Resilient Hierarchical Networked Control Systems: Secure Controls for Critical Locations and at Edge

Azwirman Gusrialdi and Zhihua Qu

Abstract Integration of information and communication technology (ICT) offers new opportunities in improving the management and operation of critical infrastructures such as power systems as it allows connection of different sensors and control components via a communication network, leading to the so-called networked control systems (NCS). However, the use of open and pervasive ICT such as internet or wireless communication technologies comes at a price of making NCS vulnerable to cyber intrusions/attacks which may cause physical damage. This chapter presents control algorithms to ensure resilient and safe operation of NCS under unknown cyber attacks. Specifically, a variant of dynamic watermarking strategies is presented by embedding encoding/decoding components of chaotic signals into the NCS for secure control for critical locations where the measurement/control signals are transmitted to/from the control center via a communication network. In addition, resilient cooperative control algorithms are discussed to ensure safe operation at edge of the NCS which consists of a large number of distributed controllable devices. Several numerical examples are provided to illustrate the proposed control strategies.

Azwirman Gusrialdi
Faculty of Engineering and Natural Sciences, Tampere University, Tampere, Pirkanmaa 33014, Finland. e-mail: azwirman.gusrialdi@tuni.fi

Zhihua Qu
Department of Electrical and Computer Engineering, University of Central Florida, Orlando, Florida 32816, USA. e-mail: qu@ucf.edu

1 Introduction

Information and communication technology (ICT) has been increasingly integrated and deployed into critical infrastructures (i.e., physical systems) such as power systems and transportation systems. ICT offers new opportunities in improving the management and operation of the critical infrastructures. In particular, ICT (also called cyber-layer) provides an efficient way and great flexibility in sharing information between sensors for monitoring purposes and controlling geographically distributed small devices over a communication network which is also known as networked control systems (NCS).

In practice, the control of large-scale complex systems such as power grid is performed in a hierarchical manner. Critical locations are controlled remotely at the control station/center, that is the measurement/control signals are transmitted to/from the control station via a communication network. For example, system protection, i.e., protective relaying is a very crucial component for ensuring the reliability of power system operation. Advanced protective relay schemes involve telecommunications for monitoring and remotely tripping or controlling the breakers of critical equipment in order to clear power faults [1]. Another example is wide-area monitoring and control of power system using real-time measurements from phasor measurement units (PMUs) [2]. To this end, each generator sends its measurement to a cloud or virtual machine which computes the control input. The control inputs are then sent back to the generator for damping the wide-area oscillations. On the other hand, controls at the edge of critical infrastructures call for scalable decision making algorithms to deal with the large number of small and distributed controllable devices. For example, as more Distributed Energy Resources (DERs) - distributed generation, batteries, and controllable loads - are being integrated into the distribution network of future power system, centralized control algorithm where all the data processing and computation are performed at a control center/station will need to be replaced by distributed control algorithm performed by each individual DER by exchanging local information via a communication network to compute their decisions. Distributed optimization and control algorithms have several potential advantages over centralized approaches including scalability to the system's size, robustness with respect to failure of individual agent, and preserving data privacy [3]. It is evident that ICT plays an important role in realizing efficient controls for critical locations and at the edge of the critical infrastructures.

The use of open and pervasive ICT such as internet or wireless communication technologies comes at a price of making NCS vulnerable to cyber intrusions/attacks which may cause physical damage to the critical infrastructure due to the tight coupling between the physical system and cyber-layer [4, 5]. An example of cyber attacks on critical infrastructure is the synchronized and coordinated attack on the Ukraine power grid in 2015 [6], causing a 6-hour blackout and affecting hundreds of thousands of customers. Unfortunately, traditional security solutions in the ICT domain, focussing on data secrecy, integrity, and availability, are not sufficient to ensure the security of NCS [7]. System and control theories have shown promises in analyzing and ensuring security of NCS against intelligent attacks by leveraging fundamental understanding of the physical system dynamics and its interconnection with the cyber components [8]. In this chapter, secure controls for critical locations and at edge of NCS will be presented and discussed from the perspective of system and control theory.

Traditionally, secure control for critical locations is realized by implementing detection algorithm to investigate whether the system is healthy or operating abnormally. A standard and classical detection method is the residual-based detector scheme which is also known as passive detection [9]. However, such detection scheme is undermined by coordinated and stealthy network attacks launched by sophisticated/intelligent adversaries [4]. Recently, there have been efforts in developing active detection methods to detect stealthy attacks launched by intelligent adversaries. The idea is to exploit the knowledge of physical system and alter the system's input or dynamics to detect stealthy attacks [7]. An example of active detection method is physical watermarking achieved by inserting a noisy control input on top of the optimal input of a system [10, 11]. Since the measurement is correlated to the physical watermark through the system dynamics, the absence of watermark in the system output is an indication of a faulty behavior. Other active detection methods include a moving target approach by modifying system matrices or adding additional dynamics [12, 13]. However, these methods may increase installation costs and degrade control performance of NCS in the absence of attacks. Section 2 of this chapter presents a variant of dynamic watermarking based methods to ensure secure control for critical locations. To this end, encoding/decoding components of chaotic signals are embedded into the NCS and designed to detect any stealthy system integrity attacks and also preserve control performance of the NCS in the absence of attacks.

Secure distributed control at the edge of critical infrastructure introduces new challenges due to the system's size and the interaction between the subsystems via the physical interconnection and/or the communication network which prevents the implementation of the previously mentioned approaches. Most of the results on secure distributed control are based on detecting and identifying the attacks followed by isolating the compromised subsystems, see for example [14–17]. However, the strategies have limitations on communication network topology, type of attacks (attacker's strategy) or number of compromised nodes and distributed control problem under consideration. Furthermore, one important issue that needs to be considered in all of these approaches is that the stability of the system may already have been compromised before the attack is detected. Since cyber-attacks cannot be foreseen in advance, it is therefore desirable to design distributed control algorithms so that the overall system becomes resilient against unknown attacks. Such algorithms which are capable of maintaining or restoring systems performance under unexpected events are commonly referred to as resilient control algorithms. Examples of resilient control strategies in power grid include removing/neglecting compromised data [18] and self-organizing of communication architecture [19] in order to mitigate the adverse effects of attacks. While resilient control algorithm is able to ensure the boundedness of physical variables under attacks, operating point of the compromised system may still violate the operational constraint. Hence, it is necessary to guarantee both the resilience and safety of the NCS. In Section 3 of this chapter, distributed control algorithms to ensure the resilient and safe operation of NCS are presented. Specifically, a virtual system interconnected with the distributed control algorithms originally designed under nominal operation of NCS is introduced. The virtual system acts as an anchor which maintains the NCS to operate around its nominal operating point under unknown attacks. Details of the results presented in this chapter including their analysis and proofs can be found in [20–24].

2 Resilient Control for Critical Locations

Consider a networked control system where the physical plant is monitored and controlled remotely via a network by a control center as illustrated in Fig. 1.

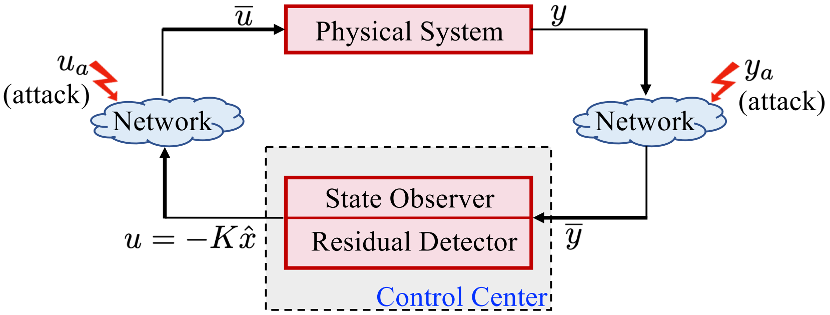


Fig. 1: Network control system and potential cyber attack

Specifically, dynamics of the physical plant is given by the following linear time-invariant systems:

$$\dot{x} = Ax + B\overline{u}, \quad y = Cx, \tag{1}$$

where $x, \overline{u}, y$ denote respectively the plant state, actual control signal applied by the plant, and the plant output/measurement. The measurement is sent to a control center via a communication network. The control center then computes the input signal u which will be sent back to the plant via a network. Furthermore, it is assumed that the triplet (A,B,C) is controllable and observable. The control center implements the following observer-based state feedback control:

$$\dot{\hat{x}} = A\hat{x} + Bu + L(\overline{y} - \hat{y}), \quad \hat{y} = C\hat{x}, \quad u = -K\hat{x}, \tag{2}$$

where $\hat{x}$ denotes the state estimate, $\overline{y}, \hat{y}$ are the measurement received and the output estimate respectively. Moreover gain matrices K, L are chosen such that matrices

$(A-BK)$ and $(A-LC)$ are Hurwitz and the desired performance is achieved in the absence of attacks.

In practice, the communication network may be subject to (unknown) attacks. In other words, the control signal and measurement transmitted via the network may be corrupted given that the attacker gains access to the communication network. To reflect this situation, we write both the received measurement and control signals as

$$\bar{y} = y + y_a,\ \ \bar{u} = u + u_a, \tag{3}$$

where y_a, u_a are the output and input vectors injected to the communication network by the attacker, respectively. In order to detect the presence of such intrusions, the control center is normally equipped with a detection algorithm which detects abnormality such as bad data. For example, the following fault detector based on threshold test [4] over the output residue $z = \bar{y} - \hat{y}$ is widely employed.

$$\begin{cases} \|Wz\| \leq \gamma & \text{normal operation} \\ \|Wz\| > \gamma & \text{abnormal operation} \end{cases}, \tag{4}$$

where W is a weighting matrix and $\gamma \geq 0$ is a threshold chosen by the control center operator.

The adversary aims at launching *stealthy* system integrity attack, that is to steer and manipulate the state of the physical plant to any state that she/he wants (i.e., unsafe state) without being detected by residual detector (4), i.e., $\|Wz\| \leq \gamma$. In addition, if $z - z_n = 0$ where z_n denotes the output residual of the nominal system, i.e., $z_n = (y_n - \hat{y}_n)$ where $y_n/\hat{y}_n$ is the nominal system/observer output of the unattacked control system, then the attack is called *perfectly stealthy*. On the other hand, the control center aims at detecting the presence of such perfectly stealthy attack and further ensuring resiliency of the networked control system against such attack. In the following, we will demonstrate how the adversary launches perfectly stealthy system integrity attack and how the control center could detect the presence of such attack.

2.1 Launching Stealthy Attack

In this subsection, we will discuss how the adversary can launch perfectly stealthy system integrity attack. First, let us assume that the adversary has the information of matrices A, B, and C in model (1) and he/she has gained access to the communication network to inject signals u_a, y_a in (3). Next, consider the case where the attack vectors u_a, y_a are generated by

$$\begin{aligned} &\dot{x}_a = Ax_a + Bu_a,\ \ x_a(t_0) = 0, \\ &u_a = -K_a x_a + Hy + r_a,\ \ y_a = -Cx_a \end{aligned} \tag{5}$$

with $r_a(t) = 0$ for $t \in [0, t_0]$ and for some starting time t_0. Then, the overall dynamics of (1) and (2) under attack (5) and together with the nominal overall dynamics become

$$\begin{cases} \dot{x} = Ax + B(-K\hat{x} - K_a x_a + Hy + r_a) \\ \dot{x}_a = Ax_a + B(-K_a x_a + Hy + r_a) \\ \dot{\hat{x}} = A\hat{x} - BK\hat{x} + L(y + y_a - \hat{y}) \\ \dot{x}_n = Ax_n - BK\hat{x}_n \\ \dot{\hat{x}}_n = A\hat{x}_n - BK\hat{x}_n + L(y_n - \hat{y}_n) \end{cases}, \quad \begin{cases} y = Cx \\ y_a = -Cx_a \\ \hat{y} = C\hat{x} \\ y_n = Cx_n \\ \hat{y}_n = C\hat{x}_n \end{cases}.$$

Applying the state transformation

$$x \longrightarrow x' \overset{\triangle}{=} x - x_a, \quad \hat{x} \longrightarrow e_a \overset{\triangle}{=} x' - \hat{x}, \quad \hat{x}_n \longrightarrow e_n \overset{\triangle}{=} x_n - \hat{x}_n,$$

the state space model becomes

$$\begin{cases} \dot{x}' = (A - BK)x' + BKe_a \\ \dot{x}_a = (A - BK_a + BHC)x_a + BHCx' + Br_a \\ \dot{e}_a = (A - LC)e_a \\ \dot{x}_n = (A - BK)x_n + BKe_n \\ \dot{e}_n = (A - LC)e_n \end{cases}.$$

Consider now the vector $w = e_a - e_n$. It follows that its dynamics are governed by

$$\dot{w} = (A - LC)w, \;\; z - z_n = Cw,$$

with $w(t_0) = 0$. It can be observed that since matrix $(A - LC)$ is Hurwitz, we have $w(t) \equiv 0$ and consequently $z(t) = z_n(t)$ holds for the observations for all $t \in [0, \infty)$ regardless whether there is an attack or not. In other words, the adversary successfully injects system attack vectors u_a, y_a into the network while evading any residual-based detection, i.e., the attack is perfectly stealthy. Intuitively speaking, the adversary exploits the linearity of the system and by using the knowledge of the physical system he/she is capable of designing the output attack vector y_a to cancel out the perturbation on the plant output induced by the input attack vector u_a.

In order to implement perfectly stealthy attack (5), in addition to system matrices A, B and C the adversary also needs to know real-time measurement of the plant output. However, no information of the control input or any other information at the control center, e.g., K and L is required to launch the attack. The adversary cannot only modify the equilibrium point of the plant state but also manipulate the dynamic response of the physical plant by means of exogenous injection r_a and by choosing matrices K_a and H. For example, in order to make the dynamics of the overall system unstable while keeping the attacker's own model stable by itself, the attacker can choose matrices K_a, H in (5) such that $(A - BK_a)$ is stable but $(A - BK_a + BHC)$ is unstable. This can be done with the knowledge of the plant (i.e., matrices A, B and C only), and is independent of the control design (matrix K).

Next, the perfectly stealthy attack described previously is illustrated using simulation on Quadraple-Tank Process with linearized system model described in [25].

It is assumed that the adversary starts launching system integrity attack by injecting exogenous signal r_a in (5) from time $t_0 = 50$ to manipulate the dynamic response of the physical plant. As can be observed from Fig. 2a, the adversary is able to make the state of the physical system deviate from the desired one. Furthermore, the attack cannot be detected by detector in (4) as the measurement residual between the measurement and observer output remains zero as shown in Fig. 2b.

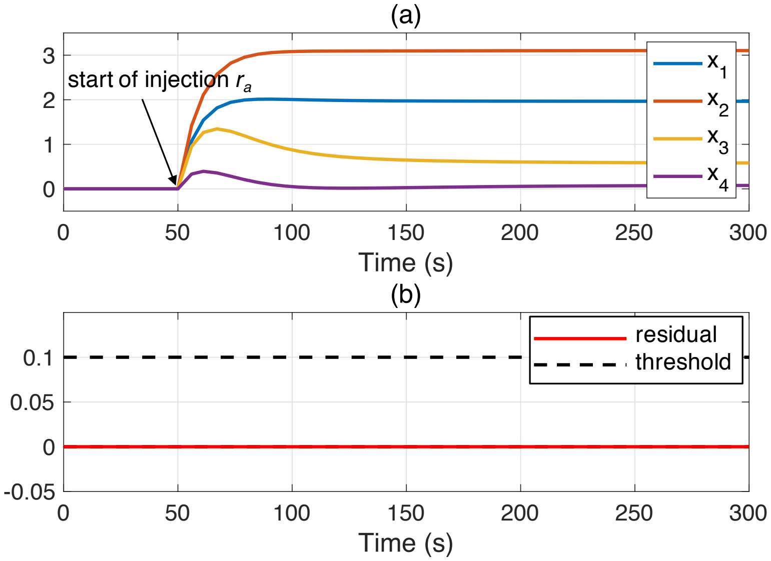


Fig. 2: Perfectly stealthy attack on Quadraple-Tank Process: (a) plant state x where x_i denotes the deviation of water level at the i-th tank from the stationary operating point, (b) residual $\|Wz\|$ and threshold $\gamma = 0.1$

2.2 *Detecting Stealthy Attack*

As demonstrated in the previous subsection, standard attack detection algorithm is not sufficient to detect an attack launched by intelligent adversary. To overcome this problem, the attack detection (4) will be enhanced by embedding nonlinear encoding/decoding components of chaotic signals as illustrated in Fig. 3.

Specifically, at the control center side, the control input which will be transmitted via the communication network is encoded by a nonlinear function generated by a time-varying signal. The compromised observed-based state feedback control with the encoding component can be written as

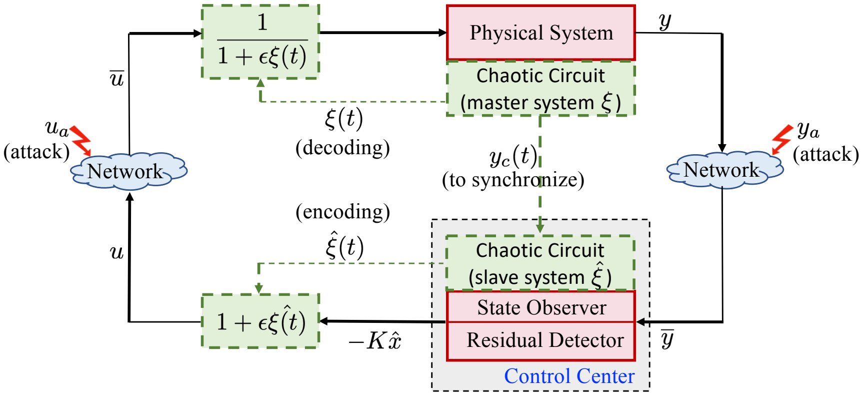


Fig. 3: Protection of networked control system against perfectly stealthy system integrity attacks by embedding nonlinear encoding/decoding components

$$\begin{aligned}
\dot{\hat{x}} &= A\hat{x} + \frac{1}{1+\varepsilon\hat{\xi}}Bu + L(\overline{y}-\hat{y}), \\
u &= -[1+\varepsilon\hat{\xi}]K\hat{x}, \quad ,\hat{y} = C\hat{x}, \quad \overline{y} = y + y_a,
\end{aligned} \tag{6}$$

where $\hat{\xi} \in \mathbb{R}$ denotes the *dynamic encoding signal* and $\varepsilon > 0$ is a scalar value. At the plant side, the encoded control input signal is decoded using another nonlinear function. Dynamics of the compromised physical plant with the decoding component is given by

$$\dot{x} = Ax + \frac{1}{1+\varepsilon\xi}B\overline{u}, \quad y = Cx, \quad \overline{u} = u + u_a, \tag{7}$$

where $\xi \in \mathbb{R}$ denotes the *dynamic decoding signal* and the scalar constant ε is chosen to ensure $\varepsilon|\xi| \leq 0.5$ and $\varepsilon|\hat{\xi}| \leq 0.5$. Intuitively speaking, by adding the nonlinear encoding/decoding components the NCS structure (6), (7) does not hold the linearity property. As a result, it will not be possible for the adversary to launch perfectly stealthy attack using only information of A, B, C. The encoding/decoding signals are generated such that the following conditions are satisfied: (i) the nominal performance of the NCS in the absence of attacks is preserved; (ii) the robustness of NCS against attacks is guaranteed. First, it can be observed from Fig. 3 that if both the decoding and encoding signals are synchronized, i.e., $\lim_{t\to\infty}|\xi(t)-\hat{\xi}(t)| = 0$, the NCS with encoding/decoding components (6), (7) will then recover its nominal performance. Hence, an additional *scalar* output signal y_c called the *synchronization signal* is introduced to guarantee synchronization between the encoding and decoding signals. The synchronization signal is transmitted from the plant side to the control center side as shown in Fig. 3 so that the encoding signal at the control center side will synchronize to the decoding signal at the plant side. Due to this configuration, the physical plant is also called *master* system while the control center is called *slave* system.

The encoding/decoding signals can be generated by any types of chaotic circuits (oscillators), as long as they can be synchronized using an output feedback, which will make it very difficult for the adversary to imitate. One possible choice of such chaotic circuits is Chua's circuit [26, 27]. Specifically, the master system runs the following dynamics

$$\begin{aligned} C_1\dot{v}_1 &= \frac{1}{R_1}(v_2 - v_1) - g(v_1), \\ C_2\dot{v}_2 &= \frac{1}{R_1}(v_1 - v_2) + I, \\ L_1\dot{I} &= -v_2 - R_2 I, \quad y_c = v_1, \end{aligned} \tag{8}$$

where parameters L_1 is an inductor, R_1, R_2 are resistors, C_1, C_2 are capacitors, $v_1, v_2 \in \mathbb{R}$ denote the voltages, $I \in \mathbb{R}$ is the current, and $g(\cdot)$ is a nonlinear function defined as

$$g(v_1) = \begin{cases} \overline{d}v_1 + (\overline{d} - \underline{d})E & \text{if } v_1 \leq E, \\ \overline{d}v_1 > \gamma & \text{if } |v_1| < E, \\ \overline{d}v_1 + (\underline{d} - \overline{d})E & \text{if } v_1 \geq E \end{cases}$$

with $\underline{d} < -1/(R_1 + R_2) < \overline{d} < 0$ and $E > 0$ are constants. Similarly, the slave system runs the following dynamics using the signal received from the master system

$$\begin{aligned} C_1\dot{\hat{v}}_1 &= \frac{1}{R_1}(\hat{v}_2 - \hat{v}_1) - g(\hat{v}_1) + l_c(y_c - \hat{y}_c), \\ C_2\dot{\hat{v}}_2 &= \frac{1}{R_1}(\hat{v}_1 - \hat{v}_2) + \hat{I}, \\ L_1\dot{\hat{I}} &= -\hat{v}_2 - R_2\hat{I}, \quad \hat{y}_c = \hat{v}_1, \end{aligned} \tag{9}$$

where $l_c > 0$ is the coupling gain, $\hat{v}_1, \hat{v}_2, \hat{I}$ are the estimates of v_1, v_2, I, respectively. The parameters, initial conditions, and coupling gain l_c are chosen such that all the master system's variables v_1, v_2, I are both chaotic and uniformly bounded and further the errors $v_1 - \hat{v}_1, v_2 - \hat{v}_2, I - \hat{I}$ are exponentially stable, i.e., both chaotic oscillators are synchronized.

As can be observed, outputs of the chaotic circuits cannot be decoded without the full knowledge of its specific class and parameters together with real-time information of such nonlinear signal, which makes it very hard for the adversary to imitate the plant behaviour properly. In addition, the synchronization signal y_c can be transmitted via a more secure communication channel, separated from the communication network used to transmit the control and output vectors, to further prevent any eavesdropping. In contrast to physical plant's control and output signals of higher dimensions and at different locations, securing a scalar signal such as the synchronization signal is much easier to accomplish.

After ensuring that both chaotic circuits can be synchronized, the next step is to choose both the encoding and decoding signals in (6), (7). For example, both $\xi, \hat{\xi}$

can be chosen as

$$\xi = \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 I, \quad \hat{\xi} = \alpha_1 \hat{v}_1 + \alpha_2 \hat{v}_2 + \alpha_3 \hat{I} \tag{10}$$

with $\alpha_i \geq 0$ and $\sum_i \alpha_i = 1$. For the parameters and coupling gain chosen to ensure synchronization between the master and slave systems, it can be shown that the NCS (6), (7) with encoding/decoding components generated by chaotic circuits (8), (9) is global asymptotically stable in the absence of attacks and also input-to-state stable with respect to attack vector u_a, y_a. In addition, after the two oscillators achieving synchronization the perturbed measurement residual $(z - z_n)$ can be calculated as

$$z - z_n = -C \int_{t_0}^{t} \frac{\varepsilon \xi(\eta)}{1 + \varepsilon \xi(\eta)} e^{(A-LC)(t-\eta)} B u_a(\eta) d\eta$$

which equals to zero (i.e., $z = z_n$) only if there is no attack (or any attack affecting the system), i.e., $u_a = 0$ (or $Bu_a = 0$). Hence, the perfectly stealthy attack can be detected using residual-based attack detector (4). Note that in practice the control center operator needs to choose ε to exceed the detector threshold γ since the magnitude of $z - z_n$ increases as ε increases. Furthermore, since it is in general difficult to generate attack vectors u_a, y_a to compensate the effect of cyber attacks, the proposed NCS structure can also be utilized to detect other types of stealthy attacks.

Let us now return to the previous example of Quadraple-Tank process. As demonstrated in Subsection 2.1, an intelligent adversary is able to launch a perfectly stealthy attack in order to manipulate dynamic response of the physical plant. Fig. 4 shows simulation results for the case of applying the proposed attack-aware NCS structure with embedded encoding/decoding components. As can be observed from Fig. 4b, as the attack being launched the residual shows the oscillating behaviour and as a result the residual detector is triggered. Hence, it can be confirmed that the perfectly stealthy system integrity attack can be detected. The proposed attack-aware NCS structure is also scalable for networked physical systems as the synchronization signal can be multi-cast from the master system to all physical systems equipped with their own slaves.

3 Resilient and Safe Control at The Edge

Cooperative control is one of control design tools that has shown a great promise in optimizing and controlling thousands to millions of devices at the edge of networked control systems [28, 29]. Briefly speaking, the objective of cooperative control is to steer the entity of interest (i.e., physical variable) of each individual system, denoted by $x_i \in \mathbb{R}$, to achieve a non-trivial consensus using only local information. In other words, for an NCS consisting of n individual subsystems we have

$$\lim_{t \to \infty} x_i(t) = c^* \text{ for all individual system } i, \tag{11}$$

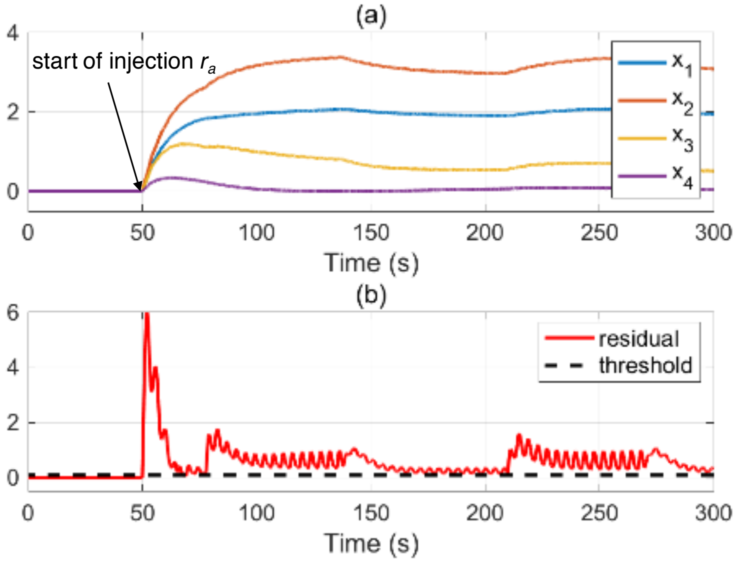


Fig. 4: Detection of perfectly stealthy attack by embedding nonlinear encoding/decoding components: (a) plant state x where x_i denotes the deviation of water level at the i-th tank from the stationary operating point, (b) residual $\|Wz\|$ and threshold $\gamma = 0.1$

or

$$\lim_{t\to\infty} x(t) = x^* = c^*\mathbf{1}, \tag{12}$$

where $x = [x_1, x_2, \cdots, x_n]^T$ and $c^* \in \mathbb{R}$ denotes the nominal operating condition of the overall system. The entity of interest x_i can vary depending on the applications. For example, in optimization and control of power system, x_i can represent the utilization ratio of active power [30] or reactive power [31] produced by the individual distributed generation. Cooperative control which achieves the objective (12) in general is given by the following dynamics

$$\dot{x}_i = \sum_{j=1}^{n} s_{ij}(x_j - x_i), \tag{13}$$

where $s_{ij} = 1$ if the i-th system can receive information from system j via the communication network (i.e., system j is a neighbor of system i) and $s_{ij} = 0$ otherwise. The cooperative control (13) can be written in a compact form as

$$\dot{x} = -L_s x, \tag{14}$$

where L_s is also called a Laplacian matrix which satisfies $L_s\mathbf{1} = 0$. The nominal operating condition c^* in (12) is calculated depending on the information structure (i.e., communication network topology) of the cooperative control algorithms which can be summarized as follows.

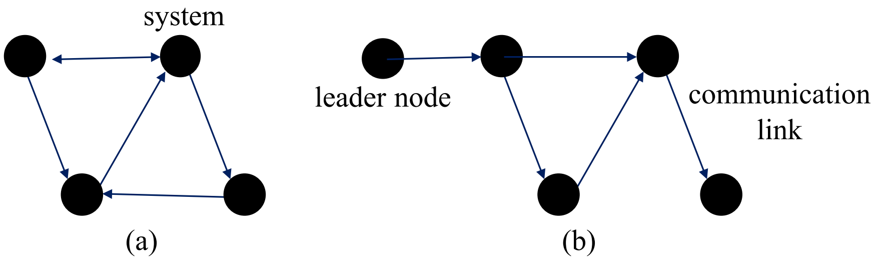


Fig. 5: (a) leaderless, (b) leader-following information structure (communication network topology) for cooperative control algorithm

1. *Leaderless* cooperative control whose information structure is shown in Fig. 5a. Specifically, the communication network structure is given by a strongly connected directed graph, that is every node/system can be reached from any other nodes by following a set of directed edges (communication links) as depicted in Fig. 5a. The nominal operating condition of leaderless cooperative control depends on initial conditions of all the systems in the network. Specifically, it is given by $c^* = v_1^T x(0)$ where v_1 denotes the left eigenvector corresponding to zero eigenvalue of the Laplacian matrix L_s and $x(0)$ is the initial condition of the state $x(t)$. Leaderless cooperative control has been used in different applications, for example to distributively regulate the frequency in power network as discussed in [32].
2. *Leader-following* cooperative control whose communication network topology is illustrated in Fig. 5b. Here the leader node (aggregator/control center/higher level control) provides a reference value, denoted by x_r, that needs to be tracked by all the systems in the network. The cooperative control (14) for leader-following case can be written as

$$\dot{x} = Ax + Bx_r \tag{15}$$

where matrix A is Hurwitz and vector $B \in \mathbb{R}^n$ with its i-th element equals to one if node i can receive information from the leader node and zero otherwise. The consensus (12) is guaranteed given that there exists a sequence of edges (communication links) from the leader node to every other nodes in the network as depicted in Fig. 5b. In addition, the operating condition x^* is given by $x^* = x_r\mathbf{1}$. Leader-following cooperative control has been utilized to distributively regulate the power output of multiple photovoltaic generators in a distribution network [30] and also for real-time scheduling of electric vehicles' charging at a highway [33].

3. The last one is the combination of cooperative control (13) and distributed optimization algorithm designed to solve the following optimization problem

$$\begin{aligned} \underset{x_1,\cdots,x_n}{\text{minimize}} \quad & \sum_{i=1}^{n} f_i(y_i) \\ \text{subject to} \quad & x_1 = \cdots = x_n, \\ & h(y_1,\cdots,y_n,x_1,\cdots,x_n) = 0, \end{aligned} \tag{16}$$

where function $f_i(y_i)$ is strictly convex w.r.t. decision variable x_i. Cooperative control algorithm to solve optimization problem (16) is given by [34]

$$\dot{x}_i = \sum_{j=1}^{n} s_{ij}(x_j - x_i) - k_i g_i(x_i) \tag{17}$$

where $k_i > 0$ is a step size gain and g_i is the subgradient of f_i w.r.t. x_i. Cooperative control (17) can also be written in a compact form as

$$\dot{x} = -L_s x - \overline{K} g(x), \tag{18}$$

where $\overline{K} = diag\{k_i\}$, $g(x) = [g_1(x_1),\cdots,g_n(x_n)]^T$ and the communication network topology is given by a connected bidirectional graph. Furthermore, the operating condition x^* is given by the solution to optimization problem (16). This particular class of cooperative control algorithms has been used to control the reactive power of distributed generations in a distribution network so that the bus voltages are maintained within a certain limit [31], [24].

3.1 Cooperative Control and Intelligent Adversary

While the information and communication technologies (ICT) facilitates the implementation of cooperative control algorithms, it is known that ICT is vulnerable to cyber-intrusions. The adversary may distort the communication channel by adding exogenous signals to modify the neighbors' information that a specific system receives. Therefore, the cooperative control (13) under potential attacks can be written as

$$\dot{x}_i = \sum_{j=1}^{n} s_{ij}(\tilde{x}_{i,j} - \tilde{x}_{i,i}), \tag{19}$$

where

$$\tilde{x}_{i,j} = x_j + \delta_{i,j}, \quad j \in \{\mathscr{N}_i \cup i\}.$$

Here, $\mathscr{N}_i$ is the set of neighbors of node j, i.e., node $j \in \mathscr{N}_i$ if and only if $s_{ij} = 1$ and $\delta_{i,j}$ denotes the injection inserted by the attacker. The attacker aims at destabilizing the overall system or steering the system outside its safety operational constraint without being noticed. In the worst case, the adversary may gain the full knowledge of the network (i.e., matrix L_s), and he/she may attempt to compromise as many as communications links as possible by false data injection. It will be demonstrated in Section 3.3 that the adversary could make the system violate its operational constraint by compromising a small fraction of communication links with bounded injection. The reason that the adversary does not have to have much (or the full) knowledge of the system is because, unless there is a designated leader, a consensus-based cooperative system treats all the entities equally and let all the information propagate throughout the system. Since it is not possible to secure all the communication channels, in the following a resilient cooperative control algorithm is presented to ensure safe operation of the NCS against unknown attacks.

3.2 Resilient and Safe Cooperative Control

The objective is to ensure resilient and safe operation of cooperative controls described previously against unknown attacks. In other words, in addition to ensuring the physical variable x to be bounded, we also aim at maintaining the steady state of x within a safe region around the nominal operating condition, that is

$$\|x(t) - x^*\| \leq \varepsilon \tag{20}$$

for a large t where ε is a pre-defined threshold value. The definition of safety in (20) is motivated by a variety of stability problems in power system. For example, it is important to maintain the frequency or voltages in power grid tightly around the nominal operating value, which can be formulated as in (20).

Design of resilient and safe cooperative control consists of two main steps. In the first step, each subsystem in the network checks and removes the excessively large values of information that it receives from its neighbors. Mathematically, this step can be written as

$$s_{ij} = \begin{cases} 1 & \text{if } \|\tilde{x}_{i,j}\| < \sigma \\ 0 & \text{otherwise} \end{cases}, \tag{21}$$

where σ is a threshold chosen by the designer. The threshold σ is chosen depending on the operational range of the physical variables to be controlled. Threshold-based strategy in (21) can also be utilized to isolate faulty system in the network. After applying (21), the leaderless cooperative control under potential attacks can be written as

$$\dot{x} = -L_s(x - d), \tag{22}$$

where $d_i = \sum_{j=1}^{n} \delta_{i,j}$. Similarly, we can write respectively the leader-following cooperative control and distributed algorithm for solving optimization problem (16) under potential attacks as

$$\dot{x} = Ax + Bx_r + d, \tag{23}$$

and

$$\dot{x} = -L_s(x-d) - \overline{K}g(x). \tag{24}$$

Due to (21), it can be observed that the injection $\|d\|$ is bounded. Note that if there exists faulty systems isolated from the network as a result of (21), then the networked control systems (22), (23) and (24) will be composed of a smaller number of subsystems than the original system, called healthy subsystems and the matrix L_s or A, B represent the communication network topology between the healthy subsystems/nodes. Hence, the above framework can be utilized to address both cyber attacks and also faulty subsystems.

The injection d may be chosen by the adversary to steer the steady state of the networked control system away from the nominal operating condition x^*, i.e., violating (20). In order to overcome this issue, in the second step a resilient and safe cooperative control will be designed by introducing a virtual system with the same number of nodes as the physical system and interconnected with the cooperative system as illustrated in Fig. 6. The virtual system in principle acts as an anchor which will maintain the networked control systems to operate around its optimal operating point under unknown attacks. The cooperative controls (22), (23), (24) interconnected with the virtual system are respectively given by

$$\text{leaderless}\begin{cases}\dot{x} = -L_s(x-d) + \beta\Omega z\\ \dot{z} = -L_h z - \beta\Upsilon x\end{cases}, \tag{25}$$

$$\text{leader-following}\begin{cases}\dot{x} = Ax + \beta\Omega z + Bx_r + d\\ \dot{z} = A_h z - \beta\Upsilon x + \beta B_h x_r\end{cases}, \tag{26}$$

and

$$\text{distributed optimization}\begin{cases}\dot{x} = -L_s(x-d) - \beta\overline{K}g + \beta\Omega z\\ \dot{z} = -L_h z - \beta\Upsilon x\end{cases}. \tag{27}$$

Here, z is the state of the virtual system, scalar $\beta > 0$ is the control gain which adjusts the strength of interconnection between the cooperative and virtual systems, matrices A_h, L_h denote the "internal" dynamics of the virtual system, and Ω, Υ, B_h are the interconnection matrices. The virtual systems (i.e., matrices A_h, L_h) together with its interconnection (i.e., matrices Ω, Υ, B_h) and control gain β need to be designed such that: (i) its interconnection with the networked systems does not impact convergence of the cooperative control; (ii) the robustification strategy is automatically activated when attacks appear anywhere in the system; (iii) the virtual nodes maintain stability of the networked control system under bounded attack signals, i.e., mitigation measures embedded. These properties are highly desirable in designing resilient control algorithms since in practice the attacks cannot be foreseen in advance.

The design of virtual systems in (25), (26) and (27) can be summarized as follows.

1. For the resilient leaderless cooperative control (25), matrix L_h is chosen to be a Laplacian matrix corresponding to arbitrary strongly connected directed graph.

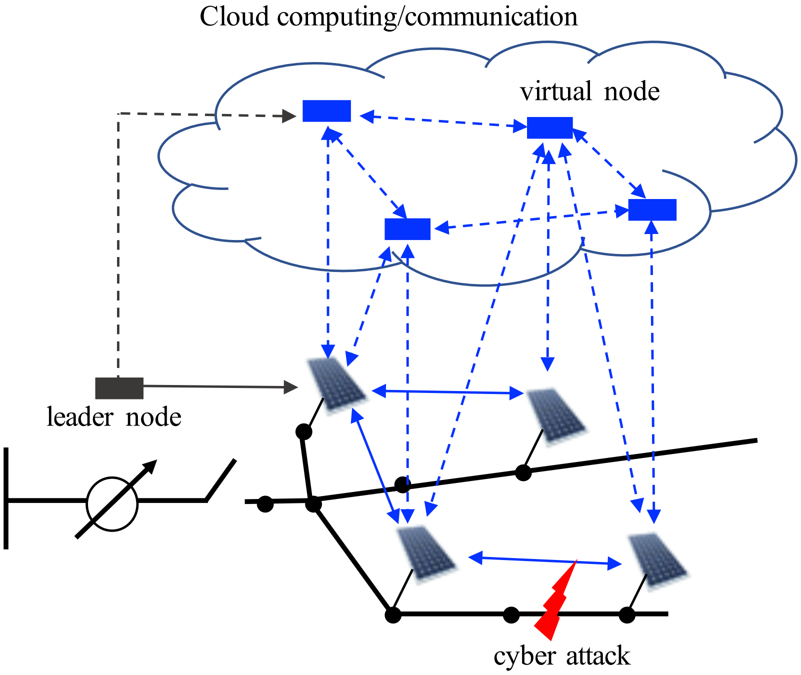


Fig. 6: Resilient design of cooperative control: Interconnection of the cooperative system and virtual system. The dashed-line represent information flow for robustification of cooperative system

Furthermore, we set $\Omega = L_s$ and matrix Υ is chosen as $\Upsilon = \Gamma_h^{-1} L_s^T \Gamma_s$ where $\Gamma_s = diag\{\nu_1\}$ and $\Gamma_h = diag\{\nu_{h1}\}$ with $\nu_{h1}^T L_h = 0$.

2. For the resilient leader-following cooperative control (26), matrix A_h is chosen to be any sparse Hurwitz matrix. Furthermore, Ω is chosen to be any invertible sparse matrix and $\Upsilon = P_h^{-1} \Omega^T P$ where matrices $P, P_h > 0$ satisfy $A^T P + PA < 0$ and $A_h^T P_h + P_h A_h < 0$, respectively. Vector B_h is then calculated as $B_h = \Upsilon \mathbf{1}$.
3. For resilient distributed optimization algorithm (27), we set matrices $L_h = \Omega = \Upsilon = M \Lambda^{\frac{1}{2}} M^T$ where $\Lambda = diag\{0, \lambda_2(L_s), \cdots, \lambda_n(L_s)\}$ and $M = [\nu_1, \cdots, \nu_n]$ with ν_i is the eigenvector of symmetric matrix L_s associated with the eigenvalue $\lambda_i(L_s)$.

In addition, using Lyapunov stability analysis it can be shown that for a sufficiently large value of β and the above choices of interconnection matrices, the state x converges to the operating point around x^*. Specifically, the steady state of physical variable x for leaderless and leader-following cooperative control algorithms can be explicitly calculated as

$$\begin{aligned} \text{leaderless: } & \lim_{t\to\infty} x(t) = x^* + (I+\beta^2 M_g)^{-1}[c_1\mathbf{1}+\beta c_2\mathbf{1}+d^e], \\ \text{leader-following: } & \lim_{t\to\infty} x(t) = x^* - (A+\beta^2 \Omega A_h^{-1} P_h^{-1} \Omega^T P)^{-1} d^e, \end{aligned} \tag{28}$$

where c_1, c_2 are some constants which depend upon initial conditions $x(0), z(0)$ and $d(0)$, matrix M_g satisfies $\Upsilon = L_h M_g$. Note that $d(t)$ can be decomposed into $d(t) = d^e + \tilde{d}(t)$. Hence, from (28) minimum value of the control gain β which ensures the perturbed NCS to operate within a distance ε from its nominal operating condition x^* can be calculated. In practice, the designer can use the upper bound of d^e to calculate the minimum gain β from (28), for example by simply setting $d^e = \sigma$ where σ is defined in (21). For distributed algorithm (27) we can write

$$L_h x^e = (L_h + \beta^2 I)^{-1}[L_s d^e - \beta \overline{K} g(x^e)]$$

where $x^e = \lim_{t\to\infty} x(t)$. It can be observed that $x^e \to c\mathbf{1}$ as control gain β increases. Furthermore, noting that function f_i is strictly convex we have $c \to c^*$ for sufficiently large $\beta > 0$. Hence, the control gain β can be adaptively adjusted so that x_i approximately reaches consensus, i.e., $\|x - c\mathbf{1}\| < \varepsilon$ and since the subgradient $g(x^e)$ is bounded it can be observed that x converges to a point around $c^*\mathbf{1}$ accordingly.

The virtual system can be realized by taking advantage of the cloud computing/communication in combination with software-defined networking (SDN) [35] which has been shown to be a promising architecture for promoting distributed decision making in cyber-physical systems [36]. Briefly speaking, SDN provides a flexibility to direct traffic in a network as it separates the part of the networking infrastructure that decides where information is being sent from the part where the data actually moves, and allows the decision making part to happen in the software application. In addition, as its name suggests the virtual node is not a physical node and its state has no physical meaning which makes it less observable to the adversary. While the addition of such a virtual system incurs an additional cost of increased communication, such a burden is manageable and the corresponding computation is minimal since both the communication and computation are performed distributively and using one of the standard network technologies. The framework has been recently utilized to deal with partially unknown nonlinear systems [37] and also multiple types of actuator attacks [38].

3.3 An Illustrative Example

The resilient and safe cooperative control described in the previous subsection is applied to voltage control problem in a distribution network with high penetration of renewable energy sources [24]. High penetration of renewable energy sources or distributed generations (DGs) in distribution network may lead to local congestion, e.g., over-voltage problem. One possible approach to overcome this issue is by distributively controlling the reactive power of DGs such as the voltage deviation of all DG buses satisfy the operational constraint of

$$|1 - V_i| \leq 0.05 p.u.$$

where V_i denotes the voltage of the ith DG. The problem can then be formulated as optimization problem in the form of (16) given by

$$\begin{aligned} \underset{x_1,\cdots,x_n}{\text{minimize}} \quad & \sum_{i=1}^{n} (V_i - V_i^*)^2 \\ \text{subject to} \quad & x_1 = \cdots = x_n, \\ & \text{AC power flow}, \end{aligned} \tag{29}$$

where x_i denotes the utilization ratio of reactive power of DG i. The first constraint means that all DGs contribute equally to the voltage regulation while the second constraint physically couples the decision variable x_i with the voltage V_i. The values $V_i^* \in (0.95, 1.05)$ denote the operating condition of the system voltages in order to ensure power quality and are calculated at a higher level control authority by solving a distributed optimal power flow [39]. Given that the total maximum available reactive power is sufficient to regulate the voltages, then there exists a consensus solution x^* to optimization (29). The solution can be calculated in a distributed manner using distributed algorithm (18) where the communication graph is assumed to be connected and undirected.

Cooperative control (18) is implemented in IEEE-8500 node system consisting of seven photovoltaics (PVs) as shown in Fig. 7 and communication network topology of the PVs is given in Fig. 8. First, consider the nominal operation under cooperative control (18) in the absence of attacks. As can be observed from Fig.9a and Fig.9b,

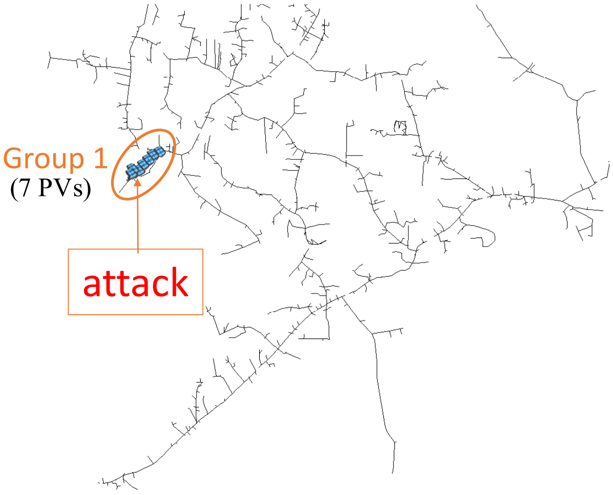


Fig. 7: IEEE 8500-node system

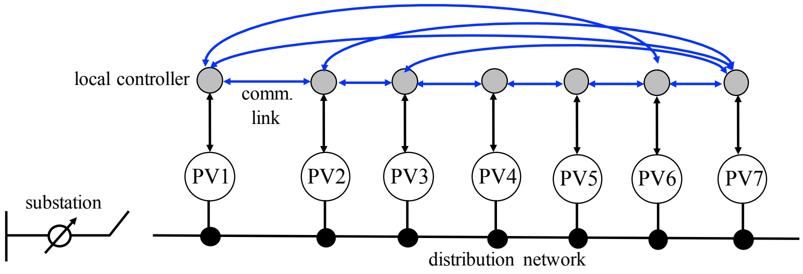


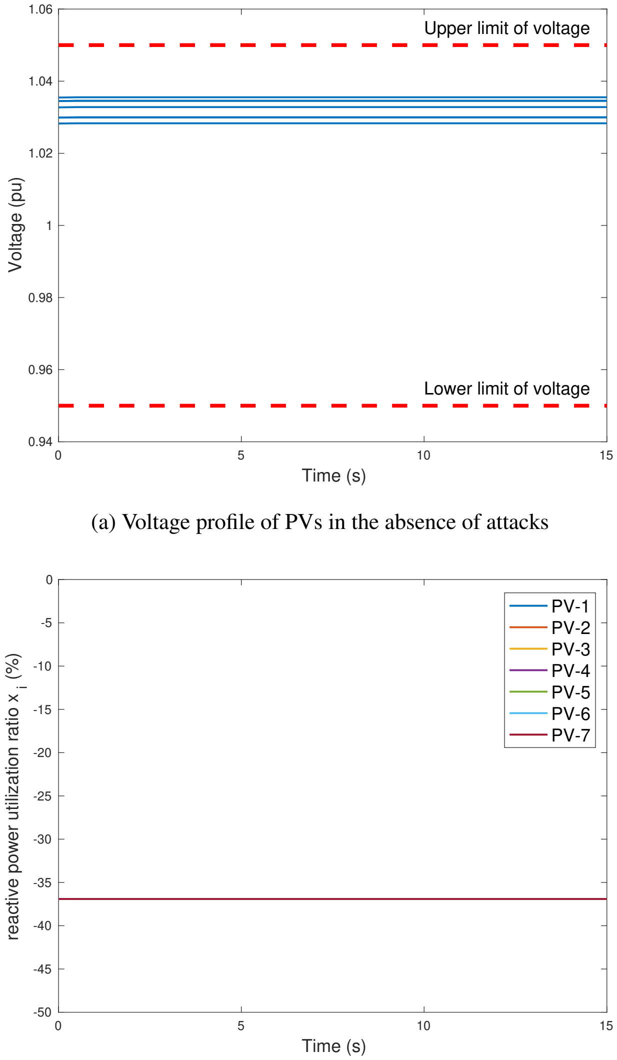
Fig. 8: Communication network topology for cooperative control

cooperative control (18) is able to maintain the system voltages within the limit while ensuring all PVs contribute equally to the voltage regulation. Next, assume that the information sent from PV-6 is being compromised. Simulation results for cooperative control under attack (24) are shown in Fig. 10. As can be observed from Fig. 10a, even though the states x are still bounded, the adversary is able to make the system voltages violate the operational constraint, i.e., yielding an over-voltage problem, by injecting bounded signal into the communication link. In addition, we can see from Fig. 10b that the reactive power utilization ratios also fail to reach a consensus. Finally, in order to maintain resilient and safe operation of the system voltages, we apply resilient cooperative control (27) under attacks whose results are shown in Fig. 11. As can be observed, the system voltages are regulated within the operational constraint and the reactive power utilization ratios are close to the nominal operating condition x^*.

4 Conclusions

The chapter presents resilient hierarchical networked control systems. First, a variant of dynamic watermarking strategies is presented by embedding encoding/decoding components of chaotic signals into the NCS for secure control for critical locations where the measurement/control signals are transmitted to/from the control center via a communication network. Next, resilient cooperative control algorithms by introducing a virtual system which acts as an anchor are discussed to ensure safe operation at the edge of the NCS which consists of a large number of control devices. The proposed control algorithms can be implemented using the state-of-the-art networking technologies such as cloud computing/communication and software-defined networking. The performance of resilient control strategies are demonstrated using several numerical examples.

Acknowledgements The work of A. Gusrialdi was supported by the Academy of Finland under Academy Project decision number 330073. The work of Z. Qu is supported in part by

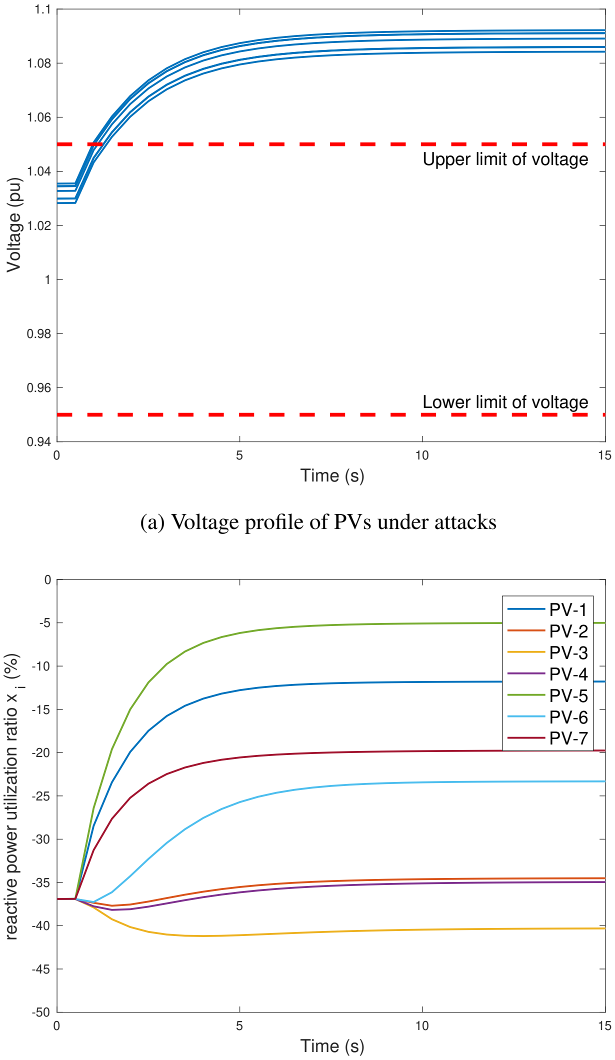


(a) Voltage profile of PVs in the absence of attacks

(b) Reactive power utilization ratio of PVs in the absence of attacks

Fig. 9: Cooperative control (18) in the absence of attacks

US National Science Foundation under grant ECCS-1308928, by US Department of Energy's awards DE-EE0009152, DE-EE0009028, DE-EE0007998, DE-EE0007327, DE-EE0006340, and DE-EE0009339.



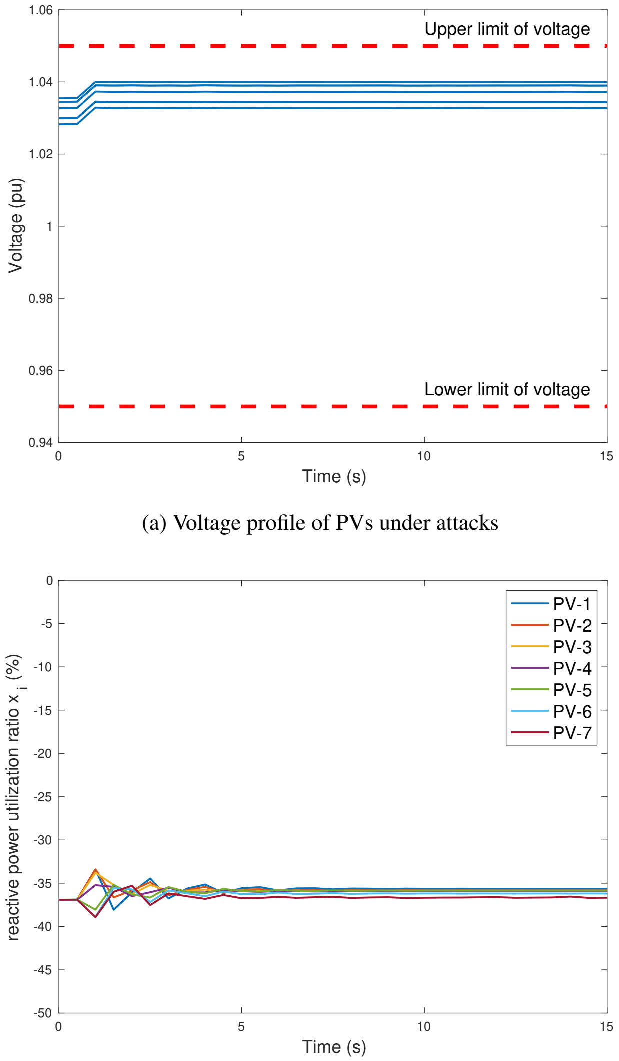
(a) Voltage profile of PVs under attacks

(b) Reactive power utilization ratio of PVs under attacks

Fig. 10: Cooperative control under attack (24). System voltages violate the operational constraint

References

1. Blume, S.W.: High Voltage Protection for Telecommunications, vol. 44. John Wiley & Sons (2011)



(a) Voltage profile of PVs under attacks

(b) Reactive power utilization ratio of PVs under attacks

Fig. 11: Resilient and safe cooperative control againts attack (27). System voltages can be maintained within the operational constraint

2. Chakrabortty, A., Khargonekar, P.P.: Introduction to wide-area control of power systems. In: Proceedings of American Control Conference, pp. 6758–6770. IEEE (2013)
3. Molzahn, D.K., Dörfler, F., Sandberg, H., Low, S.H., Chakrabarti, S., Baldick, R., Lavaei, J.: A survey of distributed optimization and control algorithms for electric power systems. IEEE Transactions on Smart Grid **8**(6), 2941–2962 (2017)

4. Gusrialdi, A., Qu, Z.: Smart grid security: Attacks and defenses. In: J. Stoustrup, A. Annaswamy, A. Chakrabortty, Z.Q. (Eds.) (eds.) Smart Grid Control: An Overview and Research Opportunities, pp. 199–223. Springer Verlag (2018)
5. Liu, X., Qian, C., Hatcher, W.G., Xu, H., Liao, W., Yu, W.: Secure internet of things (iot)-based smart-world critical infrastructures: Survey, case study and research opportunities. IEEE Access **7**, 79,523–79,544 (2019)
6. Pultarova, T.: Cyber security - ukraine grid hack is wake-up call for network operators [news briefing]. Engineering Technology **11**(1), 12–13 (2016)
7. Weerakkody, S., Sinopoli, B.: Challenges and opportunities: Cyber-physical security in the smart grid. In: J. Stoustrup, A. Annaswamy, A. Chakrabortty, Z. Qu (eds.) Smart Grid Control: An Overview and Research Opportunities, pp. 257–273. Springer Verlag (2019)
8. Dibaji, S.M., Pirani, M., Flamholz, D.B., Annaswamy, A.M., Johansson, K.H., Chakrabortty, A.: A systems and control perspective of cps security. Annual Reviews in Control **47**, 394–411 (2019)
9. Frank, P.M.: Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy: A survey and some new results. automatica **26**(3), 459–474 (1990)
10. Mo, Y., Weerakkody, S., Sinopoli, B.: Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs. IEEE Control Systems Magazine **35**(1), 93–109 (2015)
11. Satchidanandan, B., Kumar, P.R.: Dynamic watermarking: Active defense of networked cyber–physical systems. Proceedings of the IEEE **105**(2), 219–240 (2016)
12. Weerakkody, S., Sinopoli, B.: Detecting integrity attacks on control systems using a moving target approach. In: 2015 54th IEEE Conference on Decision and Control (CDC), pp. 5820–5826. IEEE (2015)
13. Teixeira, A., Shames, I., Sandberg, H., Johansson, K.H.: Revealing stealthy attacks in control systems. In: 2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton), pp. 1806–1813. IEEE (2012)
14. Pasqualetti, F., Bicchi, A., Bullo, F.: Consensus computation in unreliable networks: A system theoretic approach. IEEE Transactions on Automatic Control **57**(1), 90–104 (2011)
15. LeBlanc, H.J., Zhang, H., Koutsoukos, X., Sundaram, S.: Resilient asymptotic consensus in robust networks. IEEE Journal on Selected Areas in Communications **31**(4), 766–781 (2013)
16. Huang, Y., Tang, J., Cheng, Y., Li, H., Campbell, K.A., Han, Z.: Real-time detection of false data injection in smart grid networks: An adaptive cusum method and analysis. IEEE Systems Journal **10**(2), 532–543 (2014)
17. Zhuang, P., Deng, R., Liang, H.: False data injection attacks against state estimation in multiphase and unbalanced smart distribution systems. IEEE Transactions on Smart Grid **10**(6), 6000–6013 (2019)
18. Abhinav, S., Modares, H., Lewis, F.L., Davoudi, A.: Resilient cooperative control of dc microgrids. IEEE Transactions on Smart Grid **10**(1), 1083–1085 (2019)
19. Cameron, C., Patsios, C., Taylor, P., Pourmirza, Z.: Using self-organizing architectures to mitigate the impacts of denial-of-service attacks on voltage control schemes. IEEE Transactions on Smart Grid **10**(3), 3010–3019 (2019)
20. Joo, Y., Qu, Z., Namerikawa, T.: Resilient control of cyber-physical system using nonlinear encoding signal against system integrity attacks. IEEE Transactions on Automatic Control (2020, submitted)
21. Gusrialdi, A., Qu, Z., Simaan, M.A.: Competitive interaction design of cooperative systems against attacks. IEEE Transactions on Automatic Control **63**(9), 3159–3166 (2018)
22. Gusrialdi, A., Qu, Z., Simaan, M.: Robust design of cooperative systems against attacks. In: Proceedings of American Control Conference, pp. 1456–1462 (Portland, OR, June 4-6, 2014)
23. Gusrialdi, A., Qu, Z., Simaan, M.A.: Game theoretical designs of resilient cooperative systems. In: Proceedings of European Control Conference, pp. 1705–1711 (2015)
24. Gusrialdi, A., Xu, Y., Qu, Z., Simaan, M.A.: Resilient cooperative voltage control for distribution network with high penetration distributed energy resources. In: Proceedings of European Control Conference, pp. 1533–1539 (2020)

25. Johansson, K.H.: The quadruple-tank process: A multivariable laboratory process with an adjustable zero. IEEE Transactions on control systems technology **8**(3), 456–465 (2000)
26. Matsumoto, T.: A chaotic attractor from chua's circuit. IEEE Transactions on Circuits and Systems **31**(12), 1055–1058 (1984)
27. Matsumoto, T., Chua, L., Komuro, M.: The double scroll. IEEE Transactions on Circuits and Systems **32**(8), 797–818 (1985)
28. Qu, Z.: Cooperative control of dynamical systems: applications to autonomous vehicles. Springer Science & Business Media (2009)
29. Gusrialdi, A., Xu, Y., Qu, Z., Simaan, M.A.: A real-time big-data control-theoretical framework for cyber-physical human systems. In: M.J. Blondin, P.M. Pardalos, J.S. Sanchis (eds.) Computational Intelligence and Optimization Methods for Control Engineering, pp. 149–172. Springer Verlag (2019)
30. Xin, H., Qu, Z., Seuss, J., Maknouninejad, A.: A self-organizing strategy for power flow control of photovoltaic generators in a distribution network. IEEE Transactions on Power Systems **26**(3), 1462–1473 (2010)
31. Maknouninejad, A., Qu, Z.: Realizing unified microgrid voltage profile and loss minimization: A cooperative distributed optimization and control approach. IEEE Transactions on Smart Grid **5**(4), 1621–1630 (2014)
32. Zhao, C., Mallada, E., Dörfler, F.: Distributed frequency control for stability and economic dispatch in power networks. In: Proc. American Control Conference, pp. 2359–2364. IEEE (2015)
33. Gusrialdi, A., Qu, Z., Simaan, M.A.: Distributed scheduling and cooperative control for charging of electric vehicles at highway service stations. IEEE Transactions on Intelligent Transportation Systems **18**(10), 2713–2727 (2017)
34. Yang, T., Yi, X., Wu, J., Yuan, Y., Wu, D., Meng, Z., Hong, Y., Wang, H., Lin, Z., Johansson, K.H.: A survey of distributed optimization. Annual Reviews in Control **47**, 278–305 (2019)
35. Kreutz, D., Ramos, F.M., Verissimo, P., Rothenberg, C.E., Azodolmolky, S., Uhlig, S.: Software-defined networking: A comprehensive survey. Proceedings of the IEEE **103**(1), 14–76 (2015)
36. Freris, N.M., et al.: A software defined architecture for cyberphysical systems. In: Fourth International Conference on Software Defined Systems, pp. 54–60 (2017)
37. Huang, X., Dong, J.: Adp-based robust resilient control of partially unknown nonlinear systems via cooperative interaction design. IEEE Transactions on Systems, Man, and Cybernetics: Systems (2020)
38. Huang, X., Dong, J.: A robust dynamic compensation approach for cyber-physical systems against multiple types of actuator attacks. Applied Mathematics and Computation **380**, 125,284 (2020)
39. Xu, Y., Sun, W., Qu, Z.: Renewable energy integration and system operation challenge: Control and optimization of millions of devices. In: H. Jiang, Y. Zhang, E. Muljadi (eds.) New Technologies for Power System Operation and Analysis. Elsevier (2020)