the synchronization of the VSMs, which could cause undesired fluctuations in output power, overheating in the transmission lines due to overcurrents or lead to the disconnection of the VSMs.

B. Secure Control Objective

We propose securing the microgrid with two mechanisms: (i) anomaly detectors co-located at each VSMs to detect corrupted COI-frequency signals ω_C using only local data; (ii) a secure state estimator at the CC to counter corrupted signals ω_j. We briefly describe these mechanisms here.

1) Attack detector and corrector: At each VSM, an anomaly detector uses local data to detect whether the COI-frequency ω^B received from the CC has been corrupted by the attack vector a^B. Each anomaly detector only has access to the local data, namely frequency ω_j, electric power output $P_{e,j}$, power input $P_{s,j}$ and the received COI-frequency $\omega^B_{C,j}$. Using the local data, the anomaly detector then counters the potentially corrupted received COI-frequency

$$\omega^B_C = \omega^e_C + a^B, \tag{5}$$

where $\omega^e_C : \mathbb{R}_{\geq 0} \to \mathbb{R}^N$ is the COI-frequency computed at the CC, given by

$$\omega^e_{C,j} := \frac{\sum_{j\in\mathbb{N}_{[1,N]}} M_j \omega^e_j}{\sum_{j\in\mathbb{N}_{[1,N]}} M_j} \in \mathbb{R},\ j \in \mathbb{N}_{[1,N]}, \tag{6}$$

where $\omega^e_j : \mathbb{R}_{\geq 0} \to \mathbb{R}$ are estimates of the frequency ω_j at each VSM using the received measurements ω^A_j which may have been attacked by a^A_j according to (3).

This is mitigated by designing $\omega_{C,j}$ which switches between the received COI-frequency $\omega^B_{C,j}$ and the locally estimated COI-frequency $\omega^d_{C,j}$ based on attack detection rules defined in Section III, i.e.,

$$\omega_{C,j}(t) = \begin{cases} \omega^d_{C,j}(t), & \text{attack detected,} \\ \omega^B_{C,j}(t), & \text{otherwise.} \end{cases} \tag{7}$$

These rules and the locally computed COI-frequency $\omega^d_{C,j}$ are designed to possess the following property.

Property 1: Consider the FEPS model (1), (2) with $\omega_{C,j}$ given by (7), where $\omega^d_{C,j} : \mathbb{R}_{\geq 0} \to \mathbb{R}$ is the corrected COI-frequency computed using local data, i.e., the received COI-frequency $\omega^B_{C,j}$, the j-th VSM's power output $P_{e,j}$ and active power set point $P_{s,j}$. The corrected COI-frequency $\omega^d_{C,j}$ and attack detection rules are designed such that $\omega_{C,j}$ in (7) is within a margin $K_\omega \in \mathbb{R}_{\geq 0}$ of the computed COI-frequency $\omega^e_{C,j}$, i.e., $|\omega_{C,j}(t) - \omega^e_{C,j}(t)| \leq K_\omega$, for $t \in \mathbb{R}_{\geq 0}$.
In Section III, we show how Property 1 can be achieved.

2) Secure state estimator: The secure state estimator is deployed at the CC to provide estimates ω^e_j of the actual angular frequency ω_j with the following property.

Property 2: Consider the FEPS model (1), (2) with ω_C defined by (7) which satisfies Property 1. For all $\Delta_\omega \in \mathbb{R}_{>0}$, there exist $K_e = K_e(\Delta_\omega) \in \mathbb{R}_{>0}$ such that the error between the estimates ω^e_j and the true angular frequencies ω_j satisfy $|\omega^e_j(t) - \omega_j(t)| \leq K_e$, for all $t \in \mathbb{R}_{\geq 0}$, initial conditions $\omega^e_j(0) \in \mathbb{B}_{\Delta_\omega}$ and $\omega_j(0) \in \mathbb{B}_{\Delta_\omega}$.
Note that Property 2 gives an upper bound on the estimation error that is independent of the attack a_A on the transmitted angular frequencies ω_j. In Section IV, we show how a secure state estimator can be designed to achieve Property 2.

3) Securing the microgrid: With the aforementioned mitigation mechanisms in place, we have the microgrid model (1), (2), (7). For the rest of the paper, we will work with the model written in the following form by taking the state $\tilde{x}$, input $\tilde{u}$ and measured output $\tilde{y}$ to be $\tilde{x} = [\delta_1, \ldots, \delta_{N-1}, \omega_1, \ldots, \omega_N]^\intercal$, $\tilde{y} = [\omega_1, \ldots, \omega_N]^\intercal$, and $\tilde{u} = [P_{s,1}, \ldots, P_{s,N}]^\intercal$. We can then write the FEPS model (1), (2), (5) and (7) as

$$\dot{\tilde{x}} = [f_1(\tilde{x}, \tilde{u}, m), \ldots, f_N(\tilde{x}, \tilde{u}, m)]^\intercal, \tag{8}$$

where $m(t)$ captures the (unknown) deviation of the model from nominal, due to the mechanisms for mitigating attacks, as follows

$$m(t) = \begin{cases} \omega^d_C(t) - \omega^{\mathrm{n}}_C(t), & \text{attack detected,} \\ \omega^e_C(t) - \omega^{\mathrm{n}}_C(t), & \text{otherwise,} \end{cases} \tag{9}$$

where the purpose of $\omega^d_{C,j}$ and $\omega^e_{C,j}$ was explained in Sections II-B.1 and II-B.2, respectively.

At this juncture, we make the following assumption that the system is uniformly bounded for all input $\tilde{u}$.

Assumption 2: For all $\Delta_x \in \mathbb{R}_{>0}$, there exists $K_x \in \mathbb{R}_{>0}$ such that the solution $\tilde{x}$ to the microgrid model (1), (2) and (7) satisfies $\tilde{x}(t) \in \mathbb{B}_{K_x}$, for all $t \in \mathbb{R}_{\geq 0}$, bounded input $\tilde{u}$ and initial condition $\tilde{x}(0) \in \mathbb{B}_{\Delta_x}$.

Showing that Assumption 2 holds is challenging even in the nominal case without attacks, see [12] for the model without virtual friction and [4] for the FEPS-model considered in this paper. Proving that Assumption 2 holds for our setup with the mitigation mechanisms will be the focus of future work. Nonetheless, we will see in simulations presented in Sect. V that Assumption 2 is satisfied. The rest of this paper focuses on the design and validation of the two attack mitigation strategies.

III. Attack detector and corrector (AD)

The attack detector and corrector (AD) uses only locally available data ω_j and $P_{e,j}$ to compute fall-back signals $\omega^d_{C,j}$. The signals $\omega^d_{C,j}$ are estimates of ω^e_C from (6). These are estimated with the desired nominal conditions in mind, i.e., in the absence of attack vectors $a^A = 0$ and $a^B = 0$.

A. Design of fall-back signal ω_C^d

We make the (simplifying) assumption that for each VSM j, the remaining microgrid can be represented by a single *equivalent generator* with frequency $\omega_{C,j}^e$. The angular difference between VSM j and this equivalent generator is denoted by $\delta_{C,j} = \theta_j - \theta_{C,j}^e$, where $\theta_j \in \mathbb{T}$ is the rotor angle of the j-th VSM and $\theta_{C,j}^e \in \mathbb{T}$ is the rotor angle of the equivalent generator. Using the FEPS model (1), (2) for this simplified two-generator system, the actual output power of VSM j can be approximated by

$$P_{e,j} \approx -\alpha_{j0}\sin(\varphi_{0j}) + \alpha_j \sin(\delta_{C,j}^e - \varphi_j), \qquad (10)$$

where $(\alpha_{j0}, \alpha_j) \in \mathbb{R}_{\geq 0}^2$, $(\varphi_{0j}, \varphi_j) \in \mathbb{T}^2$ are parameters of the electric connection between VSM j and the equivalent generator. Solving (10) for $\delta_{C,j}$ and taking the time derivative yields

$$\dot{\delta}_{C,j}^e \approx \frac{\dot{P}_{e,j}}{\alpha_j \sqrt{1 - \left(\frac{P_{e,j} + \alpha_{0j}\sin(\varphi_{0j})}{\alpha_j}\right)^2}}. \qquad (11)$$

For a reasonable grid, the maximal output power P_e^{max} of the machine is much smaller than the grid coupling, i.e., $\alpha_j \gg P_e^{max} \geq |P_{e,j}|$, such that the dependency on $P_{e,j}$ in the denominator can be disregarded to avoid singularities for certain values of $P_{e,j}$. Therefore, (11) becomes $\dot{\delta}_{C,j}^e \approx \beta_j \dot{P}_{e,j}$, where $\beta_j := \frac{1}{\alpha_j} \in \mathbb{R}_{>0}$. Using the relation $\omega_{C,j}^e = \omega_j - \dot{\delta}_{C,j}^e$ and by noting from definitions that $\dot{\delta}_{C,j}^e := \dot{\theta}_j - \dot{\theta}_{C,j}^e = \omega_j - \omega_{C,j}^e$, we obtain an estimate $\omega_{C,j}^d$ of ω_C^e using

$$\omega_{C,j}^d := \omega_j - \beta_j \dot{P}_{e,j}, \qquad (12)$$

where the β_j can be determined by curve-fitting using an initial set of training data. At steady state, clearly $\dot{P}_{e,j} = 0$, such that $\omega_{C,j}^d = \omega_j = \omega_{C,j}^e$.

B. Detection rules

Finally, detection rules determine, when the signal $\omega_{C,j}^B$ is considered not trustworthy (and thus when $\omega_{C,j}^d$ is fed to the VSM algorithm instead of $\omega_{C,j}$). We will use the following attack detection rules: $|\omega_{C,j}^B - \omega_{C,j}^d| > \Delta_f^d$ for more than T_f^d, and $\omega_{C,j}^B$ jumps by more than Δ_s^d. The parameters $\Delta_f^d > 0$ and $\Delta_s^d > 0$ are to be tuned. These rules are motivated by the fact that $\dot{\omega}_C$ is limited by the inertia in the system and the fact that there can be no constant offset between ω_C^e and $\omega_{C,j}^d$.

C. Achieving Property 1

We first show that the estimation accuracy between the estimate $\omega_{C,j}^d$ and the transmitted $\omega_{C,j}^e$ can be made small up to a margin by tuning the parameters β_j.

Proposition 1: Consider the FEPS model (8) with the estimate ω_C^d given by (12) and ω^e satisfying Property 2. Let Assumption 2 hold. For any $(\Delta_\delta, \Delta_\omega, \epsilon_\omega) \in \mathbb{R}_{>0}^3$, there exist $\beta = \beta(\epsilon_\omega) \in \mathbb{R}_{\geq 0}$ and $\nu_\omega = \nu_\omega(\Delta_\delta, \Delta_\omega)$ such that by choosing β_j in (12) as $\beta_j = \beta$, the following holds

$$|\omega_{C,j}^d(t) - \omega_{C,j}^e(t)| \leq \epsilon_\omega + \nu_\omega, \quad t \in \mathbb{R}_{\geq 0},\ j \in \mathbb{N}_{[1,N]}, \ (13)$$

for all initial conditions $\delta(0) \in \mathbb{B}_{\Delta_\delta}$ and $\omega(0) \in \mathbb{B}_{\Delta_\omega}$. Next, we show that by implementing the AD based on (7) and (12), we can achieve Property 1.

Theorem 1: Consider the FEPS model (8) with the AD defined by (7), ω_C^d from (12) and ω^e satisfying Prop. 2. Let Assumption 2 hold. For any $(\Delta_\delta, \Delta_\omega, \epsilon_\omega) \in \mathbb{R}_{>0}^3$, there exist $\beta = \beta(\epsilon_\omega) \in \mathbb{R}_{\geq 0}$ and $K_e = K_e(\Delta_\delta, \Delta_\omega, \epsilon_\omega)$ such that by choosing β_j in (12) as $\beta_j = \beta$, Property 1 is satisfied.

IV. Secure state estimator

In this section, we present a secure state estimator that possesses Property 2. Given that uncertainty in the microgrid parameters is unavoidable, we present a novel observer design which overcomes this, in addition to mitigating attacks on the transmitted measurements. These observers are based on the linearized FEPS model.

A. Linearized microgrid model

According to Lemma 1, in the absence of attacks (i.e., $a^A = 0$ and $a^B = 0$), the state $\tilde{x}$ of the microgrid model (1)-(4) converges to $x^* = [(\delta^*)^\intercal, (\omega^*)^\intercal]$, with $\delta^* \in \mathbb{R}^{N-1}$ and $\omega^* \in \mathbb{R}^N$ defined as in [4, Theorem 1]. We linearize around the stable operating point given by x^*. Deviations are denoted by $x = \tilde{x} - x^*$, $y = \tilde{y} - y^*$ and $u = \tilde{u} - u^*$, and we define matrices $\mathbf{M}$, $\mathbf{G}$, and $\mathbf{H}$ as follows:

$$\mathbf{M} = \text{diag}\left(\frac{1}{M_1}, \frac{1}{M_2}, \ldots, \frac{1}{M_N}\right), \qquad \begin{aligned} [\mathbf{G}]_{jk} &= \frac{\partial f_j}{\partial \omega_k}, \\ [\mathbf{H}]_{jk} &= \left.\frac{\partial f_j}{\partial \delta_{k+1}}\right|_{x^*, u^*}, \end{aligned}$$

where

$$\frac{\partial f_j}{\partial \omega_k} = \begin{cases} \dfrac{F_j \omega_n}{\sum M_i} - \dfrac{\omega_n}{M_j}\left(F_j + D_j\right), & j = k, \\ \dfrac{M_k F_j \omega_n}{M_j \sum M_i}, & j \neq k, \end{cases}$$

$$\frac{\partial f_j}{\partial \delta_k} = \begin{cases} -\dfrac{1}{M_j}\displaystyle\sum_{\substack{l=1 \\ l \neq j}}^{N} a_{jl}\cos(\delta_j^* - \delta_l^* - \varphi_{jl}), & j = k, \\ \dfrac{\alpha_{jk}}{M_j}\cos(\delta_j^* - \delta_k^* - \varphi_{jk}), & j \neq k. \end{cases}$$

The linearized model then can be written in the form

$$\dot{x} = \mathbf{A}x + \mathbf{B}u + \mathbf{E}m,\ y = \mathbf{C}x + a^A, \qquad (14)$$

with

$$\begin{aligned} \mathbf{A} &= \left[\begin{array}{c:c:c} \mathbf{0}^{(\mathbf{N-1})\times(\mathbf{N-1})} & -\mathbf{1}^{(\mathbf{N-1})\times \mathbf{1}} & \mathbf{I}^{(\mathbf{N-1})} \\ \hdashline \mathbf{H} & \multicolumn{2}{c}{\mathbf{G}} \end{array}\right], \\ \mathbf{B} &= \left[\begin{array}{c} \mathbf{0}^{(\mathbf{N-1})\times(\mathbf{N-1})} \\ \hdashline \mathbf{M} \end{array}\right], \\ \mathbf{C} &= \left[\begin{array}{cc} \mathbf{0}^{\mathbf{N}\times(\mathbf{N-1})} & \mathbf{I}^{(\mathbf{N})} \end{array}\right], \\ \mathbf{E} &= \left[\mathbf{0}^{(\mathbf{N-1})\times 1}, \frac{\omega_n F_1}{M_1}, \ldots, \frac{\omega_n F_N}{M_N}\right]^\intercal. \end{aligned} \qquad (15)$$

It is important to note that the changes in the load consumption or network tie-line impedances impact α_{jk} and φ_{jk} in

(2) such that in a realistic microgrid, parameter uncertainty affects the matrix $\mathbf{H}$ in (15) and only a guess $\hat{\mathbf{H}}$ can be used. We will show in the following how to design an observer that is robust against such parameter uncertainty for the purpose of secure state estimation. We denote by $\hat{\mathbf{A}}$ the system matrix obtained by replacing $\mathbf{H}$ and $\mathbf{G}$ in (15) by $\hat{\mathbf{H}}$ and $\hat{\mathbf{G}}$, where $\hat{\mathbf{G}}$ is specially chosen to be

$$\hat{\mathbf{G}} = \frac{F_j + D_j}{F_j}\left[\mathbf{G} + \omega_n \mathrm{diag}\left(\frac{D_1}{M_1}, \frac{D_2}{M_2}, \dots, \frac{D_N}{M_N}\right)\right]. \quad (16)$$

This matrix $\hat{\mathbf{G}}$ has zero row sum[1], which will be exploited in the design of the robust observer in the next section.

B. Observer design in the presence of parameter uncertainty

A crucial condition of the secure state estimation algorithm in [10] is redundant observability (see Theorem 1 in [10]). We state this in the assumption below.

Assumption 3: Consider the linearized model (14) with $N \in \mathbb{N}_{>0}$ output channels where at most $Q \in \mathbb{N}_{>0}$ channels have been compromised. For every set $\mathcal{K}_\iota \subset \mathbb{N}_{[1,N]}$ with $|\mathcal{K}_\iota| \geq N - 2Q$, the pair $(\hat{\mathbf{A}}, \mathbf{C}_{\mathcal{K}_\iota})$ is observable, where $\mathbf{C}_{\mathcal{K}_\iota}$ is obtained by stacking all the rows $\kappa \in \mathcal{K}_\iota$ of $\mathbf{C}$.

Under Assumption 3, we know that for every $\mathcal{K}_\iota \subset \mathbb{N}_{[1,N]}$ with $|\mathcal{K}_\iota| \geq N - 2Q$, the following observer can be designed such that its state converges to a constant in the absence of attacks (i.e. $a^A = 0$ and $a^B = 0$)[2]:

$$\dot{\hat{x}}^{\mathcal{K}_\iota} = \hat{\mathbf{A}}\hat{x}^{\mathcal{K}_\iota} + \mathbf{B}u + \mathbf{L}^{\mathcal{K}_\iota}(y_{\mathcal{K}_\iota} - \mathbf{C}_{\mathcal{K}_\iota}\hat{x}^{\mathcal{K}_\iota}),\ \iota \in \mathbb{N}_{[1,|\mathcal{K}_\iota|]} \quad (17)$$

where $y_{\mathcal{K}_\iota}$ is the stacking of all $\kappa \in \mathcal{K}_\iota$ components of the output y and $\mathbf{L}^{\mathcal{K}_\iota}$ is an observer gain matrix to be designed such that the matrix $\hat{\mathbf{A}} - \mathbf{L}^{\mathcal{K}_\iota}\mathbf{C}_{\mathcal{K}_\iota}$ is Hurwitz. Since the pair $(\hat{\mathbf{A}}, \mathbf{C}_{\mathcal{K}_\iota})$ is observable, such a matrix $\mathbf{L}^{\mathcal{K}_\iota}$ exists.

Furthermore, due to the parameter uncertainty captured by the matrix $\hat{\mathbf{A}}$, we provide additional design conditions on the observer gain matrix $\mathbf{L}^{\mathcal{K}_\iota}$ such that the estimates of the angular frequency $\hat{\omega}_j^{\mathcal{K}_\iota}$ for $j \in \mathbb{N}_{[1,|\mathcal{K}_\iota|]}$ converge to a constant $\tilde{\omega}^*_{\mathcal{K}_\iota} \in \mathbb{R}^{|\mathcal{K}_\iota|}$. Note that $\tilde{\omega}^*_{\mathcal{K}_\iota}$ may be different from the synchronization point $\omega^*_{\mathcal{K}_\iota}$ from Lemma 1. We provide an observer gain matrix $\mathbf{L}_{\mathcal{K}_\iota}$ that achieves this below.

Proposition 2: Consider the linearized microgrid model (14) under Assumption 3 in the absence of attacks ($a^A = 0$ and $a^B = 0$), and the observer (17). Let the observer gain matrix $\mathbf{L}^{\mathcal{K}_\iota}$ be

$$\mathbf{L}^{\mathcal{K}_\iota} = \begin{bmatrix} \mathbf{0}^{(N-1)\times|\mathcal{K}_\iota|} \\ \bar{\mathbf{L}}^{\mathcal{K}_\iota} \end{bmatrix}, \quad (18)$$

where

- the matrix $\hat{\mathbf{A}} - \mathbf{L}^{\mathcal{K}_\iota}\mathbf{C}_{\mathcal{K}_\iota}$ is Hurwitz, and
- the sub-matrix $\bar{\mathbf{L}}^{\mathcal{K}_\iota} \in \mathbb{R}^{N\times|\mathcal{K}|}$ is chosen such that the following matrix has full rank:

$$[\ \hat{\mathbf{H}} \quad \bar{\mathbf{L}}^{\mathcal{K}_\iota}\ ]. \quad (19)$$

If $\lim_{t\to\infty} u(t) = 0$, we have

$$|\hat{x}^{\mathcal{K}_\iota}(t)| \leq \hat{K}_e,\ t \in \mathbb{R}_{\geq 0}, \quad (20)$$

$$\lim_{t\to\infty} \omega_\kappa(t) - \hat{\omega}_\kappa^{\mathcal{K}_\iota}(t) = 0,\ \kappa \in \mathcal{K}_\iota, \quad (21)$$

for some $\hat{K}_e \in \mathbb{R}_{>0}$ and for all initial conditions $\hat{x}^{\mathcal{K}_\iota}(0) \in \mathbb{R}^n$.

C. Achieving Property 2: Secure estimation of ω_j

Under Assumptions 1 and 3, we can now use the secure state estimation framework from [10, Section III-B]. Two banks of observers are designed. The first bank has $n_s := \begin{pmatrix} N \\ N-Q \end{pmatrix}$ observers with state $\hat{x}^{\mathcal{S}_\beta}$, $\beta \in \mathbb{N}_{[1,n_s]}$, generated according to (17), which uses the subset $\mathcal{S}_\beta \subset \mathbb{N}_{[1,N]}$ of transmitted angular frequencies $\omega \in \mathbb{R}^N$ with cardinality $|\mathcal{S}_\beta| = N - Q$. The second bank has $n_p := \begin{pmatrix} N \\ N-2Q \end{pmatrix}$ observers with state $\hat{x}^{\mathcal{P}_\alpha}$, $\alpha \in \mathbb{N}_{[1,n_p]}$, generated according to (17), which uses the subset $\mathcal{P}_\alpha \subset \mathbb{N}_{[1,N]}$ of transmitted angular frequencies $\omega \in \mathbb{R}^N$ with cardinality $|\mathcal{P}_\alpha| = N - Q$.

Finally, the secure state estimate $\hat{x}(t)$ is chosen from the banks of observers as follows:

$$\begin{aligned} \pi_{\mathcal{S}_\beta}(t) &= \max_{\mathcal{P}_\alpha \subset \mathbb{N}_{[1,N]}, |\mathcal{P}_\alpha| = N-2Q} |\hat{x}^{\mathcal{S}_\beta}(t) - \hat{x}^{\mathcal{P}_\alpha}(t)| \\ \sigma(t) &= \operatorname*{argmin}_{\mathcal{S}_\beta \subset \mathcal{P}_\alpha, |\mathcal{S}_\beta| = N-Q} \pi_{\mathcal{S}_\beta}(t),\ \hat{x}(t) = \hat{x}^{\sigma(t)}(t). \end{aligned} \quad (22)$$

We can guarantee the following about the state estimate $\hat{x} = [\ \delta^e \quad \omega^e\ ]^\intercal$, where $\delta^e \in \mathbb{R}^{N-1}$ is the secure estimate of δ and $\omega^e \in \mathbb{R}$ is the secure estimate of the angular frequencies ω in (14) which is used to compute the COI-frequency ω_C^e defined in (6).

Proposition 3: Consider the linearized microgrid model (14) with $\lim_{t\to\infty} u(t) = 0$ and the secure state estimator (17) and (22) under Assumptions 1 and 3. There exist constants $(k, \lambda, \hat{\gamma}, \gamma^m) \in \mathbb{R}^4_{>0}$ such that

$$\begin{aligned} |x(t) - \hat{x}(t)| \leq & k e^{-\lambda t}|x(0) - \hat{x}(0)| + \hat{\gamma}\left(\sup_{s\in[0,t]} |x(s)|\right) \\ & + \gamma^m \left(\sup_{s\in[0,t]} |m(s)|\right), \quad t \in \mathbb{R}_{\geq 0}, \end{aligned} \quad (23)$$

$$\lim_{t\to\infty} \omega_j(t) - \hat{\omega}_j^{\sigma(t)}(t) = 0, \quad j \in \sigma(t), \quad (24)$$

for any initial conditions $x(0) \in \mathbb{R}^{2N-1}$, $\hat{x}(0) \in \mathbb{R}^{2N-1}$.
We obtain from Proposition 3 that in the absence of the deviation of the dynamics from the nominal captured by $m(t)$ and if the state of the linearized model $x(t)$ converges to the origin, the estimated angular frequencies ω^e converge exponentially to the true angular frequencies ω of the linearized model (14). Most crucially, the state estimation error $x(t) - \hat{x}(t)$ is independent of the attacks a^A on the CC's received measurements ω_j^A.

We are now able to show that the model mismatch $m(t)$ introduced by the attack mitigation mechanisms are bounded.

Lemma 2: Consider the linearized microgrid model (14) with input $\lim_{t\to\infty} u(t) = 0$, the secure state estimator (17), (22), and an attack detection/correction mechanism

[1] This is equivalent to the matrix $\mathbf{G}$ for a system with the same overall damping, but without frequency droop. It was shown in [6] that the δ_j of such a system have the same dynamics as the original system. The frequency-related eigenvalue of $\hat{\mathbf{A}}$ lies in the origin.

[2] We use the superscript $\mathcal{K}_\iota$ to denote affiliation with observer with state vector $\hat{x}^{\mathcal{K}_\iota}$, and subscript $\mathcal{K}_\iota$ to denote the stacking of the rows $\kappa \in \mathcal{K}_\iota$ of a vector or a matrix.

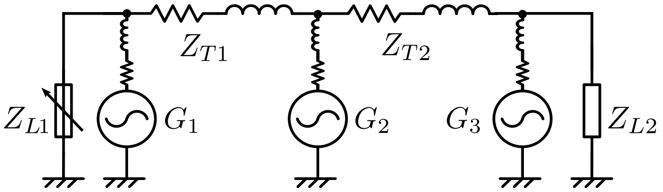


Fig. 2: Microgrid with 3 VSMs and two loads.

defined by (7) with the estimate ω_C^d given by (12) and ω_C^e given by (6). For any $(\Delta_\delta, \Delta_\omega, \epsilon_\omega) \in \mathbb{R}^3_{>0}$, there exist $\beta = \beta(\epsilon_\omega) \in \mathbb{R}_{\geq 0}$ and $K_m = K_m(\Delta_\delta, \Delta_\omega, \epsilon_\omega) \in \mathbb{R}_{>0}$ such that by choosing β_j in (12) as $\beta_j = \beta$, $m(t)$ defined in (9) satisfies $|m(t)| \leq K_m$, for all $t \in \mathbb{R}_{\geq 0}$, $x(0) \in \mathbb{B}_{\Delta_\delta} \times \mathbb{B}_{\Delta_\omega}$ and $\hat{x}(0) \in \mathbb{B}_{\Delta_\delta} \times \mathbb{B}_{\Delta_\omega}$.

We can now show that the secure state estimator presented here satisfies Property 2, which we state formally below.

Theorem 2: Consider the linearized microgrid model (14) with input $\lim_{t\to\infty} u(t) = 0$, the secure state estimator (17), (22), and an attack detection/correction mechanism defined by (7) with the estimate ω_C^d given by (12) and ω_C^e given by (6). Suppose Assumptions 1-3 hold. For any $(\Delta_\delta, \Delta_\omega, \epsilon_\omega) \in \mathbb{R}^3_{>0}$, there exist $\beta = \beta(\epsilon_\omega) \in \mathbb{R}_{\geq 0}$ and $K_e = K_e(\Delta_\delta, \Delta_\omega, \epsilon_\omega) \in \mathbb{R}_{>0}$ such that by choosing β_j in (12) as $\beta_j = \beta$, Property 2 is satisfied.

The proof of Theorem 2 is a straightforward application of Lemma 2, Assumption 2 (bounded states) and Proposition 3. Due to space limitations, we have omitted the proof.

To summarize, we have now shown that both mitigation mechanisms posses the desired Properties 1 and 2 which, together with Assumption 2, allows us to securely control a microgrid with N VSMs. We show this in the next section.

V. Simulation results

We demonstrate the proposed secure control scheme by Matlab Simulink simulations of a microgrid consisting of three VSMs G_1, G_2 and G_3, loads L_1 and L_2, connected over two tielines T_1 and T_2, cf. Fig. 2. Electric components are simulated using the Simscape Specialized Power Systems library and the VSMs are based on [1]. $L_{T1} = L_{T2} = 1$mH, $R_{T1} = R_{T2} = 0.5\Omega$ and the nominal voltage is 230V_{rms}. Attack detection rules employ $\Delta_f^d = \Delta_f^s = 0.5$Hz and $T_f^d = 0.5$s. Initially, only L_2 is connected with $P_{L2} = 6$kW and $Q_{L2} = 3$kVar. The VSMs use constants $M_j = 63Ws^2$, $D_j = 0.2Ws^2$ and $F_j = 4 \cdot D_j$. The voltages required by the FEPS model are $E = [230\ 230\ 230]$V[3]. The system is observable with a single frequency ω_j, i.e. all observability matrices constructed with $\hat{\mathbf{A}}$ and $\mathbf{C}_{\mathcal{K}_\iota}$ have full rank. The two sets of observers of the secure state estimator are $\mathcal{S} = \{\{1,2\},\{1,3\},\{2,3\}\}$ and $\mathcal{P} = \{1,2,3\}$, such that a total of 6 observers are required. The observer gains $\bar{\mathbf{L}}_{\mathcal{K}_\iota}$ are constructed by stacking the columns $\kappa \in \mathcal{K}_\iota$ of matrix $\bar{\mathbf{L}} = 75 \cdot \mathbf{1}^{(N\times N)} + 75\mathbf{I}^{(N)}$. A first order high-pass filter with time constant $T = 5$s is used for the input u to the observers, such that $\lim_{t\to\infty} u(t) = 0$. The matrix $\hat{\mathbf{G}}$ is defined

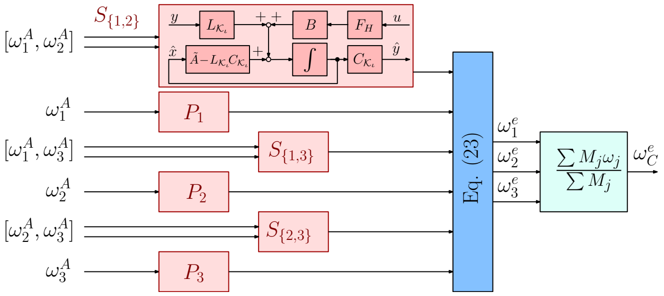


Fig. 3: The secure state estimator at the CC for a grid with 3 VSMs.

using VF-coefficients $\hat{F}_j = (F_j + D_j)$ and no frequency droop $\hat{D}_j = 0$, as was recommended at the end of Sect. IV-A. The AD constant is $\beta = 1e^{-4}$ and finally, $\hat{\mathbf{H}}$, $\hat{\mathbf{G}}$ are

$$\hat{\mathbf{G}} = \begin{bmatrix} -3.33 & 1.67 & 1.67 \\ 1.67 & -3.33 & 1.67 \\ 1.67 & 1.67 & -3.33 \end{bmatrix}, \hat{\mathbf{H}} = \begin{bmatrix} 45.4 & 43.3 \\ -90.1 & 44.7 \\ 44.7 & -88.0 \end{bmatrix}.$$

The structure of the secure state estimator is given in Fig. 3.

In the following, we simulate four events: At $t = 1$s, load 1 connects: $S_{L1} = [3\text{kW}\ 1\text{kVAr}]$, at $t = 2$s, the set-powers change to $P_s = [2\ 6\ 2]kW$, at $t = 3$s, load 1 changes to $S_{L1} = [1\text{kW}\ 0.5\text{kVAr}]$ and at $t = 4$s, the set-powers change back to $P_s = [2\ 2\ 2]kW$. We show the performance of the secure state estimator at the CC, if one of the three received frequencies is attacked as well as results with attacks on the communication channels from the CC to the VSMs[4].

A. Attack on signals sent to the CC

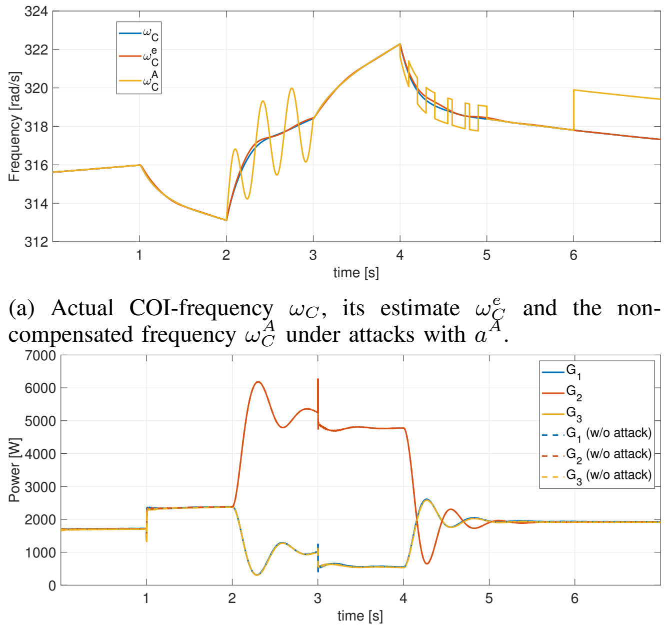
Fig. 4 shows an attack a^A on the signals sent towards the CC with $a^B = 0$: Each attack lasts for 1 second and targets one ω_j sent towards the CC. At first the attack targets ω_1 with a sine-wave of amplitude 4πrad/s, then ω_2 is targeted by a square-wave of amplitude 2rad/s and finally ω_3 sees a constant addition of 2πrad/s. Fig. 4a shows the non-compensated frequency ω_C^A, the output of the multi-observer based estimator ω_C^e and the correct COI-frequency ω_C. Fig. 4b shows the output powers of the VSMs. The system response under attacks (solid lines) is identical with the system response without attacks (dashed lines).

B. Attacks on signals sent to the VSMs

Fig. 5 shows the response of VSM 1 to an attack vector $a^B = [\mu_3 a_0^B\ \ -\mu_5 a_0^B\ \ -\mu_7 a_0^B]^\intercal$ where a_0^B is a square wave with amplitude 2rad/s. The attack cause strong disturbances on the received COI-frequency ω_C^B shown in Fig. 5a. The AD identifies the attack on the first jump of ω_C^B at $t = 2$s (dotted black line). The estimate ω_C^d follows relatively well the actual output of the CC, ω_C^e. The output power of G_1 when the AD is deactivated shows strong oscillations (blue line in Fig. 5b). When the AD is activated, the VSM uses

[3] A MATLAB script to generate the FEPS-model matrices and the linearized model can be found in [13].

[4] For lack of space we only show the results with an attack vector a^B consisting of several square waves. We have further tested undetected delay and replay attacks on the signals sent towards the VSMs and similar performance of the AD could be observed.

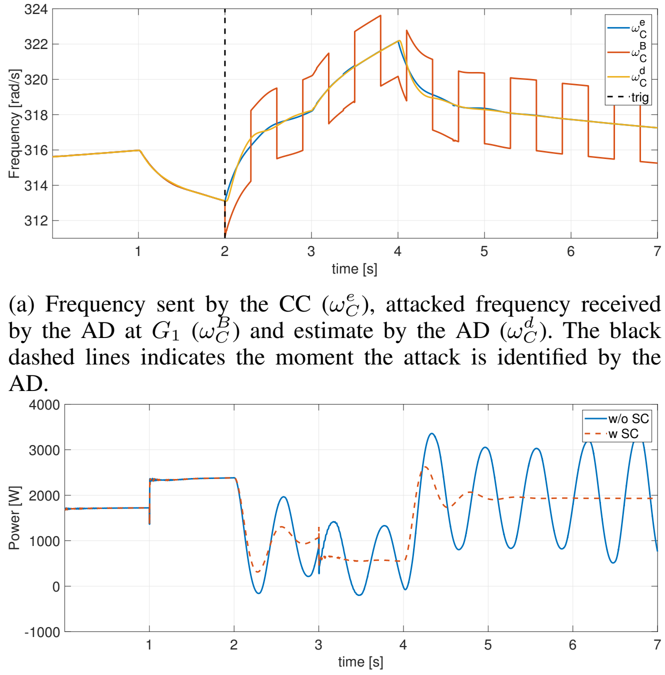


(a) Actual COI-frequency ω_C, its estimate ω_C^e and the non-compensated frequency ω_C^A under attacks with a^A.

(b) Output powers of the VSMs under the attacks and when no attacks are present in the same scenario are identical.

Fig. 4: Attack on signals sent to the CC: At $t = 2$s a sine-wave is added to ω_1, at $t = 4$s a square-wave is added to ω_2 and at $t = 6$s a constant is added to ω_3, each for 1s.

ω_C^d instead of ω_C^B as soon as the attack is identified and the output power is not affected by the attack.



(a) Frequency sent by the CC (ω_C^e), attacked frequency received by the AD at G_1 (ω_C^B) and estimate by the AD (ω_C^d). The black dashed lines indicates the moment the attack is identified by the AD.

(b) Output power of G_1 under attacks with AD deactivated (blue solid line) and activated (red dashed line).

Fig. 5: An attack with vector a^B consisting of square waves.

VI. Conclusion

We have presented a secure control strategy for a microgrid of interconnected VSMs where the communication channels are potentially under attack. The scheme consists of (i) a secure state estimator at the CC and (ii) an attack detection and corrector co-located at each VSM. A robust linear observer design was introduced that ensures zero steady-state output tracking error in the presence of uncertainty in the grid parameters. This scheme is validated in a high fidelity simulation of a microgrid with three VSMs and two loads. Future work will focus on showing that the secure system achieves synchronization.

Appendix

A. Proof of Proposition 1

Given $\epsilon_\omega \in \mathbb{R}_{>0}$, $\Delta_\delta \in \mathbb{R}_{>0}$ and $\Delta_\omega \in \mathbb{R}_{>0}$, we have

- from Assumption 2 that $K_x = K_x(\Delta_x) > 0$ where $\Delta_x := \max\{\Delta_\delta, \Delta_\omega\} > 0$, and
- $K_e > 0$ from Property 2.

Let $j \in \mathbb{N}_{[1,N]}$ and

$$\bar{\beta}_{jk} := \sum_{k\in\mathbb{N}_{[1,N]}} \alpha_{jk}\cos(\varphi_{jk}), \tag{25}$$

where $\alpha_{jk} \in \mathbb{R}_{>0}$ and $\varphi_{jk} \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ for $j \neq k$, are model parameters from (2). Note that $\bar{\beta}_{jk} \in \mathbb{R}_{>0}$ and hence we can choose $\beta_j = \left(2NK_x\bar{\beta}_{jk}\right)^{-1}\epsilon_\omega$ and $\nu_\omega := 2K_x + K_e$.

Recall that the estimate $\omega_{C,j}^d$ is given by (12) which can be rewritten in terms of ω_j and its time derivative as $\omega_{C,j}^d = \omega_j - \beta_j \sum_{k\in\mathbb{N}_{[1,N]}} \alpha_{j,k}\cos(\delta_j - \delta_k - \varphi_{jk})(\omega_j - \omega_k)$. This is obtained by taking the time derivative of $P_{e,j}$ from (2). We have from Lemma 1 that δ_j, for $j \in \mathbb{N}_{[1,N]}$ are small[5]. Hence, $\omega_{C,j}^d \approx \omega_j - \beta_j\bar{\beta}_{jk}\left(\sum_{k\in\mathbb{N}_{[1,N]}} \omega_j - \omega_k\right)$, with $\bar{\beta}_{jk}$ from (25). From Assumption 2, we have that $|\omega_j(t)| \leq K_x$, for all $t \in \mathbb{R}_{\geq 0}$, for some $K_x \in \mathbb{R}_{>0}$. Therefore, for all $t \in \mathbb{R}_{\geq 0}$,

$$|\omega_{C,j}^d(t) - \omega_j| \leq 2NK_x\beta_j\bar{\beta}_{jk}. \tag{26}$$

Next, we observe that $\omega_j - \omega_{C,j}^e = \omega_j - \omega_{C,j}^{\mathrm{n}} + \frac{\sum_{k\in\mathbb{N}_{[1,N]}} M_k(\omega_k^e - \omega_k)}{\sum_{k\in\mathbb{N}_{[1,N]}} M_k}$. According to Property 2, we have $|\omega_k^e(t) - \omega_k(t)| \leq K_e$ for all $t \in \mathbb{R}_{\geq 0}$ and $k \in \mathbb{N}_{[1,N]}$. Hence,

$$|\omega_j(t) - \omega_{C,j}^e(t)| \leq 2K_x + K_e,\ t \in \mathbb{R}_{\geq 0}. \tag{27}$$

Finally, since $|\omega_{C,j}^d(t) - \omega_{C,j}^e(t)| \leq |\omega_{C,j}^d(t) - \omega_j(t)| + |\omega_j(t) - \omega_{C,j}^e(t)|$ and using (26) and (27), we obtain the desired bound (13).

B. Proof of Theorem 1

Let $j \in \mathbb{N}_{[1,N]}$. Given $(\Delta_\delta, \Delta_\omega, \epsilon_\omega) \in \mathbb{R}^3_{>0}$, let $\beta = \beta(\epsilon_\omega) \in \mathbb{R}_{>0}$ and $\nu_\omega = \nu_o(\Delta_\delta, \Delta_\omega) \in \mathbb{R}_{>0}$ come from Proposition 1.

By definition (7) and the detection rules in Section III-B, $\omega_{C,j}(t) = \min\{\omega_{C,j}^d(t), \omega_{C,j}^B(t)\}$. Then, $|\omega_{C,j}(t) -$

[5] For exact construction of the bounds on the initial conditions Δ_δ and Δ_ω, as well as the synchronization point (δ^*, ω^*), the reader is referred to Theorem 1 of [4]

$\omega^e_{C,j}(t)| \le \min\{|\omega^d_{C,j}(t) - \omega^e_{C,j}(t)|, |a^B_j(t)|\}$. Using Proposition 1, we obtain (13) for all initial conditions $(\delta(0), \omega(0)) \in \mathbb{B}_{\Delta_\delta} \times \mathbb{B}_{\Delta_{\delta\omega}}$. Hence, for all $t \in \mathbb{R}_{\ge 0}$,

$$|\omega_{C,j}(t) - \omega^e_{C,j}(t)| \le \min\{\epsilon_\omega + \nu_\omega, |a^B_j(t)|\} \le \epsilon_\omega + \nu_\omega,$$

and we obtain Property 1 with $K_e := \epsilon_\omega + \nu_\omega \in \mathbb{R}_{>0}$.

C. Proof of Proposition 2

In steady-state, we obtain the following from (17):

$$\mathbf{0} = \left[\begin{array}{c:c:c} \mathbf{0} & -\mathbf{1} & \mathbf{I} \\ \hdashline \hat{\mathbf{H}} & \multicolumn{2}{c}{\hat{\mathbf{G}}} \end{array}\right] \hat{x}^\iota + \mathbf{L}^{\mathcal{K}_\iota}(y_{\mathcal{K}_\iota} - \hat{y}_{\mathcal{K}_\iota}), \tag{28}$$

where we omitted writing the dimensions of the matrices. We obtain the relation (28) due to the following

- the observer gain matrix $\mathbf{L}^{\mathcal{K}_\iota}$ is chosen such that the matrix $\hat{\mathbf{A}} - \mathbf{L}^{\mathcal{K}_\iota}\mathbf{C}_{\mathcal{K}_\iota}$ is Hurwitz,
- the input u satisfies $\lim_{t\to\infty} u(t) = 0$,
- $y_{\mathcal{K}_\iota}$ is bounded according to Assumption 2, and
- $\lim_{t\to\infty} y_{\mathcal{K}_\iota}(t) = \lim_{t\to\infty} \omega_{\mathcal{K}_\iota}(t) = \omega^*_{\mathcal{K}_\iota}$ according to Lemma 1, where $\omega_{\mathcal{K}_\iota}$ and $\omega^*_{\mathcal{K}_\iota}$ denote the stacking of the $\kappa \in \mathcal{K}_\iota$ components of the vectors ω and ω^*, respectively;

which implies that the state estimate $\hat{x}^{\mathcal{K}_\iota}$ is bounded and converges to a constant. Hence, we have shown (20). Next, since the observer gain matrix $\mathbf{L}^{\mathcal{K}_\iota}$ satisfies (18), we obtain the following from (28).

- By the first $N-1$ rows of (28), we have
$$\hat{\omega}^{\mathcal{K}_\iota} - \omega^* = (\hat{\omega}_1^{\mathcal{K}_\iota} - \omega_1^*)\mathbf{1}^{(N-1)}, \tag{29}$$
- By the last N rows of (28),
$$\mathbf{0} = \hat{\mathbf{H}}(\hat{\delta}^{\mathcal{K}_\iota} - \delta^*) + \hat{\mathbf{G}}(\hat{\omega}^{\mathcal{K}_\iota} - \omega^*) + \bar{\mathbf{L}}^{\mathcal{K}_\iota}(\omega_{\mathcal{K}_\iota} - \hat{\omega}^{\mathcal{K}_\iota}_{\mathcal{K}_\iota}).$$
By (29), the second term satisfies $\hat{\mathbf{G}}\mathbf{1}^{(N-1)}(\hat{\omega}_1^{\mathcal{K}_\iota} - \omega_1^*)$ and since $\hat{\mathbf{G}}$ has zero row sum, the second term is zero. Let $\hat{\zeta}^{\mathcal{K}_\iota} = [(\hat{\delta}^{\mathcal{K}_\iota} - \delta^*)^\intercal,\ (\omega_{\mathcal{K}_\iota} - \hat{\omega}^{\mathcal{K}_\iota}_{\mathcal{K}_\iota})^\intercal]^\intercal$ and (30) can be written as $\mathbf{0} = \left[\begin{array}{cc} \hat{\mathbf{H}} & \bar{\mathbf{L}}_{\mathcal{K}_\iota} \end{array}\right] \hat{\zeta}^{\mathcal{K}_\iota}$. Due to the matrix (19) being full rank, $\hat{\zeta}^{\mathcal{K}_\iota} = \mathbf{0}$ is a unique solution.

Therefore, we obtain (21) as desired.

D. Proof of Lemma 2

From (9), we have for all $t \in \mathbb{R}_{\ge 0}$ that

$$|m(t)| \le \max\{|\omega^d_C(t) - \omega^{\mathrm{n}}_C(t)|, |\omega^e_C(t) - \omega^{\mathrm{n}}_C(t)|\}. \tag{30}$$

We first obtain a bound on the second term on the RHS as follows for all $t \in \mathbb{R}_{\ge 0}$,

$$|\omega^e_C(t) - \omega^{\mathrm{n}}_C(t)| \le |\omega^e_C(t)| + |\omega^{\mathrm{n}}_C(t)| \le \hat{K}_e + K_x, \tag{31}$$

where $\hat{K}_e \in \mathbb{R}_{>0}$ and $K_x \in \mathbb{R}_{>0}$ come from Proposition 2 and Assumption 2, respectively. Next, the first term on the RHS can be bounded as follows for $t \in \mathbb{R}_{>0}$,

$$\begin{aligned} |\omega^d_C(t) - \omega^{\mathrm{n}}_C(t)| &\le |\omega^d_C(t) - \omega^e_C(t)| + |\omega^e_C(t) - \omega^{\mathrm{n}}_C(t)| \\ &\le K_{de} + \hat{K}_e + K_x, \end{aligned} \tag{32}$$

where the last inequality is obtained with $K_{de} > 0$ from Proposition 1 and from (31) we obtained earlier. Finally, from (30), (31) and (32), we conclude the proof with $K_m := K_{de} + \hat{K}_e + K_x$.

E. Sketch of proof for Proposition 3

For an arbitrary set $\mathcal{K}_\iota \subset \mathbb{N}_{[1,N]}$, the state estimation error $e^{\mathcal{K}_\iota} := x - \hat{x}^{\mathcal{K}_\iota}$ of observer ι has the following dynamics from system (14) and (17),

$$\begin{aligned} \dot{e}^{\mathcal{K}_\iota}(t) =& (\hat{\mathbf{A}} - \mathbf{L}^{\mathcal{K}_\iota}\mathbf{C}_{\mathcal{K}_\iota})e^{\mathcal{K}_\iota}(t) + (\hat{\mathbf{A}} - \mathbf{A})x(t) \\ & - \mathbf{E}m(t) + \mathbf{L}^{\mathcal{K}_\iota}a^A_{\mathcal{K}_\iota}(t), \end{aligned} \tag{33}$$

where $a^A_{\mathcal{K}_\iota}$ denotes the stacking of all the $\kappa \in \mathcal{K}$ component of the attack vector a^A. Since $\hat{\mathbf{A}} - \mathbf{L}^{\mathcal{K}_\iota}\mathbf{C}_{\mathcal{K}_\iota}$ is Hurwitz, the solution to (33) satisfies

$$\begin{aligned} |e^{\mathcal{K}_\iota}(t)| \le& k_{\mathcal{K}_\iota}\exp(-\lambda_{\mathcal{K}_\iota} t)|e^{\mathcal{K}_\iota}(0)| + \hat{\gamma}_{\mathcal{K}_\iota}\left(\sup_{s\in[0,t]}|x(s)|\right) \\ & + \gamma^m_{\mathcal{K}_\iota}\left(\sup_{s\in[0,t]}|m(s)|\right), \quad t \in \mathbb{R}_{\ge 0}, \end{aligned} \tag{34}$$

where $(k_{\mathcal{K}_\iota}, \lambda_{\mathcal{K}_\iota}, \hat{\gamma}_{\mathcal{K}_\iota}, \gamma^m_{\mathcal{K}_\iota}) \in \mathbb{R}^4_{>0}$.

The rest of the proof follows along the lines of the proof for Theorem 3 of [10], which shows that redundant observability and the corresponding multi-observer based architecture (22) allows us to arrive at the guarantee (23). Finally, (24) is obtained using Proposition 2.

References

[1] Z. Kustanovich, S. Shivratri, H. Yin, F. Reissner, and G. Weiss, "Synchronverters with fast current loops," *IEEE Transactions on Industrial Electronics*, vol. 70, no. 11, pp. 11 357–11 367, 2022.

[2] V. Mallemaci, F. Mandrile, S. Rubino, A. Mazza, E. Carpaneto, and R. Bojoi, "A comprehensive comparison of virtual synchronous generators with focus on virtual inertia and frequency regulation," *Electric Power Systems Research*, vol. 201, p. 107516, 2021.

[3] M. Blau and G. Weiss, "Synchronverters used for damping inter-area oscillations in two-area power systems," in *Int. Conf. on Renew. Energies and Power Quality (ICREPQ)*, Salamanca (Spain), 2018.

[4] F. Reissner, H. Yin, and G. Weiss, "A stability result for network reduced power systems using virtual friction and inertia," *IEEE Transactions on Smart Grid*, vol. 13, no. 3, pp. 1668–1678, 2022.

[5] F. Reissner, V. Mallemaci, F. Mandrile, R. Bojoi, and G. Weiss, "Virtual friction subjected to communication delays in a microgrid of virtual synchronous machines," *IEEE J. of Emerging and Selected Topics in Power Electronics*, vol. 11.4, pp. 3910–3923, 2023.

[6] F. Reissner and G. Weiss, "The region of attraction of a grid with virtual synchronous machines employing virtual friction," in *13th IEEE International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, Kiel, Germany, 2022.

[7] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of CPS security," *Annual Rev. in Control*, vol. 47, pp. 394–411, 2019.

[8] Y. Mo, S. Weerakkody, and B. Sinopoli, "Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 93–109, 2015.

[9] R. M. Ferrari and A. M. Teixeira, "A switching multiplicative watermarking scheme for detection of stealthy cyber-attacks," *IEEE Trans. on Automatic Control*, vol. 66, no. 6, pp. 2558–2573, 2020.

[10] M. S. Chong, H. Sandberg, and J. P. Hespanha, "A secure state estimation algorithm for nonlinear systems under sensor attacks," in *59th IEEE Conf. on Decision and Cont. (CDC)*, 2020, pp. 5743–5748.

[11] A. J. Gallo, M. S. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, "A distributed cyber-attack detection scheme with application to dc microgrids," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3800–3815, 2020.

[12] G. Weiss, F. Dörfler, and Y. Levron, "A stability theorem for networks containing synchronous generators," *Systems & Control Letters*, vol. 134, p. 104561, 2019.

[13] F. Reissner, "NRPS model for MATLAB," ZENODO. http://dx.doi.org/10.5281/zenodo.8296331, 2023.