State Estimation under False Data Injection Attacks: Security Analysis and System Protection ⋆

Liang Hu [a], Zidong Wang [a], Qing-Long Han [b], Xiaohui Liu [a]

[a] *Department of Computer Science, Brunel University London, Uxbridge, Middlesex, UB8 3PH, U.K.*

[b] *School of Software and Electrical Engineering, Swinburne University of Technology, Melbourne, VIC 3122, Australia*

Abstract

The security issue in the state estimation problem is investigated for a networked control system (NCS). The communication channels between the sensors and the remote estimator in the NCS are vulnerable to attacks from malicious adversaries. The false data injection attacks are considered. The aim of this paper to find the so-called *insecurity* conditions under which the estimation system is insecure in the sense that there exist malicious attacks that can bypass the anomaly detector but still lead to unbounded estimation errors. In particular, a *new* necessary and sufficient condition for the insecurity is derived in the case that all communication channels are compromised by the adversary. Moreover, a specific algorithm is proposed for generating attacks with which the estimation system is insecure. Furthermore, for the insecure system, a system protection scheme through which only a few (rather than all) communication channels require protection against false data injection attacks is proposed. A simulation example is utilized to demonstrate the effectiveness of the proposed conditions/algorithms in the secure estimation problem for a flight vehicle.

Key words: False data injection attacks; State estimation; Security analysis; Networked control systems.

1 Introduction

The use of communication networks in networked control systems (NCSs) makes the system vulnerable to cyber-attacks, and the possible malicious attacks on NCSs may cause negative impact on the economy, the environment and the national security. The first-ever cyber-attack in real-world control systems was reported in 2010 [5]. Since then, the cyber security of NCSs has been a hot topic of research that stirs considerable interest. In general, two kinds of attacks have been studied in NCSs [23]. One is the denial-of-service (DoS) attack that violates data *availability* through blocking information flows between different components of NCSs, and the other is the deception attack that violates data *integrity* through modifying data packets. Compared with DoS attacks, deception attacks are more difficult to detect because the adversary could keep the deception attacks stealthy to the anomaly detector in NCSs through deliberately designing the attack sequences.

The deception attacks have been first considered in [13] for the state estimation problems of power systems modelled by *static* system models. The minimum number of comprised sensors that needed to launch deception attacks has been investigated in [22]. As for *dynamic* systems, when the system model is unknown to the adversary, a specific type of deception attack called replay attack has been investigated in [18,24]. In the case that the dynamic model is known to the adversary, another type of deception attack, namely, false data injection attack, has recently been put forward. For deterministic systems without stochastic noises, fundamental issues such as detectability and identifiability for false data injection attacks have been analysed in [6,7,20] and efficient control/estimation algorithms have been developed against false data injection attacks [21]. In [19], a data encryption scheme (together with time-stamp techniques) has been adopted to detect the deception attacks and compensate the side-effects.

As is well known, stochastic models have come to play a more and more important role in characterizing noisy phenomena from real-world systems. Accordingly, it is of practical significance to investigate the cyber security of stochastic dynamic systems. As pointed in [10], the detection task of malicious behaviours for stochastic systems (with external noises) is more difficult than that for deterministic (without stochastic noises) due to the fact that the injected attack by the adversary could be mistaken as a type of noises by the protection devices. Based on the setting that the smart sensors send innovation information (rather than measurements) to the remote estimator, explicit forms of optimal attacks on remote state estimation have been presented in [8], while several attack detection methods for multi-sensor remote estimation have been proposed in [12]. A secure state estimation algorithm has been proposed in [14] for stochastic dynamic systems where a key assumption of sparse observability has been made. While the results reported in [14] are indeed interesting, it is quite possible

⋆ This work was supported in part by the Engineering and Physical Sciences Research Council (EPSRC) of the U.K., the Royal Society of the U.K., and the Alexander von Humboldt Foundation of Germany.

Email addresses: huliang724@gmail.com (Liang Hu), Zidong.Wang@brunel.ac.uk (Zidong Wang), q.han@cqu.edu.au (Qing-Long Han), XiaoHui.Liu@brunel.ac.uk (Xiaohui Liu).

that the adversary attacks at a large number of (or even all) sensors, in which case the system cannot be guaranteed to be "sparsely observable". Motivated by the above observation, we aim to investigate the case where the attacker could inject false data into measurements from any sensor and, accordingly, the results obtained would constitute one of the main contributions of our paper.

In this paper, we focus on the remote state estimation problem for a class of *stochastic* systems under possible false data injection attacks where a χ^2 detector is employed to monitor the state estimates. Note that false data injection attacks have been considered in [11,15–17] for state estimation problems of stochastic systems equipped with χ^2 detectors. In particular, an approximation method has been proposed in [16,17] to analyse the cybersecurity of the system by calculating the estimation error bound caused by the malicious attacks, and some *insecurity* conditions have been derived in [11, 15] to determine whether or not there exist malicious attacks which can cause unbounded estimation error for the state estimation system. Nevertheless, a thorough investigation reveals that 1) there is still room to improve the existing insecurity conditions; and 2) there is also an engineering need to develop a system protection scheme by using only necessary number of communication channels requiring protection against cyber-attacks.

In this paper, we aim to propose new insecurity conditions for the state estimation problem under false data injection attacks. Specifically, in the case when all communication channels are compromised by the adversary, we propose a *new* necessary and sufficient condition under which the system is insecure in the sense that the estimation error caused by attacks is unbounded. Such a new condition is shown to be concise that simplifies the existing results. In the case when only parts of the communication channels are compromised by the adversary, a sufficient condition is proposed as well. Furthermore, we propose a criterion which determines a sufficient number of communication channels that require protection. According to the criterion, only necessary number of (rather than all) communication channels need to be protected in order to make the overall system secure against the attacks.

The contributions of the paper are summarized as follows: *1) new security criteria are proposed for state estimation systems under false data injection attacks and, in the case that all communication channels are compromised by the adversary, our criteria are shown to be necessary and sufficient that simplify the existing ones; 2) an effective protection scheme is proposed for the system which is insecure under false data injection attacks; and 3) the developed criteria are applied to security analysis and system protection in the state estimation system of a flight vehicle.*

Notation: $\mathbb{N}$, $\mathbb{R}$ and $\mathbb{C}$ denote, respectively, the set of non-negative integers, the set of all real numbers, and the set of all complex numbers. $\{x(k)\}$ denotes an infinite sequence $x(1), x(2), \cdots, x(k), \cdots$. $\mathbb{R}^{n\times m}$ ($\mathbb{C}^{n\times m}$) denotes the set of all $n \times m$ real (complex) matrices, and $\mathbb{R}^n$ denotes the n dimensional Euclidean space. For $\alpha \in \mathbb{C}$, $\mathrm{Re}(\alpha)$ and $|\alpha|$ denote its real part and its modulus, respectively. For $a \in \mathbb{R}^n$, $\|a\|$ denotes its l_2 norm. For a matrix $P \in \mathbb{R}^{n\times m}$, P^T, P^{-1}, $\mathrm{Tr}\{P\}$ and $\mathrm{Rk}\{P\}$ represent its transpose, inverse, trace, and rank, respectively. For square matrix A, $\det(A)$ stands for the determinant of A, and $\rho(A)$ stands for the spectral radius of A. $\mathrm{diag}\{\cdots\}$ and I denote a block-diagonal matrix and identity matrix of compatible dimension, respectively, and I_m (0_m) denotes the $m \times m$-dimensional identity (zeros) matrix. I_m^s denotes the s-th column of $m \times m$-dimensional identity matrix I_m, e.g, $I_m^s = [\underbrace{0, \ldots, 0}_{s-1}, 1, \underbrace{0, \ldots, 0}_{m}]^T$.

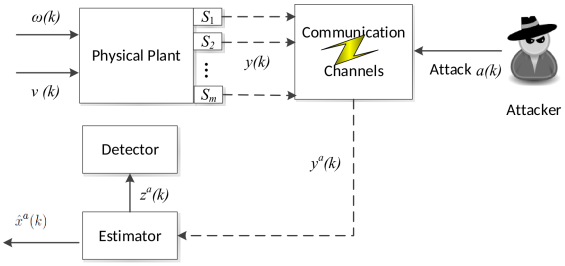


Fig. 1. Diagram of state estimation under cyber-attacks

2 Problem formulation

In this section, we describe the model of false data injection attack and analyze how the injected attacks affect the estimation system. The structure of the state estimation system under cyber-attacks is shown in Fig. 1. For presentation convenience, we first introduce the estimation system without cyber-attacks (i.e., $y^a(k) = y(k)$ in Fig. 1).

2.1 State estimation without cyber-attacks

Let the physical plant be given by:

$$\mathcal{P}: \begin{cases} x(k+1) = Ax(k) + \omega(k) \\ y(k) = Cx(k) + \nu(k) \end{cases} \tag{1}$$

where $x(k) \in \mathbb{R}^n$, $y(k) = [y_1(k), \ldots, y_m(k)]^T \in \mathbb{R}^m$ are the system state and measurement output, respectively, and $y_i(k)$ is the output of the ith sensor (labelled as S_i in Fig. 1) at time instant k. The initial state $x(0)$ has mean $\bar{x}(0)$ and covariance $\Sigma(0)$, the process noise $\omega(k) \in \mathbb{R}^n$ and the measurement noise $\nu(k) \in \mathbb{R}^m$ are assumed to be mutually uncorrelated zero-mean random signals with known covariance matrices W and R, respectively. The process noise $\omega(k)$ represents the external disturbance on dynamic systems and the measurement noise $\nu(k)$ characterises the error of sensor and/or measurement process, respectively.

The following time-invariant state estimator is proposed:

$$\mathcal{E}: \begin{cases} \hat{x}(k+1) = A\hat{x}(k) + Kz(k+1) \\ z(k+1) = y(k+1) - CA\hat{x}(k) \end{cases} \tag{2}$$

where $\hat{x}(k+1)$ and $z(k+1)$ are the state estimate and the estimation residual at time instant $k+1$, respectively.

The following two assumptions are made on the physical system and the estimator:

Assumption 1: For the system (1), the matrix pair (A, C) is observable.

Assumption 2: The estimator is stable by choosing proper estimator gain. In addition, the estimator has already converged to its steady state before time instant 0.

Defining the estimation error $\tilde{x}(k+1) \triangleq x(k+1)-\hat{x}(k+1)$, the dynamics of the estimation error follows from (1) and (2) as follows:

$$\tilde{x}(k+1) = (I-KC)(A\tilde{x}(k)+\omega(k)) - K\nu(k+1). \quad (3)$$

It is well known that the estimator is stable if and only if the matrix $(I-KC)A$ is stable [9]. In this paper, it is assumed that the estimator is stable by choosing appropriate estimator gain K.

Failure detectors are often used to detect abnormal operations. In this paper, we assume that a χ^2 failure detector is deployed. At each time instant k, the χ^2 failure detector first computes the value $g(k) = z^T(k)(C\Sigma C^T + R)^{-1}z(k)$ where Σ is the steady estimation error covariance, and then compares $g(k)$ with a prescribed threshold α. If $g(k) > \alpha$, then an alarm will be triggered. When the system operates normally (i.e. without attacks), $g(k)$ satisfies a χ^2 distribution implying low probability of a large $g(k)$ [1].

2.2 False data injection attack

Before introducing the model of false data injection attack, let us first present two assumptions on the cyber attacks over the communication channels.

Assumption 3: The adversary has perfect knowledge about the system model, that is, the values of all the matrices A, C, K, W and R described in the previous subsection are known by the attacker;

Assumption 4: The attacker has the ability to inject false data over the communication channels between the sensors and the estimator.

Under false data injection attacks, the measurement output received by the estimator is given as follows:

$$y^a(k) = Cx(k)+a(k)+\nu(k) = Cx(k)+B_a a^0(k)+\nu(k) \quad (4)$$

where $a(k) \in \mathbb{R}^m$ represents the false data injected by the attacker at time instant k. The attack vector is described by $a(k) = B_a a^0(k)$ where the injection matrix $B_a = \text{diag}\{\gamma_1, \ldots, \gamma_m\}$. Here, $\gamma_i = 1$ if the attacker is able to inject false data into the ith communication channel, otherwise $\gamma_i = 0$. The matrix B_a reflects which communication channels can be compromised by the attacker. Specifically, $B_a = 0$ means that no attacks can be injected into any communication channel, and $B_a = I_m$ implies that the attacker has the ability to inject attacks into all communication channels.

With the compromised measurement $y^a(k)$, based on the estimator $\mathcal{E}$ in (2), the dynamics of state estimation can be derived as follows:

$$\begin{aligned} \hat{x}^a(k+1) &= A\hat{x}^a(k) + Kz^a(k+1) \\ z^a(k+1) &= y^a(k+1) - CA\hat{x}^a(k) \end{aligned} \quad (5)$$

where $\hat{x}^a(k+1)$ and $z^a(k+1)$ are the state estimation and the estimation residual of system (1) at time $k+1$ using the compromised measurement (4), respectively. Without loss of generality, we assume that the attack begins at time instant 1 and $\hat{x}^a(0) = \hat{x}(0)$.

To take into account the effect of false data injection attacks on the state estimation of system (1), we define the difference between the state estimates and estimation residual of system (1) (without attacks) and system (4) (with attacks) as

$$\Delta\hat{x}(k+1) \triangleq \hat{x}^a(k+1)-\hat{x}(k+1), \Delta z(k+1) \triangleq z^a(k+1)-z(k+1).$$

For convenience, we call $\Delta\hat{x}(k+1)$ and $\Delta z(k+1)$ as the state estimation difference and the estimation residual difference, respectively. The dynamics of $\Delta z(k+1)$ and $\Delta\hat{x}(k+1)$ can be derived from (2) and (5) as follows:

$$\Delta z(k+1) = -CA\Delta\hat{x}(k) + a(k+1), \quad (6)$$

$$\begin{aligned} \Delta\hat{x}(k+1) &= A\Delta\hat{x}(k) + K\Delta z(k+1) \\ &= (I-KC)A\Delta\hat{x}(k) + Ka(k+1) \end{aligned} \quad (7)$$

where $\Delta\hat{x}(0) = \hat{x}^a(0) - \hat{x}(0) = 0$.

In the considered attack model, the purpose of the attacker is to launch a "special" data injection sequence under which the state estimation difference $\Delta\hat{x}(k)$ will diverge to ∞ without any alarm triggered by the χ^2 detector. In other words, the attacker aims to inject false data which would largely degrade the estimation performance without being detected by the detector.

It is known from the triangular inequality $\|z^a(k)\| \leq \|z(k)\| + \|\Delta z(k)\|$ that, if $\|\Delta z(k)\|$ is small, then the χ^2 detector cannot distinguish between $z^a(k)$ and $z(k)$ with high probability. As such, to make the attack sequence stealthy, the attacker launching the false data injection attack should avoid causing a large change in estimation residual difference $\Delta z(k)$ [15], which means that the inequality $\|\Delta z(k)\| \leq M$ should hold all the time, where M represents the tolerant level of the χ^2 detector. Obviously, a smaller value of M would result in a higher probability for the corresponding attack to be undetected. We assume that M is predetermined by the attacker. On the other hand, the attacker should design the attack sequence deliberately such that the sequence $\{\Delta\hat{x}(k)\}$ becomes unbounded, i.e, $\lim_{k\to\infty} \Delta\hat{x}(k) = \infty$.

Throughout the paper, the definition on system security is given as follows.

Definition 1 *The system $\mathcal{P}$ in (1) with estimator $\mathcal{E}$ in (2) is called insecure if there exists at least one attack sequence $\{a(k)\}$ such that the following two conditions are satisfied simultaneously:*

1) for the state estimation difference $\Delta\hat{x}(k)$,

$$\lim_{k\to\infty} \|\Delta\hat{x}(k)\| \to \infty; \quad (8)$$

2) for the estimation residual difference $\Delta z(k)$,

$$\|\Delta z(k)\| \leq M, \quad (9)$$

where M is a prescribed small positive constant scalar.

In the case that (8)-(9) do not hold simultaneously under false data injection attacks (4), the system $\mathcal{P}$ in (1) with estimator $\mathcal{E}$ in (2) is called secure under false data injection attacks (4).

The aim of the addressed system security problem is to analyze under what conditions there exists an attack sequence that is undetectable by the fault detector but drives the bias in state estimation to infinity.

3 Security analysis

In this section, we investigate the security of system $\mathcal{P}$ in (1) with estimator $\mathcal{E}$ in (2) in the following two cases: 1) the attacker is able to inject attacks into all communication channels, *i.e.*, $B_a = I_m$; and 2) the attacker can inject attacks into only part of the communication channels, *i.e.*, $B_a \neq I_m$.

Assume that the system matrix A in (1) has p independent eigenvectors and its Jordan form J is given by

$$J = P^{-1}AP \tag{10}$$

where

$$J = \begin{bmatrix} J_1 & 0 & 0 & \dots & 0 \\ 0 & J_2 & 0 & \dots & 0 \\ 0 & 0 & J_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & J_p \end{bmatrix}, \quad J_i = \begin{bmatrix} \lambda_i & 1 & & & \\ & \lambda_i & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & & & & \lambda_i \end{bmatrix},$$

the Jordan block $J_i \in \mathbb{C}^{n_i \times n_i}$ $(i = 1, \dots, p)$ with $|\lambda_1| \geq |\lambda_2| \geq \cdots \geq |\lambda_p|$ and $\sum_{i=1}^{i=p} n_i = n$. Denote $P = \begin{bmatrix} P_1, \dots, P_p \end{bmatrix}$ and $Q = P^{-1} = \begin{bmatrix} Q_1^T, \dots, Q_p^T \end{bmatrix}^T$, where $P_i \in \mathbb{C}^{n \times n_i}$ and $Q_i \in \mathbb{C}^{n_i \times n}$.

If $\rho(A) \geq 1$, there exists a positive integer l satisfying $1 \leq l \leq p$ such that the inequality $|\lambda_1| \geq \cdots \geq |\lambda_l| \geq 1 > |\lambda_{l+1}| \geq \cdots \geq |\lambda_p|$ is true. Furthermore, defining $\bar{l} = \sum_{i=1}^{l} n_i$, we have

$$A = PJQ = \left[\begin{array}{c:c} P_o & P_c \end{array}\right] \left[\begin{array}{c:c} \Lambda_1 & 0 \\ \hdashline 0 & \Lambda_2 \end{array}\right] \left[\begin{array}{c} Q_o \\ \hdashline Q_c \end{array}\right], \tag{11}$$

where block matrices $\Lambda_1 = \mathrm{diag}\{J_1, \dots, J_l\} \in \mathbb{C}^{\bar{l} \times \bar{l}}$, $\Lambda_2 = \mathrm{diag}\{J_{l+1}, \dots, J_p\} \in \mathbb{C}^{(n-\bar{l}) \times (n-\bar{l})}$, $P_o = \begin{bmatrix} P_1, \dots, P_l \end{bmatrix}, P_c = \begin{bmatrix} P_{l+1}, \dots, P_p \end{bmatrix}, Q_o = \begin{bmatrix} Q_1^T, \dots, Q_l^T \end{bmatrix}^T$ and $Q_c = \begin{bmatrix} Q_{l+1}^T, \dots, Q_p^T \end{bmatrix}^T$ are of appropriate dimensions.

3.1 Case 1: $B_a = I_m$

To introduce our main results, we need the following lemmas.

Lemma 2 *[3] For two matrices $M, N \in \mathbb{C}^{n \times n}$, matrices MN and NM have the same non-zero eigenvalues (counting multiplicity).*

Lemma 3 *For the system (1) with estimator (2), if $\rho(A) \geq 1$, the following matrix equation*

$$P_c X = K \tag{12}$$

has no solution, where matrix K is the estimator gain of state estimator (2) and matrix P_c is given in (11).

Proof. It is known from Lemma 2 that the matrices $(I - KC)A$ and $A(I - KC)$ have the same eigenvalues. Then, it follows from $\rho((I - KC)A) < 1$ that the inequality $\rho(A(I - KC)) < 1$ holds.

Let us prove the lemma by contradiction. Suppose that there exists a matrix solution $\tilde{X}$ to equation (12). Then we have

$$A(I - KC) = \left[\begin{array}{c:c} P_o & P_c \end{array}\right] \left[\begin{array}{c:c} \Lambda_1 & 0 \\ \hdashline 0 & \Lambda_2 \end{array}\right] \left[\begin{array}{c} Q_o \\ \hdashline Q_c \end{array}\right] (I - P_c \tilde{X} C),$$

and it follows from $Q_o P_c = 0$ and $Q_c P_c = I$ that

$$A(I - KC) = \left[\begin{array}{c:c} P_o & P_c \end{array}\right] \left[\begin{array}{c:c} \Lambda_1 & 0 \\ \hdashline 0 & \Lambda_2 \end{array}\right] \left[\begin{array}{c} Q_o \\ \hdashline Q_c - \tilde{X} C \end{array}\right].$$

Accordingly, the characteristic polynomial of matrix $A(I - KC)$, denoted by $\det(\lambda I - A(I - KC))$, can be given as follows:

$$\begin{aligned} &\det(\lambda I - A(I - KC)) \\ =&\det\left(P \lambda I \left[\begin{array}{c} Q_o \\ \hdashline Q_c \end{array}\right] - P \left[\begin{array}{c:c} \Lambda_1 & 0 \\ \hdashline 0 & \Lambda_2 \end{array}\right] \left[\begin{array}{c} Q_o \\ \hdashline Q_c - \tilde{X} C \end{array}\right] \right) \\ =&\det\left(\left[\begin{array}{c:c} P_o & P_c \end{array}\right] \left[\begin{array}{c} (\lambda I - \Lambda_1) Q_o \\ \hdashline (\lambda I - \Lambda_2) Q_c + \Lambda_2 \tilde{X} C \end{array}\right] \right) \\ =&\det(P) \det\left(\left[\begin{array}{c} (\lambda I - \Lambda_1) Q_o \\ \hdashline (\lambda I - \Lambda_2) Q_c + \Lambda_2 \tilde{X} C \end{array}\right] \right). \end{aligned}$$

Setting $\lambda = \lambda_i$ $(i \in \{1, \dots, l\})$, one can see that the last row of matrix $\lambda I - J_i$ is a zero row, which implies that there is at least a zero row in the sub-matrix $(\lambda I - \Lambda_1) Q_o$ and hence $\det(\lambda I - A(I - KC)) = 0$. In other words, we can conclude that λ_i $(i = 1, \dots, l)$ is the eigenvalue of matrix $A(I - KC)$. Noting that $|\lambda_i| \geq 1$ $(i = 1, \dots, l)$, this conclusion contradicts the inequality $\rho(A(I - KC)) < 1$. As a result, there is no solution to the matrix equation (12) and the proof is complete.

Define matrix $E = P^{-1}K$ and let $E_{s,t}$ represent the element of matrix E in the sth row and tth column. From Lemma 3, the following lemma can be easily obtained.

Lemma 4 *For the system (1) with estimator (2), let $\rho(A) \geq 1$, then, there exists at least one non-zero component in matrix E, that is, there exist integers $s \in \{1, \dots, \bar{l}\}$ and $t \in \{1, \dots, m\}$ with $\bar{l} \triangleq \sum_{i=1}^{l} n_i$ such that $E_{s,t} \neq 0$.*

Proof. Let us prove the lemma by contradiction. Assume that $E_{s,t} = 0$, $\forall s \in \{1, \dots, \bar{l}\}$, $\forall t \in \{1, \dots, m\}$. That is, $E = \left[\begin{array}{c} 0 \\ \hdashline \bar{E} \end{array}\right]$ where $\bar{E} \in \mathbb{C}^{(n-\bar{l}) \times m}$ is the sub-matrix forming by the last $n - \bar{l}$ rows of E. Then, the equation $K = P\bar{E}$ can be rewritten as follows:

$$K = PE = \left[\begin{array}{c:c} P_o & P_c \end{array}\right] \left[\begin{array}{c} 0 \\ \hdashline \bar{E} \end{array}\right] = P_c \bar{E}.$$

The equation implies that $\bar{E}$ is the solution of equation (12), which contradicts the statement in Lemma 3 that equation (12) has no solution. The proof is complete.

Before we present the necessary and sufficient condition under which the system (1) with estimator (2) is *insecure*, a procedure for generating a certain sequence of attacks is outlined in Algorithm 1.

Algorithm 1 The algorithm for generating attacks

Initialize:
Decompose matrix A in (1) as the Jordan normal form (10), choose arbitrarily a scalar $\sigma \in (0,1)$ and the positive scalar M;
Determine the integers t, r and q via Lemma 4, (17) and (18), respectively;
Set $\bar{t}_r(0) = 0$;
while $k \geq 0$ **do**
  if $\mathrm{Re}\{\lambda_q \bar{t}_r(k)\} \geq 0$ **then**
    Set $\sigma(k+1) = \sigma$;
    Set attack $a(k+1) = CA\Delta\hat{x}(k) + \sigma(k+1)MI_m^t$;
  else
    Set $\sigma(k+1) = -\sigma$;
    Set attack $a(k+1) = CA\Delta\hat{x}(k) + \sigma(k+1)MI_m^t$;
  end if
  Calculate $\Delta\hat{x}(k+1)$ according to (7);
  Calculate $\bar{t}_r(k+1)$ according to (20);
  $k = k+1$;
end while

Theorem 5 *Suppose that the attacker is able to attack all communication channels, that is, $B_a = I_m$. The system (1) with state estimator (2) is insecure if and only if $\rho(A) \geq 1$.*

Proof. (**Sufficiency**) We start by proving that, if $\rho(A) \geq 1$ in the system (1), then the state estimator (2) is *insecure*. According to Definition 1, we need to prove that there exists at least one attack sequence satisfying both (8) and (9) if $\rho(A) \geq 1$. In the following, we prove that (8) and (9) are true under the attacks generated by Algorithm 1.

According to Algorithm 1, it is known that

$$a(k+1) = CA\Delta\hat{x}(k) + \sigma(k+1)MI_m^t \tag{13}$$

where $\sigma(k+1)$ takes value on either σ or $-\sigma$ with $\sigma \in (0,1)$. It follows from (6) and (13) that

$$\Delta z(k+1) = \sigma(k+1)MI_m^t, \tag{14}$$

from which we can easily see that $\|\Delta z(k+1)\| = \sigma M < M$, and this implies that condition (9) is satisfied.

To show that the condition (8) is satisfied, we define vector $t(k) = Q\Delta\hat{x}(k)$ where $t(k) = [t_1^T(k), \ldots, t_p^T(k)]^T$ with $t_i(k) \in \mathbb{C}^{n_i}$ ($i \in \{1, 2, \ldots, p\}$). Based on (7), (11) and Lemma 4, the dynamics of $t(k)$ is derived as follows:

$$t(k+1) = Jt(k) + QK\Delta z(k+1) = Jt(k) + E\Delta z(k+1). \tag{15}$$

Substituting (14) into (15) yields

$$t(k+1) = Jt(k) + \sigma(k+1)MEI_m^t.$$

Define

$$\bar{t}(k) = \left[t_1^T(k), \ldots, t_l^T(k)\right]^T \text{ and } \underline{t}(k) = \left[t_{l+1}^T(k), \ldots, t_p^T(k)\right]^T.$$

Noting that $J = \left[\begin{array}{c:c} \Lambda_1 & 0 \\ \hdashline 0 & \Lambda_2 \end{array}\right]$, one has

$$\bar{t}(k+1) = \Lambda_1 \bar{t}(k) + \sigma(k+1)Md, \tag{16}$$

where $d = \left[I_{\bar{l}}, 0_{\bar{l}\times(n-\bar{l})}\right] EI_m^t$, *i.e.*, vector d is formed by the first $\bar{l}$ elements of the tth column of matrix E. From Lemma 4, it is known that $d \neq 0$.

Define $d = \left[d_1, \ldots, d_{\bar{l}}\right]^T$ and

$$r = \underset{1 \leq j \leq \bar{l}}{\mathrm{argmax}} \ (d_j \neq 0), \tag{17}$$

that is, d_r is the non-zero element of vector d with the maximal index. Since $1 \leq r \leq \bar{l}$ and $\sum_{i=1}^{p} n_i = \bar{l}$, there exists an integer q ($1 \leq q \leq p$) such that

$$\sum_{i=1}^{q} n_i - n_q < r \leq \sum_{i=1}^{q} n_i. \tag{18}$$

It follows from (16) that

$$\begin{bmatrix} \bar{t}_r(\cdot) \\ \bar{t}_{r+1}(\cdot) \\ \vdots \\ \bar{t}_{n_q}(\cdot) \end{bmatrix} = \begin{bmatrix} \lambda_q & 1 & & \\ & \lambda_q & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_q \end{bmatrix} \begin{bmatrix} \bar{t}_r(k) \\ \bar{t}_{r+1}(k) \\ \vdots \\ \bar{t}_{n_q}(k) \end{bmatrix} + \sigma(\cdot)M \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \tag{19}$$

where $\cdot$ is short for time instant $k+1$, $\bar{t}_j(k)$ is the jth element of vector $\bar{t}(k)$, $j \in \{r, r+1, \ldots, n_q\}$.

Noting the initial condition $\bar{t}_{j+1}(0) = 0$, it can be easily derived from (19) that $\bar{t}_{j+1}(k) = 0$, $j \in \{r, r+1, \ldots, n_q - 1\}$ and

$$\bar{t}_r(k+1) = \lambda_q \bar{t}_r(k) + \sigma(k+1)M, \tag{20}$$

and therefore

$$\begin{aligned} |\bar{t}_r(k+1)|^2 =& |\lambda_q|^2 |\bar{t}_r(k)|^2 + \sigma^2(k+1)M^2 \\ &+ 2\sigma(k+1)M\mathrm{Re}\{\lambda_q \bar{t}_r(k)\} \end{aligned} \tag{21}$$

According to Algorithm 1, it is known that $\sigma(k+1)\mathrm{Re}\{\lambda_q \bar{t}_i(k)\} \geq 0$ and $\sigma^2(k+1) = \sigma^2$. Furthermore, noticing that $|\lambda_q| \geq 1$, we have

$$|\bar{t}_r(k+1)|^2 \geq |\lambda_q|^2 |\bar{t}_r(k)|^2 + \sigma^2 M^2 \geq |\bar{t}_r(k)|^2 + \sigma^2 M^2. \tag{22}$$

Based on the inequality $|\bar{t}_r(k+1)|^2 \geq |\bar{t}_r(k)|^2 + \sigma^2 M^2$ and the initial condition $\bar{t}_r(0) = 0$, it can be inferred that $|\bar{t}_r(k+1)|^2 \geq (k+1)\sigma^2 M^2$, which implies that $\lim_{k\to\infty} |\bar{t}_r(k+1)| = \infty$ and therefore $\lim_{k\to\infty} t(k+1) = \infty$. Since $t(k+1) = Q\Delta\hat{x}(k+1)$, it can be deduced that at least one component of vector $\Delta\hat{x}(k+1)$ is unbounded, and $\lim_{k\to\infty} \|\Delta\hat{x}(k+1)\| = \infty$. To this end, the condition (8) is satisfied and we finally reach the conclusion that the system is *insecure* under the attacks generated by Algorithm 1 if $\rho(A) \geq 1$.

(**Necessity**). To prove the necessity, we just need to show that the system $\mathcal{P}$ in (1) with estimator $\mathcal{E}$ in (2) is *secure* if matrix $\rho(A) < 1$. Again, let us prove by contradiction. Assume that the system (1) with estimator (2) is *insecure*, that is, there exist attacks sequences satisfying (8) and (9). It follows from (9) that $\Delta z(k+1)$ is norm-bounded. Since $\rho(A) < 1$, based on the equation $\Delta\hat{x}(k+1) = A\Delta\hat{x}(k) + K\Delta z(k+1)$, it can be inferred that $\Delta\hat{x}(k+1)$ is norm-bounded as well. That is, condition (8) is violated and the proof is now complete.

3.2 Case 2: $B_a \neq I_m$

In this case, we assume that the attacker is able to inject false data to *only a part of* (rather than all) communication channels, i.e., $\text{Rk}\{B_a\} < m$. It can be easily seen from Theorem 5 that, if $\rho(A) < 1$, the system (1) with estimator (2) is *secure* no matter how many communication channels the attacker could hijack. As such, in this subsection, we only consider the case when $\rho(A) \geq 1$.

The following lemmas are useful in subsequent analysis.

Lemma 6 *[3] Let $A \in \mathbb{C}^{n\times m}$, $B \in \mathbb{C}^{m\times l}$ and $C \in \mathbb{C}^{k\times n}$. Assume that B has full row rank and C has full column rank. Then, $Rk\{AB\} = Rk\{A\} = Rk\{CA\}$.*

Lemma 7 *If the system $\mathcal{P}$ in (1) with estimator $\mathcal{E}$ in (2) is insecure, then 1) the attack sequence $\{a_k\}$ leading to the insecurity is unbounded, and 2) the state estimation difference $\Delta\hat{x}(k)$ can be represented in the following form:*

$$\Delta\hat{x}(k) = P_o\bar{t}(k) + P_c\underline{t}(k) \tag{23}$$

for some $\bar{t}(k) \in \mathbb{C}^{\bar{l}}$ satisfying $\lim_{k\to\infty}\bar{t}(k) = \infty$ and some bounded vector sequence $\underline{t}(k) \in \mathbb{C}^{n-\bar{l}}$, where P_o and P_c are defined in (11).

Proof. Assume that the attack sequence $\{a_k\}$ leading to the insecurity is bounded. Noting that $\rho((I - KC)A) < 1$, it follows from the dynamics of $\Delta\hat{x}(k)$ in (7) that $\Delta\hat{x}(k+1)$ is bounded. According to Definition 1, the boundedness of $\Delta\hat{x}(k+1)$ contradicts the insecurity assumption of this lemma. As such, the attack sequence $\{a_k\}$ is unbounded.

Next, we proceed to prove that $\Delta\hat{x}(k)$ can be represented as (23) and we use the same notations for P, Q, P_o, P_c, Q_o and Q_c as defined in (10)-(11). Similar to the pf of Theorem 5, we define vector $t(k) \triangleq Q\Delta\hat{x}(k)$ and write $t(k) = \left[t_1^T(k), \ldots, t_p^T(k)\right]^T$ with $t_i(k) \in \mathbb{C}^{n_i}$ ($i \in \{1, 2, \ldots, p\}$). According to (11), the dynamics of $t(k)$ can be given by

$$t(k+1) = \left[\begin{array}{c:c} \Lambda_1 & 0 \\ \hdashline 0 & \Lambda_2 \end{array}\right] \left[\begin{array}{c} \bar{t}(k) \\ \hdashline \underline{t}(k) \end{array}\right] + \left[\begin{array}{c} Q_oK \\ \hdashline Q_cK \end{array}\right] \Delta z(k+1) \tag{24}$$

As $\rho(\Lambda_2) < 1$ and $\Delta z(k)$ is norm-bounded, it is inferred that $\underline{t}(k)$ is norm-bounded. On the other hand, it is easy to see that $\Delta\hat{x}(k) = Pt(k) = \left[\begin{array}{c:c} P_o & P_c \end{array}\right] \left[\begin{array}{c} \bar{t}(k) \\ \hdashline \underline{t}(k) \end{array}\right] = P_o\bar{t}(k) + P_c\underline{t}(k)$. Since $P_c\underline{t}(k)$ is bounded and $\lim_{k\to\infty}\Delta\hat{x}(k) = \infty$, it follows that $\lim_{k\to\infty}\bar{t}(k) = \infty$ and therefore expression (23) holds, which completes the proof.

Theorem 8 *For the system $\mathcal{P}$ in (1), assume that $\rho(A) \geq 1$, $Rk\{CP_o\} = s$ and the attacker is able to inject attacks to a part of (but not all) communication channels, i.e., $Rk\{B_a\} < m$, where P_o is defined in (11). The system $\mathcal{P}$ in (1) with estimator $\mathcal{E}$ in (2) is secure if the following condition holds:*

$$Rk\big\{(I - B_a)CP_o\big\} = s. \tag{25}$$

Proof. Again, we prove the theorem by contradiction. Suppose that the system is *insecure* when condition (25) holds. It follows from Lemma 7 that (23) is true. Furthermore, noting that $\Delta z(k+1)$ is bounded, it follows from (6) and (23) that

$$a(k+1) = CP_o\Lambda_1\zeta_1(k) + O(k), \tag{26}$$

where $O(k) \triangleq CP_c\Lambda_2\zeta_2(k) + \Delta z(k+1)$ which is bounded.

Define matrix $\Phi = \left[\phi_1, \ldots, \phi_{\bar{l}}\right] = CP_o$ where the vector ϕ_i is equal to the ith column of the matrix CP_o ($1 \leq i \leq \bar{l}$). Since $\text{Rk}\{CP_o\} = s$, there exists a matrix $\Psi = \left[\phi_{i_1}, \phi_{i_2}, \ldots, \phi_{i_s}\right]$ satisfying $\text{Rk}\{\Psi\} = s$ where $1 \leq i_1 < i_2 \leq \ldots < i_s \leq \bar{l}$. Moreover, the matrix CP_o can be represented as $CP_o = \Psi X$ where $X \in \mathbb{C}^{s\times\bar{l}}$. It can be easily found that $\text{Rk}\{X\} = s$, *i.e.*, matrix X has full row rank. As a result, (26) can be represented as follows

$$a(k+1) = \Psi\xi(k) + O(k), \tag{27}$$

where $\xi(k) = X\Lambda_1\zeta_1(k)$.

According to Lemma 7, the attack sequence $\{a(k)\}$ is unbounded, the sequence $\{O(k)\}$ is bounded, and therefore the vector sequence $\{\xi(k)\}$ is unbounded.

Left-multiplying both sides of (27) by $I - B_a$ leads to

$$(I - B_a)a(k+1) = (I - B_a)\Psi\xi(k) + (I - B_a)O(k),$$

and then it follows from $a(k+1) = B_aa^0(k+1)$ and $(I - B_a)B_a = 0$ that

$$(I - B_a)\Psi\xi(k) + (I - B_a)O(k) = 0. \tag{28}$$

Since $(I - B_a)CP_o = (I - B_a)\Psi X$ and matrix X is full row rank, it is known from Lemma 6 that $\text{Rk}\big\{(I - B_a)\Psi\big\} = \text{Rk}\big\{(I - B_a)\Psi X\big\} = \text{Rk}\big\{(I - B_a)CP_o\big\}$. Noting the condition $\text{Rk}\big\{(I - B_a)CP_o\big\} = s$ in (25), it is easily found that matrix $(I - B_a)\Psi$ has full column rank. Accordingly, as $\lim_{k\to\infty}\xi(k) \to \infty$, we have $\lim_{k\to\infty}(I - B_a)\Psi\xi(k) \to \infty$. Such a result implies that $(I - B_a)\Psi\xi(k) + (I - B_a)O(k) \neq 0$, which contradicts (28). The proof is now complete.

It is known from Theorem 5 that the system $\mathcal{P}$ in (1) with estimator $\mathcal{E}$ in (2) is *insecure* when $\rho(A) \geq 1$. In this case, it is important to ensure the security by protecting some communication channels. The following corollary provides an efficient method on which communication channels need to protected.

Corollary 9 *For the system (1), assume that $\rho(A) \geq 1$ and $Rk\{CP_o\} = s$. The system $\mathcal{P}$ in (1) with estimator $\mathcal{E}$ in (2) is secure if 1) s communication channels are protected; 2) $Rk\Big\{\left[\varphi_{i_1}^T, \cdots, \varphi_{i_s}^T\right]^T\Big\} = s$, where $i_1, \ldots, i_s$ are the indexes of the protected communication channels and φ_j is the jth row of matrix CP_o ($i_1 \leq j \leq i_s$).*

Proof. Since the communication channels $i_1, \ldots, i_s$ are protected (i.e., free from cyber-attacks), according to the definition of matrix B_a, it is known that $\gamma_j = 0$ if $j \in \{i_1, \ldots, i_s\}$ and otherwise $\gamma_j = 1$. Note that

$(I - B_a)CP_o = \left[(1-\gamma_1)\varphi_1^T, \cdots, (1-\gamma_m)\varphi_m^T\right]^T$, then $\mathrm{Rk}\{(I - B_a)CP_o\} = \mathrm{Rk}\left\{\left[\varphi_{i_1}^T, \cdots, \varphi_{i_s}^T\right]^T\right\} = s$. It follows from Theorem 8 that the system (1) with state estimator (2) is *secure*, which completes the proof.

Remark 10 *It is clear that* $Rk\{CP_o\} = s \leq \bar{l}$ *and it can be found from (11) that* $\bar{l}$ *is the number of unstable eigenvalues of matrix A (counted up to multiplicity). As such, Corollary 9 implies that the number of communication channels that should be protected is not more than the number of unstable eigenvalues of matrix A.*

4 Simulation results

In this section, we consider the state estimation system of a flight vehicle [4]. The system consists of a moving vehicle installed with 3 sensors and 1 remote estimator.

4.1 System setting

The linearised discrete-time model of a simplified longitudinal flight control system is described as follows:

$$\begin{cases} x(k+1) = Ax(k) + Bu(k) + \omega(k) \\ y(k) = Cx(k) + \nu(k) \end{cases}$$

where the state variables $x \in \mathbb{R}^3$, x_1, x_2 and x_3 are the pitch angle, pitch rate and the normal velocity, respectively. The control input u is elevator control signal and the system parameter matrices are:

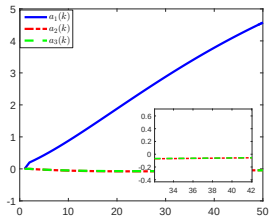
$$A = \begin{bmatrix} 0.9944 & -0.1203 & -0.4302 \\ 0.0017 & 0.9902 & -0.0747 \\ 0 & 0.8187 & 0 \end{bmatrix}, B = \begin{bmatrix} 0.4252 \\ -0.0082 \\ 0.1813, \end{bmatrix}, C = I_3,$$

and both the system and measurement noises are assumed to be uncorrelated zero-mean white noises with covariance $W = \mathrm{diag}\{0.1^2, 0.1^2, 0.01^2\}$ and $R = 0.1I_3$, respectively. Each sensor measures one of the three state variables and send the measurement through its own communication channel to the remote estimator. A stationary Kalman filter is employed in the remote estimator and a χ^2 fault detector is employed as well.

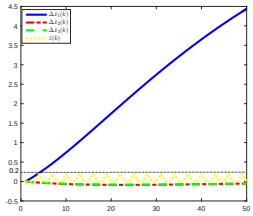
4.2 Security analysis

It can be computed that the eigenvalues of system matrix are 1, 0.9177, and 0.0669. According to Theorem 5, the estimation system of the flight vehicle is insecure. To confirm this conclusion via simulation, assume that the attacker have access to all three communication channels, and a specific deceptive attack is injected into the communication channels, which is generated according to Algorithm 1 where the parameters are chosen as $\sigma = 0.1, M = 2$. The attack sequence $a(k)$ is plotted in Fig. 2 (a). It should be noted that though the values of $a_2(k)$ and $a_3(k)$ all quite small all the time, they do not equal to zero, which shows that false data are injected to all three communication channels.

Fig. 2 (b) depicts the state estimation difference $\Delta\hat{x}(k)$ and the residual difference $\Delta\hat{z}(k)$ under the attack sequences $\{a(k)\}$. From Fig. 2 (b), it is seen that the sequence $\{\Delta\hat{x}(k)\}$ diverges to ∞ while the sequence $\{\|\Delta\hat{z}(k)\|\}$ is always less the prescribed scalar M. Here, the estimated trajectory of the vehicle under the designed attacks deviates significantly from its nominal one but this cannot be detected by the χ^2 fault detector.



(a) attack sequences



(b) estimation/residual differences

Fig. 2. State estimation under false data injection attack

4.3 System protection

Now let us consider how to protect the system from cyber-attacks. It can be computed that the eigenvector corresponding to the unstable system eigenvalue 1 is $P_o = \left[50.9530\ 1.2214\ 1.0000\right]^T$. Since $\mathrm{Rk}(CP_o) = 1$, according to Corollary 9, it is known that the state estimate system of the flight vehicle is secure if the communication channel between sensor 1 and the estimator is protected. Using our proposed method, any malicious attacks can be detected effectively by protecting only 1 rather than all 3 communication channels.

5 Conclusion

In this paper, we have considered the security issues in state estimation of networked control systems. For the case that the adversary can compromise all communication channels, a necessary and sufficient condition has been derived under which the estimation error caused by the attacks is unbounded all the time. For the case that the adversary can only compromise a part of the communication channels, a sufficient condition ensuring the security is derived as well. Moreover, a criterion on protecting a sufficient number of channels such that the estimation error is kept bounded under false data injection attacks has been proposed.

One of the future topics for our research would be a thorough investigation of the cybersecurity issue in remote estimation when the adversary has *limited rather than perfect* knowledge of the system, with the aid of new statistical techniques developed in [8, 12].

References

[1] B. D. Anderson and J. B. Moore, *Optimal Filtering*. Courier Dover Publications, 2005.

[2] C.-Z. Bai, F. Pasqualetti, and V. Gupta, "Security in stochastic control systems: Fundamental limitations and performance bounds," in *Proc. 2015 American Control Conference (ACC)*. 2015, pp. 195–200.

[3] D. S. Bernstein, *Matrix Mathematics: Theory, Facts, and Formulas*. Princeton University Press, 2009.

[4] J. Chen and R. Patton, *Robust Model-based Fault Diagnosis for Dynamic Systems*. Kluwer Academic Publishers, 1999

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

[6] M. S. Chong, M. Wakaiki, and J. P. Hespanha, "Observability of linear systems under adversarial attacks," in *2015 American Control Conference (ACC)*. 2015, pp. 2439–2444.

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

[8] Z. Guo, D. Shi, K.H. Johansson and L. Shi, "Optimal linear cyber-attack on remote state estimation," *IEEE Trans. Control Netw. Syst.*, 4 (1), 4–13, 2017.

[9] J. P. Hespanha, *Linear Systems Theory*. Princeton university press, 2009.
[10] O. Kosut, "Malicious data attacks against dynamic state estimation in the presence of random noise," in *Proc. Global Conference on Signal and Information Processing*. 2013, pp. 261–264.
[11] C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," in *Proc. American Control Conference (ACC)*. 2013, pp. 3344–3349.
[12] Y. Li, L. Shi and T. Chen, "Detection against linear deception attacks on multi-sensor remote state estimation," *IEEE Trans. Control Netw. Syst.*, in press.
[13] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. the 16th ACM conference on Computer and Communications Security*. 2009, pp. 21–32.
[14] S. Mishra, Y. Shoukry, N. Karamchandani, S. Diggavi, and P. Tabuada, "Secure state estimation against sensor attacks in the presence of noise," *IEEE Trans. Control Netw. Syst.*, 4 (1), 49–59, 2017.
[15] Y. Mo and B. Sinopoli, "False data injection attacks in cyber physical systems," in *First Workshop on Secure Control Systems*, 2010.
[16] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *Proc. IEEE Conference on Decision and Control (CDC)*. 2010, pp. 5967–5972.
[17] Y. Mo and B. Sinopoli, "On the performance degradation of cyber-physical systems under stealthy integrity attacks," *IEEE Trans. Autom. Control*, 61 (9), 2618–2624, 2016.
[18] Y. Mo, S. Weerakkody, and B. Sinopoli, "Physical authentication of control systems: designing watermarked control inputs to detect counterfeit sensor outputs," *IEEE Trans. Control Syst. Technol.*, 35 (1), 93–109, 2015.
[19] Z.-H. Pang and G.-P. Liu, "Design and implementation of secure networked predictive control systems under deception attacks," *IEEE Trans. Control Syst. Technol.*, 20 (5), 1334–1342, 2012.
[20] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, 58 (11), 2715–2729, 2013.
[21] Y. Shoukry and P. Tabuada, "Event-triggered state observers for sparse sensor noise/attacks," *IEEE Trans. Autom. Control*, 61 (8), 2079–2091, 2016.
[22] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Proc. IEEE Conference on Decision and Control (CDC)*. 2010, pp. 5991–5998.
[23] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, 51, 135–148, 2015.
[24] M. Zhu and S. Martínez, "On the performance analysis of resilient networked control systems under replay attacks," *IEEE Trans. Autom. Control*, 59 (3), 804–808, 2014.

Liang Hu received the B.E.degree in Detection, Guidance and Control and M.E. degree in Control Science and Engineering from Harbin Institute of Technology, China, in 2008 and 2010, respectively, and the Ph.D. degree from Brunel University London, U.K., in 2016.

He is currently a Lecturer in the School of Computer Science and Informatics at De Montfort University, U.K. Prior to that, he was a Research Fellow within the School of Electronics, Electrical Engineering & Computer Science at Queens University Belfast from 2016 to 2017. His research interests includes signal processing, control and decision and their applications in autonomous systems and intelligent transport systems.

Zidong Wang was born in Jiangsu, China, in 1966. He received the B.Sc. degree in mathematics in 1986 from Suzhou University, Suzhou, China, and the M.Sc. degree in applied mathematics in 1990 and the Ph.D. degree in electrical engineering in 1994, both from Nanjing University of Science and Technology, Nanjing, China.

He is currently Professor of Dynamical Systems and Computing in the Department of Computer Science, Brunel University London, U.K. From 1990 to 2002, he held teaching and research appointments in universities in China, Germany and the UK. Prof. Wang's research interests include dynamical systems, signal processing, bioinformatics, control theory and applications. He has published more than 300 papers in refereed international journals. He is a holder of the Alexander von Humboldt Research Fellowship of Germany, the JSPS Research Fellowship of Japan, William Mong Visiting Research Fellowship of Hong Kong.

Prof. Wang serves (or has served) as the Editor-in-Chief for Neurocomputing and an Associate Editor for 12 international journals, including IEEE Transactions on Automatic Control, IEEE Transactions on Control System Technology, IEEE Transactions on Neural Networks, IEEE Transactions on Signal Processing, and IEEE Transactions on Systems, Man, and Cybernetics - Systems. He is a Fellow of the IEEE, a Fellow of the Royal Statistical Society and a member of program committee for many international conferences.

Qing-Long Han received the B.Sc. degree in Mathematics from Shandong Normal University, Jinan, China, in 1983, and the M.Sc. and Ph.D. degrees in Control Engineering and Electrical Engineering from East China University of Science and Technology, Shanghai, China, in 1992 and 1997, respectively.

From September 1997 to December 1998, he was a Post-doctoral Researcher Fellow with the Laboratoire d'Automatique et d'Informatique Industielle, Ecole Sup érieure d'Ing'enieurs de Poitiers, Universit é de Poitiers, France. From January 1999 to August 2001, he was a Research Assistant Professor with the Department of Mechanical and Industrial Engineering at Southern Illinois University at Edwardsville, USA. From September 2001 to December 2014, he was Laureate Professor, Associate Dean (Research and Innovation) with the Higher Education Division, and Founding Director of the Centre for Intelligent and Networked Systems at Central Queensland University, Australia. From December 2014 to May 2016, he was Deputy Dean (Research) with the Griffith Sciences, and a Professor with the Griffith School of Engineering, Griffith University, Australia. In May 2016, he joined Swinburne University of Technology, Australia, where he is currently Pro Vice-Chancellor (Research Quality) and Distinguished Professor. In March 2010, he was appointed Chang Jiang (Yangtze River) Scholar Chair Professor by Ministry of Education, China.

Prof. Han is one of The World's Most Influential Scientific Minds: 2014-2016 and is a Highly Cited Researcher in Engineering according to Thomson Reuters. He is an Associate Editor of a number of international journals including IEEE Transactions on Industrial Electronics, IEEE Transactions on Industrial Informatics, IEEE Transactions on Cybernetics, and Information Sciences. His research interests include networked control systems, neural networks, time-delay systems, multi-agent systems and complex dynamical systems.

Xiaohui Liu received the B.Eng. degree in computing from Hohai University, Nanjing, China, in 1982 and the Ph.D. degree in computer science from Heriot-Watt University, Edinburg, U.K., in 1988.

He is currently a Professor of Computing at Brunel University. He leads the Intelligent Data Analysis (IDA) Group, performing interdisciplinary research involving artificial intelligence, dynamic systems, image and signal processing, and statistics, particularly for applications in biology, engineering and medicine. Professor Liu serves on editorial boards of four computing journals, founded the biennial international conference series on IDA in 1995, and has given numerous invited talks in bioinformatics, data mining and statistics conferences.