

Weak Resilience of Networked Control Systems

Tomonori Sadamoto^{1,2}, Henrik Sandberg³, Bart Besselink³, Takayuki Ishizaki¹
Jun-ichi Imura¹, and Karl Henrik Johansson³

Abstract—In this paper, we propose a method to establish a networked control system that maintains its stability in the presence of certain undesirable incidents on local controllers. We call such networked control systems *weakly resilient*. We first derive a necessary and sufficient condition for the weak resilience of networked systems. Networked systems do not generally satisfy this condition. Therefore, we provide a method for designing a compensator which ensures the weak resilience of the compensated system. Finally, we illustrate the efficiency of the proposed method by a power system example based on the IEEE 14-bus test system.

I. INTRODUCTION

Many infrastructure and industrial processes, e.g., power networks [1], [2], transportation networks [3] and fabrication plants [4], are integrations of computer-based cyber systems and physical processes. By emerging advanced technologies, the level of integration of the cyber and physical systems has intensified. Along with this, several challenging problems in control system design arise.

Resilient system design is one of the most challenging problem for cyber-physical systems. The concept of resilient system design, which means control system design in an adversarial and uncertain cyber environment, has been introduced in [5]. Furthermore, in [6], the authors have discussed a conceptual property of resilient control systems. Moreover, in [7], the authors have proposed resilient controller design for cyber-physical networked systems under Denial of Service (DoS) attacks which lead to severe time-delays and degradation of control performance. However, it is still an open problem to design resilient systems maintaining an acceptable level of operation or service in face of undesirable incidents on cyber systems, e.g., adversarial attacks and faults caused by human errors.

On the other hand, in [8], the authors have proposed a method for constructing systems whose stability is maintained against any modification of local controllers, which stabilize local subsystems disconnected in the networked system. In this method, we design a supervisory compensator such that the compensated networked system has the property that the stability of the overall closed-loop system is guaranteed against any modification of locally stabilizing

controllers. However, no characterization of compensated networked systems having this property has been shown.

This paper continues the research of [8] and establishes its connection to resilient control design, for the first time. First, we define weakly resilient networked systems such that the overall closed-loop system maintains its stability in the presence of any undesirable incidents on local controllers that maintain local stability (to be defined in Section II). To clarify the class of networked systems which are weakly resilient against undesirable incidents on local controllers, we provide a necessary and sufficient characterization of weakly resilient networked systems. However, networked systems do not generally satisfy the shown necessary condition. Thus, we provide a design method to make a given networked system weakly resilient. Finally, we show the efficiency of the proposed system design through a power system example based on the IEEE 14-bus test system [9].

This paper is organized as follows. In Section II, we introduce and characterize weakly resilient networked systems. In Section III, we consider compensator design such that the networked system is weakly resilient. In Section IV, we show the efficiency of the proposed system design through a numerical example. Finally, concluding remarks are provided in Section V.

Notation: Denote the set of real numbers by \mathbb{R} , the set of complex numbers by \mathbb{C} . Denote the n -dimensional identity matrix by I_n , where we omit the subscript n when no confusion occurs. For $\mathbb{N} := \{1, \dots, N\}$, denote the block-diagonal matrix having matrices M_1, \dots, M_N on its diagonal by $\text{dg}(M_i)_{i \in \mathbb{N}}$. We omit the subscript $i \in \mathbb{N}$ when no confusion occurs. Given signals $x_1(t) \cdots x_N(t)$, denote $x(t) := [x_1^T(t), \dots, x_N^T(t)]^T$, where we omit the time variable t when no confusion occurs. Denote by $\Sigma : u(t) \mapsto y(t)$ a finite-dimensional linear time-invariant system. Given $\kappa : y_1 \mapsto u_1$ and $\Sigma : \{u_1, u_2\} \mapsto \{y_1, y_2\}$, (Σ, κ) denotes the (well-posed) interconnected system with the external input u_2 and external output y_2 . For example, given

$$\kappa : \begin{cases} \dot{\xi} = K\xi + Hy_1 \\ u_1 = M\xi \end{cases}$$

and

$$\Sigma : \begin{cases} \dot{x} = Ax + B_1u_1 + B_2u_2 \\ y_1 = C_1x \\ y_2 = C_2x, \end{cases}$$

(Σ, κ) is the system described by

$$(\Sigma, \kappa) : \begin{cases} \begin{bmatrix} \dot{x} \\ \dot{\xi} \end{bmatrix} = \begin{bmatrix} A & B_1M \\ HC_1 & K \end{bmatrix} \begin{bmatrix} x \\ \xi \end{bmatrix} + \begin{bmatrix} B_2 \\ 0 \end{bmatrix} u_2 \\ y_2 = C_2x. \end{cases}$$

¹Department of Mechanical and Environmental Informatics, Graduate School of Information Science and Engineering, Tokyo Institute of Technology; 2-12-1, Meguro, Tokyo, Japan:
{sadamoto@cyb., ishizaki@, imura@}mei.titech.ac.jp

²Research Fellow of the Japan Society for the Promotion of Science

³School of Electrical Engineering, Automatic Control, Royal Institute of Technology (KTH), SE-100 44 Stockholm, Sweden:
{bart.besselink, hsan, kallej}@ee.kth.se

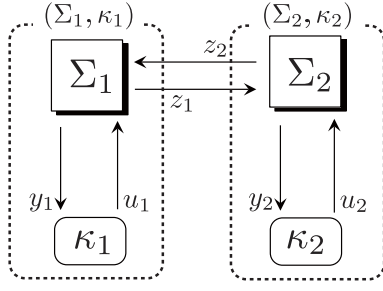


Fig. 1. Overall closed-loop system $(\Sigma, \{\kappa_i\})$

Denote the transfer matrix of the system $\Sigma : u \mapsto y$ by $\Sigma(s)$. The \mathcal{L}_2 -norm of a square integrable function $v(t) : \mathbb{R} \rightarrow \mathbb{R}^n$ is defined by $\|v(t)\|_{\mathcal{L}_2} := (\int_0^\infty v^T(t)v(t)dt)^{\frac{1}{2}}$. The \mathcal{H}_∞ -norm of a stable proper transfer matrix G is defined by $\|G(s)\|_{\mathcal{H}_\infty} := \sup_{\omega \in \mathbb{R}} \|G(j\omega)\|$, where $\|\cdot\|$ denotes the induced 2-norm.

II. WEAKLY RESILIENT NETWORKED SYSTEMS

A. Definition of Weakly Resilient Networked Systems

In this paper, for simplicity, we deal with a cyber-physical networked system composed of two subsystems, which represent dynamical processes in the physical world, and two local controllers, which represent cyber systems. We first give the dynamics of the cyber-physical networked system. For $i \in \{1, 2\}$, the i -th subsystem dynamics are described by

$$\Sigma_i : \begin{cases} \dot{x}_i = A_i x_i + J_i z_j + B_i u_i \\ z_i = S_i x_i \\ y_i = C_i x_i + D_i z_j, \end{cases} \quad j \neq i, \quad (1)$$

where $x_i \in \mathbb{R}^{n_i}$ is the state, $z_i \in \mathbb{R}^{p_i}$ is the subsystem interaction output, $u_i \in \mathbb{R}^{m_i}$ and $y_i \in \mathbb{R}^{q_i}$ are used for interconnection to the i -th local controller explained below. We suppose that z_i and y_i are measurable. The interconnection of Σ_1 and Σ_2 is given by

$$\Sigma : \begin{cases} \dot{x} = Ax + Bu \\ y = Cx, \end{cases} \quad (2)$$

where

$$A = \begin{bmatrix} A_1 & J_1 S_2 \\ J_2 S_1 & A_2 \end{bmatrix}, B = \begin{bmatrix} B_1 & 0 \\ 0 & B_2 \end{bmatrix}, C = \begin{bmatrix} C_1 & D_1 S_2 \\ D_2 S_1 & C_2 \end{bmatrix}. \quad (3)$$

For this networked system Σ , we consider designing local controllers to guarantee the stability of the whole closed-loop system. More specifically, for $i \in \{1, 2\}$, we consider the i -th local controller generating u_i from y_i described by

$$\kappa_i : y_i \mapsto u_i, \quad i \in \{1, 2\}. \quad (4)$$

We denote the set of κ_1 and κ_2 by $\{\kappa_i\}_{i \in \{1, 2\}}$. We omit the subscript $i \in \{1, 2\}$ if no confusion occurs. The entire system $(\Sigma, \{\kappa_i\})$ is shown in Fig. 1. In this paper, we suppose that there exists $\{\kappa_i\}$ stabilizing $(\Sigma, \{\kappa_i\})$.

The local controllers in a cyber environment are sometimes vulnerable to adversaries and may be drastically modified.

For example, in power grids, a local controller stabilizing the frequency of power grids may be modified by attackers to cause power outages. In addition, the controllers may be misconfigured by human errors, which result in malfunctions of the system. In the face of such undesirable incidents, the whole networked system is required to maintain an acceptable level of operation, or at least preserve the stability of the networked system.

As an example of undesirable incidents, let us suppose the following adversarial attack on the local controllers. Local controllers are modified by the attackers to achieve a desirable behavior of the system. However, since the modification with explicit consideration of the overall system dynamics is difficult, the attacker is supposed to focus on the dynamics of the local closed-loop system (Σ_i, κ_i) as shown in Fig. 1, i.e., neglecting the interconnection to $\Sigma_j, j \neq i$. Furthermore, to avoid the detection of attacks as much as possible, we suppose that attackers do not destroy the stability of the local closed-loop system. In view of this, we consider attacks that preserve the stability of local closed-loop systems (Σ_i, κ_i) . In this setting, we define networked systems whose overall stability is guaranteed against any adversarial attacks in the above class as follows:

Definition 1: For each $i \in \{1, 2\}$, consider Σ_i in (1) and κ_i in (4). Define Σ in (2) and the set of locally stabilizing controllers as

$$\mathcal{K}_i := \{\kappa_i | (\Sigma_i, \kappa_i) \text{ is stable}\} \quad (5)$$

for $i \in \{1, 2\}$. The system Σ is said to be *weakly resilient* if $(\Sigma, \{\kappa_i\})$ is stable for any $\kappa_i \in \mathcal{K}_i, i \in \{1, 2\}$.

The reason why we adopt the term *weak resilience* for this condition is that there does not exist a locally stabilizing controller that destabilizes the overall system Σ . Hence, weak resilience, in this sense, appears to be a minimum requirement for the resilience of networked systems.

In the next subsection, we will provide a characterization of weakly resilient networked systems.

B. Characterization of Weakly Resilient Networked Systems

In this subsection, we show a necessary and sufficient condition for the resilience of networked systems in the sense of Definition 1. For simplicity, we assume that the input and output signals of Σ_i in (1) are scalar, i.e.,

$$z_i \in \mathbb{R}, \quad u_i \in \mathbb{R}, \quad y_i \in \mathbb{R}, \quad i \in \{1, 2\}.$$

In this setting, we give the following theorem:

Theorem 1: For each $i \in \{1, 2\}$, consider Σ_i in (1) and κ_i in (4). Define Σ in (2). Suppose (A_i, B_i) is controllable and (A_i, C_i) is observable for each $i \in \{1, 2\}$. The system Σ is *weakly resilient* if, and only if, Σ is a cascade system, i.e.,

$$J_i S_j = 0, \quad D_i S_j = 0 \quad (6)$$

for either $i = 1$ or $i = 2$ and with $j \neq i$.

We emphasize that the cascade property of the system is not only a sufficient condition, but also necessary. In other

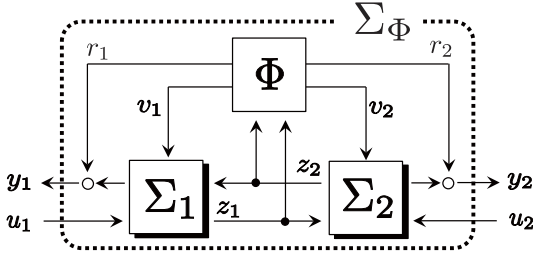


Fig. 2. Compensated system $\Sigma_\Phi := (\Sigma, \Phi)$

words, if the system does not have any cascade realization, the system is not weakly resilient. However, in general, networked systems are not necessarily cascade. Thus, in the next section, let us consider designing a compensator to make networked systems weakly resilient.

III. COMPENSATOR DESIGN FOR WEAK RESILIENCE

In this section, instead of Σ in (2), we deal with networked systems with additional input signals described as

$$\Sigma : \begin{cases} \dot{x} = Ax + Bu + Rv \\ y = Cx + r, \end{cases} \quad (7)$$

where A , B , and C are defined as in (3), and $v \in \mathbb{R}^p$ and $r \in \mathbb{R}^q$ are the additional input signals from the compensator introduced next. We suppose that (A, R) is controllable.

For this system, we consider designing a compensator described by

$$\Phi : \begin{cases} \dot{\phi} = \Lambda\phi + \Gamma z \\ r = \Xi\phi \\ v = \Theta\phi, \end{cases} \quad (8)$$

where $\phi \in \mathbb{R}^n$. Denote the compensated system by $\Sigma_\Phi := (\Sigma, \Phi)$. The network structure of this compensated system is shown in Fig. 2. In this setting, the following corollary follows from Theorem 1:

Corollary 1: Given Σ in (7), consider Φ in (8). Define the interconnected system $\Sigma_\Phi := (\Sigma, \Phi)$. Then, Σ_Φ is weakly resilient if, and only if, $\Sigma_\Phi(s)$ satisfies

$$\Sigma_\Phi(s) = \begin{bmatrix} C_1(sI - A_1)^{-1}B_1 & \sigma(s) \\ 0 & C_2(sI - A_2)^{-1}B_2 \end{bmatrix} \quad (9)$$

with a proper transfer function $\sigma(s)$, or $\Sigma_\Phi(s)$ has a similar lower-triangular form.

Next, we consider designing a compensator such that the transfer matrix $\Sigma_\Phi(s)$ has the form (9). As a related work, noninteracting control based on geometric control theory has been proposed in the literature, e.g., [10], [11], where several off-diagonal elements of the transfer matrix are canceled. However, in general, the diagonal elements of the transfer matrix cannot be arbitrarily designed by the existing methods. Thus, existing methods do not enable us to construct $\Sigma_\Phi(s)$ having the form (9) because the i -th diagonal element of $\Sigma_\Phi(s)$ in (9) must be $C_i(sI - A_i)^{-1}B_i$.

To overcome this difficulty, in this paper, we consider designing a compensator by taking another approach, which was recently developed in [8]. For simplicity, we assume that

$D_i = 0$ in (1). Note that the system Σ in (7) is not a cascade. In this setting, we provide the following compensator on the basis of the state-space expansion technique proposed in [8]:

Proposition 1: Given Σ in (7), consider Φ in (8) with

$$\Lambda = \begin{bmatrix} A_1 & J_1 S_2 \\ 0 & A_2 \end{bmatrix} + R\Theta, \quad \Gamma = \begin{bmatrix} 0 & 0 \\ J_2 & 0 \end{bmatrix}, \quad \Xi = -\text{dg}(C_i), \quad (10)$$

where Θ is given such that it stabilizes $A + R\Theta$. Then, $\Sigma_\Phi := (\Sigma, \Phi)$ is weakly resilient.

Proof: The compensated system Σ_Φ is described by

$$\Sigma_\Phi : \begin{cases} \begin{bmatrix} \dot{\phi} \\ \dot{x} \\ y \end{bmatrix} = \begin{bmatrix} \Lambda & \Gamma \text{dg}(S_i) \\ R\Theta & A \end{bmatrix} \begin{bmatrix} \phi \\ x \end{bmatrix} + \begin{bmatrix} 0 \\ B \end{bmatrix} u \\ y = -\text{dg}(C_i)\phi + \text{dg}(C_i)x. \end{cases} \quad (11)$$

Taking the coordinate transformation $\chi = x - \phi$, we have

$$\begin{cases} \begin{bmatrix} \dot{\phi} \\ \dot{\chi} \\ y \end{bmatrix} = \begin{bmatrix} A + R\Theta & \Gamma \text{dg}(S_i) \\ 0 & A \end{bmatrix} \begin{bmatrix} \phi \\ \chi \end{bmatrix} + \begin{bmatrix} 0 \\ B \end{bmatrix} u \\ y = \text{dg}(C_i)\chi \end{cases} \quad (12)$$

with

$$A := \begin{bmatrix} A_1 & J_1 S_2 \\ 0 & A_2 \end{bmatrix}.$$

Hence, the transfer matrix $\Sigma_\Phi(s)$ has the form (9). Thus, Σ_Φ is weakly resilient. \blacksquare

We note that the compensator Φ in (8) and (10) relies on the use of two control inputs, i.e., v and r . Existing methods in noninteracting control generally only use the signal v . However, the use of only v does generally not allow for obtaining a compensated system of the specific form (9). To this end, the additional control input r is exploited in the controller Φ in (8) and (10).

Furthermore, in Proposition 1, it is shown that the whole closed-loop system $(\Sigma_\Phi, \{\kappa_i\})$ preserves its internal stability against any undesirable incidents on local controllers as long as (Σ_i, κ_i) is stable.

Finally, we show a result on performance degradation of the whole networked system under attacks on local controllers as follows. For simplicity, we take $\phi(0) = 0$ and the initial state of each local controller as zero. We consider a closed-loop system $(\Sigma_\Phi, \{\kappa_i\})$ where Σ_Φ is given as (11), and define x as the state of Σ in this closed-loop system. Furthermore, define χ as the state in the closed-loop system of (12) with local controllers of $\{\kappa_i\}$. In this setting, it follows that

$$\|x(t)\|_{\mathcal{L}_2} \leq (1 + \gamma)\|\chi(t)\|_{\mathcal{L}_2} \quad (13)$$

for all $x(0) = \chi(0) = x_0 \in \mathbb{R}^n$ where $\gamma := \|(sI - (A + R\Theta))^{-1}\Gamma\|_{\mathcal{H}_\infty}$. Note that χ represents the state of the cascade system without interconnection from Σ_1 to Σ_2 . Thus, we can see from (13) that the performance of the overall closed-loop system is bounded by that of the local closed-loop systems. In general, it is not clear to what extent the performance of the whole closed-loop system is deteriorated under attacks on local controllers. In contrast, the compensated system Σ_Φ has an advantage that the

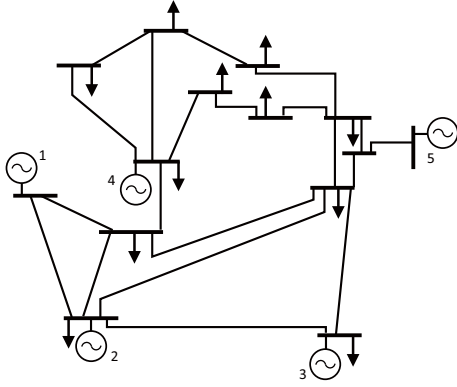


Fig. 3. IEEE 14-bus test system

performance deterioration of the overall closed-loop system can be evaluated by that of the local closed-loop systems.

Remark 1: In [8], we have dealt with a similar compensator Φ but it made the transfer matrix Σ_Φ diagonal. In this case, it has been shown that the rank of Γ in (8) coincides with the sum of the rank of J_i for $i \in \{1, 2\}$. Compared to this, Γ in (10) is a lower-rank matrix. Note that the low-rankness of Γ has a direct relationship to the decay rate of Hankel singular values of Φ . Thus, the compensator provided in this paper has a potential to be approximated by a lower-dimensional system as compared to the compensator considered in [8].

Remark 2: Even if z_i in (1) is not measurable, we can construct a compensator such that the compensated system is weakly resilient by using an observer as follows: We design an observer using

$$w = Sx$$

as a measurable output signal of Σ in (7). Define

$$O : \begin{cases} \dot{\hat{x}} = (A - HS)\hat{x} + \text{dg}(B_i)u + Hw + Rv \\ \hat{z} = \Gamma\hat{x}, \end{cases} \quad (14)$$

where H is given such that $A - HS$ is Hurwitz. Let Φ be given by (10) using \hat{z} instead of z . Then, (Σ, Φ, O) is weakly resilient.

IV. NUMERICAL SIMULATION

A. Power Network Model

In this section, we show the efficiency of the proposed weakly resilient system design through a numerical example. We deal with the IEEE 14-bus power test system provided by [9], where the system involves five generators and 11 loads. The power system is shown in Fig. 3. For $k \in \{1, \dots, 5\}$, the k -th generator dynamics is described by

$$G_{[k]} : \begin{cases} \dot{\zeta}_{[k]} = A_{[k]}\zeta_{[k]} + b_{[k]}u_{[k]} + b_{[k]}v_{[k]} + b_{[k]}^\tau\tau_{[k]} \\ \delta_{[k]} = c\zeta_{[k]}, \end{cases} \quad (15)$$

where the states of $\zeta_{[k]} \in \mathbb{R}^4$ represent the phase angle difference, angular velocity difference, mechanical input difference, and valve position difference. In addition, $u_{[k]} \in \mathbb{R}$

and $v_{[k]} \in \mathbb{R}$ are the angular velocity difference command, $\tau_{[k]} \in \mathbb{R}$ is the electric torque difference from the connected generators, and $\delta_{[k]} \in \mathbb{R}$ is the phase angle difference. Furthermore, the system matrices in (15) are given by

$$A_{[k]} := \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & -D_{[k]}/M_{[k]} & -1/M_{[k]} & 0 \\ 0 & 0 & -1/T_{[k]} & 1/T_{[k]} \\ 0 & 1/K_{[k]} & 0 & -R_{[k]}/K_{[k]} \end{bmatrix}$$

$$b_{[k]} := \frac{1}{K_{[k]}}e_4^4, \quad b_{[k]}^\tau := \frac{1}{M_{[k]}}e_2^4, \quad c := (e_1^4)^\top, \quad (16)$$

where $e_i^n \in \mathbb{R}^n$ is the i -th column of I_n and $M_{[k]}$, $D_{[k]}$, $T_{[k]}$, $K_{[k]}$ and $R_{[k]}$ are an inertia constant, damping coefficient, turbine time constant, governor time constant, and droop characteristic, respectively. These parameters are randomly chosen from the intervals $[0.01, 1]$, $[0.4, 11]$, $[0.01, 0.02]$, $[0.03, 0.7]$ and $[0.01, 0.05]$, respectively. Note that the unit of all physical variables is [p.u.] unless otherwise stated. Furthermore, all loads are modeled as constant power loads, see [9].

We give the interconnection structure among generators by

$$\tau = -Y\delta, \quad (17)$$

where $\tau := [\tau_{[1]}, \dots, \tau_{[5]}]^\top$ and $\delta := [\delta_{[1]}, \dots, \delta_{[5]}]^\top$. In (17), Y compatible with the interconnection structure among generators is calculated by using MATPOWER [9].

Finally, the first to third generators are clustered as the first subsystem, and the others are clustered as the second subsystem. Interconnecting these two subsystems, we have a system Σ in (7) where the state variable is defined as $x = [\zeta_{[1]}^\top, \dots, \zeta_{[5]}^\top]^\top$, and input signals are defined as $u = [u_{[1]}, \dots, u_{[5]}]^\top$ and $v = [v_{[1]}, \dots, v_{[5]}]^\top$. Furthermore, the measurement signal is taken as the angle differences, i.e., $y = [\delta_{[1]}, \dots, \delta_{[5]}]^\top$. For the system matrices of Σ in (7), A is given by

$$A = \text{dg}(A_{[k]}) - \text{dg}(b_{[k]}^\tau)Y(I_5 \otimes c)$$

where \otimes denotes the Kronecker product. In addition, B , R and C are given as the matrices compatible with u , v and y .

B. Demonstration of Compensator Design

In this section, we show the efficiency of the compensator design for the power network given in the previous section.

First, we design the local controllers such that the power flow of the whole closed-loop system tracks a reference signal when no adversarial attacks occur in the local controllers. Since the power flow depends on the angle differences among generators, we construct the local controllers such that the angle difference $y \in \mathbb{R}^5$ tracks a given reference angle signal, denoted by $y^d \in \mathbb{R}^5$. More specifically, given Σ in (7), we consider an augmented system whose states are \hat{x} and the error between y and y^d . For this augmented system, the local controllers $\{\kappa_i\}$ in (4) are designed by LQR design techniques.

To calculate the transient responses of the closed-loop system, we give an initial state of the system and that of the

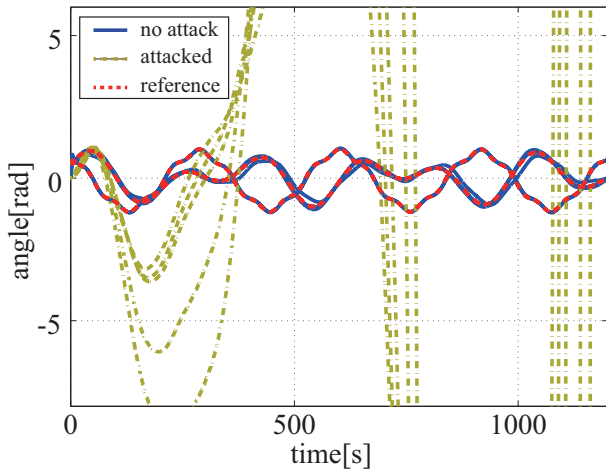


Fig. 4. Transient responses of all generators in $(\Sigma, \{\kappa_i\})$ without using compensator Φ

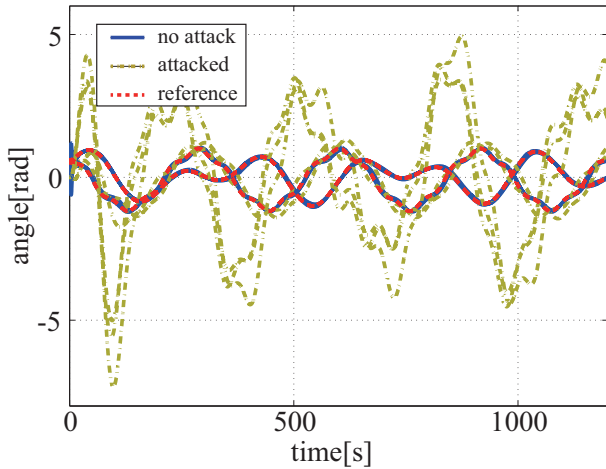


Fig. 5. Transient responses of all generators in $(\Sigma_\Phi, \{\kappa_i\})$

controllers as zero. Furthermore, we give the same reference signal in each subsystem, and each reference signal is taken as a random signal.

In Fig. 4, the blue solid (resp. red dotted) lines show the transient responses (resp. reference signals) of the angle differences of all generators when no attacks occur. We can see from this figure that the transient responses track the reference signals. Furthermore, suppose that the local controllers are modified such that the tracking performance of individual local closed-loop systems gets worse, even though the local closed-loop systems are stable. In Fig. 4, the yellow dash-dotted lines depict the transient responses in this case. We can see from this figure that the instability of the closed-loop system is induced by the attack on the local controllers.

For the augmented networked system, we design Φ in (8) and (10) by minimizing γ in (13), and construct a compensated system (Σ, Φ) . The transient responses of the angle differences of all generators in the case of $(\Sigma_\Phi, \{\kappa_i\})$ are depicted in Fig. 5, where the legends are the same as

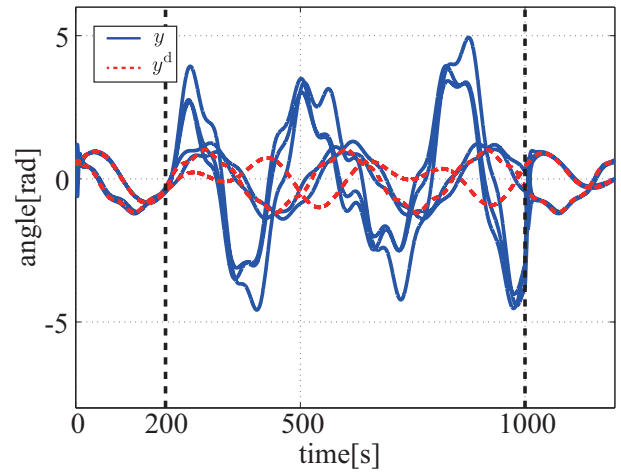


Fig. 6. Demonstration of the power system operation under attacks on local controllers

those in Fig. 4. Furthermore, the (attacked) local controllers are the same as those shown above. From Fig. 5, even though the performance of the closed-loop system becomes worse when the local controllers are attacked, it should be emphasized that the stability of the whole system is preserved under attacks on local controllers by compensating the networked system by Φ .

Finally, we numerically demonstrate the operation of the compensated power system under attacks on local controllers. To simulate this, we suppose a situation where local controllers are attacked while operating the whole system. We plot transient responses of the angle difference of all generators by the blue solid lines in Fig. 6 during $t \in [0, 200)$. Subsequently, we suppose that an attack occurs in the two local controllers at $t = 200$ such that the tracking performance of individual local closed-loop systems gets worse. We can see from this figure around $t \in [200, 1000)$ that the stability of the whole system is preserved even though the tracking performance gets worse. Finally, we suppose that the controllers are recovered at $t = 1000$. As a result, the tracking performance is recovered. As shown in this numerical demonstration, the guarantee of the whole system stability against attacks on local controllers enables us to recover the controller while operating the whole power system.

V. CONCLUSION

In this paper, we have proposed a method to establish a networked control system that maintains its stability in the presence of certain undesirable incidents on local controllers. We call such networked control systems *weakly resilient*. To clarify the class of weakly resilient networked systems, we have provided a necessary and sufficient condition of weakly resilient networked systems. However, networked systems do not generally satisfy the necessary condition shown here in general. Thus, we have provided a method for designing a compensator such that the compensated networked system is weakly resilient. Finally, we have shown the efficiency of

the proposed method through a power system example of the IEEE 14-bus test system.

In this paper, we have dealt with network systems composed of two subsystems, and shown a necessary and sufficient characterization of weakly resilient network systems. The generalization of this characterization to networked systems composed of an arbitrary number of subsystems is under investigation. Furthermore, we have shown a fundamental result of weakly resilient system design under undesirable incidents on local controllers preserving the stability of the local closed-loop system. The extension of this result to incidents destabilizing the system, e.g., the stuxnet attack [12], is amongst the topics of future works.

ACKNOWLEDGMENT

This work was supported by CREST, JST. This work was also supported by Grant-in-Aid for JSPS Fellows Grant Number 14J11344.

REFERENCES

- [1] A. Giani, S. Sastry, K. H. Johansson, and H. Sandberg, "The VIKING project: an initiative on resilient control of power networks," in *Proc. of International Symposium on Resilient Control Systems*, 2009, pp. 31–35.
- [2] P. Kundur, *Power system stability and control*. McGraw-Hill Education, 1994.
- [3] M. G. H. Bell and Y. Iida, *Transportation network analysis*. Wiley, 1997.
- [4] E. D. Knapp and J. T. Langill, *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress, 2014.
- [5] C. G. Rieger, D. Gertman, and M. McQueen, "Resilient control systems: next generation design research," in *Proc. of International Conference on Human System Interactions*, 2009, pp. 632–636.
- [6] D. Wei and K. Ji, "Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights," in *Proc. of International Symposium on Resilient Control Systems*, 2010, pp. 15–22.
- [7] Y. Yuan, Q. Zhu, F. Sun, Q. Wang, and T. Basar, "Resilient control of cyber-physical systems against denial-of-service attacks," in *Proc. of International Symposium on Resilient Control Systems*, 2013, pp. 54–59.
- [8] T. Sadamoto, T. Ishizaki, and J. Imura, "Hierarchical distributed control for networked linear systems," in *Proc. Conference on Decision and Control*, 2014, pp. 2447–2452.
- [9] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, 2011.
- [10] A. S. Morse and W. Wonham, "Status of noninteracting control," *IEEE Transactions on Automatic Control*, vol. 16, no. 6, pp. 568–581, 1971.
- [11] J. C. Willems and C. Commault, "Disturbance decoupling by measurement feedback with stability or pole placement," *SIAM Journal on Control and Optimization*, vol. 19, no. 4, pp. 490–504, 1981.
- [12] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *Security & Privacy, IEEE*, vol. 9, no. 3, pp. 49–51, 2011.
- [13] K. Zhou, J. C. Doyle, and K. Glover, *Robust and optimal control*. Prentice Hall New Jersey, 1996, vol. 40.