Chapter 10
Resilient Control of Nonlinear Cyber-Physical Systems: Higher-Order Sliding Mode Differentiation and Sparse Recovery-Based Approaches

Shamila Nateghi, Yuri Shtessel, Christopher Edwards, and Jean-Pierre Barbot

10.1 Introduction

Cyber-physical system security including information security, protection of CPS from being attacked and detection in adversarial environments have been considered in the literature (Pasqualetti et al. 2013; Jafarnia-Jahromi et al. 2012; Antsaklis 2014; Nekouei et al. 2018; Cardenas et al. 2008). Cryptography and Randomization are the two main approaches to protect a CPS against disclosure attacks: Cryptography is an approach to prevent third parties or the public from reading private messages by defining some protocols (Chen et al. 2016; Diffie and Hellman 1976). Randomization is a defensive strategy to confuse the potential attacker about deterministic rules and information of the system (Farokhi et al. 2017).

However, another challenge is to ensure that the CPS can continue functioning properly if a cyber-attack has happened. If the defense strategy just relies on detection, then the system's performance still degrades, and the threat of the same attack recur-

Portions of Sect. 10.6.4; ©2018 IEEE. Reprinted, with permission, from paper https://doi.org/10.1109/VSS.2018.8460426 in the proceedings of the 2018 VSS Workshop Portions of Sect. 10.6.5; ©2018 IEEE. Reprinted, with permission, from paper https://doi.org/10.1109/CDC.2018.8619354 in the proceedings of the 2018 IEEE CDC Conference.

S. Nateghi (✉) · Y. Shtessel
University of Alabama in Huntsville, Huntsville, AL, USA
e-mail: sb0086@uah.edu

Y. Shtessel
e-mail: shtessy@uah.edu

C. Edwards
The University of Exeter, Exeter, UK
e-mail: C.Edwards@exeter.ac.uk

J.-P. Barbot
QUARTZ Laboratory, ENSEA, Cergy-Pontoise, France
e-mail: barbot@ensea.fr

M. Abbaszadeh and A. Zemouche (eds.), *Security and Resilience in Cyber-Physical Systems*, https://doi.org/10.1007/978-3-030-97166-3_10

ring is not diminished. In addition, in the interval between the onset of the attack and detection, the system could experience significant damage (Jafarnia-Jahromi et al. 2012). A good example of such a scenario is the Stuxnet (Chen 2010). The Maroochy attack happened because of the lack of detection and resilience mechanisms as well (Slay and Miller 2007). In RQ-170, the absence of resilience control caused the system to be unable to defend itself against the spoofing attack (Hartmann and Steup 2013).

It is suggested in Dibaji et al. 2019 that information security mechanisms must be complemented by specially designed resilient control systems until the system is restored to normal operation. The focus of this chapter is on the reconstruction of the cyber-attack as a step to provide resilient control for a CPS.

The control/estimation algorithms are proposed in the literature for recovering CPS performance online if an attacker penetrates the information security mechanisms. A game-theoretic approach that provides resilience consists of trying to minimize the damage that an attacker can apply to the system or maximize the price of attacking a system. For example, a zero-sum stochastic differential game between a defender and an attacker is used to find an optimal control design to provide system security in Zhu and Başar (2011). Event-triggered control schemes instead of time-triggered schemes, which are based on how frequent the attacks occur, are an appropriate strategy to increase the resilience of CPS (Heemels et al. 2012). Event-triggered control is especially used to mitigate the effect of a disruption attack (Cetinkaya et al. 2016). Mean Subsequence Reduced as a resilient control approach ignores suspicious values and computes the control input at every moment (LeBlanc et al. 2013; Dibaji et al. 2017). In trust-based approaches, a function of trust value between the nodes of the system is defined since some of the nodes of the system may be untrustworthy (Ahmed et al. 2015). In Fawzi et al. (2014), authors found the number of attacks that can be tolerated so that the state of the system can still be exactly recovered. They designed a secure local control loop to improve the resilience of the system. In Jin et al. (2017), new adaptive control architectures that can foil malicious sensors and actuator attacks are developed for linear CPS without reconstructing the attacks, by means of feedback control only.

The mentioned approaches suffer some limitations including: I. It is assumed that the maximum number of malicious sensors in the network is known and bounded. Once the number of attacked sensors exceeds the upper bound, the proposed secure estimation or resilient control schemes fail to work. II. Only specific types of malicious actions acting on the cyber layer are considered. III. Only special structures of the cyber-physical system are considered.

On the other hand, the Sliding Mode Control and Higher-Order Sliding Mode Control (SMC/HOSM) and observation/differentiation techniques can handle systems of arbitrary relative degree perturbed by bounded attacks of arbitrary shape. The Sliding Mode Observers/differentiators (SMO/D) are capable of estimating the system states and reconstruct the bounded attacks asymptotically or in finite time (Fridman et al. 2007; Utkin 1992; Shtessel et al. 2014; Fridman et al. 2008; Levant 2003; Nateghi and Shtessel 2018; Nateghi et al. 2020a, 2018a, b) while addressing the outlined challenges.

Detection and observation of a scalar attack by a SMO has been accomplished for a linearized differential-algebraic model of an electric power network when plant and sensor attacks do not occur simultaneously (Wu et al. 2018). An adaptive SMO is designed coupled with a parameter estimator and a robust differentiator for detection and reconstruction of attacks in linear cyber-physical systems in Huang et al. (2018) when state and sensor attacks do not happen simultaneously. In Nateghi et al. (2020b, 2021), fixed-gain and adaptive-gain SMO are proposed for the online reconstruction of sensor attacks. Especially, dynamic filters that address the attack propagation dynamics are employed for attack reconstruction. A probabilistic risk mitigation model for cyber-attacks against Phasor Measurement Unit (PMU) networks is presented in Mousavian et al. (2014), where a risk mitigation technique determines whether a certain PMU should be kept connected to the network or removed while minimizing the maximum threat level for all connected PMUs. In Taha et al. (2016), the sliding mode-based observation algorithm is used to reconstruct the attacks asymptotically. This reconstruction is approximate only since pseudo-inverse techniques are used. In the above mentioned studies, which use a Sliding Mode approach for resilient control of CPSs, they all consider linear CPS and have their specific limitations.

In this chapter, online cyber-attack reconstruction for nonlinear CPSs is investigated. Two complement cases are considered: (I) When the number of sensors is less than the number of potential sparse attacks. A sparse signal recovery (SR) algorithm with a finite time convergence property (Yu et al. 2017) is used to reconstruct the attacks and presented in Sect. 10.3. (II) when the number of sensors is equal or greater than the number of potential attacks. A certain number of sensors are assumed to be protected from cyber-attacks. A higher-order sliding mode observer/differentiator (Fridman et al. 2008) is applied to estimate the states and reconstruct the attacks provided in Sect. 10.4. The proposed algorithm ensures finite-time state estimation of observable variables and asymptotic estimation of the unobservable variables for the case when the system has asymptotically stable internal dynamics. In order to maintain the CPS closed-loop dynamics to be the same as those prior to the attacks, it is proposed to clean the corrupted measurements, as soon as the attacks are reconstructed, thus preventing the attack propagation to the CPS through feedback control. Actuator attacks are also cleaned from the reconstructed actuator attacks. The effectiveness of the proposed algorithms in Sects. 10.3 and 10.4 to estimate the states and reconstruct the attacks are tested on the attacked US WECC power network system.

10.2 Mathematical Modeling

Consider the following nonlinear CPS which is completely observable and asymptotically stable affected by attack

$$\dot{x} = f_1(t) + B_1(x)(u + d_u(t)), \tag{10.1}$$

where $x \in R^n$ presents the state vector of CPS, $f_1(x) \in R^n$ is a smooth vector field, $y \in R^p$ denotes the sensor measurement vector, and $u \in R^{q_1}$ is the control signal. The $d_u \in R^{q_1}$ and $d_y \in R^{q_2}$ are the actuator and sensor attack, respectively. The vector $C_x \in R^p$ is the output smooth vector field, $B_1(x) \in R^{n \times q_1}$ and $D_1 \in R^{p \times q_2}$ denote the attack/fault distribution matrices.

The output feedback control signal u is a function of sensor measurement y which can be corrupted by the sensor attacks. This is

$$u(y) = \gamma(C(x) + d_y) = \gamma(x + D_1 d_y). \tag{10.2}$$

Replacing control signal u in CPS (10.1) to find the closed-loop CPS model gives

$$\begin{aligned} \dot{x} &= f_1(t) + B_1(x)(\gamma(x, d_y), d_u(t)) = f_1(t) + B_1(x)(\gamma(x, d_y) + B_1(x)d_u(t) \\ y &= C(x) + D_1 d_y(t). \end{aligned} \tag{10.3}$$

Assume that u can be written as

$$\gamma(x, d_y) = \gamma_1(x) + \gamma_2(d_y), \tag{10.4}$$

then, the closed-loop CPS (10.3) is given as

$$\begin{aligned} \dot{x} &= f_1(t) + B_1(x)(\gamma(x, d_y), d_u(t)) \\ &= f_1(t) + B_1(x)\gamma_1(x) + B_1(x)\gamma_2(d_y) + B_1(x)d_u(t) \\ y &= C(x) + D_1 d_y(t). \end{aligned} \tag{10.5}$$

Therefore, the CPS (10.1) after applying control signal u is presented as

$$\begin{aligned} \dot{x} &= f(t) + B_1(x)d_x(t) \\ y &= C(x) + D_1 d_y(t), \end{aligned} \tag{10.6}$$

where

$$\begin{aligned} f(x) &= f_1(x) + B_1(x)\gamma_1(x) \\ d_x(t) &= \gamma_2(d_y) + d_u(t), \end{aligned} \tag{10.7}$$

where $d_x(t)$ represents the plant/state attack.

Define the attack signal $d(t) \in R^q$ where $q = q_1 + q_2$ as

$$d = \begin{bmatrix} d_x \\ d_y \end{bmatrix}, \tag{10.8}$$

where $d_x \in R^{q_1}$ and $d_y \in R^{q_2}$, and

$$\begin{aligned} B(x) &= \begin{bmatrix} B_1(x) \; 0_1 \end{bmatrix} \\ D &= \begin{bmatrix} 0_2 \; D_1 \end{bmatrix}, \end{aligned} \tag{10.9}$$

where $B_1(x) \in R^{n\times q_1}$, $D_1 \in R^{p\times(q-q_1)}$, $0_1 \in R^{n\times(q-q_1)}$, $0_2 \in R^{p\times q_1}$. Then, the closed-loop CPS (10.6) is rewritten as

$$\begin{aligned} \dot{x} &= f(x) + B(x)d(t) \\ y &= C(x) + Dd(t). \end{aligned} \tag{10.10}$$

10.2.1 Problem Statement

The problem is two-fold
1. Develop an observation algorithm that reconstructs online the state $x \in R^n$ and attack signal $d(t) \in R^q$ in CPS (10.10) so that

$$\begin{aligned} \hat{x}(t) &\to x(t) \\ \hat{d}(t) &\to d(t). \end{aligned} \tag{10.11}$$

2. Develop an observation algorithm that reconstructs online the state $x \in R^n$, the plant attack signal $d_x(t) \in R^{q_1}$, and sensor attack signal $d_y(t) \in R^{q_2}$ in CPS (10.6) as shown in the table below so that

$$\begin{aligned} \hat{x}(t) &\to x(t) \\ \hat{d}_x(t) &\to d_x(t) \\ \hat{d}_y(t) &\to d_y(t) \end{aligned} \tag{10.12}$$

as time increases.

Attack plan	$d_u(t) \neq 0$	$d_y(t) \neq 0$	Access to all sensors	Need to know the system model
Stealth attack		√		
Deception attack	√			
Replay attack	√	√	√	
Covert attack	√	√		√
False data injection attack		√		√

Remark 10.1 As soon as the sensor attack $d_y(t)$ and the state attack $d_x(t)$ are estimated/reconstructed the measurement $y = C(x) + D_1 d_y(t)$ could be cleaned as

$$y_{clean} = y - D_1\hat{d}_y(t) = C(\hat{x}) + D_1(d_y(t) - \hat{d}_y(t)) \to y_{clean} = C(\hat{x}). \tag{10.13}$$

Next, the clean measurement y_{clean} can be used in the feedback control of CPS. This allows blocking the propagation of the sensor attack to the dynamics of CPS through the feedback control. The modified actuator commands are also cleaned from estimated actuator attacks, i.e., the actuator attack $d_u(t)$ can be estimated/reconstructed from (10.7) as $\hat{d}_u(t) = \hat{d}_y(t) - \gamma_2(\hat{d}_y)$, and the system (10.5) dynamics converge to

$$\dot{x} = f_1(x) + B_1(x)(u + d_u(t) - \hat{d}_u(t)) \rightarrow \dot{x} = f_1(t) + B_1(x)u \tag{10.14}$$

as time increases.

In this chapter, attack reconstruction is divided to two cases: when the number of potential attacks is (I) greater or equal, and (II) less than the number of sensors. In the following two sections, the mentioned cases are investigated.

10.3 Preliminary: Sparse Recovering Algorithm

The problem of recovering an unknown input signal from measurements is well known, as a left invertibility problem, as seen in Sain and Massey (1969), Barbot et al. (2009), but this problem was only treated in the case where the number of measurements is equal or greater than the number of unknown inputs. The left invertibility problem in the case of fewer measurements than unknown inputs has no solution or more exactly has an infinity of solutions.

Note that the input signals can be considered sparse or compressive for transmission. The compressive sensing theory could be a proper candidate to deal with these constraints. Sparse recovery algorithm is used to address this problem. The problem is to find the exact recovery under sparse assumption denoted for the sake of simplicity as "Sparse Recovery", i.e., finding a concise representation of a signal which is described as

$$\kappa = \Theta(s + \varepsilon), \tag{10.15}$$

where $s \in R^N$ are the unknown inputs with no more than j non-zero entries, $\kappa \in R^M$ are the measurements, ε is a measurement noise, and $\Theta \in R^M \times N$ is a matrix where $M < N$.

Assumption 10.1 The matrix Θ satisfies the Restricted Isometry Property (RIP) condition of j-order with constant $\zeta_j \in (0, 1)$ (ζ_j is as small as possible for computational reasons).

Note that the condition of RIP in compressive sensing is an essential requirement that ensures the recovery of sparse signal vectors. RIP property provides the necessary and sufficient requirements for the compressive sensing matrix; however, it is not robust enough for consideration under the noise.

Assumption 10.1 implies that for any j sparse of signal s, i.e., vectors with at most j non-zero elements, the following condition is verified

$$(1-\zeta_s)\|s\|_2^2 \leq \|\Theta s\|_2^2 \leq (1+\zeta_s)\|s\|_2^2. \tag{10.16}$$

Consider Γ as the index set of non-zero elements of Θ, then (10.16) is equivalent to Yu et al. (2017), Candes and Tao (2005)

$$1-\zeta_s \leq eig(\Theta_\Gamma^T \Theta_\Gamma) \leq 1+\zeta_s, \tag{10.17}$$

where Θ_Γ is the sub-matrix of Θ with active nodes. The problem of SR is often cast as an optimization problem that minimizes a cost function constructed by leveraging the observation error term and the sparsity inducing term (Yu et al. 2017), i.e.,

$$s^* = arg \quad \min_{s \in R^N} \frac{1}{2}\|\kappa - \Theta s\|_1^2 + \lambda \Lambda(s), \tag{10.18}$$

where the sparsity term $\Lambda(s)$ can be replaced by $\Lambda(s) = \|s\|_1 \equiv \sum_i |s_i|$ as long as the RIP conditions hold. The $\lambda > 0$ in (10.18) is the balancing parameter and s^* is the critical point, i.e., the solution of (10.15).

For sparse vectors s with j-sparsity, where j must be equal or smaller than $\frac{M-1}{2}$, solution to the SR problem is unique and coincides with the critical point of (10.15) when the RIP condition for Θ with order $2j$ is verified (Yu et al. 2017). Under the sparse Assumption 10.1 of s and fulfilling j-RIP condition of matrix, the estimate of the sparse signal s as proposed in Yu et al. (2017) is

$$\begin{aligned} &\mu \dot{\nu}(t) = -\lceil \nu(t) + (\Theta^T \Theta - I_{N \times N}) a(t) - \Theta^T \kappa \rfloor^\beta \\ &\hat{s} = a(t), \end{aligned} \tag{10.19}$$

where $\nu \in R^N$ is the state vector, $\hat{s}(t)$ represents the estimate of the sparse signal s of (10.15), and $\mu > 0$ is a time-constant determined by the physical properties of the implementing system. Note that $\lceil . \rfloor = |.|^\beta sign(.)$ and $a(t) = H_\lambda(\nu)$, where $H_\lambda(.)$ is a continuous soft thresholding function and is defined as

$$H_\lambda(\nu) = max(|\nu| - \lambda, 0) sgn(\nu), \tag{10.20}$$

where $\lambda > 0$ is chosen with respect to the noise and the minimum absolute value of the non-zero terms.

Under Assumption 10.1 the state ν of (10.19) converges in finite time to its equilibrium point ν^*, and $\hat{s}(t)$ in (10.19) converges in finite time to s^* of (10.18).

10.4 Attack Reconstruction When the Number of Potential Attacks is Greater Than the Number of Sensors

The nonlinear CPS in (10.10) is considered when the number of potential attacks is greater than the number of sensors, i.e.,

$$\begin{aligned} \dot{x} &= f(x) + B(x)d(t) \\ y &= C(x) + Dd(t) \qquad where \quad q > p. \end{aligned} \tag{10.21}$$

Assumption 10.2 It is assumed that the attack vector is sparse, meaning that numerous attacks are possible, but the attacks are not coordinated, and only few non-zero attacks happen at the same time, i.e., the index set of non-zero attacks is presented as

$$\begin{aligned} &\Phi_{\Gamma} = \{k_1, k_2, \ldots, k_j\}, \quad j < q \quad where \\ &2j + 1 \leq p. \end{aligned} \tag{10.22}$$

The objective is to reconstruct online the time-varying attack sparse vector based on the sensor measurement in CPS (10.21).

10.4.1 System Transformation

Feeding the sensor measurements under attack, y, of the CPS (10.21) to the input of the low-pass filter that facilitates filtering out the possible measurement noise gives Nateghi et al. (2018b)

$$\dot{z} = \frac{1}{\tau}(-z + C(x) + D(x)d(t)), \tag{10.23}$$

whose output $z \in R^p$, is available. Then, the CPS in (10.21) is rewritten as

$$\begin{aligned} \dot{\xi} &= \eta(\xi) + \Omega d(t) \\ \psi &= C\xi, \end{aligned} \tag{10.24}$$

where $\psi \in R^p$, and

$$\begin{aligned} &\xi = \begin{bmatrix} z \\ x \end{bmatrix}_{(p+n)\times 1} \quad , \quad \eta(\xi) = \begin{bmatrix} -\frac{1}{\tau}I & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} z \\ x \end{bmatrix} + \begin{bmatrix} \frac{1}{\tau}C(x) \\ f(x) \end{bmatrix} \\ &\Omega = \begin{bmatrix} \frac{1}{\tau}B(x) \\ B(x) \end{bmatrix} = \left[\Omega_1, \Omega_2, \ldots, \Omega_q\right]_{(p+n)\times q} \\ &C = \left[C_1, C_2, \ldots, C_{p+n}\right] = \left[I_{p\times p} \quad 0_{p\times n}\right]. \end{aligned} \tag{10.25}$$

Assumption 10.3 The transformed CPS (10.25) is assumed to have a vector relative degree $r=\{r_1, r_2, \dots, r_p\}$, i.e.,

$$\begin{aligned}&\Gamma_{\Omega_j}\Gamma_\eta^{\lambda}\psi_i(\xi)=0 \quad \forall j=1,\dots,q \quad \forall\lambda<r_i-1 \quad \forall i=1,\dots,p\\&\Gamma_{\Omega_j}\Gamma_\eta^{r_i-1}\psi_i(\xi)\neq 0 \quad for \quad at \quad least \quad one \quad 1\leq j\leq q.\end{aligned} \tag{10.26}$$

Assumption 10.4 The distribution $\Gamma = span\{b_1, b_2, \dots, b_q\}$ is involutive, where b_i is the ith column of matrix B in (10.21). This means that no new direction is generated by the Lie bracket of the distribution vector fields. This ensures that the zero dynamics (when exist) can be rewritten independently of the unknown input.

Assumption 10.5 Here it is assumed that there are no zero dynamics in system (10.24), i.e., total relative degree equal to the system's (10.10) order: $n=r_1+r_2+\cdots+r_p$.
Assuming that the Assumptions (10.4) and (10.5) are satisfied, then input–output dynamics of system (10.24) are presented as Fridman et al. (2008)

$$\dot{\Upsilon}_i=\begin{bmatrix}0\;1\;0\dots0\\0\;0\;1\;\dots0\\\vdots\;\vdots\;\vdots\;\dots\vdots\\0\;0\;0\;\;0\;\;0\end{bmatrix}\Upsilon_i+\begin{bmatrix}0\\0\\\vdots\\L_f^{r_i}\psi_i(\xi)\end{bmatrix}+\begin{bmatrix}0\\0\\\vdots\\\sum_{j=1}^{q}L_{\Omega_j}L_f^{r_i-1}\psi_i(\xi)d_i\end{bmatrix}, \tag{10.27}$$

where

$$\Upsilon_i=\begin{bmatrix}\Upsilon_1^i(\xi)\\\Upsilon_2^i(\xi)\\\vdots\\\Upsilon_{r_i}^i(\xi)\end{bmatrix}=\begin{bmatrix}\psi_i(\xi)\\L\psi_i(\xi)\\\vdots\\L_f^{r_i-1}\psi_i(\xi)\end{bmatrix} \quad for \quad i=1,\dots,p, \tag{10.28}$$

where $\psi_i(\xi)$ is the ith entry of vector $\psi(\xi)$. Each of system output ψ_i at its own relative degree r_i, satisfies following equation (Fridman et al. 2008)

$$\dot{\Upsilon}_{r_i}^i(\xi)=L_f^{r_i}\psi_i(\xi)+\sum_{j=1}^{\alpha}L_{\Omega_j}L_f^{r_i-1}\psi_i d_i \quad i=1,\dots,p. \tag{10.29}$$

Therefore, system (10.24) can be rewritten as the following algebraic equation

$$Z_p=F(\xi)d(t), \tag{10.30}$$

where

$$Z_p=\begin{bmatrix}\dot{\Upsilon}_{r_1}^1\\\vdots\\\dot{\Upsilon}_{r_p}^p\end{bmatrix}-\begin{bmatrix}L_f^{r_1}\psi_1(\xi)\\\vdots\\L_f^{r_p}\psi_p(\xi)\end{bmatrix}, \tag{10.31}$$

where $Z_p \in R^p$, $F(\xi) \in R^{p\times q}$, and

$$F(\xi) = \begin{bmatrix} L_{\Omega_1}L_f^{r_1-1}\psi_1 & L_{\Omega_2}L_f^{r_1-1}\psi_1 & \ldots & L_{\Omega_q}L_f^{r_1-1}\psi_1 \\ L_{\Omega_1}L_f^{r_2-1}\psi_2 & L_{\Omega_2}L_f^{r_2-1}\psi_2 & \ldots & L_{\Omega_q}L_f^{r_2-1}\psi_2 \\ \vdots & & & \vdots \\ L_{\Omega_1}L_f^{r_P-1}\psi_P & L_{\Omega_2}L_f^{r_p-1}\psi_p & \ldots & L_{\Omega_q}L_f^{r_P-1}\psi_p \end{bmatrix}. \tag{10.32}$$

Remark 10.2 The derivative $\dot{\Upsilon}^1_{r_1}, \ldots, \dot{\Upsilon}^p_{r_p}$ are computed exactly in finite time using higher-order sliding mode differentiators (Fridman et al. 2008; Levant 2003). The details about the HOSMC differentiation algorithms and their parametric tuning can be found in Fridman et al. (2008), Levant (2003).

10.4.2 Attack Reconstruction

Assumption 10.6 The matrix $F(\xi)$ in (10.30)–(10.32) is assumed to satisfy the RIP condition as in Assumption 10.1.

The attack in (10.30) is reconstructed using the SR Algorithm as

$$\begin{aligned} \mu\dot{\nu}(t) &= -\lceil \nu(t) + (F(\xi)^T F(\xi) - I_{N\times N})a(t) - F(\xi)^T Z_p \rfloor^\beta \\ \hat{d} &= a(t), \end{aligned} \tag{10.33}$$

where $\hat{d}(t)$ represents the estimate of the sparse signal $d(t)$ of (10.30).

Under Assumption 10.6, the $\hat{d}(t)$ in (10.33) converges in finite time to $d(t)$ of (10.30) (Yu et al. 2017).

10.5 Attack Reconstruction When the Number of Sensors is Greater Than the Number of Potential Sensor Attacks

Consider the nonlinear CPS model under the state and sensor attack in (10.10) when the number of sensors is greater than the number of sensor attacks, that is

$$\begin{aligned} \dot{x} &= f(x) + B_1(x)d_x(t) \\ y &= C(x) + D_1 d_y(t) \qquad where \quad p > q - q_1, \end{aligned} \tag{10.34}$$

where $y \in R^p$, $d_x(t) \in R^{q_1}$ and $d_y(t) \in R^{q-q_1}$. Since there are more sensors than potential sensor attacks in CPS (10.34), there exists a nonsingular output transformation $M \in R^{R\times R}$ so that

$$\bar{y} = M^{-1}y = M^{-1}C(x) + M^{-1}D_1 d_y, \tag{10.35}$$

where the matrix M is selected to satisfy the condition

$$M^{-1}D = \begin{bmatrix} 0_3 \\ D_2 \end{bmatrix}, \tag{10.36}$$

where $0_3 \in R^{p_1 \times (q-q_1)}$, $D_2 \in R^{(p-p_1)\times(q-q_1)}$, and $p - p_1 \leq q - q_1$. The transformed sensor measurement vector in (10.35) is partitioned as

$$\bar{y} = \begin{bmatrix} \bar{y}_1 \\ \bar{y}_2 \end{bmatrix}, \tag{10.37}$$

where $\bar{y}_1 \in R_1^p$ and $\bar{y}_2 \in R^{p-p_1}$.

Next, CPS (10.34) is presented in a partitioned format in accordance with (10.37) as

$$\begin{aligned} \dot{x} &= f(x) + B_1(x)d_x(t) \\ \bar{y}_1 &= C_1(x) \\ \bar{y}_2 &= C_2(x) + D_2 d_y(t). \end{aligned} \tag{10.38}$$

$C_1 \in R^{p_1}$ and $C_2 \in R^{p-p_1}$.

Remark 10.3 The virtual measurement $\bar{y}_1$ in (10.38) is not affected by the attack corruption signal and can be classified as a protected measurement.

Assumption 10.7 The number of protected measurements is equal or greater than the number of plant attacks, i.e.,

$$q_1 \leq p_1. \tag{10.39}$$

Remark 10.4 Equation (10.39) gives that the number of unprotected measurements is equal or less than the number of attacks that may corrupt the measurements, i.e.,

$$p - p_1 \leq q - q_1. \tag{10.40}$$

The considered problem is: given the nonlinear CPS dynamics in Eq. (10.38) with virtual protected $\bar{y}_1 \in R_1^p$ and $\bar{y}_2 \in R^{p-p_1}$ unprotected sensors, and attack signals $d_x \in R^{q_1}$ on the plant and $d_y \in R^{q-q_1}$ on the sensors (sensor corruption signals), reconstruct the attack signals. The attack reconstruction is to be accomplished in two steps:

Step 1: The plant state $x(t)$ and the attack $d_x(t)$ vectors are estimated by applying the HOSM observer, described in the next section, with respect to the protected output $\bar{y}_1$ only, so that

$$\hat{x}(t) \to x(t), \quad \hat{d}_x(t) \to d_x(t) \tag{10.41}$$

in finite time, where $\hat{x}(t)$ and $\hat{d}_x(t)$ are the estimation of CPS states and the reconstruction of plant attack, respectively.

Step 2: Given the state $\hat{x}(t)$, which is estimated online, the unprotected sensor attack d_y is then estimated by applying the SR algorithm described in Sect. 10.3.

10.5.1 State Attack Reconstruction

Consider the part of CPS (10.38) associated with the virtual measurements protected from the attacks

$$\begin{aligned} \dot{x} &= f(x) + B_1(x)d_x(t) \\ \bar{y}_1 &= C_1(x). \end{aligned} \tag{10.42}$$

Note that only q_1 out of p_1 virtual protected measurements are employed, and that the other $p_1 - q_1$ virtual protected measurements can be used at the second step of the proposed algorithm. The aforementioned modifications are addressed by defining $\bar{y}_1$ and B_1 in (10.42) as $\bar{y}_1 = [\bar{y}_{11}, \ldots, \bar{y}_{1q_1}]^T$, $B_1 = [b_1, b_2, \ldots, b_{q_1}] \in R^{n\times q_1}$, where $b_i \in R^n, \forall i = 1, 2, \ldots, q_1$ are smooth vector fields defined on an open $\Omega \subset R^n$. The problem is to estimate the states of nonlinear CPS (10.42) with unknown input, and reconstruct the state attack vector $d_x(t)$.

Assume that the CPS in (10.42) has the vector relative degree $r = \{r_1, r_2, \ldots, r_{q_1}\}$ as it is defined in Assumption 10.3.

Assumption 10.8 The matrix

$$L(x) = \begin{bmatrix} L_{b_1}(L_f^{r_1-1}\bar{y}_1) & L_{b_2}(L_f^{r_1-1}\bar{y}_1) & \ldots & L_{b_{q_1}}(L_f^{r_1-1}\bar{y}_1) \\ L_{b_1}(L_f^{r_2-1}\bar{y}_2) & L_{b_2}(L_f^{r_2-1}\bar{y}_2) & \ldots & L_{b_{q_1}}(L_f^{r_2-1}\bar{y}_2) \\ \vdots & & & \vdots \\ L_{b_1}(L_f^{r_{q_1}-1}\bar{y}_{q_1}) & L_{b_2}(L_f^{r_{q_1}-1}\bar{y}_{q_1}) & \ldots & L_{b_{q_1}}(L_f^{r_{q_1}-1}\bar{y}_{q_1}) \end{bmatrix} \tag{10.43}$$

is full rank.

If the CPS in (10.42) satisfies Assumptions (10.4) and (10.8), then the CPS given by Eq. (41) with the involutive distribution $\Gamma = span\{b_1, b_2, \ldots, b_{q_1}\}$ and total relative degree $r = \sum_{i=1}^{q_1} r_i \leq n$ can be rewritten as Fridman et al. (2008)

$$\dot{\delta}_i = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \delta_i + \begin{bmatrix} 0 \\ 0 \\ \vdots \\ L_f^{r_i}\bar{y}_{1_i}(x) \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \sum_{j=1}^{m} L_{b_j} L_f^{r_i-1}\bar{y}_{1_i}(x)d_x(t) \end{bmatrix} \tag{10.44}$$
$$\forall i = 1, \ldots, q_1$$
$$\dot{\gamma} = g(\delta, \gamma),$$

where

$$\delta = \begin{bmatrix} \delta_1 \\ \delta_2 \\ \vdots \\ \delta_{q_1} \end{bmatrix}, \quad \delta_i = \begin{bmatrix} \delta_{i_1} \\ \delta_{i_2} \\ \vdots \\ \delta_{i_{r_1}} \end{bmatrix} = \begin{bmatrix} \eta_{i_1}(x) \\ \eta_{i_2}(x) \\ \vdots \\ \eta_{i_{r_1}}(x) \end{bmatrix} = \begin{bmatrix} \bar{y}_{1i}(x) \\ L_f \bar{y}_{1i}(x) \\ \vdots \\ L_f^{r_i-1} \bar{y}_{1i}(x) \end{bmatrix} \in R^{r_i} \quad \forall i = 1, \ldots, q_1$$

$$\gamma = \begin{bmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_{n-r} \end{bmatrix} = \begin{bmatrix} \eta_{r+1}(x) \\ \eta_{r+2}(x) \\ \vdots \\ \eta_n(x) \end{bmatrix}. \tag{10.45}$$

Assumption 10.9 The norm-bounded solution of the internal dynamics (10.44) $\dot{\gamma} = g(\delta, \gamma)$ is assumed to be locally asymptotically stable (Fridman et al. 2008) as it is mentioned in (A3).

The variables $\eta_{r+1}(x), \eta_{r+2}(x), \ldots, \eta_n(x)$ are defined to satisfy

$$L_{b_j}\eta_i(x) = 0 \quad \forall i = r+1, \ldots, n, \quad \forall j = 1, \ldots, q_1, \tag{10.46}$$

if Assumption 10.4 is satisfied, then it is always possible to find $n - r$ functions $\eta_{r+1}(x), \eta_{r+2}(x), \ldots, \eta_n(x)$ such that

$$\Psi(x) = col\{\eta_{11}(x), \ldots, \eta_{1r_1}(x), \eta_{q_1 1}(x), \ldots, \eta_{q_1 r_{q_1}}(x), \eta_{r+1}(x), \ldots, \eta_n(x)\} \in R^n. \tag{10.47}$$

is a local diffeomorphism in a neighborhood of any point $x \in \bar{\Omega} \subset \Omega \subset R^n$, which means that

$$x = \Psi^{-1}(x)(\delta, \gamma). \tag{10.48}$$

To estimate the derivatives $\delta_{ij}, \forall i = 1, \ldots, q_1, \forall j = 1, \ldots, r_i$ of the outputs y_i in finite time, higher-order sliding mode differentiators (Levant 2003) are used

$$\begin{aligned}
&\dot{z}_0^i = \nu_0^i, \quad \nu_0^i = -\lambda_0^i |z_0^i - y_i(t)|^{(r_i/(r_i+1))} sign(z_0^i - y_i(t)) + z_1^i \\
&\dot{z}_1^i = \nu_1^i, \quad \nu_1^i = -\lambda_1^i |z_1^i - \nu_0^i|^{((r_i-1)/r_i)} sign(z_1^i - \nu_0^i) + z_2^i \\
&\vdots \\
&\dot{z}_{r_i-1}^i = \nu_{r_i-1}^i, \quad \nu_{r_i-1}^i = -\lambda_{r_i-1}^i |z_{r_i-1}^i - \nu_{r_i-2}^i|^{(1/2)} sign(z_{r_i-1}^i - \nu_{r_i-2}^i) + z_{r_i}^i \\
&\dot{z}_{r_i}^i = -\lambda_{r_i}^i sign(z_{r_i}^i - \nu_{r_i-1}^i),
\end{aligned} \tag{10.49}$$

for $i = 1, \ldots, q_1$.

By construction

$$\begin{aligned}
&\hat{\delta}_1^1 = \hat{\eta}_1^1(x) = z_0^1, \quad \dots, \quad \hat{\delta}_{r_1}^1 = \hat{\eta}_{r_1}^1(x) = z_{r_1-1}^1, \quad \hat{\dot{\delta}}_1^1 = \hat{\dot{\eta}}_{r_1}^1(x) = z_{r_1}^1 \\
&\vdots \\
&\hat{\delta}_1^{q_1} = \hat{\eta}_1^{q_1} = z_0^{q_1}, \quad \dots, \quad \hat{\delta}_{r_{q_1}}^{q_1} = \hat{\eta}_{r_{q_1}}^{q_1} = z_{r_{q_1}-1}^{q_1}, \quad \hat{\dot{\delta}}_{r_{q_1}}^{q_1} = \hat{\dot{\eta}}_{r_{q_1}}^{q_1} = z_{r_{q_1}}^1 .
\end{aligned} \tag{10.50}$$

Therefore, the following exact estimates are available in finite time

$$\hat{\delta}_i = \begin{bmatrix} \hat{\delta}_{i1} \\ \hat{\delta}_{i2} \\ \vdots \\ \hat{\delta}_{ir_1} \end{bmatrix} = \begin{bmatrix} \hat{\eta}_{i1}(\hat{x}) \\ \hat{\eta}_{i2}(\hat{x}) \\ \vdots \\ \hat{\eta}_{ir_1}(\hat{x}) \end{bmatrix} \in R^{r_i} \quad \forall i = 1, \dots, q_1 \quad \hat{\delta} = \begin{bmatrix} \hat{\delta}^1 \\ \hat{\delta}^2 \\ \vdots \\ \hat{\delta}^{q_1} \end{bmatrix} \in R^{r_t}. \tag{10.51}$$

Integrating the second equation in (10.44) and replacing δ by $\hat{\delta}$, the internal dynamics is given as

$$\dot{\hat{\gamma}} = g(\hat{\gamma}, \hat{\delta}), \tag{10.52}$$

and with some initial condition from the stability domain of the internal dynamics, a asymptotic estimate $\hat{\gamma}$ can be obtained locally as

$$\hat{\gamma} = \begin{bmatrix} \hat{\gamma}_1 \\ \hat{\gamma}_2 \\ \vdots \\ \hat{\gamma}_{n-r} \end{bmatrix} = \begin{bmatrix} \hat{\eta}_{r+1}(x) \\ \hat{\eta}_{r+2}(x) \\ \vdots \\ \hat{\eta}_n(x) \end{bmatrix}. \tag{10.53}$$

Therefore, the asymptotic estimate for the mapping (10.49) is identified as

$$\Psi(\hat{x}) = col\{\hat{\eta}_{11}(\hat{x}), \dots, \eta_{1r_1}(\hat{x}), \dots, \eta_{q_1 r_{q_1}}(\hat{x}), \hat{\eta}_{r+1}(\hat{x}), \hat{\eta}_n(\hat{x})\}. \tag{10.54}$$

The asymptotic estimate $\hat{x}$ of the state vector x of CPS (10.42) can be easily identified via (10.51) and (10.53) as

$$\hat{x} = \Psi^{-1}(\hat{\delta}, \hat{\gamma}). \tag{10.55}$$

An asymptotic estimate $\hat{d}_x(t)$ of the cyber state attack $d_x(t)$ in (10.42) can be identified as Nateghi et al. (2018a)

$$\hat{d}_x(t) = L^{-1}(\Psi^{-1}(\hat{\delta}, \hat{\gamma})) \left[\begin{bmatrix} \hat{\dot{\delta}}_{1r_1} \\ \hat{\dot{\delta}}_{2r_2} \\ \vdots \\ \hat{\dot{\delta}}_{qr_q} \end{bmatrix} - \begin{bmatrix} L_f^{r_1} y_1(\Psi^{-1}(\hat{\delta}, \hat{\gamma})) \\ L_f^{r_2} y_2(\Psi^{-1}(\hat{\delta}, \hat{\gamma})) \\ \vdots \\ L_f^{r_q} y_q(\Psi^{-1}(\hat{\delta}, \hat{\gamma})) \end{bmatrix} \right], \tag{10.56}$$

where $L^{-1}(\Psi^{-1}(\hat{\delta}, \hat{\gamma})) = \sum_{j=1}^{q} L_{b_j} L_f^{r_i - 1} \bar{y}_{1_i}(x)$.

10.5.2 Sensor Attacks Reconstruction

After the state vector $x(t)$ and the plant attack $d_x(t)$ of CPS (10.34) are reconstructed in (10.55) and (10.56), then the sensor attacks $d_y(t)$ can be reconstructed as the following discussion: Consider the attacked part of system (10.38) as

$$\begin{aligned} \dot{x} &= f(x) + B_1(x)d_x(t) \\ \bar{y}_2 &= C_2(x) + D_2 d_y(t), \end{aligned} \tag{10.57}$$

where $y_2 \in R^{p-q_1}$, $D_2 \in R^{(p-q_1)\times(q-q_1)}$, $d_y(t) \in R^{q-q_1}$.

Two cases that cover all possible situations are considered to reconstruct the sensor attack $d_y(t)$.

Case 1: If the number of sensor attacks and the number of corrupted sensors is the same, i.e., $p - q_1 = q - q_1$, and D_2 is invertible, then using $\hat{x}$ estimated by the SMO in (10.55), there is a unique solution for estimation of sensor attack as Nateghi et al. (2018a)

$$\hat{d}_y(t) = D_2^{-1}(y_2 - C_2(\hat{x})). \tag{10.58}$$

Case 2: If the number of sensor attacks is greater than the number of corrupted sensors, i.e., $p - q_1 < q - q_1$ and the following assumption is verified for sensor attack d_y.

Assumption 10.10 It is assumed that the sensor attack vector $d_y \in R^{q-q_1}$ is sparse, meaning that there is only a small number of non-zero sensor attacks at any point in time.

Assumption 10.11 Matrix D_2 satisfies the RIP condition in Assumption 10.1.

Under Assumptions (10.10) and (10.11), then the attack vector $d(t)$ in (10.57) is reconstructed using the SR algorithm presented in Sect. 10.3 as

$$\hat{d}_y(t) = a(t), \tag{10.59}$$

where $v \in R^q$ is the state vector, $\hat{d}_y(t)$ represents the estimate of the sparse signal $d_y(t)$, and $\mu > 0$ is a time-constant determined by the physical properties of the implementing system. The sensor attack estimation in (10.59) converges in finite time to sensor attack $d_y(t)$ in CPS (10.34) (Yu et al. 2017).

10.6 Case Study: Cyber Attack Reconstruction in the US Western Electricity Coordinating Council Power System

In a real-world electrical power network, only small groups of generator rotor angles and rates are directly measured, and typical attacks aim at injecting disturbance signals that mainly affect the sensor-less generators (Wu et al. 2018). The CPS that motivates the results presented in this section is the US WECC power system (Scholtz 2004; Pasqualetti et al. 2015) under attack with three generators and six buses. The proposed approaches in Sects. 10.4 and 10.5 are applied to the linearized model of the US WECC, to estimate the states and reconstruct the attacks affected the considered WECC.

10.6.1 Mathematical Model of Electrical Power Network

The descriptor (Differential Algebraic Equations (DAE)) swing mathematical model is adopted to describe the electromechanical behavior of the considered electrical power networks (Taha et al. 2016; Yu et al. 2017). The DAE swing mathematical model for a power network stabilized by a linear output feedback controller is given by Yu et al. (2017):

$$\begin{aligned} &\begin{bmatrix} I & 0 & 0 \\ 0 & M_g & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \dot{\delta} \\ \dot{\omega} \\ \dot{\theta} \end{bmatrix} = - \begin{bmatrix} 0 & -I & 0 \\ L^{\theta}_{g,g} & E_g & L^{\theta}_{g,l} \\ L^{\theta}_{l,g} & 0 & L^{\theta}_{l,l} \end{bmatrix} \begin{bmatrix} \delta \\ \omega \\ \theta \end{bmatrix} + \begin{bmatrix} 0 \\ B_{\omega} \\ B_{\theta} \end{bmatrix} d(t) + \begin{bmatrix} 0 \\ P_{\omega} \\ P_{\theta} \end{bmatrix} \\ &y = Cx + Dd(t), \end{aligned} \tag{10.60}$$

where $x = \begin{bmatrix} \delta^T & \omega^T & \theta^T \end{bmatrix} \top^T$ is the vector of states of the system, $\delta \in R^a$, $\omega \in R^a$ and $\theta \in R^b$ are vectors of the phase angles of the source measured in rad, generator speed deviations from synchronous measured in rad/s, and the bus angles measured in rad, respectively. The index a is the number of generators, and b is the number of buses in the electrical system. The vector $y \in R^p$ is the sensor measurement vector, the vector $d \in R^q$ is the attack vector, and $B \in R^{(2a+b)\times q}$, $D \in R^{p\times q}$ are the attack distribution matrices; P_{ω}, P_{θ} are known changes in the mechanical input power to the generators or real power demand at the loads. The matrices E_g, $M_g \in R^{a\times a}$ are diagonal matrices whose non-zero entries consist of the damping coefficients and the normalized inertias of the generators, respectively. Finally, the matrices $L^{\theta}_{g,g}$, $L^{\theta}_{g,l}$, $L^{\theta}_{l,g}$ $L^{\theta}_{l,l}$ form the following symmetric susceptance matrix

$$L^{\theta} = \begin{bmatrix} L^{\theta}_{g,g} & L^{\theta}_{g,l} \\ L^{\theta}_{l,g} & L^{\theta}_{l,l} \end{bmatrix} \tag{10.61}$$

that is the Laplacian associated with the susceptance-weighted graph.

Assumption 10.12 The matrix $L^{\theta}_{l,l}$ is nonsingular (such an assumption usually holds in practical electric power systems).

Note that the following terms that appear in the electric power network model (59)

$$\begin{bmatrix} 0 \\ B_{\omega} \\ B_{\theta} \end{bmatrix} d(t) + \begin{bmatrix} 0 \\ P_{\omega} \\ P_{\theta} \end{bmatrix} \tag{10.62}$$

are due to the output feedback control that processes the output corrupted by the attack signal.

10.6.2 Transformation of DAE to ODE

Assuming (A10) holds, then the variable θ can be expressed as

$$\theta = (R^{\theta}_{l,l})^{-1}(-R^{\theta}_{l,g}\delta + P_{\theta} + B_{\theta}d) \tag{10.63}$$

substituting (10.63) into (10.60) gives

$$\begin{aligned} \begin{bmatrix} \dot{\delta} \\ \dot{\omega} \end{bmatrix} &= \begin{bmatrix} \phi_{\delta}(\delta, \omega) \\ \phi_{\omega}(\delta, \omega) \end{bmatrix} + \begin{bmatrix} 0 \\ P_{\theta\omega} \end{bmatrix} + \begin{bmatrix} 0 \\ B_{\theta\omega} \end{bmatrix} d(t) \\ y &= C \begin{bmatrix} \delta \\ \omega \end{bmatrix} + Dd(t), \end{aligned} \tag{10.64}$$

where

$$\begin{aligned} &\begin{bmatrix} \phi_{\delta}(\delta, \omega) \\ \phi_{\omega}(\delta, \omega) \end{bmatrix} = \begin{bmatrix} 0 & I_{p\times p} \\ M_g^{-1}(-R^{\theta}_{g,g} + R^{\theta}_{g,l}(R^{\theta}_{l,l})^{-1}R^{\theta}_{l,g}) & -M_g^{-1}E_g \end{bmatrix} \begin{bmatrix} \delta \\ \omega \end{bmatrix} \\ &P_{\theta\omega} = M_g^{-1}(P_{\omega} - R^{\theta}_{g,l}(R^{\theta}_{l,l})^{-1}P_{\theta}),\ B_{\theta\omega} = M_g^{-1}(B_{\omega} - R^{\theta}_{g,l}(R^{\theta}_{l,l})^{-1}B_{\theta}). \end{aligned} \tag{10.65}$$

10.6.3 Parameterization of Mathematical Model of Western Electricity Coordinating Council Power System

The electrical power network considered here is a classical nine-bus configuration adopted from Scholtz (2004), Pasqualetti et al. (2015). It consists of 3 generators $\{g_1, g_2, g_3\}$ and 6 load buses $\{b_1, \ldots, b_6\}$. Therefore, we have $\omega = \begin{bmatrix}\omega_1 & \omega_2 & \omega_3\end{bmatrix}\mathrm{T}^T \in R^3$, $\delta = \begin{bmatrix}\delta_1 & \delta_2 & \delta_3\end{bmatrix}\mathrm{T}^T \in R^3$, and $\theta \in R^6$.

The matrices $E_g, M_g \in R^{a\times a}$ are given as

$$M_g = \begin{bmatrix} 0.125 & 0 & 0 \\ 0 & 0.034 & 0 \\ 0 & 0 & 0.016 \end{bmatrix}, E_g = \begin{bmatrix} 0.125 & 0 & 0 \\ 0 & 0.068 & 0 \\ 0 & 0 & 0.048 \end{bmatrix}. \tag{10.66}$$

The symmetric susceptance matrix L^θ including $L^\theta_{g,g} \in R^{3\times3}$, $L^\theta_{g,l} \in R^{3\times6}$, $L^\theta_{l,g} \in R^{6\times3}$, $L^\theta_{l,l} \in R^{6\times6}$ is equal to

$$L^\theta = \begin{bmatrix} 0.058 & 0 & 0 & -0.058 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.063 & 0 & 0 & -0.063 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.059 & 0 & 0 & 0.059 & 0 & 0 & 0 \\ -0.058 & 0 & 0 & 0.0265 & 0 & 0 & -0.085 & -0.092 & 0 \\ 0 & -0.063 & 0 & 0 & 0.296 & 0 & -0.161 & 0 & -0.072 \\ 0 & 0 & -0.059 & 0 & 0 & 0.330 & 0 & -0.170 & -0.101 \\ 0 & 0 & 0 & -0.085 & -0.161 & 0 & 0.246 & 0 & 0 \\ 0 & 0 & 0 & -0.092 & 0 & -0.170 & 0 & 0.262 & 0 \\ 0 & 0 & 0 & 0 & -0.072 & -0.101 & 0 & 0 & 0.173 \end{bmatrix}. \tag{10.67}$$

The inputs P_ω and P_θ are defined as

$$P_\omega = \begin{bmatrix} 0.716 \ 1.62 \ 0.85 \end{bmatrix} \mathsf{T}^T, P_\theta = \begin{bmatrix} 0 \ -1.25 \ 0.94 \ 0 \ -1 \ 0 \end{bmatrix} \mathsf{T}^T . \tag{10.68}$$

10.6.4 Reconstruction of Attacks via Sparse Recovery Algorithm: The Number of Potential Attacks is Greater Than the Number of Sensors

Consider the WECC power system (10.60) under attack signal $d = \begin{bmatrix} d_x^T & d_y^T \end{bmatrix}^T \in R^{18}$ where $d_x \in R^{12}$, and $d_y \in R^6$ are the attacks of the plant and sensors, respectively. The attacks d_x,d_y are further decoupled as follows:

$$d_1 = \begin{bmatrix} d^\delta_{x_{(3\times1)}} \\ d^\omega_{x_{(3\times1)}} \\ d^\theta_{x_{(6\times1)}} \end{bmatrix}, d_2 = \begin{bmatrix} d^\delta_{y_{(3\times1)}} \\ d^\omega_{y_{(3\times1)}} \end{bmatrix}, \tag{10.69}$$

where d_x^δ, d_x^ω, d_x^θ are attacks on δ, ω, θ, and d_y^δ, d_y^ω are attacks on measurements of δ and ω, respectively. It is considered that

$$\begin{aligned}
B_\delta &\in R^{3\times 18} = \begin{bmatrix} I_{3\times 3} \; 0_{3\times 15} \end{bmatrix}\\
B_\omega &\in R^{3\times 18} = \begin{bmatrix} 0_{3\times 3} \; I_{3\times 3} \; 0_{3\times 12} \end{bmatrix}\\
B_\theta &\in R^{6\times 18} = \begin{bmatrix} 0_{6\times 6} \; I_{6\times 6} \; 0_{6\times 6} \end{bmatrix}\\
D_\delta &\in R^{3\times 18} = \begin{bmatrix} 0_{3\times 12} \; I_{3\times 3} \; 0_{3\times 3} \end{bmatrix}\\
D_\omega &\in R^{3\times 18} = \begin{bmatrix} 0_{3\times 15} \; I_{3\times 3} \end{bmatrix}.
\end{aligned} \tag{10.70}$$

The corrupted sensor measurements $y = \begin{bmatrix} \delta \\ \omega \end{bmatrix} \in R^6$ are fed to the low-pass filter (10.23) and the new variable ξ is defined as

$$\xi = \begin{bmatrix} z \\ y \end{bmatrix} \in R^{12}, \tag{10.71}$$

where $z = \begin{bmatrix} z_{1_{3\times 1}} \\ z_{2_{3\times 1}} \end{bmatrix} \in R^6$ is the output of LPF.

Then, the WECC (10.60) with the LPF (10.23)–(10.25) is presented as

$$\begin{aligned}
\dot{\xi} = &\begin{bmatrix} \frac{-1}{\tau} & 0 & \frac{1}{\tau} & 0 \\ 0 & \frac{-1}{\tau} & 0 & \frac{1}{\tau} \\ 0 & 0 & 0 & 1 \\ 0 & 0 & M_g^{-1}(-P^\theta_{g,g} + P^\theta_{g,l}(R^\theta_{l,l})^{-1} R^\theta_{l,g}) & -M_g^{-1}E_g \end{bmatrix} \times \xi + \begin{bmatrix} \frac{1}{\tau} D_\delta \\ \frac{1}{\tau} D_\omega \\ B_\delta \\ B_{\delta\omega} \end{bmatrix} d + \\
&\begin{bmatrix} 0 \\ 0 \\ 0 \\ -M_g^{-1}P^\theta_{g,l} + P^{\theta -1}_{l,l} P_\theta + M_g^{-1}P_\omega) \end{bmatrix}\\
\psi = &\begin{bmatrix} I_{6,6} \; 0_{6,6} \end{bmatrix} \xi.
\end{aligned} \tag{10.72}$$

Considering $\psi = \begin{bmatrix} \psi_1 \; \psi_2 \end{bmatrix}^T$ where $\psi_{1_{(3\times 1)}} = z_{1_{(3\times 1)}}$, $\psi_{2_{(3\times 1)}} = z_{2_{(3\times 1)}}$, then

$$\dot{z}_1 = \frac{1}{\tau}(-z_1 + \delta + d_2^\delta), \dot{z}_2 = \frac{1}{\tau}(-z_2 + \omega + d_2^\omega). \tag{10.73}$$

To verify if the (10.73) satisfies the RIP condition in Assumption 10.1, (10.17), the Eq. (10.73) is rewritten in a format of (10.15) as Nateghi et al. (2018b)

$$\begin{bmatrix} \dot{z}_1 + \frac{1}{\tau} z_1 - \frac{1}{\tau}\delta \\ \dot{z}_2 + \frac{1}{\tau} z_2 - \frac{1}{\tau}\omega \end{bmatrix} = \begin{bmatrix} 0_{3\times 3} & 0_{3\times 3} & 0_{3\times 6} & (\frac{1}{\tau})I_{3\times 3} & 0_{3\times 3} \\ 0_{3\times 3} & 0_{3\times 3} & 0_{3\times 6} & 0_{3\times 3} & (\frac{1}{\tau})I_{3\times 3} \end{bmatrix} \begin{bmatrix} d_1^\delta \\ d_1^\omega \\ d_1^\theta \\ d_2^\delta \\ d_2^\omega \end{bmatrix}. \tag{10.74}$$

Apparently, $F(\xi)$ in (10.74) doesn't satisfy the RIP condition (10.17), therefore, another differentiation of $\dot{z}_1, \dot{z}_2$ is required:

$$\ddot{z}_1 = \frac{1}{\tau}(-\dot{z}_1 + \dot{\delta} + \dot{d}_2^{\delta}), \ddot{z}_2 = \frac{1}{\tau}(-\dot{z}_2 + \dot{\omega} + \dot{d}_2^{\omega}). \tag{10.75}$$

Taking into account the output filter dynamics (10.23), and bearing in mind that

$$\dot{\delta} = \omega + B_{\delta} d = (\tau \dot{z}_2 + z_2 - d_2^{\omega}) + B_{\delta} d \tag{10.76}$$

and

$$\begin{aligned} \dot{\omega} &= \phi_{21}\delta + \phi_{22}\omega + P_{\theta\omega} + B_{\theta\omega} d(t) \\ &= \phi_{21}(\tau \dot{z}_1 + z_1 - d_2^{\delta}) + \phi_{22}(\tau \dot{z}_2 + z_2 - d_2^{\omega}) + P_{\theta\omega} + B_{\theta\omega} d(t), \end{aligned} \tag{10.77}$$

where $B_{\theta\omega} d(t) = M_g^{-1} d_{g,l}^{\omega} - M_g^{-1} p_{g,l}^{\theta} (p_{l,l}^{\theta})^{-1} d_1^{\theta}$
then (10.75) is rewritten as

$$\tilde{Z} = \tilde{F} \tilde{d} \tag{10.78}$$

where

$$\tilde{Z}_m = \begin{bmatrix} \ddot{z}_1 + \frac{1}{\tau}\dot{z}_1 - \dot{z}_2 - \frac{1}{\tau} z_2 \\ \ddot{z}_2 + \frac{1}{\tau}\dot{z}_2 - \phi_{21}\dot{z}_1 - \frac{1}{\tau}\phi_{21} z_1 - \phi_{22}\dot{z}_2 - \frac{1}{\tau}\phi_{22} z_2 - \frac{1}{\tau} P_{\theta\omega} \end{bmatrix} \tag{10.79}$$

$$\tilde{F} = \begin{bmatrix} \frac{1}{\tau} & 0 & 0 & 0 & -\frac{1}{\tau} & \frac{1}{\tau} & 0 \\ 0 & \frac{M_g^{-1}}{\tau} & \frac{M_g^{-1} P_{g,l}^{\theta} (P_{l,l}^{\theta})^{-1}}{\tau} & \frac{-\phi_{21}}{\tau} & \frac{-\phi_{22}}{\tau} & 0 & \frac{1}{\tau} \end{bmatrix} \tag{10.80}$$

$$\tilde{d}_{24\times 1} = \left[(d_1^{\delta})^T \; (d_1^{\omega})^T \; (d_1^{\theta})^T \; (d_2^{\delta})^T \; (d_2^{\omega})^T \; (\dot{d}_2^{\delta})^T \; (\dot{d}_2^{\omega})^T \right]^T . \tag{10.81}$$

Now, $\tilde{F}$ in (10.80) satisfies the RIP condition (10.17), therefore, the SR algorithm can be applied to (10.78).

Remark 10.5 The derivatives $\ddot{z}_1$, $\ddot{z}_2$, $\dot{z}_1$ and $\dot{z}_2$ that appear in the entries of the virtual measurement vector $\tilde{Z}_m$ are obtained using HOSM differentiators (Fridman et al. 2008).

Assumption 10.13 The sensor attack signals d_2^{δ} and d_2^{ω} are assumed to be slow with respect to system (10.17) dynamics. In other words, it is assumed $\dot{d}_s^{\delta} \approx 0$ and $d_s^{\omega} \approx 0$ (Nateghi et al. 2018b).

Assumption 10.14 The attacks are assumed to be not coordinated, and only two out of possible 18 attacks of following attack signal

$$d_{18\times 1} = \left[(d_1^{\delta})^T \ (d_1^{\omega})^T \ (d_1^{\theta})^T \ (d_2^{\delta})^T \ (d_2^{\omega})^T \right]^T , \tag{10.82}$$

are assumed to happen (it is not known which ones), the other 16 unknown attacks are assumed non-existent. These two attacks are recovered using the SR algorithm described in Sect. 3 applied to filtered WECC power system (10.72).

10.6.4.1 Simulation Results

The simulation results have been obtained via MATLAB.

Simulation Experiment 1 *Two constant attacks* $(d_1^{\omega})_2 = -1$ *which is the second entry of* d_1^{ω}*, and* $(d_2^{\omega})_1 = 1$ *affect the filtered WECC power system (10.72) at the time* $t = 0.4$ *s, and* $\tau = 0.01$*. The SR algorithm was used to recover the attacks. The results of the simulations are shown in Fig. 10.1. The simulated two non-zero attacks, which are shown by dash line and dot line, are accurately recovered in finite time, while the estimated values of other zero attacks, which are shown by solid lines, converge to zero in finite time. In Figs. 10.1, 10.2 and 10.3, Attack1 and Attack2 are used to describe the real attack signals and* $d_1 - d_{18}$ *display the reconstructed plant and sensor attacks.*

Simulation Experiment 2 *Two time-varying attacks,* $(d_1^{\omega})_1 = sin(\pi t)$ *and* $(d_1^{\omega})_2 = sin(\pi t)$ *affect the filtered WECC power system (10.60) at the time* $t = 0.4$ *s. The simulated two time-varying non-zero attacks are accurately recovered in finite time, which are illustrated by dash line and dot line, while the estimated values of other 16 zero attacks appear to converge to zero in finite time. The solid lines illustrate them.*

Simulation Experiment 3 *Two non-zero attacks are generated and affected the filtered WECC power system (10.60) at the time* $t = 0.4$ *s, the plant attack is time varying* $(d_1^{\omega})_2 = sin(\pi t)$*, and sensor attack is constant* $(d_2^{\omega})_1 = -1$*. The simulation result in Fig. 10.3 shows 2 non-zero and 16 zero attacks were accurately recovered in finite time.*

The Simulation results in Figs. 10.1, 10.2 and 10.3 show that SR algorithm can reconstruct the time-varying sparse attack signal in finite time.

10.6.5 Reconstruction of Attacks and Estimation of States: The Number of Sensors is Greater Than the Number of Potential Sensor Attacks

In this section, we investigate the WECC power system (10.60) as a nonlinear system when we have more sensors rather than potential sensor attacks, i.e., there are 6 sensor

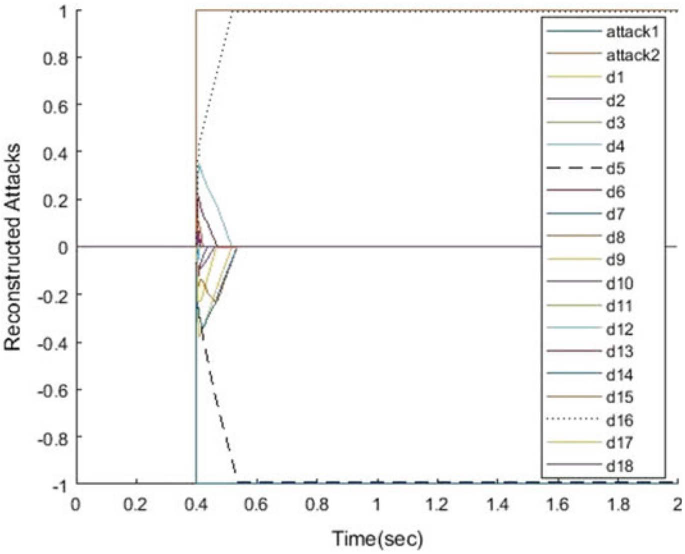

Fig. 10.1 Reconstruction of Two Constant Plant Attack and Sensor Attack in a Sparse Attack Signal, ©2018 IEEE. Reprinted, with permission, from Nateghi et al. (2018b)

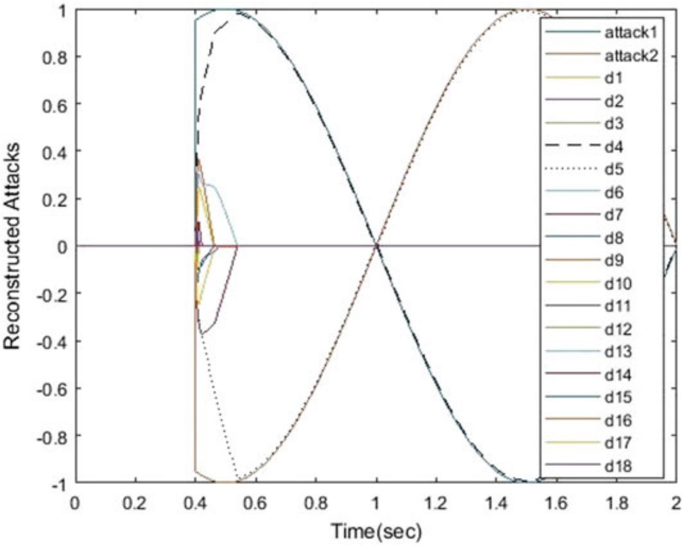

Fig. 10.2 Reconstruction of Two Time Varying Plant Attack in a Sparse Attack Signal, ©2018 IEEE. Reprinted, with permission, from Nateghi et al. (2018b)

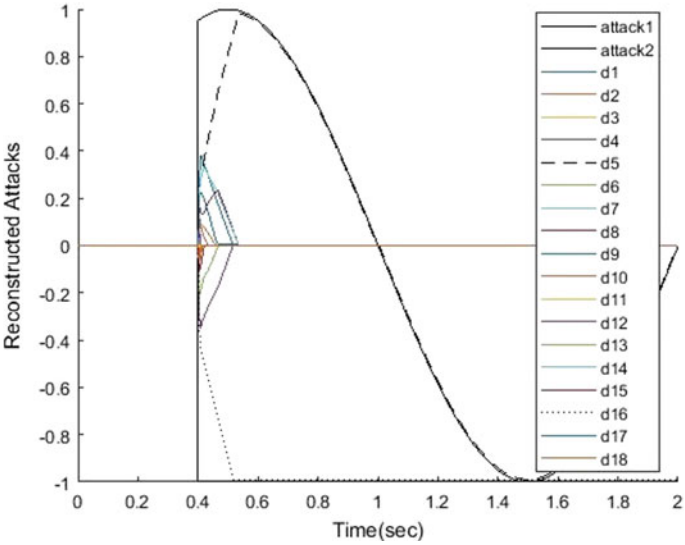

Fig. 10.3 Reconstruction of Time Varying Plant Attack and Constant Sensor Attack in a Sparse Attack Signal, ©2018 IEEE. Reprinted, with permission, from Nateghi et al. (2018b)

measurements and 3 plant attacks. The matrices B and D in (10.60) are defined in such a way that plant attack d_x and sensor attack d_y can be written separately as follows:

$$\begin{bmatrix} I & 0 & 0 \\ 0 & M_g & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \dot{\delta} \\ \dot{\omega} \\ \dot{\theta} \end{bmatrix} = - \begin{bmatrix} 0 & -I & 0 \\ R^{\theta}_{g,g} & E_g & R^{\theta}_{g,l} \\ R^{\theta}_{l,g} & 0 & R^{\theta}_{l,l} \end{bmatrix} \begin{bmatrix} \delta \\ \omega \\ \theta \end{bmatrix} + \begin{bmatrix} 0 \\ I \\ 0 \end{bmatrix} d_x(t) + \begin{bmatrix} 0 \\ P_{\omega} \\ P_{\theta} \end{bmatrix}$$
$$y = \begin{bmatrix} C_{\delta} & 0 \\ 0 & C_{\omega} \end{bmatrix} \begin{bmatrix} \delta \\ \omega \end{bmatrix} + \begin{bmatrix} D_{\delta} \\ D_{\omega} \end{bmatrix} d_y(t), \tag{10.83}$$

where

$$C_{\delta} = I_3 \ , C_{\omega} = I_3 \ , D_{\delta} = 0_{3\times 6} \ , D_{\omega} \in R^{3\times 6} = \begin{bmatrix} 0\ 1\ 2\ 0\ 1\ 1 \\ 1\ 0\ 0\ 2\ 1\ 0 \\ 0\ 0\ 1\ 0\ 1\ 0 \end{bmatrix}. \tag{10.84}$$

The WECC power system (10.84) can be rewritten as

$$\begin{bmatrix} \dot{\delta} \\ \dot{\omega} \end{bmatrix} = \begin{bmatrix} \omega \\ M_g^{-1}(-R^{\theta}_{g,g} + R^{\theta}_{g,l}(R^{\theta}_{l,l})^{-1} R^{\theta}_{l,g})\delta - M_g^{-1} E_g \omega + P_{\theta\omega} \end{bmatrix} + \bar{B} d_x(t)$$
$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} \bar{C}_{\delta} \\ \bar{C}_{\omega} \end{bmatrix} \begin{bmatrix} \delta \\ \omega \end{bmatrix} + \begin{bmatrix} 0 \\ D_{\omega} \end{bmatrix} d_y(t) \tag{10.85}$$

where

$$\begin{aligned} P_{\theta\omega} &= M_g^{-1}(P_\omega - L_{g,l}^\theta (L_{l,l}^\theta)^{-1} P_\theta) \\ B_{\theta\omega} &= M_g^{-1}(B_\omega - L_{g,l}^\theta (L_{l,l}^\theta)^{-1} B_\theta) \\ \bar{C}_\delta &= \begin{bmatrix} I_3 \; 0_3 \end{bmatrix}, \quad \bar{C}_\omega = \begin{bmatrix} 0_3 \; I_3 \end{bmatrix}, \quad \bar{B} = \begin{bmatrix} 0_3 \\ M_g^{-1} \end{bmatrix}. \end{aligned} \tag{10.86}$$

Remark 10.6 It can be verified that D_ω satisfies the RIP condition defined in (10.16).

Suppose that the following three plant attacks (Nateghi et al. 2018a)

$$d_x = \begin{bmatrix} d_{x1} \\ d_{x2} \\ d_{x3} \end{bmatrix} = (t-10) \begin{bmatrix} sin(0.5t) \\ 0.5cos(0.5t) \\ 0.5sin(0.5t) + 0.5cos(0.5t) \end{bmatrix} \tag{10.87}$$

and the time-varying sensor attack

$$d_y = 1(t-10). \begin{bmatrix} 0 \; 0 \; 0 \; 0.5cos(0.5t) \; 0 \; 0 \end{bmatrix} \tag{10.88}$$

affect system (10.83) at $t = 10$ s.

The states $\hat{\delta}$, $\hat{\omega}$ and plant attacks $d_x(t)$ in (10.83) are reconstructed by using HOSM observer. Then, the estimated $\hat{\omega}$ is used in to give

$$y_2 - \hat{\omega} = D_\omega d_y(t). \tag{10.89}$$

The SR algorithm described in Sect. 10.3 can be applied to reconstruct the sparse $d_y(t)$ in WECC power system (10.89), where only one out of six potential attacks $d_{y1} \dots d_{y6}$ is non-zero.

10.6.5.1 Simulation Results

The MATLAB software is used to simulate the system. The simulated plant attacks d_{x1}, d_{x2}, d_{x3} and sensor attack $d_{y1} \dots d_{y6}$ are accurately recovered in finite time and are shown in Figs. 10.4 and 10.5, respectively. Reconstructed attacks are used for cleaning the corrupted plant input and measurements. Figures 10.6 and 10.7 compare the corrupted measurements with the measurements when the system is not under attack, and with the compensated measurements after being attacked.

Therefore, simulation results illustrate that compensated measurements converge to the measurements without attack in finite time. As a result, actual measurements are recovered from corrupted ones in finite time by using the HOSM observer and SR algorithm.

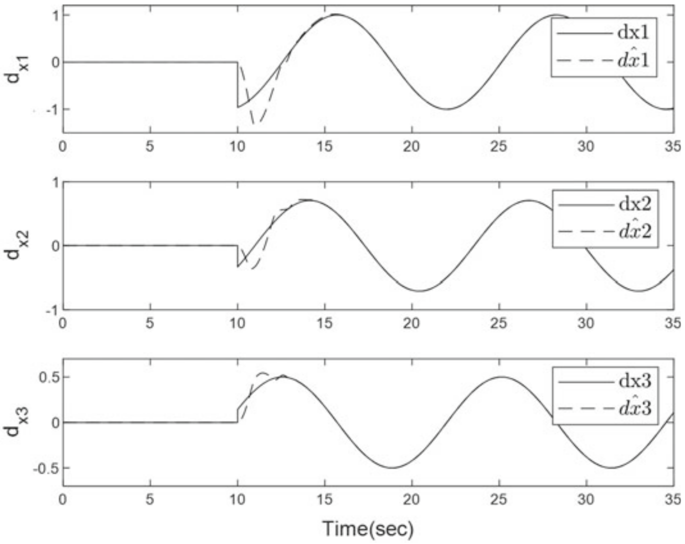

Fig. 10.4 Plant Attack $d_{x_1}, d_{x_2}, d_{x_3}$ Compare with its Reconstruction $\hat{d}_{x_1}, \hat{d}_{x_2}, \hat{d}_{x_3}$, ©2018 IEEE. Reprinted, with permission, from Nateghi et al. (2018a)

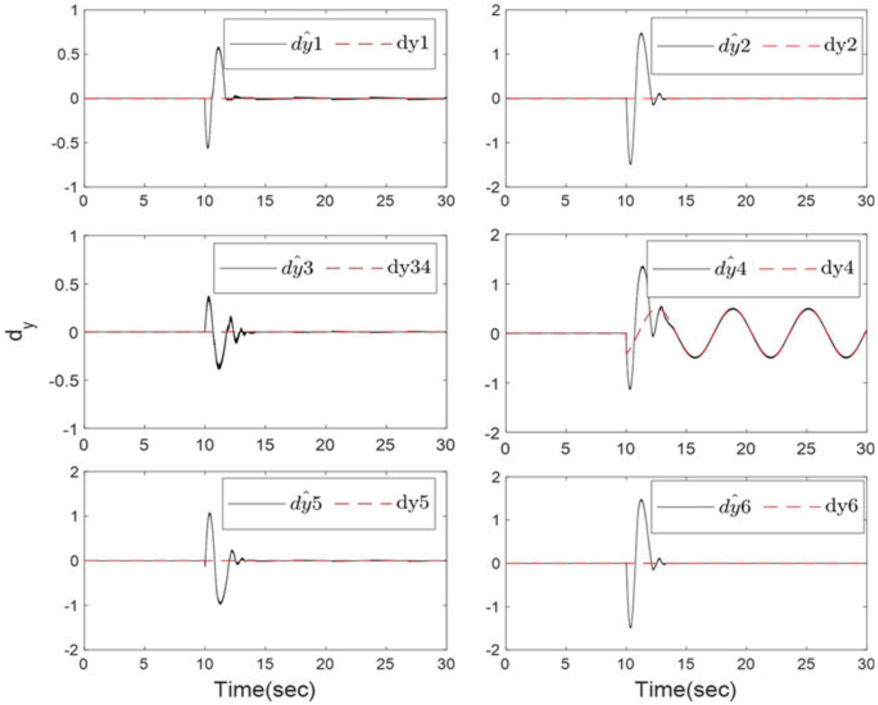

Fig. 10.5 Sensor Attack d_y Reconstruction, ©2018 IEEE. Reprinted, with permission, from Nateghi et al. (2018a)

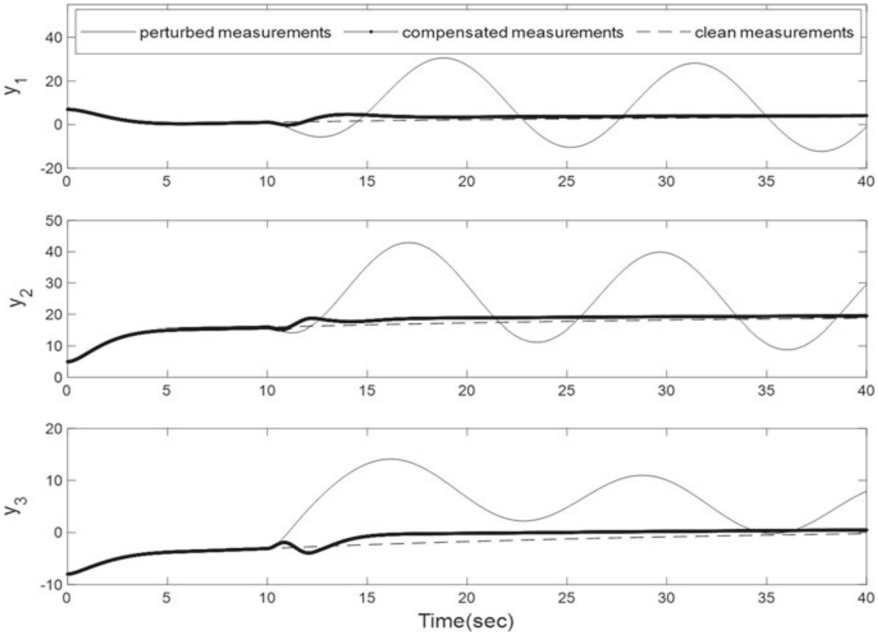

Fig. 10.6 Corrupted WECC Power System Sensor Measurements y_1, y_2, y_3 Compared with the Compensated Measurements and to the Measurements without Attacks, ©2018 IEEE. Reprinted, with permission, from Nateghi et al. (2018a)

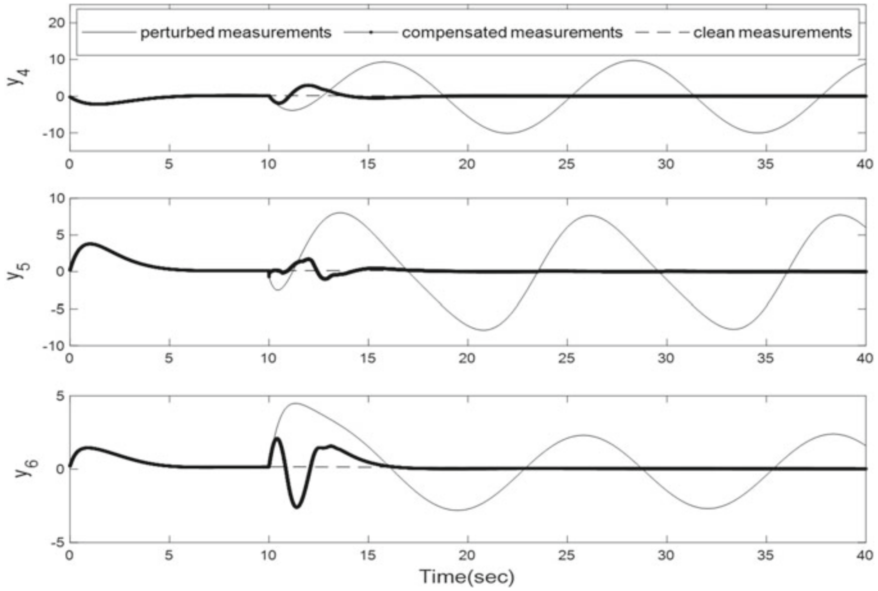

Fig. 10.7 Corrupted WECC Power System Sensor Measurements y_4, y_5, y_6 Compared with the Compensated Measurements and to the Measurements without Attacks (Nateghi et al. 2018a)

10.7 Conclusions

In this chapter, considering the nonlinear cyber-physical systems under deception attacks and sparse sensor attacks, two complimentary cases are investigated. In the first case, when the number of potential attacks is greater than the number of sensor measurements, attacks are reconstructed using higher-order sliding mode differentiation techniques in concert with the SR algorithm, when only several unknown attacks out of all possible attacks are non-zero. In the second case, when the number of sensor measurements is equal or greater than the number of potential sensor attacks, the states of the system and the state attacks are reconstructed online using a HOSM observer. A SR algorithm is used to reconstruct the stealth sensor attacks to the unprotected sensors. The effectiveness of the proposed algorithms to estimate the states and reconstruct the attacks are tested on the US WECC power network system. The simulation results confirm that the attacks degrade the performance of CPS under attack and imply that cleaning the measurements from the reconstructed attacks before using them in the feedback control can elevate CPS performance close to the one without attack.

References

A. Ahmed, K.A. Bakar, M.I. Channa, K. Haseeb, A.W. Khan, A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks. Front. Comput. Sci. **9**(2), 280–296 (2015)

P. Antsaklis, Goals and challenges in cyber-physical systems research editorial of the editor in chief. IEEE Trans. Autom. Control **59**(12), 3117–3119 (2014)

J.-P. Barbot, D. Boutat, T. Floquet, An observation algorithm for nonlinear systems with unknown inputs. Automatica **45**(8), 1970–1974 (2009)

E. Candes, T. Tao, Decoding by linear programming. IEEE Trans. Inf. Theory **51**(12), 4203–4215 (2005)

A.A. Cardenas, S. Amin, S. Sastry, Secure control: towards survivable cyber-physical systems, in *2008 The 28th International Conference on Distributed Computing Systems Workshops* (IEEE, 2008), pp. 495–500

A. Cetinkaya, H. Ishii, T. Hayakawa, Networked control under random and malicious packet losses. IEEE Trans. Autom. Control **62**(5), 2434–2449 (2016)

T.M. Chen, Stuxnet, the real start of cyber warfare?[editor's note]. IEEE Netw. **24**(6), 2–3 (2010)

S. Chen, M. Ma, Z. Luo, An authentication scheme with identity-based cryptography for m2m security in cyber-physical systems. Secur. Commun. Netw. **9**(10), 1146–1157 (2016)

S.M. Dibaji, H. Ishii, R. Tempo, Resilient randomized quantized consensus. IEEE Trans. Autom. Control **63**(8), 2508–2522 (2017)

S.M. Dibaji, M. Pirani, D.B. Flamholz, A.M. Annaswamy, K.H. Johansson, A. Chakrabortty, A systems and control perspective of cps security. Annu. Rev. Control **47**, 394–411 (2019)

W. Diffie, M. Hellman, New directions in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976)

F. Farokhi, I. Shames, N. Batterham, Secure and private control using semi-homomorphic encryption. Control Eng. Pract. **67**, 13–20 (2017)

H. Fawzi, P. Tabuada, S. Diggavi, Secure estimation and control for cyber-physical systems under adversarial attacks. IEEE Trans. Autom. Control **59**(6), 1454–1467 (2014)

L. Fridman, A. Levant, J. Davila, Observation of linear systems with unknown inputs via high-order sliding-modes. Int. J. Syst. Sci. **38**(10), 773–791 (2007)

L. Fridman, Y. Shtessel, C. Edwards, X.-G. Yan, Higher-order sliding-mode observer for state estimation and input reconstruction in nonlinear systems. Int. J. Robust Nonlinear Control IFAC-Affiliated J. **18**(4–5), 399–412 (2008)

K. Hartmann, C. Steup, The vulnerability of uavs to cyber attacks-an approach to the risk assessment, in *5th International Conference on Cyber Conflict (CYCON 2013)* (IEEE, 2013), pp. 1–23

W.P. Heemels, K.H. Johansson, P. Tabuada, An introduction to event-triggered and self-triggered control, in *IEEE 51st Ieee Conference on Decision and Control (CDC)* (IEEE, 2012), pp. 3270–3285

X. Huang, D. Zhai, J. Dong, Adaptive integral sliding-mode control strategy of data-driven cyber-physical systems against a class of actuator attacks. IET Control Theory Appl. **12**(10), 1440–1447 (2018)

A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, G. Lachapelle, Gps vulnerability to spoofing threats and a review of antispoofing techniques. Int. J. Navig. Obs. **2012** (2012)

X. Jin, W.M. Haddad, T. Yucelen, An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems. IEEE Trans. Autom. Control **62**(11), 6058–6064 (2017)

H.J. LeBlanc, H. Zhang, X. Koutsoukos, S. Sundaram, Resilient asymptotic consensus in robust networks. IEEE J. Sel. Areas Commun. **31**(4), 766–781 (2013)

A. Levant, Higher-order sliding modes, differentiation and output-feedback control. Int. J. Control **76**(9–10), 924–941 (2003)

S. Mousavian, J. Valenzuela, J. Wang, A probabilistic risk mitigation model for cyber-attacks to pmu networks. IEEE Trans. Power Syst. **30**(1), 156–165 (2014)

S. Nateghi, Y. Shtessel, Robust stabilization of linear differential inclusion using adaptive sliding mode control. Annu. Am. Control Conf. (ACC) **2018**, 5327–5331 (2018)

S. Nateghi, Y. Shtessel, J.-P. Barbot, C. Edwards, Cyber attack reconstruction of nonlinear systems via higher-order sliding-mode observer and sparse recovery algorithm. IEEE Conf. Decis. Control (CDC) **2018**, 5963–5968 (2018a)

S. Nateghi, Y. Shtessel, J.-P. Barbot, G. Zheng, L. Yu, Cyber-attack reconstruction via sliding mode differentiation and sparse recovery algorithm: electrical power networks application, in *2018 15th International Workshop on Variable Structure Systems (VSS)* (2018b), pp. 285–290

S. Nateghi, Y. Shtessel, R. Rajesh, S.S. Das, Control of nonlinear cyber-physical systems under attack using higher order sliding mode observer, in *2020 IEEE Conference on Control Technology and Applications (CCTA)* (IEEE, 2020a), pp. 1–6

S. Nateghi, Y. Shtessel, C. Edwards, Cyber-attacks and faults reconstruction using finite time convergent observation algorithms: electric power network application. J. Frankl. Inst. **357**(1), 179–205 (2020b)

S. Nateghi, Y. Shtessel, C. Edwards, Resilient control of cyber-physical systems under sensor and actuator attacks driven by adaptive sliding mode observer. Int. J. Robust Nonlinear Control (2021)

E. Nekouei, M. Skoglund, K.H. Johansson, Privacy of information sharing schemes in a cloud-based multi-sensor estimation problem, in *2018 Annual American Control Conference (ACC)*. (IEEE, 2018), pp. 998–1002

F. Pasqualetti, F. Dorfler, F. Bullo, Attack detection and identification in cyber-physical systems. IEEE Trans. Autom. Control **58**(11), 2715–2729 (2013)

F. Pasqualetti, F. Dorfler, F. Bullo, Control-theoretic methods for cyberphysical security: geometric principles for optimal cross-layer resilient control systems. IEEE Control Syst. Mag. **35**(1), 110–127 (2015)

M. Sain, J. Massey, Invertibility of linear time-invariant dynamical systems. IEEE Trans. Autom. Control **14**(2), 141–149 (1969)

E. Scholtz, Observer-based monitors and distributed wave controllers for electromechanical disturbances in power systems, Ph.D. dissertation, Massachusetts Institute of Technology (2004)

Y. Shtessel, C. Edwards, L. Fridman, A. Levant et al., *Sliding Mode Control and Observation*, vol. 10 (Springer, 2014)

J. Slay, M. Miller, Lessons learned from the maroochy water breach, in *International Conference on Critical Infrastructure Protection* (Springer, 2007), pp. 73–82

A.F. Taha, J. Qi, J. Wang, J.H. Panchal, Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs. IEEE Trans. Smart Grid **9**(2), 886–899 (2016)

V.I. Utkin, Manipulator control system, in *Sliding Modes in Control and Optimization* (Springer, 1992), pp. 239–249

C. Wu, Z. Hu, J. Liu, L. Wu, Secure estimation for cyber-physical systems via sliding mode. IEEE Trans. Cybern. **48**(12), 3420–3431 (2018)

L. Yu, G. Zheng, J.-P. Barbot, Dynamical sparse recovery with finite-time convergence. IEEE Trans. Signal Process. **65**(23), 6146–6157 (2017)

Q. Zhu, T. Başar, Robust and resilient control design for cyber-physical systems with an application to power systems, in *2011 50th IEEE Conference on Decision and Control and European Control Conference* (IEEE, 2011), pp. 4066–4071