Optimal Switching Attacks and Countermeasures in Cyber-Physical Systems

Guangyu Wu, Gang Wang, *Member, IEEE*, Jian Sun, *Member, IEEE*, and Lu Xiong

***Abstract*—The work analyzes dynamic responses of a healthy plant under optimal switching data-injection attacks on sensors and develops countermeasures from the vantage point of optimal control. This is approached in a cyber-physical system setting, where the attacker can inject false data into a selected subset of sensors to maximize the quadratic cost of states and the energy consumption of the controller at a minimal effort. A 0-1 integer program is formulated, through which the adversary finds an optimal sequence of sets of sensors to attack at optimal switching instants. Specifically, the number of compromised sensors per instant is kept fixed, yet their locations can be dynamic. Leveraging the embedded transformation and mathematical programming, an analytical solution is obtained, which includes an algebraic switching condition determining the optimal sequence of attack locations (compromised sensor sets), along with an optimal state-feedback-based data-injection law. To thwart the adversary, however, a resilient control approach is put forward for stabilizing the compromised system under arbitrary switching attacks constructed based on a set of state-feedback laws, each of which corresponds to a compromised sensor set. Finally, an application using power generators in a cyber-enabled smart grid is provided to corroborate the effectiveness of the resilient control scheme and the practical merits of the theory.**

***Index Terms*—Data-injection attacks, dynamic set, resilient control, switching condition.**

I. Introduction

CYBER-PHYSICAL systems (CPSs) inherit the communication structure of the Internet of Things (IoT), yet they place more emphasis on the monitoring and control of entities in the physical world [1]. These systems are typically composed of a set of networked agents, that includes sensors, actuators, controllers, and communication devices. Heterogeneous devices are connected to collaboratively control the physical processes over high-speed communication networks [2]. CPSs realize the feedback and information exchange between the cyberspace and the physical world. Nonetheless, the deep integration of physical and information systems brings potential threats too [3]. Real-world applications are safety-critical: their failure can cause irreparable harm to the physical system being controlled and to people who rely on it. As a typical application of CPSs, the cyber-enabled smart grid comprises a large number of servers, computers, meters, phasor measurement units, generators, and so on. By blocking the information exchange between the users and the electricity sectors or destroying the data integrity [4], [5], the adversary can affect the electricity price and increase the energy consumption of generators [6].

To enhance the security of CPSs, the defender should be aware of diverse attack behaviors that the CPS may suffer as well as understand the attacker's intention [7]. Malicious attacks on CPSs can be launched at the physical layer, network layer [8], and application layer [9]. A common way to enhance the resilience of CPSs is to implement defense strategies against known attack patterns [10]. The resilient control or estimation focuses on mitigating the normal operation of attacked systems or restoring the actual state variables with certain acceptable error bounds [11]. Most advances impose assumptions on the attacker's abilities [12] or on its behavior patterns [13]. The resilient controller under fixed delay or out-of-order transmissions was proposed to optimize the worst-case performance [14]. An output-feedback controller under deception attacks with stochastic characteristics was designed to guarantee the prescribed security in probability while obtaining an upper bound of a quadratic cost criterion [15].

On the other hand, studying the adversary's optimal attack schedule can in turn offer insight on devising effective defense strategies [16]. A family of cyber attacks with switching behaviors has attracted attention, which can be categorized into two groups: 1) location-switching attacks and 2) signal-switching attacks. The attack signal can be, for instance, a switching signal turning on or off electrical devices and change the network topology [17] or a continuous false signal injected into controllers or actuators. State recovery under location switching attacks with known or unknown switching frequencies was studied in [18]. Stochastic linear

Manuscript received March 26, 2019; revised July 27, 2019; accepted September 24, 2019. The work of G. Wu and J. Sun was supported in part by NSFC under Grant 61522303, Grant U1509215, and Grant 61621063, and in part by the Program for Changjiang Scholars and Innovative Research Team in University under Grant IRT1208. The work of G. Wang was supported by NSF under Grant 1514056 and Grant 1711471. The work of L. Xiong was supported in part by NSFC under Grant 51975414, and in part by the National Key Research and Development Program of China 2018 under Grant YFB0105101. This article was recommended by Associate Editor Y. Zhao. *(Corresponding author: Gang Wang.)*

G. Wu and L. Xiong are with the Clean Energy Automotive Engineering Center, School of Automotive Studies, Tongji University, Shanghai 201804, China (e-mail: wuguangyu@tongji.edu.cn; xiong_lu@tongji.edu.cn).

G. Wang is with the Department of Electrical and Computer Engineering, University of Minnesota, Minneapolis, MN 55455 USA (e-mail: gangwang@umn.edu).

J. Sun is with the State Key Laboratory of Intelligent Control and Decision of Complex Systems, Beijing Institute of Technology, Beijing 100081, China, and also with the School of Automation, Beijing Institute of Technology, Beijing 100081, China (e-mail: sunjian@bit.edu.cn).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSMC.2019.2945067

systems under attacks were modeled as switching systems with unknown inputs, followed by a multiple model approach for resilient state estimation [19]. Precisely, the attacker decides when and where to launch an attack based on a Markov process. Switching DoS attacks on multiple communication lines with limited attacking times were examined [20]. The optimal switching sequence can be found by solving an integer program using an exhaustive search.

Despite the considerable success on switching attacks, the response of dynamic systems under switching data-injection attacks that can alter system dynamics (rather than estimation error or network topology) has not been studied. There are two critical challenges: Q1) Whether and how one can design an optimal switching data-injection law to maximize damage to the control system from the vantage point of the attacker? and Q2) How can one design an enhanced feedback control law to restore stability and maintain control performance of the system under such switching data-injection attacks? We answer these two questions in this article considering switching data-injection attacks on sensors. In our previous works [21], [22], attacks on actuators were considered, that aim at maximizing a quadratic state cost. In contrast, this article takes the standpoint of the attacker and focuses on designing attacks to maximize the controller's effort. Last but not least, a defense framework to stabilize the compromised system is proposed here. Specifically, the optimal switching data-injection attack design problem is formulated as a 0-1 integer programming problem [22], for which we develop an analytical solution of optimizing a nonlinear fractional function of the switching input.

This article studies the data-injection attacks that aim at manipulating the control signal and corrupting the system dynamics. Typically, CPSs comprise a large amount of sensing devices that are distributed in an unprotected, or even harmful environment. The malicious attacker can perform the node capture attack to crack the communication code, and manipulate purposefully the information exchanged with neighboring nodes or with the control center. To "benchmark" the worst-case performance due to comprised control signals, the sequence of optimal attack locations (namely, set of sensors) along with the corresponding optimal data-injection law over an attack duration is addressed. In this context, the set of attack locations is also termed as a compromised set. In a nutshell, the main contributions of this article are summarized as follows.

c1) We formulate the optimal switching data-injection attack design problem as a 0-1 integer programming problem. An analytical solution is established, including an algebraic switching condition along with a state-feedback-based data-injection law.

c2) We develop a novel resilient control scheme to mitigate the effect of attacks and enhance the closed-loop system, that entails identifying uncertainty matrices associated with different compromised sets and designing output-feedback controller gains. Our proposed control law can stabilize systems under even the worst-case attacks, while ensuring a bounded control cost.

The rest of this article is organized as follows. In Section II, the attack model is given. In Section III, the optimal switching attack design problem is formulated and studied. In Section IV, a resilient control scheme is put forward to defend against the switching attack with arbitrary switching sequences. Numerical tests using power generators are presented in Section V, while this article is concluded in Section VI.

II. Attack Model

We consider a healthy but possibly unstable plant described by a linear time-invariant (LTI) system

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t) \tag{1a}$$

$$\boldsymbol{y}(t) = \boldsymbol{C}\boldsymbol{x}(t) \tag{1b}$$

$$\boldsymbol{u}(t) = \boldsymbol{K}\boldsymbol{y}(t) \tag{1c}$$

where $\boldsymbol{x}(t) \in \mathbb{R}^n$ is the state vector, $\boldsymbol{u}(t) \in \mathbb{R}^k$ is the control input, and $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C})$ are the system matrices of suitable dimensions. To stabilize the LTI system, the output-feedback control with some gain matrix $\boldsymbol{K} \in \mathbb{R}^{k\times m}$ is considered. In the context of switching attacks, the plant is supposed to comprise a large number of sensor nodes; that is, m is large. At time t, each node sends its measurement to a central controller via a vulnerable wireless network. Before characterizing the worst-case attack consequence, we make several standard assumptions on the knowledge and attack ability of the adversary.

Assumption 1: The adversary has perfect knowledge of the system parameters in (1), namely, $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$, and $\boldsymbol{K}$ matrices.

Assumption 2: The adversary can capture the target sensor nodes and crack the passwords of their communication channels before launching attacks.

Assumption 3: When an attack occurs, the adversary injects datum $d_{a,j}^0 u_a(t)$ into compromised sensor $j \in \mathcal{S}(t) \subseteq \{1,\ldots,m\}$, where $\mathcal{S}(t)$ collects the indices of all attacked sensors at time t; $u_a(t)$ is a global component that the attacker can optimize over, yet the local components $d_{a,j}^0$ can be different across sensors, which are arbitrarily selected by the adversary *a priori* and kept fixed throughout the attack. After the attack, the aggregated signal $\boldsymbol{y}(t) + \boldsymbol{d}_a(t)u_a(t)$ is transmitted to the controller, where $\boldsymbol{d}_a(t) := [d_{a,1}(t) \ \cdots \ d_{a,m}(t)]^\top$ with $d_{a,j}(t) = d_{a,j}^0$ if $j \in \mathcal{S}$ and $d_{a,j}(t) = 0$ otherwise. Moreover, $\boldsymbol{d}_a$ can be viewed as an "indicator" vector, which signifies the locations of the attacked sensors.

Following conventions, we use accordingly symbols $\boldsymbol{x}_c$, $\boldsymbol{y}_c$, and $\boldsymbol{u}_c$ to denote the state, measurement, and control vectors of the (compromised) LTI system under attack. Precisely, the attacked system can be described as

$$\dot{\boldsymbol{x}}_c(t) = \boldsymbol{A}\boldsymbol{x}_c(t) + \boldsymbol{B}\boldsymbol{u}_c(t) \tag{2a}$$

$$\boldsymbol{y}_c(t) = \boldsymbol{C}\boldsymbol{x}_c(t) + \boldsymbol{d}_a(t)u_a(t) \tag{2b}$$

$$\boldsymbol{u}_c(t) = \boldsymbol{K}\boldsymbol{y}_c(t). \tag{2c}$$

For ease of understanding, consider the setup described in Fig. 1, where the system consists of three sensor nodes. Suppose that the adversary can compromise only one node at a time. If the adversary compromises Sensor 1 at time t_1,

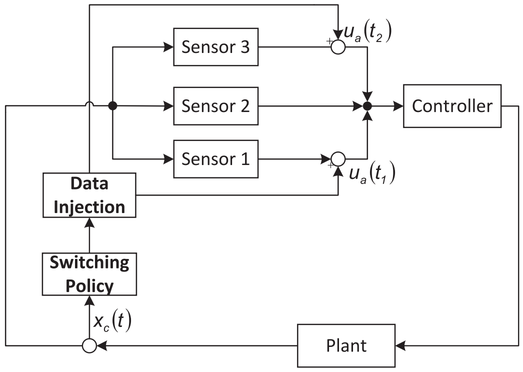


Fig. 1. Switching data-injection attack framework.

it holds that $\boldsymbol{d}_a(t_1) = [d^0_{a,1}\ 0\ 0]^\top$ with attack component $d^0_{a,1}$ determined by the attacker at the starting time t_0; and if Sensor 3 is attacked at time t_2, then $\boldsymbol{d}_a(t_2) = [0\ 0\ d^0_{a,3}]^\top$. Correspondingly, the false data $\boldsymbol{d}_a(t_1)u_a(t_1)$ and $\boldsymbol{d}_a(t_2)u_a(t_2)$ are injected into the measurement vectors $\boldsymbol{y}(t_1) = \boldsymbol{C}\boldsymbol{x}_c(t_1)$ and $\boldsymbol{y}(t_2) = \boldsymbol{C}\boldsymbol{x}_c(t_2)$ [see (1b)] to yield the compromised measurement vectors $\boldsymbol{y}_c(t_1)$ and $\boldsymbol{y}_c(t_2)$ [see (2b)].

In the traditional linear quadratic regulator (LQR) control, the goal of the system operator is to minimize the standard quadratic cost function involving the state variables and the controller effort over a fixed horizon; see standard textbook, e.g., [23]. On the contrary, the goal of the attacker is to maximize the aforementioned quadratic cost of the controller, therefore degrading the control performance, by choosing a sequence of instants to inject false data into a subset of sensors while maintaining a low attack cost.

On the other hand, the injected data can be understood as an adversarial interference produced by certain electrical equipment in a dynamic system. Due to physical limitations however, these equipment cannot produce an arbitrarily large interference signal, so the amplitude of $u_a(t)$ should be kept as small as possible. Considering any finite-time horizon $[t_0,\ t_f]$, two meaningful objective functions for optimal attack design are given by

$$J_a = \frac{1}{2}\boldsymbol{x}_c^\top(t_f)\boldsymbol{G}\boldsymbol{x}_c(t_f) + \frac{1}{2}\int_{t_0}^{t_f}\left[\boldsymbol{u}_c^\top(t)\boldsymbol{Q}\boldsymbol{u}_c(t) - \gamma u_a^2(t)\right]dt \quad (3)$$

and

$$J_b = \frac{1}{2}\boldsymbol{x}_c^\top(t_f)\boldsymbol{G}\boldsymbol{x}_c(t_f) + \frac{1}{2}\int_{t_0}^{t_f}\left[\boldsymbol{x}_c^\top(t)\boldsymbol{Q}\boldsymbol{x}_c(t) - \gamma u_a^2(t)\right]dt \quad (4)$$

where $\boldsymbol{G}$ and $\boldsymbol{Q}$ are symmetric, positive semidefinite matrices of suitable dimensions, and $\gamma > 0$ is a weighting coefficient, both chosen by the attacker. Their values tradeoff between the damage to the healthy plant and the attack cost. Specifically, too large (eigenvalues of) $\boldsymbol{Q}$ or too small γ values may incur instability of the plant under attack. If the adversary prefers a minimal energy cost and selects a larger γ value relative to (eigenvalues of) $\boldsymbol{Q}$, then the resultant $u_a(t)$ is able to render the system states to deviate from their actual values, and the stability of the attacked system may not lose.

Upon plugging (2b) and (2c) into (3), the objective function J_a can be rewritten as

$$J_a = \frac{1}{2}\boldsymbol{x}_c^\top(t_f)\boldsymbol{G}\boldsymbol{x}_c(t_f) + \frac{1}{2}\int_{t_0}^{t_f}\Big[\boldsymbol{x}_c^\top(t)\tilde{\boldsymbol{Q}}\boldsymbol{x}_c(t) + 2u_a(t)\boldsymbol{s}^\top(t)\boldsymbol{x}_c(t) + \tilde{\gamma}(t)u_a^2(t)\Big]dt \quad (5)$$

where the coefficients are given by

$$\tilde{\boldsymbol{Q}} := \boldsymbol{C}^\top\boldsymbol{K}^\top\boldsymbol{Q}\boldsymbol{K}\boldsymbol{C} \quad (6a)$$

$$\boldsymbol{s}(t) := \boldsymbol{C}^\top\boldsymbol{K}^\top\boldsymbol{Q}\boldsymbol{K}\boldsymbol{d}_a(t) \quad (6b)$$

$$\tilde{\gamma}(t) := \boldsymbol{d}_a^\top(t)\boldsymbol{K}^\top\boldsymbol{Q}\boldsymbol{K}\boldsymbol{d}_a(t) - \gamma. \quad (6c)$$

To guarantee existence of an optimal solution, the adversary needs to design $\boldsymbol{Q}$ and γ such that $\tilde{\gamma}(t) < 0$ [23]. It is clear from (5) that maximizing the controller energy consumption in J_a amounts to maximizing integrations of both the state quadratic $\boldsymbol{x}_c^\top(t)\tilde{\boldsymbol{Q}}\boldsymbol{x}_c(t)$ and the cross term $u_a(t)\boldsymbol{s}^\top(t)\boldsymbol{x}_c(t)$ (between u_a and $\boldsymbol{x}_c$). In comparison, only the integration of the state quadratic is maximized in J_b. In other words, if the adversary is solely interested in damaging the system state, the objective function J_b is preferred; but if the control cost of the attacked system is of interest too, then, J_a is preferred.

III. Optimal Switching Attack Design

In a large-scale CPS setting, compromising all communication channels necessarily requires a large amount of energy. The adversary with limited budget is instead inclined to attack only few sensors, possibly those of lowest security levels or with most vulnerable communication channels. Due to the limited computing resources and channel cracking capabilities, this article focuses on a practical setting where the adversary can attack a fixed number of sensors at a time. On the other hand, it is also not wise or optimal for the attacker to constantly attack a fixed set of sensors. A smart yet affordable strategy is to select a size-fixed set of sensors to effect attacks at every attack instant, to yield the worst-case system response. This dynamic attack strategy is to switch the attack among multiple sensor sets from time to time.

The goal of the attacker is to determine an optimal switching sequence of sensor sets to attack with an optimal data-injection law, so as to maximize the objective value J_a or J_b. When there are m sensors and the adversary can attack say $\ell \ll m$ sensors at a time, the total number of candidate attacks (i.e., size-ℓ sensor sets) is $M := \binom{m}{\ell}$. With slight abuse of notation, the M sensor sets (namely, the M sets of ℓ-sensor combinations) can be represented by the indicator vectors $\{\boldsymbol{d}_a^i\}_{i=1}^M$ defined in Assumption 3.

Example 1: If $m = 3$ and $\ell = 2$, there are $M = \binom{3}{2}$ sensor sets; that is, $\{1, 2\}$, $\{1, 3\}$, and $\{2, 3\}$ collecting the indices of the attacked sensors. Each of the three sensor sets can be uniquely represented by $\boldsymbol{d}_a^1 := [d^0_{a,1}\ d^0_{a,2}\ 0]^\top$, $\boldsymbol{d}_a^2 := [d^0_{a,1}\ 0\ d^0_{a,3}]^\top$, and $\boldsymbol{d}_a^3 := [0\ d^0_{a,2}\ d^0_{a,3}]^\top$.

From Fig. 1, if the input to the controller is compromised, the control signal (output of the controller) will be disturbed, so will the system dynamics. The control signal under the described switching data-injection attacks can be given by

$$\boldsymbol{u}_c(t) = \boldsymbol{K}\left[\boldsymbol{C}\boldsymbol{x}_c(t) + \sum_{j=1}^{M} w_j(t)\boldsymbol{d}_a^j u_a(t)\right] \tag{7}$$

where the switch input vector $\boldsymbol{w} := [w_1 \ \cdots \ w_M]$ belongs to

$$\mathcal{W}_0 := \left\{\boldsymbol{w}(t) \,\middle|\, \sum_{j=1}^{M} w_j(t) = 1, \text{ and } w_j(t) \in \{0, 1\} \ \forall j\right\}. \tag{8}$$

Per attack instant $t \geq t_0$, since only one sensor set (namely, $\boldsymbol{d}_a^j$ for some j) is to be chosen, its corresponding switch input $w_j(t)$ is set 1, while the others are set 0. Observe that the components of $\boldsymbol{d}_a^j$ are time invariant and known to the attacker. Therefore, the values of $\boldsymbol{w}(t) := [w_1(t) \ \ldots \ w_M(t)]^\top$ at different t signify the compromised sensor sets at corresponding instants. If two consecutive compromised sets (i.e., before and after some instant t) are different, then instant t is a switching instant, namely, the time at which the value of $\boldsymbol{w}(t)$ changes. The compromised sets at all switching instants define the so-called switching sequence

$$\boldsymbol{\zeta} := \{(\boldsymbol{w}(t_0), u_a(t_0)), \ \ldots, \ (\boldsymbol{w}(t_N), u_a(t_N))\} \tag{9}$$

where $t_0 \leq t_1 \leq \cdots \leq t_N \leq t_f$, the set $\{t_1, \ldots, t_N\}$ collects all switching instants, and N is the total number of switching operations.

In general, the attacker can assume the same objective function for all sensor sets. In certain settings of practical interest, the attacker may prefer different objective functions when different sensor sets are compromised. In Example 1, if the attacker aims to induce a larger deviation to state $x_{c,1}$ ($\boldsymbol{x}_c = [x_{c,1} \ x_{c,2} \ x_{c,3}]^\top$) when sensor set $\{1, 2\}$ is attacked, the attacker can simply use a diagonal matrix $\boldsymbol{Q}_1$ with entry $Q_1(1,1)$ greater than $Q_1(2,2)$ and $Q_1(3,3)$, where $\boldsymbol{Q}_1$ belongs to the objective function for set $\{1, 2\}$. This prompts us to choose an objective function that sums the excited local objective functions at every instant, that is

$$\widehat{J}_a = \sum_{j=1}^{M} w_j J_a^j \ \text{ and } \ \widehat{J}_b = \sum_{j=1}^{M} w_j J_b^j \tag{10}$$

where J_a^j or J_b^j is obtained by replacing $\boldsymbol{Q}$ and γ in (3) or (4) with $\boldsymbol{Q}_j$ and γ_j.

Putting (2), (7), and (10) together, the optimal switching data-injection attack design problem is to find $\boldsymbol{w}(t)$ and $u_a(t)$ that

$$\max \quad \widehat{J}_a \ \text{ or } \ \widehat{J}_b \tag{11a}$$

$$\text{s.t.} \quad \dot{\boldsymbol{x}}_c(t) = \boldsymbol{A}_a\boldsymbol{x}_c(t) + \sum_{j=1}^{M} w_j(t)\boldsymbol{b}_a^j u_a(t) \tag{11b}$$

$$\boldsymbol{u}_c(t) = \boldsymbol{K}\left[\boldsymbol{C}\boldsymbol{x}_c(t) + \sum_{j=1}^{M} w_j(t)\boldsymbol{d}_a^j u_a(t)\right] \tag{11c}$$

$$\boldsymbol{w}(t) \in \mathcal{W}_0 \ \ \forall t \tag{11d}$$

where the coefficients $\boldsymbol{A}_a := \boldsymbol{A} + \boldsymbol{BKC}$ and $\boldsymbol{b}_a^j := \boldsymbol{BK}\boldsymbol{d}_a^j$ for all $j = 1, \ldots, M$. In (11), the optimal switching data-injection attack design problem is formulated as a 0-1 integer program. If the binary variables $\{w_j(t)\}_{j=1}^M$ and the corresponding constraint (11d) are not present, (11) is LQR, whose optimal solution can be readily obtained in the closed-form leveraging Pontryagin's maximum principle (see [23]). In fact, constraint (11d) renders (11) nonconvex and NP-hard in general [24]. Fortunately, but if an optimal solution of $\boldsymbol{w}(t)$ is successfully found, then the optimal switching sequence $\boldsymbol{\zeta}$ can be easily recovered.

Interestingly enough, if we view the attacked system (2) as a linear switched system (see [25] for related definitions), the problem of optimal switch data-injection attack design on an LTI system in (11) can be treated as the optimal control problem of a linear switched system. As far as optimal control of switched systems is concerned, there is no closed-form solution in general, even for linear ones [26]. Recent efforts have primarily focused on the open-loop systems. Specifically, minimizing a quadratic cost on the state variables, an algebraic switching condition was developed for the open-loop linear switched systems [27], by leveraging the so-termed embedded transformation [28]. This result was further generalized to the multiple objective case [29]. For general closed-loop systems, whether and how one can obtain a closed-form expression of the switching condition remains unclear. Indeed, the attacked system (2) constitutes a special closed-loop system involving scalar control (instead of vector) $u_a(t)$, which prompts us to exploit the embedded transformation as well as recent mathematical programming advances to hopefully tackle (11).

The idea of the embedded transformation is to relax each binary constraint $w_j(t) \in \{0, 1\}$ to a box one $w_j(t) \in [0, 1]$, followed by solving a convex problem. Rather than dealing with constraint (11d), we consider the switch input vector $\boldsymbol{w}(t)$ belonging to the following convex set:

$$\mathcal{W}_1 := \left\{\boldsymbol{w}(t) \,\middle|\, \sum_{j=1}^{M} w_j(t) = 1, \text{ and } 0 \leq w_j(t) \leq 1 \ \ \forall j\right\}. \tag{12}$$

After replacing the last constraint $\boldsymbol{w}(t) \in \mathcal{W}_0$ with $\boldsymbol{w}(t) \in \mathcal{W}_1$ in (11), we arrive at the following embedded switching data-injection attack design problem:

$$\max \quad (11\text{a}) \tag{13a}$$

$$\text{s.t.} \quad (11\text{b}), \ (11\text{c}), \text{ and } \boldsymbol{w}(t) \in \mathcal{W}_1 \tag{13b}$$

which boils down to an optimal control problem of LQR type and whose optimal solution can be obtained leveraging Pontryagin's maximum principle. If luckily, the optimal solution of $\boldsymbol{w}(t)$ in (13) takes values at $\boldsymbol{w}(t) \in \mathcal{W}_0$ for all t, one can verify that the resulting solution is also the optimal solution of the original problem (11). To see this, we discuss the following two cases depending on whether J_a or J_b is maximized.

A. Maximizing $\widehat{J}_a$

Before applying the embedded transformation, we first simplify $\widehat{J}_a$. According to (10), $\widehat{J}_a$ can be written as

$$\widehat{J}_a = \frac{1}{2}\boldsymbol{x}_c^\top(t_f)\boldsymbol{G}\boldsymbol{x}_c(t_f) + \frac{1}{2}\sum_{j=1}^{M} w_j \int_{t_0}^{t_f}\left[\boldsymbol{u}_c^\top(t)\boldsymbol{Q}_j\boldsymbol{u}_c(t) - \gamma_j u_a^2(t)\right]dt. \tag{14}$$

For notational brevity, the dependence on t will be neglected. Since $\boldsymbol{w} \in \mathcal{W}_0$, it can be easily checked that

$$\left(\sum_{j=1}^{M} w_j \boldsymbol{d}_a^j\right)^{\top} \boldsymbol{K}^{\top} \left(\sum_{j=1}^{M} w_j \boldsymbol{Q}_j\right) \sum_{j=1}^{M} w_j \boldsymbol{K}\boldsymbol{d}_a^j = \sum_{j=1}^{M} w_j \boldsymbol{d}_a^{j\top} \boldsymbol{K}^{\top} \boldsymbol{Q}_j \boldsymbol{K}\boldsymbol{d}_a^j$$

and

$$\left(\sum_{j=1}^{M} w_j \boldsymbol{d}_a^j\right)^{\top} \boldsymbol{K}^{\top} \left(\sum_{j=1}^{M} w_j \boldsymbol{Q}_j\right) \boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_c = \sum_{j=1}^{M} w_j \boldsymbol{d}_a^{j\top} \boldsymbol{K}^{\top} \boldsymbol{Q}_j \boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_c.$$

Following (6), define for all $j = 1, \ldots, M$ that:

$$\tilde{\boldsymbol{Q}}_j := \boldsymbol{K}^{\top} \boldsymbol{Q}_j \boldsymbol{K} \tag{15a}$$

$$\tilde{\gamma}_j := \boldsymbol{d}_a^{j\top} \boldsymbol{K}^{\top} \boldsymbol{Q}_j \boldsymbol{K} \boldsymbol{d}_a^j - \gamma_j \tag{15b}$$

$$\boldsymbol{s}_j := \boldsymbol{C}^{\top} \boldsymbol{K}^{\top} \boldsymbol{Q}_j \boldsymbol{K} \boldsymbol{d}_a^j. \tag{15c}$$

Expanding (14), $\widehat{\mathcal{J}}_a$ can be further simplified into

$$\widehat{\mathcal{J}}_a = \frac{1}{2}\boldsymbol{x}_c^{\top}(t_f)\boldsymbol{G}\boldsymbol{x}_c(t_f) + \frac{1}{2}\sum_{j=1}^{M} w_j \int_{t_0}^{t_f} \left(\boldsymbol{x}_c^{\top} w_j \tilde{\boldsymbol{Q}}_j \boldsymbol{x}_c + 2\boldsymbol{x}_c^{\top}\boldsymbol{s}_j u_a + \tilde{\gamma}_j u_a^2\right) dt. \tag{16}$$

If the objective function $\widehat{\mathcal{J}}_a$ in (10) is adopted, we have the following result.

Theorem 1: Consider the performance index (16) for the attacked system (2). Then, the optimal switching condition of the switching attack for the original design problem (11) is given by

$$i(t) := \arg\max_{j \in \{1,\ldots,M\}} \; q_i(t) - f_j^2(t)/\tilde{\gamma}_j \tag{17}$$

and the optimal data-injection law

$$u_a(t) := -f_{i(t)}/\tilde{\gamma}_{i(t)} \tag{18}$$

where

$$f_j(t) := \boldsymbol{s}_j^{\top \boldsymbol{x}_c}(t) + \boldsymbol{b}_a^{j\top}(t)\boldsymbol{\lambda}(t) \quad \forall j = 1, \ldots, M \tag{19}$$

and $\boldsymbol{\lambda}(t) := [\lambda_1(t) \; \cdots \; \lambda_n(t)]^{\top}$ is the solution of

$$\dot{\boldsymbol{\lambda}}(t) = -\tilde{\boldsymbol{Q}}_{i(t)}\boldsymbol{x}_c(t) - u_a(t)\boldsymbol{s}_{i(t)} - \boldsymbol{A}_a^{\top}\boldsymbol{\lambda}(t) \tag{20}$$

with the boundary condition $\boldsymbol{\lambda}(t_f) = \boldsymbol{G}\boldsymbol{x}(t_f)$.

Proof: Our proof starts with Pontryagin's maximum principle for the relaxed problem (13) (see [23]), which is followed by showing that the optimal solution of $\boldsymbol{w}$ is always achieved at one of the vertices of the polytope $\mathcal{W}_1$. Hence, the relaxation is tight, which recovers the optimal solution of the original challenging nonconvex problem (11). Toward this objective and using (21), the Hamilton function for (13) is given by

$$H = \boldsymbol{x}_c^{\top} \sum_{j=1}^{M} w_j \tilde{\boldsymbol{Q}}_j \boldsymbol{x}_c + 2\boldsymbol{x}_c^{\top} \sum_{j=1}^{M} w_j \boldsymbol{s}_j u_a + \sum_{j=1}^{M} w_j \tilde{\gamma}_j u_a^2 - \boldsymbol{\lambda}^{\top}\left(\boldsymbol{A}_a \boldsymbol{x}_c + \sum_{j=1}^{M} w_j \boldsymbol{b}_a^j u_a\right). \tag{21}$$

To ensure existence of a meaningful solution, the adjustable parameters $\boldsymbol{Q}_j$, γ_j, and $\{\boldsymbol{d}_a^j\}_{j=1}^M$ should be designed such that $\partial^2 H/\partial u_a^2 < 0$ [30]. Upon defining $\tilde{\boldsymbol{\gamma}} := [\tilde{\gamma}_1 \; \cdots \; \tilde{\gamma}_M]^{\top}$, we deduce that for all $\boldsymbol{w} \in \mathcal{W}_1$, the following holds:

$$\partial^2 H/\partial u_a^2 = \sum_{j=1}^{M} w_j \boldsymbol{d}_a^{j\top} \boldsymbol{K}^{\top} \boldsymbol{Q}_j \boldsymbol{K} \boldsymbol{d}_a^j - \gamma_j = \boldsymbol{w}^{\top}\tilde{\boldsymbol{\gamma}} < 0. \tag{22}$$

That is, function H is strictly concave with a unique maximum given by the stationary point of the gradient in u_a. By setting $\partial H/\partial u_a = 0$, we arrive at

$$u_a = -\sum_{j=1}^{M} w_j \frac{\boldsymbol{s}_j^{\top \boldsymbol{x}_c} + \boldsymbol{b}_a^{j\top}\boldsymbol{\lambda}}{\boldsymbol{d}_a^{j\top}\boldsymbol{K}^{\top}\boldsymbol{Q}_j\boldsymbol{K}\boldsymbol{d}_a^j - \gamma_j} = -\sum_{j=1}^{M} w_j \frac{f_j}{\tilde{\gamma}_j}. \tag{23}$$

By the co-state equation $\dot{\boldsymbol{\lambda}} = -\partial H/\partial \boldsymbol{x}_c$, we have that

$$\dot{\boldsymbol{\lambda}} = -\sum_{j=1}^{M} w_j \tilde{\boldsymbol{Q}}_j \boldsymbol{x}_c - \sum_{j=1}^{M} w_j \boldsymbol{s}_j u_a - \boldsymbol{A}_a^{\top}\boldsymbol{\lambda}.$$

Let $\boldsymbol{f} := [f_1 \; \cdots \; f_M]^{\top}$ and $\boldsymbol{q} := [q_1 \; \cdots \; q_M]^{\top}$. Plugging (23) into (21) yields

$$H = \boldsymbol{\lambda}^{\top}\boldsymbol{A}_a\boldsymbol{x}_c + \frac{\boldsymbol{w}^{\top}\boldsymbol{q}}{2} - \frac{\left(\boldsymbol{w}^{\top}\boldsymbol{f}\right)^2}{2\boldsymbol{w}^{\top}\tilde{\boldsymbol{\gamma}}}$$

where $q_i = \boldsymbol{x}_c^{\top}\tilde{\boldsymbol{Q}}\boldsymbol{x}_c$. Evidently, as only the last two terms in H depend on $\boldsymbol{w}$, maximizing H with respect to $\boldsymbol{w} \in \mathcal{W}_1$ is equivalent to maximize the following reduced Hamilton function over $\mathcal{W}_1$:

$$\bar{H} := \frac{\boldsymbol{w}^{\top}\boldsymbol{q}}{2} - \frac{\left(\boldsymbol{w}^{\top}\boldsymbol{f}\right)^2}{2\boldsymbol{w}^{\top}\tilde{\boldsymbol{\gamma}}} := \frac{\varphi(\boldsymbol{w})}{2} - \frac{\psi^2(\boldsymbol{w})}{2\phi(\boldsymbol{w})}.$$

The derivatives of $\phi(\boldsymbol{w})$ and $\psi(\boldsymbol{w})$ with respect to w_j are given by

$$\dot{\phi} = \tilde{\gamma}_j, \quad \text{and} \quad \dot{\psi} = f_j. \tag{24}$$

The second derivative of $\bar{H}$ with respect to w_j is

$$\frac{\partial^2 \bar{H}}{\partial w_j^2} = -\frac{\left(f_j\phi - \tilde{\gamma}_j\psi\right)^2}{\phi^3} \geq 0. \tag{25}$$

Likewise, the second partial derivative of $\bar{H}$ with respect to w_j and w_k can be found as

$$\frac{\partial \bar{H}}{\partial w_j \partial w_k} = -\frac{(f_j\phi - \tilde{\gamma}_j\psi)(f_k\phi - \tilde{\gamma}_k\psi)}{\phi^3}. \tag{26}$$

Define $\boldsymbol{z} := [z_1 \; \cdots \; z_M]^{\top}$ with entries given by $z_j = f_j\phi - \tilde{\gamma}_j\psi$. Then, based on (25) and (26), the Hessian matrix of $\bar{H}$ can be written as follows:

$$\frac{\partial^2 \bar{H}}{\partial \boldsymbol{w}^2} = -\frac{1}{\phi^3}\begin{bmatrix} z_1^2 & z_1 z_2 & \cdots & z_1 z_M \\ z_2 z_1 & z_2^2 & \cdots & z_2 z_M \\ \vdots & \vdots & \ddots & \vdots \\ z_M z_1 & z_M z_2 & \cdots & z_M^2 \end{bmatrix} = \frac{\boldsymbol{z}\boldsymbol{z}^{\top}}{-\phi^3} \succeq \boldsymbol{0}$$

which confirms that function $\bar{H}$ is convex over $\mathcal{W}_1$.

Maximizing H over $\boldsymbol{w} \in \mathcal{W}_1$ reduces to maximizing convex $\bar{H}$ over a convex feasibility set $\boldsymbol{w} \in \mathcal{W}_1$. In this case, the minimum is always attained at one of the vertices of the polytope determined by the M box constraints in $\mathcal{W}_1$ [31]. It is evident

Algorithm 1: Optimal Switching Data-Injection Attack Algorithm

```
Determine d_a^j for all compromised sensor sets j ∈ {1, ..., M}.
Set: G, Q_j, and γ_j according to the attacker's preference.
for i = 1, ..., M do
  | Solve (29);
end
Initialize: attack horizon [t_0, t_f], and S(t_0).
Estimate: initial state x_c(t_0).
while t ≤ t_f do
  | for i = 1, ..., M do
  |   | Compute (19);
  |   | Evaluate β_j(t) = q_j(t) − f_j^2(t)/γ̃_j;
  | end
  | if i := arg max_j{β_j} then
  |   | Compute (28);
  |   | ẋ_c(t) = A_a x_c(t) + b_a^i u_a(t);
  |   | λ(t) = P_i x_c(t);
  | end
end
```

that the vertices of $\mathcal{W}_1$ coincide with the standard basis vectors $\boldsymbol{w}_j \in \mathbb{R}^M$ (whose jth entry is one, and remaining entries are zero), satisfying $\boldsymbol{w}_j \in \mathcal{W}_0$. Hence, the optimal solution of the relaxed problem recovers the optimal solution of the original nonconvex problem. Concretely, we have that

$$\max_{\boldsymbol{w}\in\mathcal{W}_1} \bar{H}(\boldsymbol{w}) = \max_{j\in\{1,\ldots,M\}} q_j(t) - f_j^2(t)/\tilde{\gamma}_j \tag{27}$$

and the optimal switching instants are given by the time when $\boldsymbol{w}^*(t)$ changes. This completing the proof. ■

Regarding Theorem 1, we have the following observations.

Remark 1: By simply comparing the values $\{q_j(t) - f_j^2(t)/\tilde{\gamma}_j\}$ for all sensor sets at each instant, the attacker achieves an optimal switch input.

Remark 2: In the steady state, the optimal data-injection law is a state-feedback signal given by

$$u_a(t) = -\frac{1}{\tilde{\gamma}_i}\left(\boldsymbol{s}_i^\top + {\boldsymbol{b}_a^i}^\top \boldsymbol{P}_i\right)\boldsymbol{x}_c(t) \tag{28}$$

where $\boldsymbol{P}_i \in \mathbb{S}_+^{n\times n}$ is the solution of the Riccati equation

$$\boldsymbol{P}_i\boldsymbol{A}_a + \boldsymbol{A}_a^\top\boldsymbol{P}_i - \frac{1}{\tilde{\gamma}_i}\left(\boldsymbol{P}_i\boldsymbol{b}_a^i + \boldsymbol{s}_i\right)\left({\boldsymbol{b}_a^i}^\top\boldsymbol{P}_i + \boldsymbol{s}_i^\top\right) + \boldsymbol{Q}_i = \boldsymbol{0}. \tag{29}$$

Remark 3: To find $u_a(t_0)$ in (28), the adversary has to estimate the initial state $\boldsymbol{x}_c(t_0)$ from sensor measurements $\boldsymbol{y}(t)$ of the healthy plant for $t \le t_0$, using, e.g., a Luenberger observer, before launching attacks.

B. Maximizing J_b

According to (10), $\widehat{J}_b$ can be written as

$$\begin{aligned}\widehat{J}_b = &\frac{1}{2}\boldsymbol{x}_c^\top(t_f)\boldsymbol{G}\boldsymbol{x}_c(t_f)\\ &+ \frac{1}{2}\sum_{j=1}^M w_j\int_{t_0}^{t_f}\left[\boldsymbol{x}_c^\top(t)\boldsymbol{Q}_j\boldsymbol{x}_c(t) - \gamma_j u_a^2(t)\right]dt.\end{aligned} \tag{30}$$

If the objective function $\widehat{J}_b$ is adopted, we have the following theorem.

Theorem 2: The optimal switching condition of the switching attack that maximizes the performance index (30) for the attacked system (2) is given by

$$i(t) := \arg\max_{j\in\{1,\ldots,M\}} \boldsymbol{x}_c^\top\boldsymbol{Q}_j\boldsymbol{x}_c + \frac{1}{\gamma_j}\left({\boldsymbol{b}_a^j}^\top\boldsymbol{\lambda}\right)^2 \tag{31}$$

with the optimal data-injection law being

$$u_a(t) := \frac{1}{\gamma_i}{\boldsymbol{b}_a^j}^\top\boldsymbol{\lambda}(t) \tag{32}$$

where $\boldsymbol{\lambda}(t)$ is the solution of

$$\dot{\boldsymbol{\lambda}}(t) = -\boldsymbol{Q}_i\boldsymbol{x}_c(t) - \boldsymbol{A}_a^\top\boldsymbol{\lambda}(t) \tag{33}$$

with the boundary condition $\boldsymbol{\lambda}(t_f) = \boldsymbol{G}\boldsymbol{x}(t_f)$.

Proof: Appealing again to the Pontryagin's maximum principle, the Hamilton function is given by

$$\begin{aligned}H = &\frac{1}{2}\sum_{j=1}^M w_j\left[\boldsymbol{x}_c^\top(t)\boldsymbol{Q}_j\boldsymbol{x}_c(t) - \gamma_j u_a^2(t)\right]\\ &+ \boldsymbol{\lambda}^\top(t)\left[\boldsymbol{A}_a\boldsymbol{x}_c(t) + \sum_{j=1}^M w_j\boldsymbol{b}_a^j u_a(t)\right].\end{aligned} \tag{34}$$

The co-state equation confirms that

$$\dot{\boldsymbol{\lambda}}(t) = -\sum_{j=1}^M w_j\boldsymbol{Q}_j\boldsymbol{x}_c(t) - \boldsymbol{A}_a^\top\boldsymbol{\lambda}(t) \tag{35}$$

and by means of the coupled equation, it further holds that

$$u_a(t) = \sum_{j=1}^M \frac{w_j}{\gamma_j}{\boldsymbol{b}_a^j}^\top\boldsymbol{\lambda}(t). \tag{36}$$

Substituting (36) into (34) yields

$$\bar{H} = \sum_{j=1}^M w_j\boldsymbol{x}_c^{\top\boldsymbol{Q}_j}\boldsymbol{x}_c + \sum_{j=1}^M\sum_{j=1}^M \frac{w_j w_k}{\gamma_j\gamma_k}\left(\boldsymbol{\lambda}^\top\boldsymbol{b}_a^j\right)\left(\boldsymbol{\lambda}^{\top\boldsymbol{b}_a^k}\right).$$

Maximizing $\bar{H}$ over $\boldsymbol{w}(t) \in \mathcal{W}_1$ now boils down to solving the following quadratic programming problem:

$$\underset{\boldsymbol{w}}{\text{maximize}} \quad \boldsymbol{w}^\top\boldsymbol{H}\boldsymbol{w} + \boldsymbol{w}^\top\boldsymbol{q} \tag{37a}$$

$$\text{subject to} \quad \boldsymbol{w} \in \mathcal{W}_1 \tag{37b}$$

where $\boldsymbol{H} := \boldsymbol{h}\boldsymbol{h}^\top$ with $\boldsymbol{h} := [(\boldsymbol{\lambda}^\top\boldsymbol{b}_a^1)/\gamma_1 \cdots (\boldsymbol{\lambda}^\top\boldsymbol{b}_a^M)/\gamma_M]^\top$ and $\boldsymbol{q} := [(\boldsymbol{x}_c^{\top\boldsymbol{Q}_1}\boldsymbol{x}_c)\cdots(x_c^{\top\boldsymbol{Q}_M}\boldsymbol{x}_c)]^\top$.

Evidently, function $\bar{H}$ is convex in $\boldsymbol{w}$. Again, the optimal solution of maximizing $\bar{H}(\boldsymbol{w})$ over $\boldsymbol{w} \in \mathcal{W}_1$ is attained (at least) at one of the vertices of the polytope determined by $\mathcal{W}_1$, hence proving that the switch input $\boldsymbol{w}(t)$ obtains its optimal solution in $\mathcal{W}_0$. Concretely, we have that

$$\max_{\boldsymbol{w}\in\mathcal{W}_1}\bar{H}(\boldsymbol{w}) = \max_{j\in\{1,\ldots,M\}}\boldsymbol{x}_c^\top\boldsymbol{Q}_j\boldsymbol{x}_c + \frac{1}{\gamma_j}\left(\boldsymbol{\lambda}^{\top\boldsymbol{b}_a^j}\right)^2 \tag{38}$$

completing the proof. ■

IV. Countermeasure Design

After exploiting the attack strategy from the perspective of the adversary, it is of paramount importance to pursue defense schemes (countermeasures) to mitigate the attacks. The problem of interest is to design an enhanced output-feedback controller to stabilize the attacked system, such that the control performance is preserved in a well-defined sense.

The countermeasure against switching attacks has mainly focused on the network topology attack and the DoS attack [20]. The resilient control against location switching attacks has not been investigated in the literature. Compared with the existing efforts that use cover network information, or have a subset of sensors immune to attacks destroying the feasibility of stealthy attacks [32], this article develops a resilient control scheme that tolerates intrusions. In general, resilience means that the operator maintains an acceptable level of operational normalcy despite attacks. Before presenting the countermeasure design, we start by introducing the definition of a resilient control scheme.

Definition 1: A feedback control law $\tilde{\boldsymbol{u}}$ is said to be resilient if it can stabilize the plant under a sequence of attacks arbitrarily constructed based on a set of state-feedback laws, while guaranteeing an acceptable cost, that is, for some given bound $\tilde{J}$, the following holds:

$$\tilde{J} \leq \tilde{J}^{*} \tag{39}$$

where

$$\tilde{J} = \int_0^{\infty} \left(\boldsymbol{x}_c^{\top} \tilde{\boldsymbol{Q}} \boldsymbol{x}_c + \tilde{\boldsymbol{u}}^{\top} \tilde{\boldsymbol{R}} \tilde{\boldsymbol{u}} \right) dt. \tag{40}$$

The operator has the freedom to select the two weighting matrices $\tilde{\boldsymbol{Q}} \succ \boldsymbol{0}$ and $\tilde{\boldsymbol{R}} \succ \boldsymbol{0}$ to compensate for the control performance degradation of the healthy plant. The state of the healthy system can be reconstructed using, e.g., a Luenberger observer [33]. If the attacker injects false data into a set of sensors over a period of time, the reconstruction error $\boldsymbol{e}_c(t)$ may diverge and the alarm will be triggered if it exceeds a threshold

$$\begin{cases} \dot{\hat{\boldsymbol{x}}}(t) = \boldsymbol{A}\hat{\boldsymbol{x}}(t) + \boldsymbol{B}u_c(t) + \boldsymbol{L}[\boldsymbol{y}_c(t) - \hat{\boldsymbol{y}}(t)] \\ \hat{\boldsymbol{y}}(t) = \boldsymbol{C}\hat{\boldsymbol{x}}(t) \end{cases}$$

$$\dot{\boldsymbol{e}}_c(t) = (\boldsymbol{A} - \boldsymbol{L}\boldsymbol{C})\boldsymbol{e}_c(t) + \boldsymbol{L}\boldsymbol{d}_a u_a(t)$$

where $\boldsymbol{e}_c(t) := \boldsymbol{x}_c(t) - \hat{\boldsymbol{x}}(t)$ and $\boldsymbol{L}$ is a gain matrix.

The attacked system can be modeled as a switched system consisting of M modes

$$\text{Mode } j\text{: } \dot{\boldsymbol{x}}_{c,j}(t) = \left(\boldsymbol{A}_a + \boldsymbol{B}\boldsymbol{K}\Delta\boldsymbol{K}_j\right)\boldsymbol{x}_{c,j}(t),\ j = 1, \ldots, M.$$

Consider for example, if J_a is maximized, substituting (28) into (11b), we have

$$\Delta\boldsymbol{K}_j = -\frac{1}{\tilde{\gamma}_{jj}} \left[\boldsymbol{d}_a^j \left(\boldsymbol{s}_j^{\top} + {\boldsymbol{B}_a^j}^{\top} \boldsymbol{P}_j \right) \right]. \tag{41}$$

The attacker uses matrices $\Delta\boldsymbol{K}_j$ at time t_j and switches to $\Delta\boldsymbol{K}_{j'}$ at $t_{j'}$. The attacker may change the attack locations randomly according to a stochastic model, or optimally with respect to an unknown criterion. As such, matrices $\Delta\boldsymbol{K}_j$ can be treated as a switching uncertainty of the healthy plant. The guaranteed cost control approach can be adopted to mitigate the attacks [34]. Once the detector detects an attack, or that the system response is considerably altered such that the attack is exposed, the defender needs to estimate the sensor links that have been compromised, as well as identify the uncertainty matrices $\Delta\boldsymbol{K}_j$. Recent advances on identifying the attack set from sensor measurements (e.g., [35]) assume attacks on the state equations, and do not utilize the information of the attacked state $\boldsymbol{x}_c$. The proposed identification problem is generally NP-hard, and reducing-complexity algorithms are presented. We adopt the following steps to defend against switching attacks.

Step 1 (Attack Extraction): As the false data injected into sensor measurements

$$\boldsymbol{f}_a(t) = u_a(t)\boldsymbol{d}_a^j. \tag{42}$$

The defender should find historical false data $\boldsymbol{f}_a(t) := [f_a^1(t) \ \cdots \ f_a^n(t)]^{\top}$ to identify the uncertainty matrix $\Delta\boldsymbol{K}_j$. The goal of this step is to extract $\boldsymbol{f}_a(t)$ and sort the timestamp of $\boldsymbol{f}_a(t)$ into M parts, namely, $\boldsymbol{O}_1, \ldots, \boldsymbol{O}_M$, each of which corresponds to a compromised sensor set. In Example 1, if $f_a^1(t) < \delta$, where $\delta > 0$ is a preselected threshold to account for computation and measurement inaccuracies, then $t \in \boldsymbol{O}_3$ (referring to set $\{2, 3\}$); if $f_a^2(t) < \delta$, $t \in \boldsymbol{O}_2$ (referring to set $\{1, 3\}$). If $f_a^3(t) < \delta$, then $t \in \boldsymbol{O}_1$ (referring to set $\{1, 2\}$). In this article, we assume that the control center is able to reset the attacked system under a known initial condition, and compare the attacked sensor measurements with $\boldsymbol{y}_v(t)$ from a virtual healthy system, namely

$$\dot{\boldsymbol{x}}_v(t) = \boldsymbol{A}_a \boldsymbol{x}_v(t) \tag{43a}$$

$$\boldsymbol{y}_v(t) = \boldsymbol{C}\boldsymbol{x}_v(t). \tag{43b}$$

Upon defining

$$\boldsymbol{e}_x = \boldsymbol{x}_c - \boldsymbol{x}_v$$

$$\boldsymbol{e}_y = \boldsymbol{y}_c - \boldsymbol{y}_v$$

we obtain that

$$\dot{\boldsymbol{e}}_x(t) = \boldsymbol{A}_a \boldsymbol{e}_x(t) + \boldsymbol{B}\boldsymbol{K}\boldsymbol{f}_a(t) \tag{44a}$$

$$\boldsymbol{e}_y(t) = \boldsymbol{C}\boldsymbol{e}_x(t) + \boldsymbol{f}_a(t) \tag{44b}$$

where $\boldsymbol{e}_x(0) = \boldsymbol{0}$. Vector $\boldsymbol{f}_a(t)$ can be calculated by the comparison result $\boldsymbol{e}_y(t)$, and once $\boldsymbol{f}_a(t)$ is recovered, the compromised sensors are found.

Step 2 (Attack Identification): The defender makes use of the data whose timestamp was collected in $\boldsymbol{O}_j$ to identify the unknown parameter matrices $\Delta\boldsymbol{K}_j$, using the common least-squares algorithm by solving

$$\min_{\Delta\boldsymbol{K}_j} \sum_{t \in \boldsymbol{O}_j} \left\| \boldsymbol{f}_a(t) - \Delta\boldsymbol{K}_j \boldsymbol{x}_c(t) \right\|_2^2. \tag{45}$$

In practice, $\boldsymbol{e}_y$ can be induced by, e.g., link failures in system components, noise in communication channels, or intentional attacks. If the online identification algorithm converges, there exists a state-feedback data-injection attack [36] (different from random attacks [37] or constant switching attacks [38]).

Step 3 (Resilient Control): To circumvent switching attacks, the controller needs to be redesigned in a way to be resilient. The system implements a feedback control law $\tilde{\boldsymbol{u}}$ on the attacked system, which is obtained according to the following design criterion. The system operator selects a positive-definite matrix $\tilde{\boldsymbol{P}}$ *a priori*, and its objective is to design a resilient control gain $\tilde{\boldsymbol{K}}$ for the switching data-injection attacks, by solving the linear matrix inequality (LMI) in (48).

Theorem 3: The feedback control law $\tilde{\boldsymbol{u}}(t) = \tilde{\boldsymbol{K}}\boldsymbol{y}_c(t)$ is resilient with respect to the cost function (40). That is, for arbitrary switching sequences, the attacked system

$$\dot{\boldsymbol{x}}_c(t) = \sum_{j=1}^{M} w_j(t)\tilde{\boldsymbol{A}}_j\boldsymbol{x}_c(t) \tag{46}$$

is asymptotically stable, and $\tilde{J}$ satisfies

$$\tilde{J} \le \boldsymbol{x}_0^\top \tilde{\boldsymbol{P}}\boldsymbol{x}_0 \tag{47}$$

if there exist a symmetric matrix $\tilde{\boldsymbol{P}} \succ \boldsymbol{0}$ and a scalar $\bar{\gamma} > 0$ such that the following LMI holds:

$$\begin{bmatrix} \tilde{\boldsymbol{A}}_i^\top \bar{\boldsymbol{P}} + \bar{\boldsymbol{P}}\tilde{\boldsymbol{A}}_i + \tilde{\boldsymbol{Q}} & \tilde{\boldsymbol{K}}^\top \\ \tilde{\boldsymbol{K}} & -\tilde{\boldsymbol{R}}^{-1} \end{bmatrix} \le \bar{\gamma}\boldsymbol{I} \tag{48}$$

where $\boldsymbol{x}_0$ is the initial state, and $\tilde{\boldsymbol{A}}_j := \boldsymbol{A} + \boldsymbol{B}\tilde{\boldsymbol{K}}(\boldsymbol{C} + \Delta\boldsymbol{K}_j)$ for all $j = 1, \ldots, M$.

Proof: Choose a common Lyapunov function

$$V(x) = \boldsymbol{x}_c^\top(t)\tilde{\boldsymbol{P}}\boldsymbol{x}_c(t) \tag{49}$$

for some symmetric matrix $\tilde{\boldsymbol{P}} \succ \boldsymbol{0}$. The time derivative of $V(x)$ can be found as

$$\begin{aligned} \dot{V}(x) &= \dot{\boldsymbol{x}}_c^\top(t)\tilde{\boldsymbol{P}}\boldsymbol{x}_c(t) + \boldsymbol{x}_c^\top(t)\tilde{\boldsymbol{P}}\dot{\boldsymbol{x}}_c(t) \\ &= \boldsymbol{x}_c^\top(t)\sum_{j=1}^{M} w_j(t)\Big(\tilde{\boldsymbol{A}}_j^\top\tilde{\boldsymbol{P}} + \tilde{\boldsymbol{P}}\tilde{\boldsymbol{A}}_j\Big)\boldsymbol{x}_c(t). \end{aligned}$$

By the common Lyapunov function method, if the following holds:

$$\boldsymbol{x}_c^\top(t)\Big(\tilde{\boldsymbol{A}}_j^\top\tilde{\boldsymbol{P}} + \tilde{\boldsymbol{P}}\tilde{\boldsymbol{A}}_j + \tilde{\boldsymbol{Q}} + \tilde{\boldsymbol{K}}^\top\tilde{\boldsymbol{R}}\tilde{\boldsymbol{K}}\Big)\boldsymbol{x}_c(t) \le 0 \tag{50}$$

then

$$\dot{V}(x) \le -\boldsymbol{x}_c^\top(t)\Big(\tilde{\boldsymbol{Q}} + \tilde{\boldsymbol{K}}^\top\tilde{\boldsymbol{R}}\tilde{\boldsymbol{K}}\Big)\boldsymbol{x}_c(t) \le 0 \tag{51}$$

for $w_j(t) \in \{0, 1\}\ \forall j$. That is, the attacked system is asymptotically stable. From (51), it is also evident that

$$\boldsymbol{x}_c^\top\tilde{\boldsymbol{Q}}\boldsymbol{x}_c + \tilde{\boldsymbol{u}}^\top\tilde{\boldsymbol{R}}\tilde{\boldsymbol{u}} \le -\dot{V}(x). \tag{52}$$

Since $\boldsymbol{x}_c(\infty) = \boldsymbol{0}$ holds for the stable closed-loop system, we deduce that

$$\tilde{J} \le -\int_0^\infty \dot{V}(x)dt = \boldsymbol{x}_0^\top\tilde{\boldsymbol{P}}\boldsymbol{x}_0. \tag{53}$$

The Schur compliment further confirms that (50) is equivalent to the LMI in (48), which completes the proof. ■

V. ILLUSTRATIVE EXAMPLES

In this section, we provide several numerical tests to showcase the effectiveness of the proposed resilient control scheme as well as the practical merits of our theory.

A. Power Generator

Consider a remotely controlled power generator described by the following normalized swing equation [39]:

$$\dot{\delta}(t) = \omega(t) \tag{54a}$$

$$M\dot{\omega}(t) = -D\omega(t) - P_f(t) + u(t) \tag{54b}$$

where δ and ω denote the phase angle and frequency deviation of the generator (rotor), respectively; $u(t)$ is the mechanical power provided for the generator; and M and D are the inertia and damping coefficients, respectively. The term $P_f(t) = b\sin(\delta(t))$ represents the electric power flow from the generator to the bus, where b is the susceptance of the transmission line. Upon linearizing the model at the nominal point $\omega = \delta = 0$ with $M = D = b = 1$, and defining the state $\boldsymbol{x} := [\delta\ \omega]^\top$, we obtain an LTI system as in (1) whose parameters are given by

$$\boldsymbol{A} = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, \quad \boldsymbol{B} = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$$

$$\boldsymbol{C} = \boldsymbol{I}, \quad \boldsymbol{K} = -\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}.$$

We consider a practical scenario where the adversary can alter the mechanical power supplied to the generator, through breaking the integrity of the sensor signal measuring δ and ω of the generator. Specifically, the adversary injects a state-feedback signal into the control signal, which will make the generator increase its power generation, and correspondingly, increase the power flow P_f along the transmission line. Choose without loss of generality that $\boldsymbol{Q}_1 = \boldsymbol{Q}_2 = \boldsymbol{I}$ and $\gamma_1 = \gamma_2 = 6$. The attack vectors are $\boldsymbol{d}_a^1 = [1\ 0]^\top$ and $\boldsymbol{d}_a^2 = [0\ 1]^\top$, i.e., the attacker compromises one sensor every time. Then, one can write that $\boldsymbol{s}_1 = [1\ 0]$ and $\boldsymbol{s}_2 = [0\ 4]$. The healthy plant under switching attacks becomes a switched system of two modes.

Using Theorem 1, the switching condition (17) becomes

$$i(t) := \arg\max_{j\in\{1,2\}} z_j \tag{55}$$

where

$$z_1 = \frac{1}{4}|\delta - \lambda_2|, \quad \text{and} \quad z_2 = \frac{1}{4}|4\omega - 2\lambda_2|.$$

The state trajectories of the system under switching attacks and those of the health plant are presented in Fig. 2, along with the switching instants between the two nodes given in Fig. 3. Observe that the attack stays in Mode 1 during the period [0.195, 0.278] s, yet it switches to Mode 2 at $t = 0.278$ s, and stays there till $t = 2.18$ s.

Choose $\boldsymbol{Q}_1 = 2\boldsymbol{I}$ and keep other parameters unchanged. Fig. 4 compares the simulation results under the optimal switching attacks and under random switching attacks subject to (55) with $z_1 \sim \mathbb{U}[0, 1]$ and $z_2 = 0.8$. Their corresponding performance indices [see (16)] are 93.5 and 51.5, respectively.

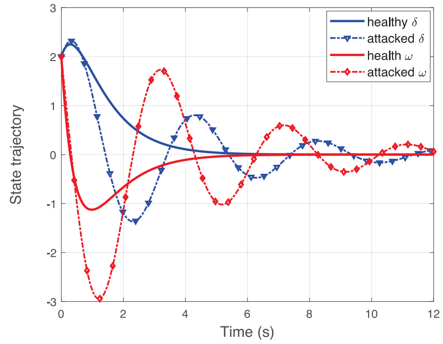


Fig. 2. State trajectories under optimal switching attacks.

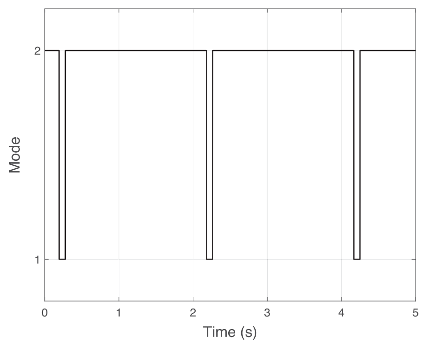


Fig. 3. Optimal switching instants.

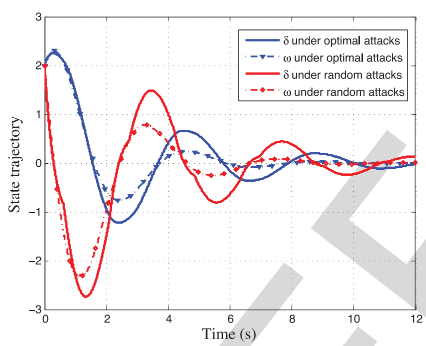


Fig. 4. Comparison results between optimal switching attacks and random switching attacks.

Invoking Theorem 3, a resilient control gain matrix can be obtained as

$$\tilde{\boldsymbol{K}} = -\begin{bmatrix} 1.59 & 0.28 \\ -0.1 & 0.89 \end{bmatrix}.$$

After implementing a resilient state-feedback control scheme, the state trajectories of the plant under attacks and the healthy plant are depicted in Fig. 5, where the upper bound on the cost was $\tilde{J}^* = 47.2$.

B. Power Systems

Now, consider a power system comprising several power generators and load buses. Following (54), the dynamics per generator can be modeled by a set of linear swing equations:

$$\dot{\delta}_i(t) = \omega_i(t) \tag{56a}$$

$$M_i\dot{\omega}_i(t) = -D_i\omega_i(t) - P_f^j(t) + u_i(t) \tag{56b}$$

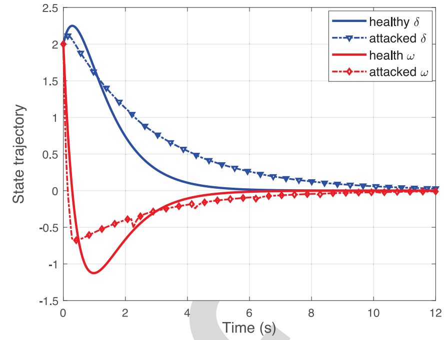


Fig. 5. State trajectories under the proposed resilient control.

for $i = 1, \ldots, n_g$, where n_g is the total number of generators. We consider a PID load frequency controller, namely

$$u_i = -\left(K_i^P\omega_i + K_i^I\int_0^t \omega_i\, dt + K_i^D\dot{\omega}_i\right) \tag{57}$$

where the controller parameters $K_i^P \geq 0$, $K_i^I \geq 0$, and $K_i^D \geq 0$ are the proportional gain, integral gain, and derivative gain, respectively. The overall power system dynamics of n_g generators can be compactly expressed as the following linear descriptor system:

$$\begin{bmatrix} \boldsymbol{I} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{M}+\boldsymbol{K}^D & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \end{bmatrix}\begin{bmatrix} \dot{\boldsymbol{\delta}} \\ \dot{\boldsymbol{\omega}} \\ \dot{\boldsymbol{\theta}} \end{bmatrix}$$

$$= -\begin{bmatrix} \boldsymbol{0} & -\boldsymbol{I} & \boldsymbol{0} \\ \boldsymbol{B}_{GG}+\boldsymbol{K}^I & \boldsymbol{D}_G+\boldsymbol{K}^P & \boldsymbol{B}_{GL} \\ \boldsymbol{B}_{LG} & \boldsymbol{0} & \boldsymbol{B}_{LL} \end{bmatrix}\begin{bmatrix} \boldsymbol{\delta} \\ \boldsymbol{\omega} \\ \boldsymbol{\theta} \end{bmatrix} - \begin{bmatrix} \boldsymbol{0} \\ \boldsymbol{P}_a^{\omega} \\ \boldsymbol{P}^L \end{bmatrix} \tag{58}$$

where vectors $\boldsymbol{\delta}$ and $\boldsymbol{\omega}$ collect accordingly the voltage phase angles and the rotor angular frequency deviations at all generator buses; vectors $\boldsymbol{\theta}$ and $\boldsymbol{P}^L$ stack up the voltage phase angles and power consumption at all load buses, respectively; and $\boldsymbol{M}$ is a diagonal matrix; and likewise for matrices $\boldsymbol{D}^G$, $\boldsymbol{D}^L$, $\boldsymbol{K}^P$, $\boldsymbol{K}^I$, and $\boldsymbol{K}^D$.

The attack design approach presented in Theorem 2 was numerically tested and verified using the IEEE 9-bus benchmark system, which has three power generators and six load buses [35]. The frequency measurements obtained may have already been strategically modified by a knowledgeable attacker to cause system frequencies to deviate from their nominal values. Here, we assume that the attacker can alter the frequencies measured at generators g_1 and g_2, and injects false data $\boldsymbol{P}_a^{\omega} := \boldsymbol{d}_a^j u_a(t)$ into the controller at victim generators.

Upon defining the state $\boldsymbol{x} := [\boldsymbol{\delta}^\top\ \boldsymbol{\omega}^\top]^\top$, the attacked system can be rewritten as

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}_a\boldsymbol{x}(t) + \boldsymbol{b}_a^j u_a(t).$$

Choose

$$\boldsymbol{K}^P = \mathrm{diag}([0.1\ 0.1\ 0.1]), \quad \boldsymbol{K} = \boldsymbol{I}$$

$$\boldsymbol{Q}_1 = \mathrm{diag}([0\ 0\ 0\ 16\ 16\ 16]), \boldsymbol{Q}_2 = \mathrm{diag}([0\ 0\ 0\ 14\ 14\ 14])$$

$$\gamma_1 = 7, \quad \gamma_2 = 11$$

$$\boldsymbol{d}_a^1 = [0.15\ 0\ 0]^\top, \quad \boldsymbol{d}_a^2 = [0\ 0.15\ 0]^\top.$$

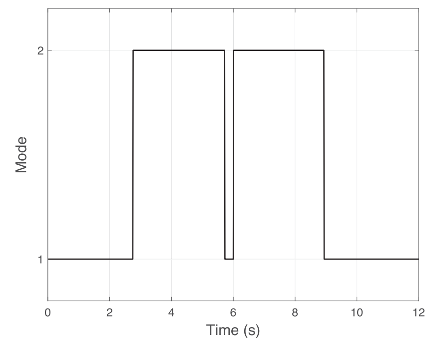


Fig. 6. Optimal switching instants.

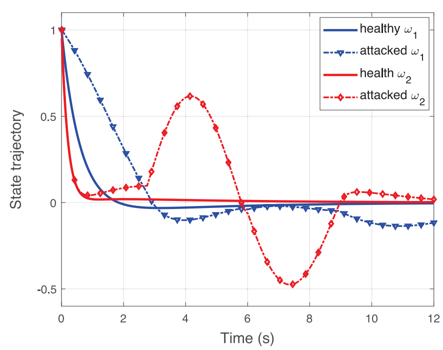


Fig. 7. State trajectories under optimal switching attacks.

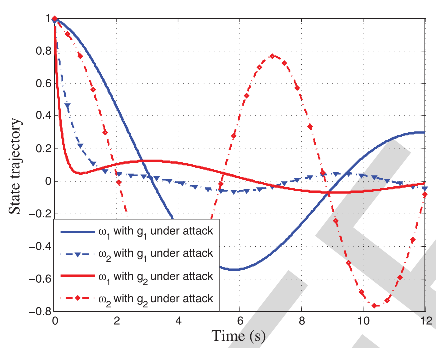


Fig. 8. State trajectories under nonswitching attacks.

Then

$$\boldsymbol{A}_a = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ -0.235 & 0.119 & 0.116 & -1.8 & 0 & 0 \\ 0.436 & -0.847 & 0.411 & 0 & -4.941 & 0 \\ 0.905 & 0.874 & -1.778 & 0 & 0 & -9.25 \end{bmatrix}$$

$$\boldsymbol{b}_a^1 = [0\ 0\ 0\ 1.2\ 0\ 0]^\top, \quad \boldsymbol{b}_a^2 = [0\ 0\ 0\ 0\ 4.4\ 0]^\top.$$

Appealing to Theorem 2, the optimal switching condition (31) becomes (55) where

$$z_1 = 16\left(x_4^2 + x_5^2 + x_6^2\right) + 0.21\lambda_4^2$$

$$z_2 = 14\left(x_4^2 + x_5^2 + x_6^2\right) + 1.76\lambda_5^2.$$

Fig. 8 shows the frequency deviation response of g_1 and g_2, when only g_1 or g_2 is under attack. Comparing Figs. 6 and 7, it is evident that at switching instants, the curves become discontinuous, which gives rise to the so-called vibration phenomenon [40]. The attacker switched four times in the simulation interval of 12 s.

VI. Conclusion

In this article, the optimal data-injection attack with switching behaviors was studied. Two different objective functions were suggested for the adversary to optimally determine the attack strategy. One focuses on the controller energy consumption, while the other considers the quadratic integration of states. The optimal attack design problem was formulated as an integer programming problem, which is hard to solve in general. By reformulating it as an optimal control problem of a linear switched system, we were able to find the optimal solution. A defense approach was developed to mitigate a class of data-injection attacks with feedback and location switching characteristics. The merits and practicability of our proposed strategies were shown by numerical simulations.

References

[1] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. Int. Conf. Distrib. Comput. Syst. Workshop*, Beijing, China, 2008, pp. 495–500.

[2] J. Ai, H. Chen, Z. Guo, G. Cheng, and T. Baker, "Mitigating malicious packets attack via vulnerability-aware heterogeneous network devices assignment," *Future Gener. Comput. Syst.*, to be published, doi: 10.1016/j.future.2019.04.034.

[3] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 40, no. 4, pp. 853–865, Jul. 2010.

[4] G. Wang, G. B. Giannakis, J. Chen, and J. Sun, "Distribution system state estimation: An overview of recent developments," *Front. Inf. Technol. Electron. Eng.*, vol. 20, no. 1, pp. 4–17, Jan. 2019.

[5] G. Wang, G. B. Giannakis, and J. Chen, "Robust and scalable power system state estimation via composite optimization," *IEEE Trans. Smart Grid*, to be published. doi: 10.1109/TSG.2019.2897100.

[6] C. Chen, K. Zhang, K. Yuan, L. Zhu, and M. Qian, "Novel detection scheme design considering cyber attacks on load frequency control," *IEEE Trans. Ind. Informat.*, vol. 14, no. 5, pp. 1932–1941, May 2018.

[7] G. Wu and J. Sun, "Optimal switching integrity attacks on sensors in industrial control systems," *J. Syst. Sci. Complex.*, to be published, doi: 10.1007/s11424-018-8067-y.

[8] W. Fang, W. Zhang, Y. Yang, Y. Liu, and W. Chen, "A resilient trust management scheme for defending against reputation time-varying attacks based on beta distribution," *Sci. China Inf. Sci.*, vol. 60, no. 4, Apr. 2017, Art. no. 040305.

[9] Y. Dong *et al.*, "An adaptive system for detecting malicious queries in Web attacks," *Sci. China Inf. Sci.*, vol. 61, no. 3, Mar. 2018, Art. no. 032114.

[10] J. Liu, Z.-G. Wu, D. Yue, and J. H. Park, "Stabilization of networked control systems with hybrid-driven mechanism and probabilistic cyber attacks," *IEEE Trans. Syst., Man, and Cybern., Syst.*, to be published.

[11] E. Mousavinejad, F. Yang, Q.-L. Han, and L. Vlacic, "A novel cyber attack detection method in networked control systems," *IEEE Trans. Cybern.*, vol. 48, no. 11, pp. 3254–3264, Nov. 2018.

[12] H. Yang, S. Ju, Y. Xia, and J. Zhang, "Predictive cloud control for networked multiagent systems with quantized signals under DoS attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published.

[13] J. Liu, Y. Gu, X. Xie, D. Yue, and J. H. Park, "Hybrid-driven-based H_∞ control for networked cascade control systems with actuator saturations and stochastic cyber attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published.

[14] Y. Pang, H. Xia, and M. J. Grimble, "Resilient nonlinear control for attacked cyber-physical systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published.

[15] D. Ding, Z. Wang, Q.-L. Han, and G. Wei, "Security control for discrete-time stochastic nonlinear systems subject to deception attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 5, pp. 779–789, May 2018.

[16] D. P. Fidler, "Was Stuxnet an act of war? Decoding a cyberattack," *IEEE Security Privacy*, vol. 9, no. 4, pp. 56–59, Jul. 2011.

[17] D. Zhang, S. K. Nguang, and L. Yu, "Distributed control of large-scale networked control systems with communication constraints and topology switching," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 47, no. 7, pp. 1746–1757, Jul. 2017.

[18] C. Liu, J. Wu, C. Long, and Y. Wang, "Dynamic state recovery for cyber-physical systems under switching location attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 14–22, Mar. 2017.

[19] S. Z. Yong, M. Zhu, and E. Frazzoli, "Resilient state estimation against switching attacks on stochastic cyber-physical systems," in *Proc. IEEE Conf. Decis. Control*, Osaka, Japan, Dec. 2015, pp. 5162–5169.

[20] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS attack scheduling in wireless networked control system," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 3, pp. 843–852, May 2016.

[21] G. Wu and J. Sun, "Optimal data integrity attack on actuators in cyber-physical systems," in *Proc. Amer. Control Conf.*, Boston, MA, USA, Jul. 2016, pp. 1160–1164.

[22] G. Wu, J. Sun, and J. Chen, "Optimal data injection attacks in cyber-physical systems," *IEEE Trans. Cybern.*, vol. 48, no. 12, pp. 3302–3312, Dec. 2018.

[23] M. M. Kogan, "Solution to the inverse problem of minimax control and worst case disturbance for linear continuous-time systems," *IEEE Trans. Autom. Control*, vol. 43, no. 5, pp. 670–674, May 1998.

[24] X. Xu and P. J. Antsaklis, "Optimal control of switched systems based on parameterization of the switching instants," *IEEE Trans. Autom. Control*, vol. 49, no. 1, pp. 2–16, Jan. 2004.

[25] D. Gorges, M. Izák, and S. Liu, "Optimal control and scheduling of switched systems," *IEEE Trans. Autom. Control*, vol. 56, no. 1, pp. 135–140, Jan. 2011.

[26] F. Zhu and P. J. Antsaklis, "Optimal control of hybrid switched systems: A brief survey," *Discr. Event Dyn. Syst.*, vol. 25, no. 3, pp. 345–364, Sep. 2015.

[27] T. Das and R. Mukherjee, "Optimally switched linear systems," *Automatica*, vol. 44, no. 5, pp. 1437–1441, May 2008.

[28] S. C. Bengea and R. A. DeCarlo, "Optimal control of switching systems," *Automatica*, vol. 41, no. 1, pp. 11–27, Jan. 2005.

[29] P. Riedinger, "A switched LQ regulator design in continuous time," *IEEE Trans. Autom. Control*, vol. 59, no. 5, pp. 1322–1328, May 2014.

[30] W. W. Lu, G. J. Balas, and E. B. Lee, "Linear quadratic performance with worst case disturbance rejection," *Int. J. Control*, vol. 73, no. 16, pp. 1516–1524, Jan. 2000.

[31] A. Bemporad, F. Borrelli, and M. Morari, "Min–max control of constrained uncertain discrete-time linear systems," *IEEE Trans. Autom. Control*, vol. 48, no. 9, pp. 1600–1606, Sep. 2003.

[32] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1216–1227, May 2014.

[33] J. Xin, N. Zheng, and A. Sano, "Subspace-based adaptive method for estimating direction-of-arrival with Luenberger observer," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 145–159, Jan. 2011.

[34] P. Jiang, H. Su, and J. Chu, "LMI approach to optimal guaranteed cost control for a class of linear uncertain discrete systems," in *Proc. Amer. Control Conf.*, vol. 1, no. 6. Chicago, IL, USA, Jun. 2000, pp. 327–331.

[35] F. Pasqualetti, F. Dörfler, and F. Bullo, "A divide-and-conquer approach to distributed attack identification," in *Proc. IEEE Conf. Decis. Control*, Osaka, Japan, 2015, pp. 5801–5807.

[36] T. Hsia and V. Vimolvanich, "An on-line technique for system identification," *IEEE Trans. Autom. Control*, vol. AC-14, no. 1, pp. 92–96, Feb. 1969.

[37] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014.

[38] A. Farraj, E. Hammad, A. Al Daoud, and D. Kundur, "A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1846–1855, Jul. 2016.

[39] A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson, "Secure control systems: A quantitative risk management approach," *IEEE Control Syst.*, vol. 35, no. 1, pp. 24–45, Feb. 2015.

[40] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[41] G. Wu, J. Sun, and J. Chen, "Optimal linear quadratic regulator of switched systems," *IEEE Trans. Autom. Control*, vol. 64, no. 7, pp. 2898–2904, Jul. 2019.

Guangyu Wu received the Ph.D. degree in control theory and control engineering from the Beijing Institute of Technology, Beijing, China, in 2018.

He is currently a Post-Doctoral Research Fellow with Tongji University, Shanghai, China. His current research interests include optimal control of switched systems, security of cyber-physical systems, and event-triggered distributed control of vehicle platoons.

Gang Wang (M'18) received the B.Eng. degree in electrical engineering and automation from the Beijing Institute of Technology, Beijing, China, in 2011, and the Ph.D. degree in electrical engineering from the University of Minnesota, Minneapolis, MN, USA, in 2018.

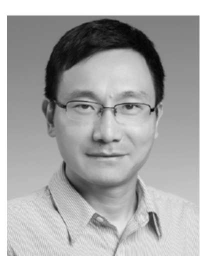
He is currently a Post-Doctoral Associate with the Department of Electrical and Computer Engineering, University of Minnesota. His current research interests include statistical signal processing, control, optimization, and deep learning with applications to data science and smart grids.

Dr. Wang was a recipient of the National Scholarship from China in 2013, the Innovation Scholarship (First Place) from China in 2017, and the Best Conference Papers at the 2017 European Signal Processing Conference and the 2019 IEEE Power & Energy Society General Meeting. He is currently serving on the editorial board of *Signal Processing*.

Jian Sun (M'10) received the bachelor's degree in automation and electric engineering from the Jilin Institute of Technology, Changchun, China, in 2001, the master's degree in mechanical and electronic engineering from the Fine Mechanics and Physics, Chinese Academy of Sciences (CAS), Changchun, in 2004, and the Ph.D. degree in control theory and engineering from CAS, Beijing, China, in 2007.

He was a Research Fellow with the Faculty of Advanced Technology, University of Glamorgan, Pontypridd, U.K., from 2008 to 2009. He was a Post-Doctoral Research Fellow with the Beijing Institute of Technology, Beijing, from 2007 to 2010. In 2010, he joined the School of Automation, Beijing Institute of Technology, where he has been a Professor since 2013. His current research interests include networked control systems, time-delay systems, and security of cyber-physical systems.

Prof. Sun is an Editorial Board Member of the IEEE TRANSACTIONS ON SYSTEMS, MAN AND CYBERNETICS: SYSTEMS, *Journal of Systems Science and Complexity*, and *Acta Automatica Sinica*.



Lu Xiong received the Ph.D. degree in vehicle engineering from Tongji University, Shanghai, China, in 2005.

He was a Post-Doctoral Researcher with the University of Stuttgart, Stuttgart, Germany, from 2008 to 2009. He is currently a Professor with the School of Automotive Studies, Tongji University. His current research interests include vehicle system dynamics and control, side-wheel/in-wheel motor drive electric vehicle control, design and control of electro-hydraulic brake system, and motion control of an intelligent/unmanned vehicle.

Optimal Switching Attacks and Countermeasures in Cyber-Physical Systems

Guangyu Wu, Gang Wang, *Member, IEEE*, Jian Sun, *Member, IEEE*, and Lu Xiong

***Abstract*—The work analyzes dynamic responses of a healthy plant under optimal switching data-injection attacks on sensors and develops countermeasures from the vantage point of optimal control. This is approached in a cyber-physical system setting, where the attacker can inject false data into a selected subset of sensors to maximize the quadratic cost of states and the energy consumption of the controller at a minimal effort. A 0-1 integer program is formulated, through which the adversary finds an optimal sequence of sets of sensors to attack at optimal switching instants. Specifically, the number of compromised sensors per instant is kept fixed, yet their locations can be dynamic. Leveraging the embedded transformation and mathematical programming, an analytical solution is obtained, which includes an algebraic switching condition determining the optimal sequence of attack locations (compromised sensor sets), along with an optimal state-feedback-based data-injection law. To thwart the adversary, however, a resilient control approach is put forward for stabilizing the compromised system under arbitrary switching attacks constructed based on a set of state-feedback laws, each of which corresponds to a compromised sensor set. Finally, an application using power generators in a cyber-enabled smart grid is provided to corroborate the effectiveness of the resilient control scheme and the practical merits of the theory.**

***Index Terms*—Data-injection attacks, dynamic set, resilient control, switching condition.**

I. Introduction

CYBER-PHYSICAL systems (CPSs) inherit the communication structure of the Internet of Things (IoT), yet they place more emphasis on the monitoring and control of entities in the physical world [1]. These systems are typically composed of a set of networked agents, that includes sensors, actuators, controllers, and communication devices. Heterogeneous devices are connected to collaboratively control the physical processes over high-speed communication networks [2]. CPSs realize the feedback and information exchange between the cyberspace and the physical world. Nonetheless, the deep integration of physical and information systems brings potential threats too [3]. Real-world applications are safety-critical: their failure can cause irreparable harm to the physical system being controlled and to people who rely on it. As a typical application of CPSs, the cyber-enabled smart grid comprises a large number of servers, computers, meters, phasor measurement units, generators, and so on. By blocking the information exchange between the users and the electricity sectors or destroying the data integrity [4], [5], the adversary can affect the electricity price and increase the energy consumption of generators [6].

To enhance the security of CPSs, the defender should be aware of diverse attack behaviors that the CPS may suffer as well as understand the attacker's intention [7]. Malicious attacks on CPSs can be launched at the physical layer, network layer [8], and application layer [9]. A common way to enhance the resilience of CPSs is to implement defense strategies against known attack patterns [10]. The resilient control or estimation focuses on mitigating the normal operation of attacked systems or restoring the actual state variables with certain acceptable error bounds [11]. Most advances impose assumptions on the attacker's abilities [12] or on its behavior patterns [13]. The resilient controller under fixed delay or out-of-order transmissions was proposed to optimize the worst-case performance [14]. An output-feedback controller under deception attacks with stochastic characteristics was designed to guarantee the prescribed security in probability while obtaining an upper bound of a quadratic cost criterion [15].

On the other hand, studying the adversary's optimal attack schedule can in turn offer insight on devising effective defense strategies [16]. A family of cyber attacks with switching behaviors has attracted attention, which can be categorized into two groups: 1) location-switching attacks and 2) signal-switching attacks. The attack signal can be, for instance, a switching signal turning on or off electrical devices and change the network topology [17] or a continuous false signal injected into controllers or actuators. State recovery under location switching attacks with known or unknown switching frequencies was studied in [18]. Stochastic linear

Manuscript received March 26, 2019; revised July 27, 2019; accepted September 24, 2019. The work of G. Wu and J. Sun was supported in part by NSFC under Grant 61522303, Grant U1509215, and Grant 61621063, and in part by the Program for Changjiang Scholars and Innovative Research Team in University under Grant IRT1208. The work of G. Wang was supported by NSF under Grant 1514056 and Grant 1711471. The work of L. Xiong was supported in part by NSFC under Grant 51975414, and in part by the National Key Research and Development Program of China 2018 under Grant YFB0105101. This article was recommended by Associate Editor Y. Zhao. *(Corresponding author: Gang Wang.)*

G. Wu and L. Xiong are with the Clean Energy Automotive Engineering Center, School of Automotive Studies, Tongji University, Shanghai 201804, China (e-mail: wuguangyu@tongji.edu.cn; xiong_lu@tongji.edu.cn).

G. Wang is with the Department of Electrical and Computer Engineering, University of Minnesota, Minneapolis, MN 55455 USA (e-mail: gangwang@umn.edu).

J. Sun is with the State Key Laboratory of Intelligent Control and Decision of Complex Systems, Beijing Institute of Technology, Beijing 100081, China, and also with the School of Automation, Beijing Institute of Technology, Beijing 100081, China (e-mail: sunjian@bit.edu.cn).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSMC.2019.2945067

systems under attacks were modeled as switching systems with unknown inputs, followed by a multiple model approach for resilient state estimation [19]. Precisely, the attacker decides when and where to launch an attack based on a Markov process. Switching DoS attacks on multiple communication lines with limited attacking times were examined [20]. The optimal switching sequence can be found by solving an integer program using an exhaustive search.

Despite the considerable success on switching attacks, the response of dynamic systems under switching data-injection attacks that can alter system dynamics (rather than estimation error or network topology) has not been studied. There are two critical challenges: Q1) Whether and how one can design an optimal switching data-injection law to maximize damage to the control system from the vantage point of the attacker? and Q2) How can one design an enhanced feedback control law to restore stability and maintain control performance of the system under such switching data-injection attacks? We answer these two questions in this article considering switching data-injection attacks on sensors. In our previous works [21], [22], attacks on actuators were considered, that aim at maximizing a quadratic state cost. In contrast, this article takes the standpoint of the attacker and focuses on designing attacks to maximize the controller's effort. Last but not least, a defense framework to stabilize the compromised system is proposed here. Specifically, the optimal switching data-injection attack design problem is formulated as a 0-1 integer programming problem [22], for which we develop an analytical solution of optimizing a nonlinear fractional function of the switching input.

This article studies the data-injection attacks that aim at manipulating the control signal and corrupting the system dynamics. Typically, CPSs comprise a large amount of sensing devices that are distributed in an unprotected, or even harmful environment. The malicious attacker can perform the node capture attack to crack the communication code, and manipulate purposefully the information exchanged with neighboring nodes or with the control center. To "benchmark" the worst-case performance due to comprised control signals, the sequence of optimal attack locations (namely, set of sensors) along with the corresponding optimal data-injection law over an attack duration is addressed. In this context, the set of attack locations is also termed as a compromised set. In a nutshell, the main contributions of this article are summarized as follows.

c1) We formulate the optimal switching data-injection attack design problem as a 0-1 integer programming problem. An analytical solution is established, including an algebraic switching condition along with a state-feedback-based data-injection law.

c2) We develop a novel resilient control scheme to mitigate the effect of attacks and enhance the closed-loop system, that entails identifying uncertainty matrices associated with different compromised sets and designing output-feedback controller gains. Our proposed control law can stabilize systems under even the worst-case attacks, while ensuring a bounded control cost.

The rest of this article is organized as follows. In Section II, the attack model is given. In Section III, the optimal switching attack design problem is formulated and studied. In Section IV, a resilient control scheme is put forward to defend against the switching attack with arbitrary switching sequences. Numerical tests using power generators are presented in Section V, while this article is concluded in Section VI.

II. Attack Model

We consider a healthy but possibly unstable plant described by a linear time-invariant (LTI) system

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t) \tag{1a}$$
$$\boldsymbol{y}(t) = \boldsymbol{C}\boldsymbol{x}(t) \tag{1b}$$
$$\boldsymbol{u}(t) = \boldsymbol{K}\boldsymbol{y}(t) \tag{1c}$$

where $\boldsymbol{x}(t) \in \mathbb{R}^n$ is the state vector, $\boldsymbol{u}(t) \in \mathbb{R}^k$ is the control input, and $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C})$ are the system matrices of suitable dimensions. To stabilize the LTI system, the output-feedback control with some gain matrix $\boldsymbol{K} \in \mathbb{R}^{k\times m}$ is considered. In the context of switching attacks, the plant is supposed to comprise a large number of sensor nodes; that is, m is large. At time t, each node sends its measurement to a central controller via a vulnerable wireless network. Before characterizing the worst-case attack consequence, we make several standard assumptions on the knowledge and attack ability of the adversary.

Assumption 1: The adversary has perfect knowledge of the system parameters in (1), namely, $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$, and $\boldsymbol{K}$ matrices.

Assumption 2: The adversary can capture the target sensor nodes and crack the passwords of their communication channels before launching attacks.

Assumption 3: When an attack occurs, the adversary injects datum $d^0_{a,j}u_a(t)$ into compromised sensor $j \in \mathcal{S}(t) \subseteq \{1, \ldots, m\}$, where $\mathcal{S}(t)$ collects the indices of all attacked sensors at time t; $u_a(t)$ is a global component that the attacker can optimize over, yet the local components $d^0_{a,j}$ can be different across sensors, which are arbitrarily selected by the adversary *a priori* and kept fixed throughout the attack. After the attack, the aggregated signal $\boldsymbol{y}(t) + \boldsymbol{d}_a(t)u_a(t)$ is transmitted to the controller, where $\boldsymbol{d}_a(t) := [d_{a,1}(t) \ \cdots \ d_{a,m}(t)]^\top$ with $d_{a,j}(t) = d^0_{a,j}$ if $j \in \mathcal{S}$ and $d_{a,j}(t) = 0$ otherwise. Moreover, $\boldsymbol{d}_a$ can be viewed as an "indicator" vector, which signifies the locations of the attacked sensors.

Following conventions, we use accordingly symbols $\boldsymbol{x}_c$, $\boldsymbol{y}_c$, and $\boldsymbol{u}_c$ to denote the state, measurement, and control vectors of the (compromised) LTI system under attack. Precisely, the attacked system can be described as

$$\dot{\boldsymbol{x}}_c(t) = \boldsymbol{A}\boldsymbol{x}_c(t) + \boldsymbol{B}\boldsymbol{u}_c(t) \tag{2a}$$
$$\boldsymbol{y}_c(t) = \boldsymbol{C}\boldsymbol{x}_c(t) + \boldsymbol{d}_a(t)u_a(t) \tag{2b}$$
$$\boldsymbol{u}_c(t) = \boldsymbol{K}\boldsymbol{y}_c(t). \tag{2c}$$

For ease of understanding, consider the setup described in Fig. 1, where the system consists of three sensor nodes. Suppose that the adversary can compromise only one node at a time. If the adversary compromises Sensor 1 at time t_1,

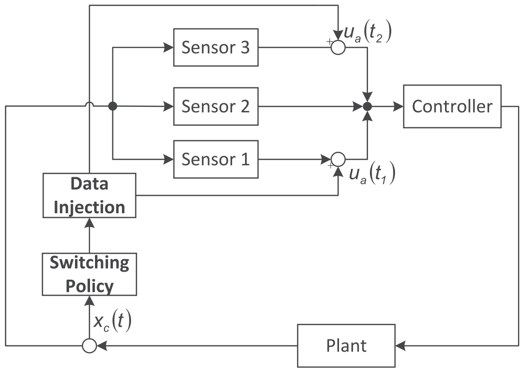


Fig. 1. Switching data-injection attack framework.

it holds that $\boldsymbol{d}_a(t_1) = [d^0_{a,1}\ 0\ 0]^\top$ with attack component $d^0_{a,1}$ determined by the attacker at the starting time t_0; and if Sensor 3 is attacked at time t_2, then $\boldsymbol{d}_a(t_2) = [0\ 0\ d^0_{a,3}]^\top$. Correspondingly, the false data $\boldsymbol{d}_a(t_1)u_a(t_1)$ and $\boldsymbol{d}_a(t_2)u_a(t_2)$ are injected into the measurement vectors $\boldsymbol{y}(t_1) = \boldsymbol{C}\boldsymbol{x}_c(t_1)$ and $\boldsymbol{y}(t_2) = \boldsymbol{C}\boldsymbol{x}_c(t_2)$ [see (1b)] to yield the compromised measurement vectors $\boldsymbol{y}_c(t_1)$ and $\boldsymbol{y}_c(t_2)$ [see (2b)].

In the traditional linear quadratic regulator (LQR) control, the goal of the system operator is to minimize the standard quadratic cost function involving the state variables and the controller effort over a fixed horizon; see standard textbook, e.g., [23]. On the contrary, the goal of the attacker is to maximize the aforementioned quadratic cost of the controller, therefore degrading the control performance, by choosing a sequence of instants to inject false data into a subset of sensors while maintaining a low attack cost.

On the other hand, the injected data can be understood as an adversarial interference produced by certain electrical equipment in a dynamic system. Due to physical limitations however, these equipment cannot produce an arbitrarily large interference signal, so the amplitude of $u_a(t)$ should be kept as small as possible. Considering any finite-time horizon $[t_0,\ t_f]$, two meaningful objective functions for optimal attack design are given by

$$J_a = \frac{1}{2}\boldsymbol{x}_c^\top(t_f)\boldsymbol{G}\boldsymbol{x}_c(t_f) + \frac{1}{2}\int_{t_0}^{t_f}\Big[\boldsymbol{u}_c^\top(t)\boldsymbol{Q}\boldsymbol{u}_c(t) - \gamma u_a^2(t)\Big]dt \quad (3)$$

and

$$J_b = \frac{1}{2}\boldsymbol{x}_c^\top(t_f)\boldsymbol{G}\boldsymbol{x}_c(t_f) + \frac{1}{2}\int_{t_0}^{t_f}\Big[\boldsymbol{x}_c^\top(t)\boldsymbol{Q}\boldsymbol{x}_c(t) - \gamma u_a^2(t)\Big]dt \quad (4)$$

where $\boldsymbol{G}$ and $\boldsymbol{Q}$ are symmetric, positive semidefinite matrices of suitable dimensions, and $\gamma > 0$ is a weighting coefficient, both chosen by the attacker. Their values tradeoff between the damage to the healthy plant and the attack cost. Specifically, too large (eigenvalues of) $\boldsymbol{Q}$ or too small γ values may incur instability of the plant under attack. If the adversary prefers a minimal energy cost and selects a larger γ value relative to (eigenvalues of) $\boldsymbol{Q}$, then the resultant $u_a(t)$ is able to render the system states to deviate from their actual values, and the stability of the attacked system may not lose.

Upon plugging (2b) and (2c) into (3), the objective function J_a can be rewritten as

$$J_a = \frac{1}{2}\boldsymbol{x}_c^\top(t_f)\boldsymbol{G}\boldsymbol{x}_c(t_f) + \frac{1}{2}\int_{t_0}^{t_f}\Big[\boldsymbol{x}_c^\top(t)\tilde{\boldsymbol{Q}}\boldsymbol{x}_c(t) + 2u_a(t)\boldsymbol{s}^\top(t)\boldsymbol{x}_c(t) + \tilde{\gamma}(t)u_a^2(t)\Big]dt \quad (5)$$

where the coefficients are given by

$$\tilde{\boldsymbol{Q}} := \boldsymbol{C}^\top\boldsymbol{K}^\top\boldsymbol{Q}\boldsymbol{K}\boldsymbol{C} \quad (6a)$$
$$\boldsymbol{s}(t) := \boldsymbol{C}^\top\boldsymbol{K}^\top\boldsymbol{Q}\boldsymbol{K}\boldsymbol{d}_a(t) \quad (6b)$$
$$\tilde{\gamma}(t) := \boldsymbol{d}_a^\top(t)\boldsymbol{K}^\top\boldsymbol{Q}\boldsymbol{K}\boldsymbol{d}_a(t) - \gamma. \quad (6c)$$

To guarantee existence of an optimal solution, the adversary needs to design $\boldsymbol{Q}$ and γ such that $\tilde{\gamma}(t) < 0$ [23]. It is clear from (5) that maximizing the controller energy consumption in J_a amounts to maximizing integrations of both the state quadratic $\boldsymbol{x}_c^\top(t)\tilde{\boldsymbol{Q}}\boldsymbol{x}_c(t)$ and the cross term $u_a(t)\boldsymbol{s}^\top(t)\boldsymbol{x}_c(t)$ (between u_a and $\boldsymbol{x}_c$). In comparison, only the integration of the state quadratic is maximized in J_b. In other words, if the adversary is solely interested in damaging the system state, the objective function J_b is preferred; but if the control cost of the attacked system is of interest too, then, J_a is preferred.

III. Optimal Switching Attack Design

In a large-scale CPS setting, compromising all communication channels necessarily requires a large amount of energy. The adversary with limited budget is instead inclined to attack only few sensors, possibly those of lowest security levels or with most vulnerable communication channels. Due to the limited computing resources and channel cracking capabilities, this article focuses on a practical setting where the adversary can attack a fixed number of sensors at a time. On the other hand, it is also not wise or optimal for the attacker to constantly attack a fixed set of sensors. A smart yet affordable strategy is to select a size-fixed set of sensors to effect attacks at every attack instant, to yield the worst-case system response. This dynamic attack strategy is to switch the attack among multiple sensor sets from time to time.

The goal of the attacker is to determine an optimal switching sequence of sensor sets to attack with an optimal data-injection law, so as to maximize the objective value J_a or J_b. When there are m sensors and the adversary can attack say $\ell \ll m$ sensors at a time, the total number of candidate attacks (i.e., size-ℓ sensor sets) is $M := \binom{m}{\ell}$. With slight abuse of notation, the M sensor sets (namely, the M sets of ℓ-sensor combinations) can be represented by the indicator vectors $\{\boldsymbol{d}_a^i\}_{i=1}^M$ defined in Assumption 3.

Example 1: If $m = 3$ and $\ell = 2$, there are $M = \binom{3}{2}$ sensor sets; that is, $\{1, 2\}$, $\{1, 3\}$, and $\{2, 3\}$ collecting the indices of the attacked sensors. Each of the three sensor sets can be uniquely represented by $\boldsymbol{d}_a^1 := [d^0_{a,1}\ d^0_{a,2}\ 0]^\top$, $\boldsymbol{d}_a^2 := [d^0_{a,1}\ 0\ d^0_{a,3}]^\top$, and $\boldsymbol{d}_a^3 := [0\ d^0_{a,2}\ d^0_{a,3}]^\top$.

From Fig. 1, if the input to the controller is compromised, the control signal (output of the controller) will be disturbed, so will the system dynamics. The control signal under the described switching data-injection attacks can be given by

$$\boldsymbol{u}_c(t) = \boldsymbol{K}\left[\boldsymbol{C}\boldsymbol{x}_c(t) + \sum_{j=1}^{M} w_j(t)\boldsymbol{d}_a^j u_a(t)\right] \tag{7}$$

where the switch input vector $\boldsymbol{w} := [w_1 \ \cdots \ w_M]$ belongs to

$$\mathcal{W}_0 := \left\{\boldsymbol{w}(t) \,\middle|\, \sum_{j=1}^{M} w_j(t) = 1, \text{ and } w_j(t) \in \{0, 1\} \ \forall j\right\}. \tag{8}$$

Per attack instant $t \geq t_0$, since only one sensor set (namely, $\boldsymbol{d}_a^j$ for some j) is to be chosen, its corresponding switch input $w_j(t)$ is set 1, while the others are set 0. Observe that the components of $\boldsymbol{d}_a^j$ are time invariant and known to the attacker. Therefore, the values of $\boldsymbol{w}(t) := [w_1(t) \ \ldots \ w_M(t)]^\top$ at different t signify the compromised sensor sets at corresponding instants. If two consecutive compromised sets (i.e., before and after some instant t) are different, then instant t is a switching instant, namely, the time at which the value of $\boldsymbol{w}(t)$ changes. The compromised sets at all switching instants define the so-called switching sequence

$$\boldsymbol{\zeta} := \{(\boldsymbol{w}(t_0), u_a(t_0)), \ \ldots, \ (\boldsymbol{w}(t_N), u_a(t_N))\} \tag{9}$$

where $t_0 \leq t_1 \leq \cdots \leq t_N \leq t_f$, the set $\{t_1, \ldots, t_N\}$ collects all switching instants, and N is the total number of switching operations.

In general, the attacker can assume the same objective function for all sensor sets. In certain settings of practical interest, the attacker may prefer different objective functions when different sensor sets are compromised. In Example 1, if the attacker aims to induce a larger deviation to state $x_{c,1}$ ($\boldsymbol{x}_c = [x_{c,1} \ x_{c,2} \ x_{c,3}]^\top$) when sensor set $\{1, 2\}$ is attacked, the attacker can simply use a diagonal matrix $\boldsymbol{Q}_1$ with entry $Q_1(1, 1)$ greater than $Q_1(2, 2)$ and $Q_1(3, 3)$, where $\boldsymbol{Q}_1$ belongs to the objective function for set $\{1, 2\}$. This prompts us to choose an objective function that sums the excited local objective functions at every instant, that is

$$\widehat{J}_a = \sum_{j=1}^{M} w_j J_a^j \ \text{ and } \ \widehat{J}_b = \sum_{j=1}^{M} w_j J_b^j \tag{10}$$

where J_a^j or J_b^j is obtained by replacing $\boldsymbol{Q}$ and γ in (3) or (4) with $\boldsymbol{Q}_j$ and γ_j.

Putting (2), (7), and (10) together, the optimal switching data-injection attack design problem is to find $\boldsymbol{w}(t)$ and $u_a(t)$ that

$$\max \quad \widehat{J}_a \ \text{ or } \ \widehat{J}_b \tag{11a}$$

$$\text{s.t.} \quad \dot{\boldsymbol{x}}_c(t) = \boldsymbol{A}_a\boldsymbol{x}_c(t) + \sum_{j=1}^{M} w_j(t)\boldsymbol{b}_a^j u_a(t) \tag{11b}$$

$$\boldsymbol{u}_c(t) = \boldsymbol{K}\left[\boldsymbol{C}\boldsymbol{x}_c(t) + \sum_{j=1}^{M} w_j(t)\boldsymbol{d}_a^j u_a(t)\right] \tag{11c}$$

$$\boldsymbol{w}(t) \in \mathcal{W}_0 \ \ \forall t \tag{11d}$$

where the coefficients $\boldsymbol{A}_a := \boldsymbol{A} + \boldsymbol{BKC}$ and $\boldsymbol{b}_a^j := \boldsymbol{BKd}_a^j$ for all $j = 1, \ldots, M$. In (11), the optimal switching data-injection attack design problem is formulated as a 0-1 integer program. If the binary variables $\{w_j(t)\}_{j=1}^M$ and the corresponding constraint (11d) are not present, (11) is LQR, whose optimal solution can be readily obtained in the closed-form leveraging Pontryagin's maximum principle (see [23]). In fact, constraint (11d) renders (11) nonconvex and NP-hard in general [24]. Fortunately, but if an optimal solution of $\boldsymbol{w}(t)$ is successfully found, then the optimal switching sequence $\boldsymbol{\zeta}$ can be easily recovered.

Interestingly enough, if we view the attacked system (2) as a linear switched system (see [25] for related definitions), the problem of optimal switch data-injection attack design on an LTI system in (11) can be treated as the optimal control problem of a linear switched system. As far as optimal control of switched systems is concerned, there is no closed-form solution in general, even for linear ones [26]. Recent efforts have primarily focused on the open-loop systems. Specifically, minimizing a quadratic cost on the state variables, an algebraic switching condition was developed for the open-loop linear switched systems [27], by leveraging the so-termed embedded transformation [28]. This result was further generalized to the multiple objective case [29]. For general closed-loop systems, whether and how one can obtain a closed-form expression of the switching condition remains unclear. Indeed, the attacked system (2) constitutes a special closed-loop system involving scalar control (instead of vector) $u_a(t)$, which prompts us to exploit the embedded transformation as well as recent mathematical programming advances to hopefully tackle (11).

The idea of the embedded transformation is to relax each binary constraint $w_j(t) \in \{0, 1\}$ to a box one $w_j(t) \in [0, 1]$, followed by solving a convex problem. Rather than dealing with constraint (11d), we consider the switch input vector $\boldsymbol{w}(t)$ belonging to the following convex set:

$$\mathcal{W}_1 := \left\{\boldsymbol{w}(t) \,\middle|\, \sum_{j=1}^{M} w_j(t) = 1, \text{ and } 0 \leq w_j(t) \leq 1 \ \ \forall j\right\}. \tag{12}$$

After replacing the last constraint $\boldsymbol{w}(t) \in \mathcal{W}_0$ with $\boldsymbol{w}(t) \in \mathcal{W}_1$ in (11), we arrive at the following embedded switching data-injection attack design problem:

$$\max \quad (11\text{a}) \tag{13a}$$

$$\text{s.t.} \quad (11\text{b}), \ (11\text{c}), \text{ and } \boldsymbol{w}(t) \in \mathcal{W}_1 \tag{13b}$$

which boils down to an optimal control problem of LQR type and whose optimal solution can be obtained leveraging Pontryagin's maximum principle. If luckily, the optimal solution of $\boldsymbol{w}(t)$ in (13) takes values at $\boldsymbol{w}(t) \in \mathcal{W}_0$ for all t, one can verify that the resulting solution is also the optimal solution of the original problem (11). To see this, we discuss the following two cases depending on whether J_a or J_b is maximized.

A. Maximizing $\widehat{J}_a$

Before applying the embedded transformation, we first simplify $\widehat{J}_a$. According to (10), $\widehat{J}_a$ can be written as

$$\widehat{J}_a = \frac{1}{2}\boldsymbol{x}_c^\top(t_f)\boldsymbol{G}\boldsymbol{x}_c(t_f) + \frac{1}{2}\sum_{j=1}^{M} w_j \int_{t_0}^{t_f}\left[\boldsymbol{u}_c^\top(t)\boldsymbol{Q}_j\boldsymbol{u}_c(t) - \gamma_j u_a^2(t)\right]dt. \tag{14}$$

For notational brevity, the dependence on t will be neglected. Since $\boldsymbol{w} \in \mathcal{W}_0$, it can be easily checked that

$$\left(\sum_{j=1}^{M} w_j \boldsymbol{d}_a^j\right)^{\top} \boldsymbol{K}^{\top} \left(\sum_{j=1}^{M} w_j \boldsymbol{Q}_j\right) \sum_{j=1}^{M} w_j \boldsymbol{K}\boldsymbol{d}_a^j = \sum_{j=1}^{M} w_j \boldsymbol{d}_a^{j\top} \boldsymbol{K}^{\top} \boldsymbol{Q}_j \boldsymbol{K}\boldsymbol{d}_a^j$$

and

$$\left(\sum_{j=1}^{M} w_j \boldsymbol{d}_a^j\right)^{\top} \boldsymbol{K}^{\top} \left(\sum_{j=1}^{M} w_j \boldsymbol{Q}_j\right) \boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_c = \sum_{j=1}^{M} w_j \boldsymbol{d}_a^{j\top} \boldsymbol{K}^{\top} \boldsymbol{Q}_j \boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_c.$$

Following (6), define for all $j = 1, \ldots, M$ that:

$$\tilde{\boldsymbol{Q}}_j := \boldsymbol{K}^{\top} \boldsymbol{Q}_j \boldsymbol{K} \tag{15a}$$

$$\tilde{\gamma}_j := \boldsymbol{d}_a^{j\top} \boldsymbol{K}^{\top} \boldsymbol{Q}_j \boldsymbol{K}\boldsymbol{d}_a^j - \gamma_j \tag{15b}$$

$$\boldsymbol{s}_j := \boldsymbol{C}^{\top} \boldsymbol{K}^{\top} \boldsymbol{Q}_j \boldsymbol{K}\boldsymbol{d}_a^j. \tag{15c}$$

Expanding (14), $\widehat{\mathcal{J}}_a$ can be further simplified into

$$\widehat{\mathcal{J}}_a = \frac{1}{2}\boldsymbol{x}_c^{\top}(t_f)\boldsymbol{G}\boldsymbol{x}_c(t_f) + \frac{1}{2}\sum_{j=1}^{M} w_j \int_{t_0}^{t_f} \left(\boldsymbol{x}_c^{\top} w_j \tilde{\boldsymbol{Q}}_j \boldsymbol{x}_c + 2\boldsymbol{x}_c^{\top}\boldsymbol{s}_j u_a + \tilde{\gamma}_j u_a^2\right) dt. \tag{16}$$

If the objective function $\widehat{\mathcal{J}}_a$ in (10) is adopted, we have the following result.

Theorem 1: Consider the performance index (16) for the attacked system (2). Then, the optimal switching condition of the switching attack for the original design problem (11) is given by

$$i(t) := \arg \max_{j \in \{1,\ldots,M\}} \; q_i(t) - f_j^2(t)/\tilde{\gamma}_j \tag{17}$$

and the optimal data-injection law

$$u_a(t) := -f_{i(t)}/\tilde{\gamma}_{i(t)} \tag{18}$$

where

$$f_j(t) := \boldsymbol{s}_j^{\top \boldsymbol{x}_c}(t) + \boldsymbol{b}_a^{j\top}(t)\boldsymbol{\lambda}(t) \quad \forall j = 1, \ldots, M \tag{19}$$

and $\boldsymbol{\lambda}(t) := [\lambda_1(t) \; \cdots \; \lambda_n(t)]^{\top}$ is the solution of

$$\dot{\boldsymbol{\lambda}}(t) = -\tilde{\boldsymbol{Q}}_{i(t)}\boldsymbol{x}_c(t) - u_a(t)\boldsymbol{s}_{i(t)} - \boldsymbol{A}_a^{\top}\boldsymbol{\lambda}(t) \tag{20}$$

with the boundary condition $\boldsymbol{\lambda}(t_f) = \boldsymbol{G}\boldsymbol{x}(t_f)$.

Proof: Our proof starts with Pontryagin's maximum principle for the relaxed problem (13) (see [23]), which is followed by showing that the optimal solution of $\boldsymbol{w}$ is always achieved at one of the vertices of the polytope $\mathcal{W}_1$. Hence, the relaxation is tight, which recovers the optimal solution of the original challenging nonconvex problem (11). Toward this objective and using (21), the Hamilton function for (13) is given by

$$H = \boldsymbol{x}_c^{\top} \sum_{j=1}^{M} w_j \tilde{\boldsymbol{Q}}_j \boldsymbol{x}_c + 2\boldsymbol{x}_c^{\top} \sum_{j=1}^{M} w_j \boldsymbol{s}_j u_a + \sum_{j=1}^{M} w_j \tilde{\gamma}_j u_a^2 - \boldsymbol{\lambda}^{\top}\left(\boldsymbol{A}_a \boldsymbol{x}_c + \sum_{j=1}^{M} w_j \boldsymbol{b}_a^j u_a\right). \tag{21}$$

To ensure existence of a meaningful solution, the adjustable parameters $\boldsymbol{Q}_j$, γ_j, and $\{\boldsymbol{d}_a^j\}_{j=1}^{M}$ should be designed such that $\partial^2 H/\partial u_a^2 < 0$ [30]. Upon defining $\tilde{\boldsymbol{\gamma}} := [\tilde{\gamma}_1 \; \cdots \; \tilde{\gamma}_M]^{\top}$, we deduce that for all $\boldsymbol{w} \in \mathcal{W}_1$, the following holds:

$$\partial^2 H/\partial u_a^2 = \sum_{j=1}^{M} w_j \boldsymbol{d}_a^{j\top} \boldsymbol{K}^{\top} \boldsymbol{Q}_j \boldsymbol{K}\boldsymbol{d}_a^j - \gamma_j = \boldsymbol{w}^{\top}\tilde{\boldsymbol{\gamma}} < 0. \tag{22}$$

That is, function H is strictly concave with a unique maximum given by the stationary point of the gradient in u_a. By setting $\partial H/\partial u_a = 0$, we arrive at

$$u_a = -\sum_{j=1}^{M} w_j \frac{\boldsymbol{s}_j^{\top \boldsymbol{x}_c} + \boldsymbol{b}_a^{j\top}\boldsymbol{\lambda}}{\boldsymbol{d}_a^{j\top}\boldsymbol{K}^{\top}\boldsymbol{Q}_j \boldsymbol{K}\boldsymbol{d}_a^j - \gamma_j} = -\sum_{j=1}^{M} w_j \frac{f_j}{\tilde{\gamma}_j}. \tag{23}$$

By the co-state equation $\dot{\boldsymbol{\lambda}} = -\partial H/\partial \boldsymbol{x}_c$, we have that

$$\dot{\boldsymbol{\lambda}} = -\sum_{j=1}^{M} w_j \tilde{\boldsymbol{Q}}_j \boldsymbol{x}_c - \sum_{j=1}^{M} w_j \boldsymbol{s}_j u_a - \boldsymbol{A}_a^{\top}\boldsymbol{\lambda}.$$

Let $\boldsymbol{f} := [f_1 \; \cdots \; f_M]^{\top}$ and $\boldsymbol{q} := [q_1 \; \cdots \; q_M]^{\top}$. Plugging (23) into (21) yields

$$H = \boldsymbol{\lambda}^{\top}\boldsymbol{A}_a \boldsymbol{x}_c + \frac{\boldsymbol{w}^{\top}\boldsymbol{q}}{2} - \frac{\left(\boldsymbol{w}^{\top}\boldsymbol{f}\right)^2}{2\boldsymbol{w}^{\top}\tilde{\boldsymbol{\gamma}}}$$

where $q_i = \boldsymbol{x}_c^{\top}\tilde{\boldsymbol{Q}}\boldsymbol{x}_c$. Evidently, as only the last two terms in H depend on $\boldsymbol{w}$, maximizing H with respect to $\boldsymbol{w} \in \mathcal{W}_1$ is equivalent to maximize the following reduced Hamilton function over $\mathcal{W}_1$:

$$\bar{H} := \frac{\boldsymbol{w}^{\top}\boldsymbol{q}}{2} - \frac{\left(\boldsymbol{w}^{\top}\boldsymbol{f}\right)^2}{2\boldsymbol{w}^{\top}\tilde{\boldsymbol{\gamma}}} := \frac{\varphi(\boldsymbol{w})}{2} - \frac{\psi^2(\boldsymbol{w})}{2\phi(\boldsymbol{w})}.$$

The derivatives of $\phi(\boldsymbol{w})$ and $\psi(\boldsymbol{w})$ with respect to w_j are given by

$$\dot{\phi} = \tilde{\gamma}_j, \quad \text{and} \quad \dot{\psi} = f_j. \tag{24}$$

The second derivative of $\bar{H}$ with respect to w_j is

$$\frac{\partial^2 \bar{H}}{\partial w_j^2} = -\frac{\left(f_j \phi - \tilde{\gamma}_j \psi\right)^2}{\phi^3} \geq 0. \tag{25}$$

Likewise, the second partial derivative of $\bar{H}$ with respect to w_j and w_k can be found as

$$\frac{\partial \bar{H}}{\partial w_j \partial w_k} = -\frac{(f_j\phi - \tilde{\gamma}_j\psi)(f_k\phi - \tilde{\gamma}_k\psi)}{\phi^3}. \tag{26}$$

Define $\boldsymbol{z} := [z_1 \; \cdots \; z_M]^{\top}$ with entries given by $z_j = f_j\phi - \tilde{\gamma}_j\psi$. Then, based on (25) and (26), the Hessian matrix of $\bar{H}$ can be written as follows:

$$\frac{\partial^2 \bar{H}}{\partial \boldsymbol{w}^2} = -\frac{1}{\phi^3}\begin{bmatrix} z_1^2 & z_1 z_2 & \cdots & z_1 z_M \\ z_2 z_1 & z_2^2 & \cdots & z_2 z_M \\ \vdots & \vdots & \ddots & \vdots \\ z_M z_1 & z_M z_2 & \cdots & z_M^2 \end{bmatrix} = \frac{\boldsymbol{z}\boldsymbol{z}^{\top}}{-\phi^3} \succeq \boldsymbol{0}$$

which confirms that function $\bar{H}$ is convex over $\mathcal{W}_1$.

Maximizing H over $\boldsymbol{w} \in \mathcal{W}_1$ reduces to maximizing convex $\bar{H}$ over a convex feasibility set $\boldsymbol{w} \in \mathcal{W}_1$. In this case, the minimum is always attained at one of the vertices of the polytope determined by the M box constraints in $\mathcal{W}_1$ [31]. It is evident

Algorithm 1: Optimal Switching Data-Injection Attack Algorithm

```
Determine d_a^j for all compromised sensor sets j ∈ {1, ..., M}.
Set: G, Q_j, and γ_j according to the attacker's preference.
for i = 1, ..., M do
    Solve (29);
end
Initialize: attack horizon [t_0, t_f], and S(t_0).
Estimate: initial state x_c(t_0).
while t ≤ t_f do
    for i = 1, ..., M do
        Compute (19);
        Evaluate β_j(t) = q_j(t) − f_j^2(t)/γ̃_j;
    end
    if i := arg max_j{β_j} then
        Compute (28);
        ẋ_c(t) = A_a x_c(t) + b_a^i u_a(t);
        λ(t) = P_i x_c(t);
    end
end
```

that the vertices of $\mathcal{W}_1$ coincide with the standard basis vectors $\boldsymbol{w}_j \in \mathbb{R}^M$ (whose jth entry is one, and remaining entries are zero), satisfying $\boldsymbol{w}_j \in \mathcal{W}_0$. Hence, the optimal solution of the relaxed problem recovers the optimal solution of the original nonconvex problem. Concretely, we have that

$$\max_{\boldsymbol{w}\in\mathcal{W}_1} \bar{H}(\boldsymbol{w}) = \max_{j\in\{1,\dots,M\}} q_j(t) - f_j^2(t)/\tilde{\gamma}_j \tag{27}$$

and the optimal switching instants are given by the time when $\boldsymbol{w}^*(t)$ changes. This completing the proof. ■

Regarding Theorem 1, we have the following observations.

Remark 1: By simply comparing the values $\{q_j(t) - f_j^2(t)/\tilde{\gamma}_j\}$ for all sensor sets at each instant, the attacker achieves an optimal switch input.

Remark 2: In the steady state, the optimal data-injection law is a state-feedback signal given by

$$u_a(t) = -\frac{1}{\tilde{\gamma}_i}\left(\boldsymbol{s}_i^\top + \boldsymbol{b}_a^{i\top}\boldsymbol{P}_i\right)\boldsymbol{x}_c(t) \tag{28}$$

where $\boldsymbol{P}_i \in \mathbb{S}_+^{n\times n}$ is the solution of the Riccati equation

$$\boldsymbol{P}_i\boldsymbol{A}_a + \boldsymbol{A}_a^\top\boldsymbol{P}_i - \frac{1}{\tilde{\gamma}_i}\left(\boldsymbol{P}_i\boldsymbol{b}_a^i + \boldsymbol{s}_i\right)\left(\boldsymbol{b}_a^{i\top}\boldsymbol{P}_i + \boldsymbol{s}_i^\top\right) + \boldsymbol{Q}_i = \boldsymbol{0}. \tag{29}$$

Remark 3: To find $u_a(t_0)$ in (28), the adversary has to estimate the initial state $\boldsymbol{x}_c(t_0)$ from sensor measurements $\boldsymbol{y}(t)$ of the healthy plant for $t \le t_0$, using, e.g., a Luenberger observer, before launching attacks.

B. Maximizing J_b

According to (10), $\widehat{J}_b$ can be written as

$$\widehat{J}_b = \frac{1}{2}\boldsymbol{x}_c^\top(t_f)\boldsymbol{G}\boldsymbol{x}_c(t_f) + \frac{1}{2}\sum_{j=1}^M w_j\int_{t_0}^{t_f}\left[\boldsymbol{x}_c^\top(t)\boldsymbol{Q}_j\boldsymbol{x}_c(t) - \gamma_j u_a^2(t)\right]dt. \tag{30}$$

If the objective function $\widehat{J}_b$ is adopted, we have the following theorem.

Theorem 2: The optimal switching condition of the switching attack that maximizes the performance index (30) for the attacked system (2) is given by

$$i(t) := \arg\max_{j\in\{1,\dots,M\}} \boldsymbol{x}_c^\top\boldsymbol{Q}_j\boldsymbol{x}_c + \frac{1}{\gamma_j}\left(\boldsymbol{b}_a^{j\top}\boldsymbol{\lambda}\right)^2 \tag{31}$$

with the optimal data-injection law being

$$u_a(t) := \frac{1}{\gamma_i}\boldsymbol{b}_a^{j\top}\boldsymbol{\lambda}(t) \tag{32}$$

where $\boldsymbol{\lambda}(t)$ is the solution of

$$\dot{\boldsymbol{\lambda}}(t) = -\boldsymbol{Q}_i\boldsymbol{x}_c(t) - \boldsymbol{A}_a^\top\boldsymbol{\lambda}(t) \tag{33}$$

with the boundary condition $\boldsymbol{\lambda}(t_f) = \boldsymbol{G}\boldsymbol{x}(t_f)$.

Proof: Appealing again to the Pontryagin's maximum principle, the Hamilton function is given by

$$H = \frac{1}{2}\sum_{j=1}^M w_j\left[\boldsymbol{x}_c^\top(t)\boldsymbol{Q}_j\boldsymbol{x}_c(t) - \gamma_j u_a^2(t)\right] + \boldsymbol{\lambda}^\top(t)\left[\boldsymbol{A}_a\boldsymbol{x}_c(t) + \sum_{j=1}^M w_j\boldsymbol{b}_a^j u_a(t)\right]. \tag{34}$$

The co-state equation confirms that

$$\dot{\boldsymbol{\lambda}}(t) = -\sum_{j=1}^M w_j\boldsymbol{Q}_j\boldsymbol{x}_c(t) - \boldsymbol{A}_a^\top\boldsymbol{\lambda}(t) \tag{35}$$

and by means of the coupled equation, it further holds that

$$u_a(t) = \sum_{j=1}^M \frac{w_j}{\gamma_j}\boldsymbol{b}_a^{j\top}\boldsymbol{\lambda}(t). \tag{36}$$

Substituting (36) into (34) yields

$$\bar{H} = \sum_{j=1}^M w_j\boldsymbol{x}_c^{\top\boldsymbol{Q}_j}\boldsymbol{x}_c + \sum_{j=1}^M\sum_{j=1}^M \frac{w_j w_k}{\gamma_j\gamma_k}\left(\boldsymbol{\lambda}^\top\boldsymbol{b}_a^j\right)\left(\boldsymbol{\lambda}^{\top\boldsymbol{b}_a^k}\right).$$

Maximizing $\bar{H}$ over $\boldsymbol{w}(t) \in \mathcal{W}_1$ now boils down to solving the following quadratic programming problem:

$$\begin{aligned} &\underset{\boldsymbol{w}}{\text{maximize}} && \boldsymbol{w}^\top\boldsymbol{H}\boldsymbol{w} + \boldsymbol{w}^\top\boldsymbol{q} && \text{(37a)}\\ &\text{subject to} && \boldsymbol{w} \in \mathcal{W}_1 && \text{(37b)}\end{aligned}$$

where $\boldsymbol{H} := \boldsymbol{h}\boldsymbol{h}^\top$ with $\boldsymbol{h} := [(\boldsymbol{\lambda}^\top\boldsymbol{b}_a^1)/\gamma_1 \cdots (\boldsymbol{\lambda}^\top\boldsymbol{b}_a^M)/\gamma_M]^\top$ and $\boldsymbol{q} := [(\boldsymbol{x}_c^{\top\boldsymbol{Q}_1}\boldsymbol{x}_c) \cdots (x_c^{\top\boldsymbol{Q}_M}\boldsymbol{x}_c)]^\top$.

Evidently, function $\bar{H}$ is convex in $\boldsymbol{w}$. Again, the optimal solution of maximizing $\bar{H}(\boldsymbol{w})$ over $\boldsymbol{w} \in \mathcal{W}_1$ is attained (at least) at one of the vertices of the polytope determined by $\mathcal{W}_1$, hence proving that the switch input $\boldsymbol{w}(t)$ obtains its optimal solution in $\mathcal{W}_0$. Concretely, we have that

$$\max_{\boldsymbol{w}\in\mathcal{W}_1} \bar{H}(\boldsymbol{w}) = \max_{j\in\{1,\dots,M\}} \boldsymbol{x}_c^\top\boldsymbol{Q}_j\boldsymbol{x}_c + \frac{1}{\gamma_j}\left(\boldsymbol{\lambda}^{\top\boldsymbol{b}_a^j}\right)^2 \tag{38}$$

completing the proof. ■

IV. Countermeasure Design

After exploiting the attack strategy from the perspective of the adversary, it is of paramount importance to pursue defense schemes (countermeasures) to mitigate the attacks. The problem of interest is to design an enhanced output-feedback controller to stabilize the attacked system, such that the control performance is preserved in a well-defined sense.

The countermeasure against switching attacks has mainly focused on the network topology attack and the DoS attack [20]. The resilient control against location switching attacks has not been investigated in the literature. Compared with the existing efforts that use cover network information, or have a subset of sensors immune to attacks destroying the feasibility of stealthy attacks [32], this article develops a resilient control scheme that tolerates intrusions. In general, resilience means that the operator maintains an acceptable level of operational normalcy despite attacks. Before presenting the countermeasure design, we start by introducing the definition of a resilient control scheme.

Definition 1: A feedback control law $\tilde{\boldsymbol{u}}$ is said to be resilient if it can stabilize the plant under a sequence of attacks arbitrarily constructed based on a set of state-feedback laws, while guaranteeing an acceptable cost, that is, for some given bound $\tilde{J}$, the following holds:

$$\tilde{J} \leq \tilde{J}^* \tag{39}$$

where

$$\tilde{J} = \int_0^\infty \left(\boldsymbol{x}_c^\top \tilde{\boldsymbol{Q}} \boldsymbol{x}_c + \tilde{\boldsymbol{u}}^\top \tilde{\boldsymbol{R}} \tilde{\boldsymbol{u}}\right) dt. \tag{40}$$

The operator has the freedom to select the two weighting matrices $\tilde{\boldsymbol{Q}} \succ \boldsymbol{0}$ and $\tilde{\boldsymbol{R}} \succ \boldsymbol{0}$ to compensate for the control performance degradation of the healthy plant. The state of the healthy system can be reconstructed using, e.g., a Luenberger observer [33]. If the attacker injects false data into a set of sensors over a period of time, the reconstruction error $\boldsymbol{e}_c(t)$ may diverge and the alarm will be triggered if it exceeds a threshold

$$\begin{cases} \dot{\hat{\boldsymbol{x}}}(t) = \boldsymbol{A}\hat{\boldsymbol{x}}(t) + \boldsymbol{B}u_c(t) + \boldsymbol{L}[\boldsymbol{y}_c(t) - \hat{\boldsymbol{y}}(t)] \\ \hat{\boldsymbol{y}}(t) = \boldsymbol{C}\hat{\boldsymbol{x}}(t) \end{cases}$$

$$\dot{\boldsymbol{e}}_c(t) = (\boldsymbol{A} - \boldsymbol{L}\boldsymbol{C})\boldsymbol{e}_c(t) + \boldsymbol{L}\boldsymbol{d}_a u_a(t)$$

where $\boldsymbol{e}_c(t) := \boldsymbol{x}_c(t) - \hat{\boldsymbol{x}}(t)$ and $\boldsymbol{L}$ is a gain matrix.

The attacked system can be modeled as a switched system consisting of M modes

$$\text{Mode } j\text{: } \dot{\boldsymbol{x}}_{c,j}(t) = \left(\boldsymbol{A}_a + \boldsymbol{B}\boldsymbol{K}\Delta\boldsymbol{K}_j\right)\boldsymbol{x}_{c,j}(t),\ \ j = 1, \ldots, M.$$

Consider for example, if J_a is maximized, substituting (28) into (11b), we have

$$\Delta\boldsymbol{K}_j = -\frac{1}{\tilde{\gamma}_{jj}}\left[\boldsymbol{d}_a^j\left(\boldsymbol{s}_j^\top + {\boldsymbol{B}_a^j}^\top \boldsymbol{P}_j\right)\right]. \tag{41}$$

The attacker uses matrices $\Delta\boldsymbol{K}_j$ at time t_j and switches to $\Delta\boldsymbol{K}_{j'}$ at $t_{j'}$. The attacker may change the attack locations randomly according to a stochastic model, or optimally with respect to an unknown criterion. As such, matrices $\Delta\boldsymbol{K}_j$ can be treated as a switching uncertainty of the healthy plant. The guaranteed cost control approach can be adopted to mitigate the attacks [34]. Once the detector detects an attack, or that the system response is considerably altered such that the attack is exposed, the defender needs to estimate the sensor links that have been compromised, as well as identify the uncertainty matrices $\Delta\boldsymbol{K}_j$. Recent advances on identifying the attack set from sensor measurements (e.g., [35]) assume attacks on the state equations, and do not utilize the information of the attacked state $\boldsymbol{x}_c$. The proposed identification problem is generally NP-hard, and reducing-complexity algorithms are presented. We adopt the following steps to defend against switching attacks.

Step 1 (Attack Extraction): As the false data injected into sensor measurements

$$\boldsymbol{f}_a(t) = u_a(t)\boldsymbol{d}_a^j. \tag{42}$$

The defender should find historical false data $\boldsymbol{f}_a(t) := [f_a^1(t)\ \cdots\ f_a^n(t)]^\top$ to identify the uncertainty matrix $\Delta\boldsymbol{K}_j$. The goal of this step is to extract $\boldsymbol{f}_a(t)$ and sort the timestamp of $\boldsymbol{f}_a(t)$ into M parts, namely, $\boldsymbol{O}_1, \ldots, \boldsymbol{O}_M$, each of which corresponds to a compromised sensor set. In Example 1, if $f_a^1(t) < \delta$, where $\delta > 0$ is a preselected threshold to account for computation and measurement inaccuracies, then $t \in \boldsymbol{O}_3$ (referring to set $\{2, 3\}$); if $f_a^2(t) < \delta$, $t \in \boldsymbol{O}_2$ (referring to set $\{1, 3\}$). If $f_a^3(t) < \delta$, then $t \in \boldsymbol{O}_1$ (referring to set $\{1, 2\}$). In this article, we assume that the control center is able to reset the attacked system under a known initial condition, and compare the attacked sensor measurements with $\boldsymbol{y}_v(t)$ from a virtual healthy system, namely

$$\dot{\boldsymbol{x}}_v(t) = \boldsymbol{A}_a\boldsymbol{x}_v(t) \tag{43a}$$
$$\boldsymbol{y}_v(t) = \boldsymbol{C}\boldsymbol{x}_v(t). \tag{43b}$$

Upon defining

$$\boldsymbol{e}_x = \boldsymbol{x}_c - \boldsymbol{x}_v$$
$$\boldsymbol{e}_y = \boldsymbol{y}_c - \boldsymbol{y}_v$$

we obtain that

$$\dot{\boldsymbol{e}}_x(t) = \boldsymbol{A}_a\boldsymbol{e}_x(t) + \boldsymbol{B}\boldsymbol{K}\boldsymbol{f}_a(t) \tag{44a}$$
$$\boldsymbol{e}_y(t) = \boldsymbol{C}\boldsymbol{e}_x(t) + \boldsymbol{f}_a(t) \tag{44b}$$

where $\boldsymbol{e}_x(0) = \boldsymbol{0}$. Vector $\boldsymbol{f}_a(t)$ can be calculated by the comparison result $\boldsymbol{e}_y(t)$, and once $\boldsymbol{f}_a(t)$ is recovered, the compromised sensors are found.

Step 2 (Attack Identification): The defender makes use of the data whose timestamp was collected in $\boldsymbol{O}_j$ to identify the unknown parameter matrices $\Delta\boldsymbol{K}_j$, using the common least-squares algorithm by solving

$$\min_{\Delta\boldsymbol{K}_j} \sum_{t \in \boldsymbol{O}_j} \left\|\boldsymbol{f}_a(t) - \Delta\boldsymbol{K}_j\boldsymbol{x}_c(t)\right\|_2^2. \tag{45}$$

In practice, $\boldsymbol{e}_y$ can be induced by, e.g., link failures in system components, noise in communication channels, or intentional attacks. If the online identification algorithm converges, there exists a state-feedback data-injection attack [36] (different from random attacks [37] or constant switching attacks [38]).

Step 3 (Resilient Control): To circumvent switching attacks, the controller needs to be redesigned in a way to be resilient. The system implements a feedback control law $\tilde{\boldsymbol{u}}$ on the attacked system, which is obtained according to the following design criterion. The system operator selects a positive-definite matrix $\tilde{\boldsymbol{P}}$ *a priori*, and its objective is to design a resilient control gain $\tilde{\boldsymbol{K}}$ for the switching data-injection attacks, by solving the linear matrix inequality (LMI) in (48).

Theorem 3: The feedback control law $\tilde{\boldsymbol{u}}(t) = \tilde{\boldsymbol{K}}\boldsymbol{y}_c(t)$ is resilient with respect to the cost function (40). That is, for arbitrary switching sequences, the attacked system

$$\dot{\boldsymbol{x}}_c(t) = \sum_{j=1}^{M} w_j(t)\tilde{\boldsymbol{A}}_j\boldsymbol{x}_c(t) \tag{46}$$

is asymptotically stable, and $\tilde{J}$ satisfies

$$\tilde{J} \le \boldsymbol{x}_0^\top \tilde{\boldsymbol{P}}\boldsymbol{x}_0 \tag{47}$$

if there exist a symmetric matrix $\tilde{\boldsymbol{P}} \succ \boldsymbol{0}$ and a scalar $\bar{\gamma} > 0$ such that the following LMI holds:

$$\begin{bmatrix} \tilde{\boldsymbol{A}}_i^\top \bar{\boldsymbol{P}} + \bar{\boldsymbol{P}}\tilde{\boldsymbol{A}}_i + \tilde{\boldsymbol{Q}} & \tilde{\boldsymbol{K}}^\top \\ \tilde{\boldsymbol{K}} & -\tilde{\boldsymbol{R}}^{-1} \end{bmatrix} \le \bar{\gamma}\boldsymbol{I} \tag{48}$$

where $\boldsymbol{x}_0$ is the initial state, and $\tilde{\boldsymbol{A}}_j := \boldsymbol{A} + \boldsymbol{B}\tilde{\boldsymbol{K}}(\boldsymbol{C} + \Delta\boldsymbol{K}_j)$ for all $j = 1, \dots, M$.

Proof: Choose a common Lyapunov function

$$V(x) = \boldsymbol{x}_c^\top(t)\tilde{\boldsymbol{P}}\boldsymbol{x}_c(t) \tag{49}$$

for some symmetric matrix $\tilde{\boldsymbol{P}} \succ \boldsymbol{0}$. The time derivative of $V(x)$ can be found as

$$\begin{aligned} \dot{V}(x) &= \dot{\boldsymbol{x}}_c^\top(t)\tilde{\boldsymbol{P}}\boldsymbol{x}_c(t) + \boldsymbol{x}_c^\top(t)\tilde{\boldsymbol{P}}\dot{\boldsymbol{x}}_c(t) \\ &= \boldsymbol{x}_c^\top(t)\sum_{j=1}^{M} w_j(t)\Big(\tilde{\boldsymbol{A}}_j^\top\tilde{\boldsymbol{P}} + \tilde{\boldsymbol{P}}\tilde{\boldsymbol{A}}_j\Big)\boldsymbol{x}_c(t). \end{aligned}$$

By the common Lyapunov function method, if the following holds:

$$\boldsymbol{x}_c^\top(t)\Big(\tilde{\boldsymbol{A}}_j^\top\tilde{\boldsymbol{P}} + \tilde{\boldsymbol{P}}\tilde{\boldsymbol{A}}_j + \tilde{\boldsymbol{Q}} + \tilde{\boldsymbol{K}}^\top\tilde{\boldsymbol{R}}\tilde{\boldsymbol{K}}\Big)\boldsymbol{x}_c(t) \le 0 \tag{50}$$

then

$$\dot{V}(x) \le -\boldsymbol{x}_c^\top(t)\Big(\tilde{\boldsymbol{Q}} + \tilde{\boldsymbol{K}}^\top\tilde{\boldsymbol{R}}\tilde{\boldsymbol{K}}\Big)\boldsymbol{x}_c(t) \le 0 \tag{51}$$

for $w_j(t) \in \{0, 1\}\ \forall j$. That is, the attacked system is asymptotically stable. From (51), it is also evident that

$$\boldsymbol{x}_c^\top\tilde{\boldsymbol{Q}}\boldsymbol{x}_c + \tilde{\boldsymbol{u}}^\top\tilde{\boldsymbol{R}}\tilde{\boldsymbol{u}} \le -\dot{V}(x). \tag{52}$$

Since $\boldsymbol{x}_c(\infty) = \boldsymbol{0}$ holds for the stable closed-loop system, we deduce that

$$\tilde{J} \le -\int_0^\infty \dot{V}(x)dt = \boldsymbol{x}_0^\top\tilde{\boldsymbol{P}}\boldsymbol{x}_0. \tag{53}$$

The Schur compliment further confirms that (50) is equivalent to the LMI in (48), which completes the proof. ■

V. Illustrative Examples

In this section, we provide several numerical tests to showcase the effectiveness of the proposed resilient control scheme as well as the practical merits of our theory.

A. Power Generator

Consider a remotely controlled power generator described by the following normalized swing equation [39]:

$$\dot{\delta}(t) = \omega(t) \tag{54a}$$

$$M\dot{\omega}(t) = -D\omega(t) - P_f(t) + u(t) \tag{54b}$$

where δ and ω denote the phase angle and frequency deviation of the generator (rotor), respectively; $u(t)$ is the mechanical power provided for the generator; and M and D are the inertia and damping coefficients, respectively. The term $P_f(t) = b\sin(\delta(t))$ represents the electric power flow from the generator to the bus, where b is the susceptance of the transmission line. Upon linearizing the model at the nominal point $\omega = \delta = 0$ with $M = D = b = 1$, and defining the state $\boldsymbol{x} := [\delta\ \omega]^\top$, we obtain an LTI system as in (1) whose parameters are given by

$$\boldsymbol{A} = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, \quad \boldsymbol{B} = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$$

$$\boldsymbol{C} = \boldsymbol{I}, \quad \boldsymbol{K} = -\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}.$$

We consider a practical scenario where the adversary can alter the mechanical power supplied to the generator, through breaking the integrity of the sensor signal measuring δ and ω of the generator. Specifically, the adversary injects a state-feedback signal into the control signal, which will make the generator increase its power generation, and correspondingly, increase the power flow P_f along the transmission line. Choose without loss of generality that $\boldsymbol{Q}_1 = \boldsymbol{Q}_2 = \boldsymbol{I}$ and $\gamma_1 = \gamma_2 = 6$. The attack vectors are $\boldsymbol{d}_a^1 = [1\ 0]^\top$ and $\boldsymbol{d}_a^2 = [0\ 1]^\top$, i.e., the attacker compromises one sensor every time. Then, one can write that $\boldsymbol{s}_1 = [1\ 0]$ and $\boldsymbol{s}_2 = [0\ 4]$. The healthy plant under switching attacks becomes a switched system of two modes.

Using Theorem 1, the switching condition (17) becomes

$$i(t) := \arg\max_{j\in\{1,2\}} z_j \tag{55}$$

where

$$z_1 = \frac{1}{4}|\delta - \lambda_2|, \quad \text{and} \quad z_2 = \frac{1}{4}|4\omega - 2\lambda_2|.$$

The state trajectories of the system under switching attacks and those of the health plant are presented in Fig. 2, along with the switching instants between the two nodes given in Fig. 3. Observe that the attack stays in Mode 1 during the period [0.195, 0.278] s, yet it switches to Mode 2 at $t = 0.278$ s, and stays there till $t = 2.18$ s.

Choose $\boldsymbol{Q}_1 = 2\boldsymbol{I}$ and keep other parameters unchanged. Fig. 4 compares the simulation results under the optimal switching attacks and under random switching attacks subject to (55) with $z_1 \sim \mathbb{U}[0, 1]$ and $z_2 = 0.8$. Their corresponding performance indices [see (16)] are 93.5 and 51.5, respectively.

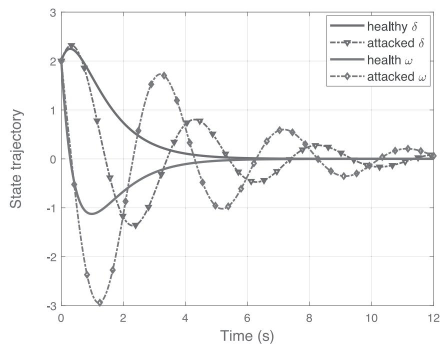


Fig. 2. State trajectories under optimal switching attacks.

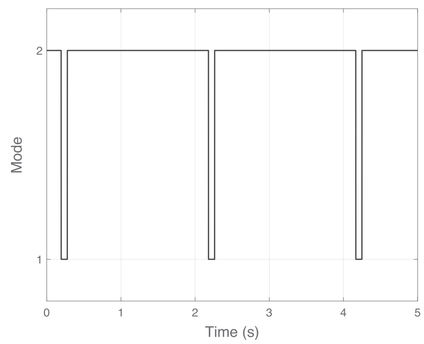


Fig. 3. Optimal switching instants.

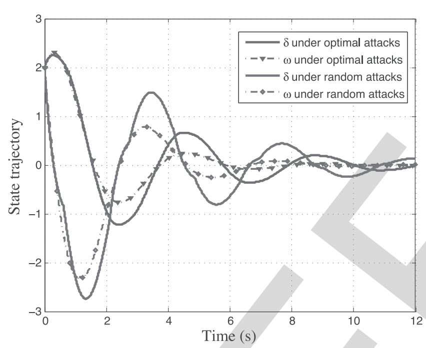


Fig. 4. Comparison results between optimal switching attacks and random switching attacks.

Invoking Theorem 3, a resilient control gain matrix can be obtained as

$$\tilde{\boldsymbol{K}} = -\begin{bmatrix} 1.59 & 0.28 \\ -0.1 & 0.89 \end{bmatrix}.$$

After implementing a resilient state-feedback control scheme, the state trajectories of the plant under attacks and the healthy plant are depicted in Fig. 5, where the upper bound on the cost was $\tilde{J}^* = 47.2$.

B. Power Systems

Now, consider a power system comprising several power generators and load buses. Following (54), the dynamics per generator can be modeled by a set of linear swing equations:

$$\dot{\delta}_i(t) = \omega_i(t) \tag{56a}$$
$$M_i \dot{\omega}_i(t) = -D_i \omega_i(t) - P_f^j(t) + u_i(t) \tag{56b}$$

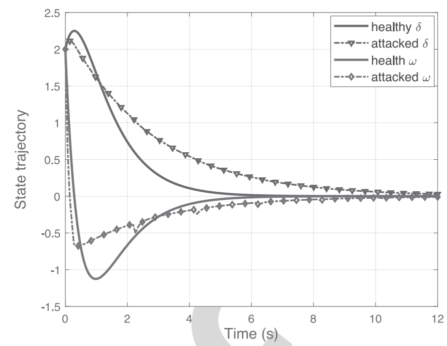


Fig. 5. State trajectories under the proposed resilient control.

for $i = 1, \ldots, n_g$, where n_g is the total number of generators. We consider a PID load frequency controller, namely

$$u_i = -\left(K_i^P \omega_i + K_i^I \int_0^t \omega_i \, dt + K_i^D \dot{\omega}_i\right) \tag{57}$$

where the controller parameters $K_i^P \geq 0$, $K_i^I \geq 0$, and $K_i^D \geq 0$ are the proportional gain, integral gain, and derivative gain, respectively. The overall power system dynamics of n_g generators can be compactly expressed as the following linear descriptor system:

$$\begin{bmatrix} \boldsymbol{I} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{M} + \boldsymbol{K}^D & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \end{bmatrix} \begin{bmatrix} \dot{\boldsymbol{\delta}} \\ \dot{\boldsymbol{\omega}} \\ \dot{\boldsymbol{\theta}} \end{bmatrix} = -\begin{bmatrix} \boldsymbol{0} & -\boldsymbol{I} & \boldsymbol{0} \\ \boldsymbol{B}_{GG} + \boldsymbol{K}^I & \boldsymbol{D}_G + \boldsymbol{K}^P & \boldsymbol{B}_{GL} \\ \boldsymbol{B}_{LG} & \boldsymbol{0} & \boldsymbol{B}_{LL} \end{bmatrix} \begin{bmatrix} \boldsymbol{\delta} \\ \boldsymbol{\omega} \\ \boldsymbol{\theta} \end{bmatrix} - \begin{bmatrix} \boldsymbol{0} \\ \boldsymbol{P}_a^{\omega} \\ \boldsymbol{P}^L \end{bmatrix} \tag{58}$$

where vectors $\boldsymbol{\delta}$ and $\boldsymbol{\omega}$ collect accordingly the voltage phase angles and the rotor angular frequency deviations at all generator buses; vectors $\boldsymbol{\theta}$ and $\boldsymbol{P}^L$ stack up the voltage phase angles and power consumption at all load buses, respectively; and $\boldsymbol{M}$ is a diagonal matrix; and likewise for matrices $\boldsymbol{D}^G$, $\boldsymbol{D}^L$, $\boldsymbol{K}^P$, $\boldsymbol{K}^I$, and $\boldsymbol{K}^D$.

The attack design approach presented in Theorem 2 was numerically tested and verified using the IEEE 9-bus benchmark system, which has three power generators and six load buses [35]. The frequency measurements obtained may have already been strategically modified by a knowledgeable attacker to cause system frequencies to deviate from their nominal values. Here, we assume that the attacker can alter the frequencies measured at generators g_1 and g_2, and injects false data $\boldsymbol{P}_a^{\omega} := \boldsymbol{d}_a^j u_a(t)$ into the controller at victim generators.

Upon defining the state $\boldsymbol{x} := [\boldsymbol{\delta}^\top \ \boldsymbol{\omega}^\top]^\top$, the attacked system can be rewritten as

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}_a \boldsymbol{x}(t) + \boldsymbol{b}_a^j u_a(t).$$

Choose

$$\boldsymbol{K}^P = \text{diag}([0.1 \ 0.1 \ 0.1]), \quad \boldsymbol{K} = \boldsymbol{I}$$
$$\boldsymbol{Q}_1 = \text{diag}([0 \ 0 \ 0 \ 16 \ 16 \ 16]), \boldsymbol{Q}_2 = \text{diag}([0 \ 0 \ 0 \ 14 \ 14 \ 14])$$
$$\gamma_1 = 7, \quad \gamma_2 = 11$$
$$\boldsymbol{d}_a^1 = [0.15 \ 0 \ 0]^\top, \quad \boldsymbol{d}_a^2 = [0 \ 0.15 \ 0]^\top.$$

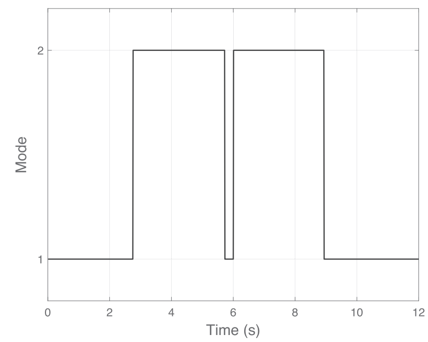


Fig. 6. Optimal switching instants.

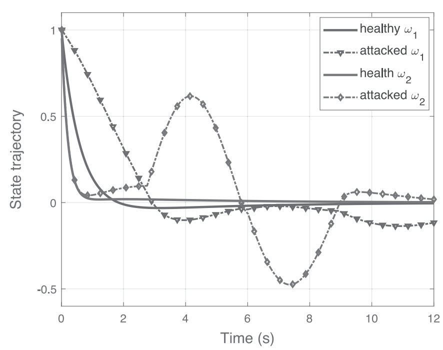


Fig. 7. State trajectories under optimal switching attacks.

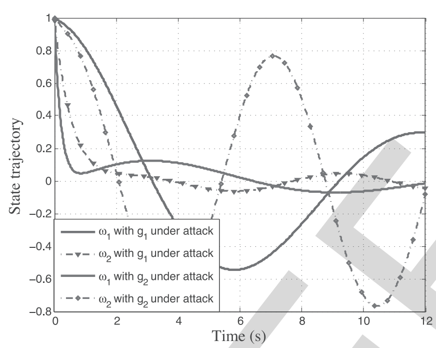


Fig. 8. State trajectories under nonswitching attacks.

Then

$$\boldsymbol{A}_a = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ -0.235 & 0.119 & 0.116 & -1.8 & 0 & 0 \\ 0.436 & -0.847 & 0.411 & 0 & -4.941 & 0 \\ 0.905 & 0.874 & -1.778 & 0 & 0 & -9.25 \end{bmatrix}$$

$$\boldsymbol{b}_a^1 = [0\ 0\ 0\ 1.2\ 0\ 0]^\top, \quad \boldsymbol{b}_a^2 = [0\ 0\ 0\ 0\ 4.4\ 0]^\top.$$

Appealing to Theorem 2, the optimal switching condition (31) becomes (55) where

$$z_1 = 16\left(x_4^2 + x_5^2 + x_6^2\right) + 0.21\lambda_4^2$$

$$z_2 = 14\left(x_4^2 + x_5^2 + x_6^2\right) + 1.76\lambda_5^2.$$

Fig. 8 shows the frequency deviation response of g_1 and g_2, when only g_1 or g_2 is under attack. Comparing Figs. 6 and 7, it is evident that at switching instants, the curves become discontinuous, which gives rise to the so-called vibration phenomenon [40]. The attacker switched four times in the simulation interval of 12 s.

VI. Conclusion

In this article, the optimal data-injection attack with switching behaviors was studied. Two different objective functions were suggested for the adversary to optimally determine the attack strategy. One focuses on the controller energy consumption, while the other considers the quadratic integration of states. The optimal attack design problem was formulated as an integer programming problem, which is hard to solve in general. By reformulating it as an optimal control problem of a linear switched system, we were able to find the optimal solution. A defense approach was developed to mitigate a class of data-injection attacks with feedback and location switching characteristics. The merits and practicability of our proposed strategies were shown by numerical simulations.

References

[1] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. Int. Conf. Distrib. Comput. Syst. Workshop*, Beijing, China, 2008, pp. 495–500.

[2] J. Ai, H. Chen, Z. Guo, G. Cheng, and T. Baker, "Mitigating malicious packets attack via vulnerability-aware heterogeneous network devices assignment," *Future Gener. Comput. Syst.*, to be published, doi: 10.1016/j.future.2019.04.034.

[3] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 40, no. 4, pp. 853–865, Jul. 2010.

[4] G. Wang, G. B. Giannakis, J. Chen, and J. Sun, "Distribution system state estimation: An overview of recent developments," *Front. Inf. Technol. Electron. Eng.*, vol. 20, no. 1, pp. 4–17, Jan. 2019.

[5] G. Wang, G. B. Giannakis, and J. Chen, "Robust and scalable power system state estimation via composite optimization," *IEEE Trans. Smart Grid*, to be published. doi: 10.1109/TSG.2019.2897100.

[6] C. Chen, K. Zhang, K. Yuan, L. Zhu, and M. Qian, "Novel detection scheme design considering cyber attacks on load frequency control," *IEEE Trans. Ind. Informat.*, vol. 14, no. 5, pp. 1932–1941, May 2018.

[7] G. Wu and J. Sun, "Optimal switching integrity attacks on sensors in industrial control systems," *J. Syst. Sci. Complex.*, to be published, doi: 10.1007/s11424-018-8067-y.

[8] W. Fang, W. Zhang, Y. Yang, Y. Liu, and W. Chen, "A resilient trust management scheme for defending against reputation time-varying attacks based on beta distribution," *Sci. China Inf. Sci.*, vol. 60, no. 4, Apr. 2017, Art. no. 040305.

[9] Y. Dong *et al.*, "An adaptive system for detecting malicious queries in Web attacks," *Sci. China Inf. Sci.*, vol. 61, no. 3, Mar. 2018, Art. no. 032114.

[10] J. Liu, Z.-G. Wu, D. Yue, and J. H. Park, "Stabilization of networked control systems with hybrid-driven mechanism and probabilistic cyber attacks," *IEEE Trans. Syst., Man, and Cybern., Syst.*, to be published.

[11] E. Mousavinejad, F. Yang, Q.-L. Han, and L. Vlacic, "A novel cyber attack detection method in networked control systems," *IEEE Trans. Cybern.*, vol. 48, no. 11, pp. 3254–3264, Nov. 2018.

[12] H. Yang, S. Ju, Y. Xia, and J. Zhang, "Predictive cloud control for networked multiagent systems with quantized signals under DoS attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published.

[13] J. Liu, Y. Gu, X. Xie, D. Yue, and J. H. Park, "Hybrid-driven-based H_∞ control for networked cascade control systems with actuator saturations and stochastic cyber attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published.

[14] Y. Pang, H. Xia, and M. J. Grimble, "Resilient nonlinear control for attacked cyber-physical systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published.

[15] D. Ding, Z. Wang, Q.-L. Han, and G. Wei, "Security control for discrete-time stochastic nonlinear systems subject to deception attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 5, pp. 779–789, May 2018.

[16] D. P. Fidler, “Was Stuxnet an act of war? Decoding a cyberattack,” *IEEE Security Privacy*, vol. 9, no. 4, pp. 56–59, Jul. 2011.

[17] D. Zhang, S. K. Nguang, and L. Yu, “Distributed control of large-scale networked control systems with communication constraints and topology switching,” *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 47, no. 7, pp. 1746–1757, Jul. 2017.

[18] C. Liu, J. Wu, C. Long, and Y. Wang, “Dynamic state recovery for cyber-physical systems under switching location attacks,” *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 14–22, Mar. 2017.

[19] S. Z. Yong, M. Zhu, and E. Frazzoli, “Resilient state estimation against switching attacks on stochastic cyber-physical systems,” in *Proc. IEEE Conf. Decis. Control*, Osaka, Japan, Dec. 2015, pp. 5162–5169.

[20] H. Zhang, P. Cheng, L. Shi, and J. Chen, “Optimal DoS attack scheduling in wireless networked control system,” *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 3, pp. 843–852, May 2016.

[21] G. Wu and J. Sun, “Optimal data integrity attack on actuators in cyber-physical systems,” in *Proc. Amer. Control Conf.*, Boston, MA, USA, Jul. 2016, pp. 1160–1164.

[22] G. Wu, J. Sun, and J. Chen, “Optimal data injection attacks in cyber-physical systems,” *IEEE Trans. Cybern.*, vol. 48, no. 12, pp. 3302–3312, Dec. 2018.

[23] M. M. Kogan, “Solution to the inverse problem of minimax control and worst case disturbance for linear continuous-time systems,” *IEEE Trans. Autom. Control*, vol. 43, no. 5, pp. 670–674, May 1998.

[24] X. Xu and P. J. Antsaklis, “Optimal control of switched systems based on parameterization of the switching instants,” *IEEE Trans. Autom. Control*, vol. 49, no. 1, pp. 2–16, Jan. 2004.

[25] D. Gorges, M. Izák, and S. Liu, “Optimal control and scheduling of switched systems,” *IEEE Trans. Autom. Control*, vol. 56, no. 1, pp. 135–140, Jan. 2011.

[26] F. Zhu and P. J. Antsaklis, “Optimal control of hybrid switched systems: A brief survey,” *Discr. Event Dyn. Syst.*, vol. 25, no. 3, pp. 345–364, Sep. 2015.

[27] T. Das and R. Mukherjee, “Optimally switched linear systems,” *Automatica*, vol. 44, no. 5, pp. 1437–1441, May 2008.

[28] S. C. Bengea and R. A. DeCarlo, “Optimal control of switching systems,” *Automatica*, vol. 41, no. 1, pp. 11–27, Jan. 2005.

[29] P. Riedinger, “A switched LQ regulator design in continuous time,” *IEEE Trans. Autom. Control*, vol. 59, no. 5, pp. 1322–1328, May 2014.

[30] W. W. Lu, G. J. Balas, and E. B. Lee, “Linear quadratic performance with worst case disturbance rejection,” *Int. J. Control*, vol. 73, no. 16, pp. 1516–1524, Jan. 2000.

[31] A. Bemporad, F. Borrelli, and M. Morari, “Min–max control of constrained uncertain discrete-time linear systems,” *IEEE Trans. Autom. Control*, vol. 48, no. 9, pp. 1600–1606, Sep. 2003.

[32] S. Bi and Y. J. Zhang, “Graphical methods for defense against false-data injection attacks on power system state estimation,” *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1216–1227, May 2014.

[33] J. Xin, N. Zheng, and A. Sano, “Subspace-based adaptive method for estimating direction-of-arrival with Luenberger observer,” *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 145–159, Jan. 2011.

[34] P. Jiang, H. Su, and J. Chu, “LMI approach to optimal guaranteed cost control for a class of linear uncertain discrete systems,” in *Proc. Amer. Control Conf.*, vol. 1, no. 6. Chicago, IL, USA, Jun. 2000, pp. 327–331.

[35] F. Pasqualetti, F. Dörfler, and F. Bullo, “A divide-and-conquer approach to distributed attack identification,” in *Proc. IEEE Conf. Decis. Control*, Osaka, Japan, 2015, pp. 5801–5807.

[36] T. Hsia and V. Vimolvanich, “An on-line technique for system identification,” *IEEE Trans. Autom. Control*, vol. AC-14, no. 1, pp. 92–96, Feb. 1969.

[37] S. Sridhar and M. Govindarasu, “Model-based attack detection and mitigation for automatic generation control,” *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014.

[38] A. Farraj, E. Hammad, A. Al Daoud, and D. Kundur, “A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems,” *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1846–1855, Jul. 2016.

[39] A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson, “Secure control systems: A quantitative risk management approach,” *IEEE Control Syst.*, vol. 35, no. 1, pp. 24–45, Feb. 2015.

[40] F. Pasqualetti, F. Dörfler, and F. Bullo, “Attack detection and identification in cyber-physical systems,” *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[41] G. Wu, J. Sun, and J. Chen, “Optimal linear quadratic regulator of switched systems,” *IEEE Trans. Autom. Control*, vol. 64, no. 7, pp. 2898–2904, Jul. 2019.

Guangyu Wu received the Ph.D. degree in control theory and control engineering from the Beijing Institute of Technology, Beijing, China, in 2018.

He is currently a Post-Doctoral Research Fellow with Tongji University, Shanghai, China. His current research interests include optimal control of switched systems, security of cyber-physical systems, and event-triggered distributed control of vehicle platoons.

Gang Wang (M’18) received the B.Eng. degree in electrical engineering and automation from the Beijing Institute of Technology, Beijing, China, in 2011, and the Ph.D. degree in electrical engineering from the University of Minnesota, Minneapolis, MN, USA, in 2018.

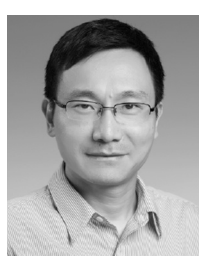
He is currently a Post-Doctoral Associate with the Department of Electrical and Computer Engineering, University of Minnesota. His current research interests include statistical signal processing, control, optimization, and deep learning with applications to data science and smart grids.

Dr. Wang was a recipient of the National Scholarship from China in 2013, the Innovation Scholarship (First Place) from China in 2017, and the Best Conference Papers at the 2017 European Signal Processing Conference and the 2019 IEEE Power & Energy Society General Meeting. He is currently serving on the editorial board of *Signal Processing*.

Jian Sun (M’10) received the bachelor’s degree in automation and electric engineering from the Jilin Institute of Technology, Changchun, China, in 2001, the master’s degree in mechanical and electronic engineering from the Fine Mechanics and Physics, Chinese Academy of Sciences (CAS), Changchun, in 2004, and the Ph.D. degree in control theory and engineering from CAS, Beijing, China, in 2007.

He was a Research Fellow with the Faculty of Advanced Technology, University of Glamorgan, Pontypridd, U.K., from 2008 to 2009. He was a Post-Doctoral Research Fellow with the Beijing Institute of Technology, Beijing, from 2007 to 2010. In 2010, he joined the School of Automation, Beijing Institute of Technology, where he has been a Professor since 2013. His current research interests include networked control systems, time-delay systems, and security of cyber-physical systems.

Prof. Sun is an Editorial Board Member of the IEEE TRANSACTIONS ON SYSTEMS, MAN AND CYBERNETICS: SYSTEMS, *Journal of Systems Science and Complexity*, and *Acta Automatica Sinica*.



Lu Xiong received the Ph.D. degree in vehicle engineering from Tongji University, Shanghai, China, in 2005.

He was a Post-Doctoral Researcher with the University of Stuttgart, Stuttgart, Germany, from 2008 to 2009. He is currently a Professor with the School of Automotive Studies, Tongji University. His current research interests include vehicle system dynamics and control, side-wheel/in-wheel motor drive electric vehicle control, design and control of electro-hydraulic brake system, and motion control of an intelligent/unmanned vehicle.