IMA Journal of Mathematical Control and Information (2015) Page 1 of 22
doi:10.1093/imamci/dnv026

An application of linear algebra theory in networked control systems: stochastic cyber-attacks detection approach

YUMEI LI* AND HOLGER VOOS
Interdisciplinary Centre for Security Reliability and Trust (SnT), University of Luxembourg, L-2721 Luxembourg
*Corresponding author. Email: yumei.li@uni.lu zwzlym@163.com

MOHAMED DAROUACH
Centre de la Recherche en Automatique de Nancy (CRAN), Universite de Lorraine, Longwy, France

AND

CHANGCHUN HUA
Institute of Electrical Engineering Yanshan University, Qinhuangdao, China

[Received on 28 November 2014; revised on 23 March 2015; accepted on 24 April 2015]

Based on the traditional linear algebra theory, this paper propose the attack detection schemes for networked control systems (NCSs) under single stochastic cyber-attack and multiple stochastic cyber-attacks aiming at multiple communication channels of NCSs, respectively. The focus is on designing an anomaly detector for NCSs under cyber-attacks. First, we construct a model of stochastic NCSs with stochastic cyber-attacks which satisfy the Markovian stochastic process. And we also introduced the stochastic attack models that NCSs are possibly exposed to. Next, based on the frequency-domain transformation technique and linear algebra theory, we propose the algebraic detection schemes for possible stochastic cyber-attacks. We transform the detector error dynamics into algebraic equations. By applying the presented approaches, residual information that is caused by different attacks is, respectively, obtained and anomalies on the control system are detected. In addition, sufficient and necessary conditions guaranteeing the detectability of the stochastic cyber-attacks are obtained. The presented detection approaches in this paper are simple, straightforward and easy to implement. The aim of this work is to use traditional mathematics tools to solve new problems that arise from the complex NCSs. Finally, two simulation examples are provided. The simulation results underline that the detection approaches are effective and feasible in practical application.

Keywords: cyber-attack detection; multiple stochastic cyber-attacks; stochastic DoS attack; stochastic data deception attack.

1. Introduction

With the popularization of the network, more and more industrial control systems are connected by using different, and even open, public networks, which are increasing the risk that networked control systems (NCSs) are exposed to cyber-attacks. Therefore, the security problem of NCSs is becoming critical. An NCS is vulnerable to these threats and successful attacks on the NCS can cause serious consequences which may lead to the loss of vital societal function, financial loss and even loss of life (Nimda worm, 2001; Moore *et al.*, 2003; New 'cyber attacks' hit S Korea; Slay & Miller, 2007; Wolf & Daly, 2009; Amin *et al.*, 2013; Tang *et al.*, 2014). Therefore, these attacks should be detected as early as possible

in order to prevent serious consequences. In recent years, the problem of cyber-attacks on controlled systems has been realized and it is currently attracting considerable attention (see, e.g. Hashim *et al.*, 2008; Liu *et al.*, 2009; Anjali & Ramesh, 2010; Eliades & Polycarpou, 2010; Metke & Ekl, 2010; Mo & Sinopoli, 2010; Andersson & Esfahani, 2011; Mohsenian-Rad & Garcia, 2011; Pasqualetti, 2012; Sridhar *et al.*, 2012; Teixeira *et al.*, 2012; Weimer *et al.*, 2012; Amin *et al.*, 2013; Rosich *et al.*, 2013; Li *et al.*, 2014b,a). For example, Andersson & Esfahani (2011) and Eliades & Polycarpou (2010) did research on the cyber security of water systems. Metke & Ekl (2010), Sridhar *et al.* (2012), Mohsenian-Rad & Garcia (2011) and Pasqualetti (2012) focused on cyber-attacks on smart grid systems. While cyber-attacks in conventional information technology (IT) systems are only influencing information, cyber-attacks on control systems are changing physical processes and hence the real world (Mohsenian-Rad & Garcia, 2011). Previous methods and tools used to protect traditional IT against cyber-attacks might finally not completely prevent successful intrusion of malware in the control system. Therefore, new approaches are needed. Although NCSs are protected by IT security measures, attackers might nevertheless find a way to get unauthorized access and compromise them by means of cyber-attacks. This cyber-attacks should be detected as soon as possible with an acceptable false alarm rate and also be identified and isolated. Therefore, there is an urgent need for an efficient cyber-attack detection system as an integral part of the cyber infrastructure, which can accurately detect cyber-attacks in a timely manner such that countering actions can be taken promptly to ensure the availability, integrity and confidentiality of the systems. These new requirements increase the interest of researchers in the development of cyber-attack detection and isolation techniques (Hashim *et al.*, 2008; Liu *et al.*, 2009; Anjali & Ramesh, 2010; Weimer *et al.*, 2012). Li *et al.* (2014b) proposed a model predictive approach for cyber-attack detection. Teixeira *et al.* (2012) considered robust H_∞ cyber-attacks estimation for control systems. And Li *et al.* (2014a) proposed a stochastic cyber-attack detection scheme based on frequency-domain transformation technique. Moreover, in practice, hackers might attempt to launch multiple attacks aiming at multiple communication channels of a control system in order to create attacks that are more stealthy and thus more likely to successful. When a hacker launches two or more cyber-attacks against a control process, usually it is claimed that the control system suffers from multiple cyber-attacks. However, existing literatures mentioned above never deal with the detection problem of multiple cyber-attacks on a control process. Furthermore, the new problems that arise from the complex control systems are challenging the traditional mathematics tools. All of these factors mentioned above motivate our research in this area.

This paper proposes the algebraic detection schemes for NCSs under stochastic cyber-attacks and disturbances. Further, it deals with the multiple stochastic cyber-attacks detection problem aiming at multiple communication channels of an NCS. The basic idea is to use suitable observers to generate residual information with regard to cyber-attacks, i.e. compromised sensor signals and controller outputs. An anomaly detector for NCSs under stochastic cyber-attacks is derived. The main contributions in the paper are as follows. First, we construct a model of NCSs with stochastic cyber-attacks which satisfy the Markovian stochastic process. And we also, respectively, introduced the stochastic attack models that NCSs are possibly exposed to, which are aiming at whole NCSs or a specific controller command input channel or sensor measurement output channel of NCSs. Next, based on the frequency-domain transformation technique, linear algebra theory and auxiliary detector error systems, we propose the algebraic attack detection schemes for NCSs subject to single stochastic cyber-attack and multiple stochastic cyber-attacks, respectively. Hashim *et al.* (2008) also used a frequency-domain analysis in the detection of denial-of-service (DoS) attacks, he proposed the detection algorithm by investigating the frequency spectrum distribution of the network traffic. However, we transform the detector error dynamics equations into algebraic equations, which make the discussion of the problem simpler and

more straightforward. Here, we consider the possible cyber-attacks as non-zero solutions of the algebraic equations and the residuals as their constant vectors. By analysing the ranks of the stochastic system matrix and the auxiliary stochastic system matrices, the residual information caused by attacks from different communication channel is, respectively, obtained. Furthermore, based on the obtained residual information, the detectability of these cyber-attacks can be determined. Some sufficient and necessary conditions guaranteeing that these attacks are detectable or undetectable are obtained. In addition, by using the linear matrix inequation (LMI) algorithm, we also propose an approach for determining the detector gain matrix.

The literatures (Teixeira *et al.*, 2010; Sundaram & Hadjicostis, 2011; Pasqualetti *et al.*, 2012) used a similar idea of analysing the error residual, however, they generally focused on using consensus dynamics in networked multi-agent systems including malicious agents. Differentiating from the literatures (Teixeira *et al.*, 2010; Sundaram & Hadjicostis, 2011; Pasqualetti *et al.*, 2012), we stress that the using of the traditional linear algebra theory in the detection of cyber-attacks, since it is the aim to use traditional mathematics tools to solve new problems that arise from NCSs. Finally, two simulation examples are provided to illustrate the effectiveness of the obtained results. In Example 6.1, we detect the cyber-attack on an NCS that is subjected to a stochastic data deception attack and disturbance. In Example 6.2, we consider a large-scale distributed networked water system that comprise of n identical subsystems and each subsystem is used the model of quadruple-tank process (QTP) in Johansson (2000). We also detect possible cyber-attacks which are aiming at two different controller command input channels on the actuator of the subsystem 1. Simulation results underline that the proposed attack detection approach is feasible and effective.

2. Preliminaries

In this section, we give precise definitions of some elementary concepts involving the rank of matrix and consistent of linear equation, which will help to understand our work well and some of them will be used in the sequel of our study.

DEFINITION 2.1 (Rank) The number of non-zero rows in the row echelon form of an $m \times n$ matrix A produced by elementary operations on A is called the rank of A.

DEFINITION 2.2 (Full row rank) We say that an $m \times n$ matrix A has full row rank if $\text{rank}(A) = m$.

DEFINITION 2.3 (Full column rank) We say that an $m \times n$ matrix A has full column rank if $\text{rank}(A) = n$.

Let $R[s]$ denote the polynomial ring with real coefficients. A matrix is called a polynomial matrix if every element of the matrix is in $R[s]$.

DEFINITION 2.4 (Normal rank Zhou *et al.*, 1996) Let $Q(s) \in R[s]$ be a $(p \times m)$ polynomial matrix. Then the normal rank of $Q(s)$, denoted by normal $\text{rank}(Q(s))$, is the rank in $R[s]$ or, equivalently, is the maximum dimension of a square submatrix of $Q(s)$ with non-zero determinant in $R[s]$.

In short, sometimes we say that a polynomial matrix $Q(s)$ has $\text{rank}(Q(s))$ in $R[s]$ when we refer to the normal rank of $Q(s)$. To show the difference between the normal rank of a polynomial matrix and the rank of the polynomial matrix evaluated at certain point, consider

$$Q(s) = \begin{bmatrix} s & 1 \\ s^2 & 1 \end{bmatrix}.$$

Then $Q(s)$ has normal rank 2 since $\det Q(s) = s - s^2 \neq 0$. However, $Q(0)$ has rank 1.

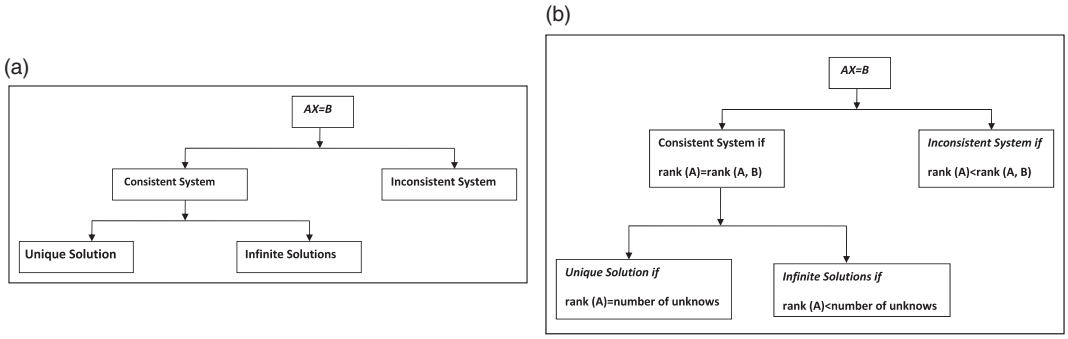

FIG. 1. (a) Consistent and inconsistent system of equations flow chart and (b) the relationships among consistent, rank and solution of equations.

DEFINITION 2.5 A system of equations $AX = B$ is consistent if there is a solution, and it is inconsistent if there is no solution.

However, a consistent system of equations does not mean a unique solution, that is, a consistent system of equations may have a unique solution or infinite solutions. This can be formulation according to the chart given in Fig. 1(a). However, how can one distinguish between a consistent and inconsistent system of equations? Moreover , if a solution exists, how do we know whether it is unique? The following lemmas give us a description in detail.

LEMMA 2.1

(1) A system of equations $AX = B$ is consistent if the rank of A is equal to the rank of the augmented matrix $[A\ B]$.

(2) A system of equations $AX = B$ is inconsistent if the rank of A is less than the rank of the augmented matrix $[A\ B]$.

LEMMA 2.2 In a system of equations $AX = B$ that is consistent, the rank of the coefficient matrix A is the same as the augmented matrix $[A\ B]$.

(1) If in addition, the rank of the coefficient matrix A is same as the number of unknowns, then the solution is unique.

(2) If the rank of the coefficient matrix A is less than the number of unknowns, then infinite solutions exist.

Figure 1(b) illustrates their relationships among consistent, rank and solution of equations $AX = B$. A linear system of equations must have either no solution, one solution or infinitely many solutions. Further, using the following lemmas, we can determine the solutions of the linear nonhomogeneous equations $AX = B$ and homogeneous equations $AX = 0$, where A is an $m \times n$ matrix.

LEMMA 2.3

(1) If the rank of $A = r = n < m$, the linear non-homogeneous equations $AX = B$ has no solution or exactly one solution. In other words, if the matrix A is of full column rank and has less columns than rows, the system will be inconsistent, or will have exactly one solution.

(2) If the rank of $A = r = m < n$, the linear non-homogeneous equations $AX = B$ will always have a solution and there will be an infinite number of solutions. In other words, if the matrix A is of full row rank and has more columns than rows, the system will always have an infinite number of solutions.

(3) If the rank of $A = r = m = n$, the linear non-homogeneous equations $AX = B$ will exactly one solution. In other words, if the matrix A is square and has full rank, the system will have a unique solution.

(4) If the rank of $A = r$, where $r < m$ and $r < n$, the linear non-homogeneous equations $AX = B$ will either have no solutions or there will be an infinite number of solutions. In other words, if the matrix A has neither full row nor full column rank, the system will be inconsistent or will have an infinite number of solutions.

LEMMA 2.4

(1) If the rank of $A = r = n < m$, the linear homogeneous equations $AX = 0$ has one solution and only zero solution. In other words, if the matrix A is of full column rank and has less columns than rows, the system will have exactly zero solution.

(2) If the rank of $A = r < n$, the linear homogeneous equations $AX = 0$ will have a non-zero solution and there will be an infinite number of solutions.

3. Problem formulation

Consider the following NCS:

$$\begin{aligned} \dot{x}(t) &= Ax(t) + B(u(t) + \alpha(t)a_k^a(t)) + E_1 w(t), \\ x(0) &= x_0, \\ y(t) &= C(x(t) + \beta(t)a_k^s(t)) + E_2 \nu(t), \end{aligned} \tag{3.1}$$

where $x(t) \in R^r$ is the state vector. x_0 is the initial state, $y(t) \in R^p$ is the measurement output, $u(t) \in R^m$ is the known input vector. $a_k^a(t) \in R^m$ denotes the actuator cyber-attack and $a_k^s(t) \in R^r$ denotes the sensor cyber-attack. $w(t)$ and $\nu(t)$ are systems noise and process noise, respectively. A, B, E_1 and C, E_2 are known constant matrices with appropriate dimensions. $\alpha(t)$ and $\beta(t)$ are Markovian stochastic processes taking the values 0 and 1 and satisfy the following probability:

$$\begin{aligned} E\{\alpha(t)\} &= \text{Prob}\{\alpha(t) = 1\} = \rho, \\ E\{\beta(t)\} &= \text{Prob}\{\beta(t) = 1\} = \sigma. \end{aligned} \tag{3.2}$$

Herein, event $\alpha(t) = 1$ (or $\beta(t) = 1$) shows the actuator (or the sensor) of the system is subjected to a cyber-attack, so an actuator cyber-attack $a_k^a(t)$ (or a sensor cyber-attack $a_k^s(t)$) occurs; event $\alpha(t) = 0$ (or $\beta(t) = 0$) means no a cyber-attack on the actuator (or on the sensor). $\rho \in [0, 1]$ (or $\sigma \in [0, 1]$) reflects the occurrence probability of the event that the actuator (or the sensor) of the system is subjected to a cyber-attack. While $\alpha(t)$ and $\beta(t)$ are independent from stochastic variables, they are also independent from measurement noises $w(t)$, $\nu(t)$ and the initial state x_0. Generally, cyber-attacks targeting NCSs mainly include DoS attacks and deception attacks. In the sequel of the paper, we introduce these attack models that can be modelled by the stochastic system model (3.1).

3.1 *Modelling stochastic cyber-attacks*

In a stochastic data DoS attack, the objective of hackers is to prevent the actuator from receiving control commands or the controller from receiving sensor measurements. Therefore, by compromising devices and preventing them from sending data, attacking the routing protocols, jamming the communication channels, flooding the communication network with random data and so on, hackers can launch a stochastic data DoS attack that satisfies Markovian stochastic processes. In a stochastic data deception attack, hackers attempt to prevent the actuator or the sensor from receiving an integrity data, therefore, they send false information $\tilde{u}(t) \neq u(t)$ or $\tilde{y}(t) \neq y(t)$ from controllers or sensors. The false information can include: inject a bias data that cannot be detected in the system, or an incorrect time when a measurement was observed; a wrong sender identity, an incorrect control input or an incorrect sensor measurement. The hacker can launch these attacks by compromising some controllers or sensors or by obtaining the secret keys.

(1) A stochastic data DoS attack that hackers might launch on the actuator and on the sensors of NCSs can be modelled as follows:

$$\begin{cases} \alpha(t) \in \{0,1\}, \quad t \geqslant t_0, \\ a_k^a(t) = -u(t) \end{cases} \quad \text{and} \quad \begin{cases} \beta(t) \in \{0,1\}, \quad t \geqslant t_0, \\ a_k^s(t) = -x(t). \end{cases} \tag{3.3}$$

(2) A stochastic data deception attack on the actuator and on the sensors of NCSs can be, respectively, modelled as follows:

$$\begin{cases} \alpha(t) \in \{0,1\}, \quad t \geqslant t_0, \\ a_k^a(t) = -u(t) + d_k^a(t) \quad \text{or} \quad a_k^a(t) = d_k^a(t) \end{cases} \quad \text{and}$$
$$\begin{cases} \beta(t) \in \{0,1\}, \quad t \geqslant t_0, \\ a_k^s(t) = -x(t) + d_k^s(t) \quad \text{or} \quad a_k^s(t) = d_k^s(t), \end{cases} \tag{3.4}$$

where $d_k^a(t)$ and $d_k^s(t)$ are deceptive data that hackers attempt to launch on the actuator and the sensor.

Now, let $T_{d_k^a y}(s) = C(sI - A)^{-1}B$ is the transfer function from the attack $d_k^a(t)$ to output measure $y(t)$. When hackers launch a data deception attack $a_k^a(t) = d_k^a(t)$ on the actuator to make $T_{d_k^a y}(s) = 0$, a zero dynamic attack occurs on the actuator. Obviously, a zero dynamic attack is undetectable. In addition, it is not possible for a hacker to launch a zero dynamic attack on the sensor, since the transfer function from the attack $d_k^s(t)$ to output $y(t)$ is $T_{d_k^s y}(s) = C \neq 0$.

4. Single stochastic cyber-attack detection scheme based on frequency-domain transformation

In this section, our objective is the anomaly detection. We assume that the following conditions are satisfied: (1) the pair (A, B) is controllable; (2) (A, C) is observable. For convenience on discussion, we ignore the influence of control inputs in the remainder of this paper because they do not affect the residual when there are no modelling errors in the system transfer matrix. Therefore, the system (3.1)

can be rewritten as follows:

$$\begin{aligned} \dot{x}(t) &= Ax(t) + \alpha(t)Ba_k^a(t) + E_1 w(t), \\ x(0) &= x_0, \\ y(t) &= Cx(t) + \beta(t)Ca_k^s(t) + E_2 v(t). \end{aligned} \tag{4.1}$$

Set up the following anomaly detector:

$$\begin{aligned} \dot{\tilde{x}}(t) &= A\tilde{x}(t) + \tilde{B}r(t), \\ \tilde{x}(0) &= 0, \\ r(t) &= y(t) - C\tilde{x}(t), \end{aligned} \tag{4.2}$$

where $\tilde{B}$ is the detector gain matrix and $r(t)$ represents the output residual.

Let $e(t) = x(t) - \tilde{x}(t)$, then we obtain the following error dynamics:

$$\begin{aligned} \dot{e}(t) &= \bar{A}e(t) + \bar{B}a_k(t) + \bar{E}_1 d(t), \\ r(t) &= Ce(t) + \bar{D}a_k(t) + \bar{E}_2 d(t), \end{aligned} \tag{4.3}$$

$$\begin{aligned} &\bar{A} = (A - \tilde{B}C), \quad \bar{B} = [B\alpha(t) \quad -\beta(t)\tilde{B}C], \\ &\bar{E}_1 = [E_1 \quad -\tilde{B}E_2], \quad \bar{D} = [0 \quad C\beta(t)], \quad \bar{E}_2 = [0 \quad E_2] \end{aligned} \tag{4.4}$$

and the vectors

$$a_k(t) = \begin{bmatrix} a_k^a(t) \\ a_k^s(t) \end{bmatrix}, \quad d(t) = \begin{bmatrix} w(t) \\ v(t) \end{bmatrix}, \quad d_1(t) = \begin{bmatrix} a_k(t) \\ d(t) \end{bmatrix}. \tag{4.5}$$

First, we give the following definition.

DEFINITION 4.1 For stochastic NCS (4.1) and detector (4.2). If a cyber-attack $a_k(t)$ on system (4.1) leads to zero output residual, then the cyber-attack is undetectable.

If $T_{dr}(s) = C(sI - \bar{A})^{-1}\bar{E}_1 + \bar{E}_2$ denotes the transfer function from stochastic disturbance $d(t)$ to output residual $r(t)$, the robust stability conditions of error dynamics (4.3) are given in term of the following lemma.

LEMMA 4.1 (Li *et al.*, 2014a) When all stochastic events $\alpha(t) = \beta(t) = 0$, there are the following conclusions:

(1) the error dynamics (4.3) without disturbances is asymptotically stable, if there exists symmetric positive-definite matrix $P > 0$ and matrix X such that the following LMI holds:

$$\Psi = A^\top P + PA - C^\top X^\top - XC + C^\top C < 0, \tag{4.6}$$

(2) the error dynamics (4.3) with disturbances $d(t)$ $(0 \neq d(t) \in L_f^2([0, \infty); R^n))$ is robustly stable, if $\|T_{dr}(s)\|_\infty < 1$ and exists symmetric positive-definite matrix $P > 0$ and matrix X such that the

following LMI holds:

$$\begin{bmatrix} \Psi & PE_1 & -XE_2 + C^\top E_2 \\ * & -I & 0 \\ * & * & -I + E_2^\top E_2 \end{bmatrix} < 0. \tag{4.7}$$

When the LMIs above are solvable, the detector gain matrix is given by $\tilde{B} = P^{-1}X$.

Next, using the frequency-domain description of the system, we transform the error dynamics (4.3) into the following linear algebraic equations:

$$Q(s)X(s) = B(s), \tag{4.8}$$

where

$$Q(s) = \begin{bmatrix} \bar{A} - sI & \bar{B} & \bar{E}_1 \\ \bar{C} & \bar{D} & \bar{E}_2 \end{bmatrix}, \quad X(s) = \begin{pmatrix} e(s) \\ a_k(s) \\ d(s) \end{pmatrix}, \quad B(s) = \begin{pmatrix} 0 \\ r(s) \end{pmatrix}.$$

REMARK 4.1 Here, since matrices $\bar{B}$ and $\bar{D}$ include the stochastic parameters $\alpha(t)$ and $\beta(t)$, the system matrix $Q(s)$ correspondingly includes these stochastic parameters. In order to obtain effective results, we introduce $E(Q(s))$ that is a mathematical expectation of the stochastic matrix $Q(s)$, then the equations (4.8) are described as

$$E(Q(s))X(s) = B(s) \tag{4.9}$$

and

$$E(Q(s)) = \begin{bmatrix} (A - \tilde{B}C) - sI & \rho B & -\sigma\tilde{B}C & E_1 & -\tilde{B}E_2 \\ C & 0 & \sigma C & 0 & E_2 \end{bmatrix}.$$

Further, by discussing the rank of stochastic matrix $E(Q(s))$, we obtain some important results.

THEOREM 4.1 For system (4.1), assume that the stochastic matrix $E(Q(s))$ has full column normal rank. The cyber-attack $a_k(s)$ $(0 \neq a_k(s) \in \bar{G})$ as $s = z_0$ is undetectable, if and only if there exists $z_0 \in \mathbb{C}$, such that

$$E(Q(z_0))Y(z_0) = 0. \tag{4.10}$$

Herein,

$$E(Q(z_0)) = E(Q(s))|_{s=z_0},$$
$$Y^T(z_0) = (e(z_0) \quad a_k^a(z_0) \quad a_k^s(z_0) \quad w(z_0) \quad v(z_0))^\top$$

$\bar{G}$ is a set of undetectable cyber-attacks.

Proof. (if) Assume that there exists $z_0 \in \mathbb{C}$ such that condition (4.10) holds, it becomes obvious that equation (4.9) as $s = z_0$ is homogeneous, i.e $B(s)|_{s=z_0} = 0 \Leftrightarrow$ the output residual $r(s)|_{s=z_0} = 0$. Therefore, by Definition 4.1, we obtain that the cyber-attack $a_k(s)$ $(0 \neq a_k(s) \in \bar{G})$ as $s = z_0$ is undetectable.

(only if) Assume that the cyber-attack $a_k(s)$ $(0 \neq a_k(s) \in \bar{G})$ as $s = z_0$ is undetectable, then by Definition 4.1, the output residual $r(s)|_{s=z_0} = 0$. And since that the stochastic matrix $E(Q(s))$ has full

column rank, there must exist $z_0 \in \mathbb{C}$ such that

$$E(Q(s))Y(s)|_{s=z_0} = 0.$$

That completes the proof of Theorem 4.1. □

REMARK 4.2 Actually, the complex number z_0 that satisfies Theorem 4.1 is called an invariant zero of the error dynamic (4.3). Therefore, if error dynamics (4.3) has an invariant zero z_0, then the cyber attack $a_k(s)$ as $s = z_0$ is undetectable. The definition of invariant zero can be found in Zhou *et al.* (1996).

THEOREM 4.2 For system (4.1), assume that the stochastic matrix $E(Q(s))$ has full column normal rank. The cyber-attack $a_k(s)$ $(0 \neq a_k(s) \in \bar{G})$ as $s = z_0$ is undetectable, if and only if there exists $z_0 \in \mathbb{C}$ such that

$$\operatorname{rank} E(Q(z_0)) < \dim(Y(z_0)). \tag{4.11}$$

Proof. (if) Since the stochastic matrix $E(Q(s))$ has full column normal rank and there is a $z_0 \in \mathbb{C}$ such that

$$\operatorname{rank} E(Q(z_0)) < \dim(Y(z_0)).$$

It becomes obvious that z_0 is an invariant zero (Zhou *et al.*, 1996) of detector error dynamics (4.3), therefore, the cyber-attack $a_k(s)$ as $s = z_0$ is undetectable.

(only if) Assume that the cyber-attack $a_k(s)$ as $s = z_0$ is undetectable, then there must exist a $z_0 \in \mathbb{C}$ such that the residual $r(z_0) = 0$ and the following equation:

$$E(Q(z_0))Y(z_0) = B(z_0) \tag{4.12}$$

is a homogeneous equation, i.e.

$$E(Q(z_0))Y(z_0) = 0. \tag{4.13}$$

If we assume

$$\operatorname{rank} E(Q(z_0)) = \dim(Y(z_0))$$

then according to Lemma 2.4, homogeneous equation (4.13) has a zero as its unique solution, i.e. $Y(z_0) = 0$. However, this contradicts with the condition that

$$Y|_{s=z_0} \neq 0$$

is a solution to (4.13). Therefore, the assumption is false, only condition (4.11) is true. This completes the proof of Theorem 4.2. □

The following theorem shows the condition that the stochastic cyber-attacks are detectable.

THEOREM 4.3 For system (4.1), assume that the stochastic matrix $E(Q(s))$ has full column normal rank. The cyber-attack $a_k(s)$ $(0 \neq a_k(s) \in G)$ is detectable, if and only if the following condition always holds for any $z_0 \in \mathbb{C}$:

$$\operatorname{rank} E(Q(z_0)) = \dim(Y(z_0)). \tag{4.14}$$

Herein, G is a set of detectable cyber-attacks.

Proof. (if) Assume that condition (4.14) always holds for any $z_0 \in \mathbb{C}$, it is obvious that the matrix $E(Q(z_0))$ has full column rank. By Lemma 2.3, the equation

$$E(Q(z_0))Y(z_0) = B(z_0) \tag{4.15}$$

has no solution or only one solution. In the following, we proof by contradiction. Assume that there exists a $z_0 \in \mathbb{C}$ such that $a_k(s)$ as $s = z_0$ is undetectable, the residual $r|_{s=z_0} = 0$ according to Definition 4.1, then equation (4.15) has one and only one zero solution, i.e.

$$Y|_{s=z_0} = 0.$$

However, this violates the given condition $0 \neq a_k(z_0) \in G$, i.e.

$$Y|_{s=z_0} \neq 0.$$

Therefore, $r(z_0) \neq 0$, for any $z_0 \in \mathbb{C}$ the cyber attack $a_k(s)$ is detectable.

(only if) Assume that there exists a $z_0 \in \mathbb{C}$ and satisfies condition (4.11). Since the matrix $E(Q(s))$ has full column normal rank, according to Theorem 4.2, $a_k(z_0)$ is undetectable. However, this is in contradiction with the given condition that $a_k(s)$ for any $z_0 \in \mathbb{C}$ is detectable. Therefore, the assumption is false, only

$$\operatorname{rank} E(Q(z_0)) = \dim(Y(z_0))$$

is true, which completes the proof of Theorem 4.3. □

REMARK 4.3 In the work, we regard stochastic attack events $\alpha(t)$ and $\beta(t)$ as the Markovian processes with the binary state (0 or 1) rather than Bernoulli processes, since they more accord with the properties of Markovian process. The reasons are as follows: (1) although the future state of an attack process does not depend on its past state like a Markovian processes and a Bernoulli process, but it depends on its current state, which is in complete accord with a Markovian processes rather than a Bernoulli process. (2) In an attack process, for all trials i of $\alpha(t) = 1$ (or $\beta(t) = 1$), the attacked probabilities ρ (or σ) for all value i do not have to be the same value, which is different with a Bernoulli process.

For example, in practice, whether the next state of a control system will be attacked or not, it depends on current state of the system. If the current state of the system is under attack, then the next state will more likely be attacked. And the attacked probability ρ (or σ) for stochastic events $\alpha(t) = 1$ (or $\beta(t) = 1$) can be either the same value or the different value for all trials i, which is complete random taken value in set [0, 1] for each trial.

5. Multiple stochastic cyber-attacks detection scheme

In order to increase the chance of an attack and to intrude more stealthily, hackers may attempt to launch stochastic cyber-attacks aiming at one or several special communication channels of an NCS. In this section, we extend the method mentioned above to the case that an NCS is subjected to multiple stochastic cyber-attacks aiming at its multiple communication channels.

REMARK 5.1 In Li *et al.* (2015), we presented the detection problem of control systems under multiple stochastic cyber-attacks in detail. However, since our aim in this work is to use traditional algebra theory to deal with new problems that arise from the complex NCSs, in the section, we put forward the algebraic detection approach for multiple stochastic cyber-attacks again in order to keep the integrity of the presented detection approach in the whole work.

Consider the following NCS with multiple stochastic cyber-attacks aiming at specific controller command input channels and sensor measurement output channels:

$$\begin{aligned}\dot{x}(t) &= Ax(t) + B\left(u(t) + \sum_{i=1}^{n_1} \alpha_i(t) f_i a_i^a(t)\right) + E_1 w(t),\\ x(0) &= x_0,\\ y(t) &= C\left(x(t) + \sum_{j=1}^{n_2} \beta_j(t) h_j a_j^s(t)\right) + E_2 v(t),\end{aligned} \tag{5.1}$$

where f_i and h_j are the attacked coefficients. $a_i^a(t) \in R, i = 1, \ldots, n_1$ and $a_j^s(t) \in R, j = 1, \ldots, n_2$ denote the actuator cyber-attack aiming at the ith controller command input channel and the sensor cyber-attack aiming at the jth sensor measurement output channel. $\alpha_i(t)$ and $\beta_i(t)$ are also Markovian stochastic processes with the binary state (0 or 1), which satisfy the following probability:

$$\begin{aligned}E\{\alpha_i(t)\} &= \text{Prob}\{\alpha_i(t) = 1\} = \rho_i, \quad i = 1, \ldots, n_1 \leqslant m,\\ E\{\beta_j(t)\} &= \text{Prob}\{\beta_j(t) = 1\} = \sigma_j, \quad j = 1, \ldots, n_2 \leqslant r.\end{aligned} \tag{5.2}$$

Herein, the event $\alpha_i(t) = 1$ (or $\beta_j(t) = 1$) shows that the ith controller command input channel on the actuator (or the jth sensor measurement output channel on the sensor) is subject to an actuator cyber-attack $a_i^a(t)$ (or a sensor cyber-attack $a_j^s(t)$); $\alpha_i(t) = 0$ (or $\beta_j(t) = 0$) means no attack on the ith (or the jth) channel. $\rho_i \in [0, 1]$ (or $\sigma_j \in [0, 1]$) reflects the occurrence probability of the event that the actuator (or the sensor) of the system is subject to a cyber-attack $a_i^a(t)$ (or $a_j^s(t)$). Similarly, $\alpha_i(t)$ and $\beta_j(t)$ are also independent from each other.

The control input matrix B and the output state matrix C are expressed as the following column vector groups, respectively:

$$B = [b_1 \quad \cdots \quad b_i \quad \cdots \quad b_m], \quad C = [c_1 \quad \cdots \quad c_j \quad \cdots \quad c_r]. \tag{5.3}$$

Herein, b_i is the ith column vectors of matrix B and c_j is the jth column vectors of matrix C. And the control input $u(t)$ and the system state $x(t)$ are written as

$$u(t) = \begin{bmatrix} u_1(t) \\ u_2(t) \\ \vdots \\ u_m(t) \end{bmatrix}, \quad x(t) = \begin{bmatrix} x_1(t) \\ x_2(t) \\ \vdots \\ x_r(t) \end{bmatrix}. \tag{5.4}$$

5.1 *Modelling a stochastic cyber-attacks on a specified communication channel*

Stochastic data DoS attacks and stochastic data deception attacks aiming at a specific controller command input channel or sensor measurement output channel of an NCS, which hackers might launch on the NCS, can be, respectively, modelled as follows:

(1) A stochastic DoS attack preventing the actuators from receiving control command of the ith control channel and the sensors from receiving sensor measure of the jth output channel can be

modelled as

$$\begin{cases} \alpha_i(t) \in \{0,1\}, \quad t \geqslant t_0, \ \ i = 1, \ldots, n_1 \leqslant m, \\ f_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}_{m\times 1}, \qquad \text{and} \\ a_i^a(t) = -u_i(t) \end{cases}$$

$$\begin{cases} \beta_j(t) \in \{0,1\}, \quad t \geqslant t_0, \ \ j = 1, \ldots, n_2 \leqslant r, \\ h_j = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}_{r\times 1}, \\ a_j^s(t) = -x_j. \end{cases} \tag{5.5}$$

(2) A stochastic data deception attack preventing the actuator from a correct control input of the *i*th control channel and the sensor from a correct sensor measurement of the *j*th output channel can be modelled as

$$\begin{cases} \alpha_i(t) \in \{0,1\}, \quad t \geqslant t_0, \ \ i = 1, \ldots, n_1 \leqslant m, \\ f_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}_{m\times 1}, \qquad \text{and} \\ a_i^a(t) = -u_i(t) + d_i^a(t) \quad \text{or} \quad a_i^a(t) = d_i^a(t) \end{cases}$$

$$\begin{cases} \beta_j(t) \in \{0,1\}, \quad t \geqslant t_0, j = 1, \ldots, n_2 \leqslant r, \\ h_j = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}_{r\times 1}, \\ a_j^s(t) = -x_j + d_j^s(t) \quad \text{or} \quad a_j^s(t) = d_j^s(t), \end{cases} \tag{5.6}$$

where $d_i^a(t)$ and $d_j^s(t)$ are deceptive data that hackers attempt to launch on the actuator and the sensor.

REMARK 5.2 In the attack models of multiple stochastic cyber-attacks mentioned above, the attacked coefficients f_i and h_j are column vectors. Herein, only the element in the ith row is 1 and the rest elements are 0 in f_i, which implies that only the ith control channel of the NCS is attacked. Similarly, only the element in the jth row is 1 and the rest elements are 0 in h_j, which implies that only the jth output channel of the NCS is attacked.

REMARK 5.3 To attack a target, hackers may launch multiple attacks aiming at multiple communication channels so that the aggression opportunities are increased and the attack target is compromised, more stealthily and successfully. For example, in order to effectively disturb the formation control of multi-vehicle systems, a hacker could launch multiple stochastic cyber-attacks, which are, respectively, aiming at different communication links among these vehicles or aiming at multiple controller command input channels of single vehicle. Obviously, the detection and isolation of multiple cyber-attacks are very important in the formation control of multi-vehicle systems. Therefore, the research on multiple cyber-attacks is significant, and requires further research.

5.2 *Multiple stochastic cyber-attack detection*

After ignored the influence of control inputs, the system (5.1) and the corresponding error dynamics can be rewritten as follows:

$$\begin{aligned} \dot{x}(t) &= Ax(t) + \sum_{i=1}^{n_1} \alpha_i(t) B f_i a_i^a(t) + E_1 w(t), \\ x(0) &= x_0, \\ y(t) &= Cx(t) + \sum_{j=1}^{n_2} \beta_j(t) C h_j a_j^s(t) + E_2 v(t) \end{aligned} \tag{5.7}$$

and

$$\begin{aligned} \dot{e}(t) &= \bar{A} e(t) + \sum_{i=1}^{n} \bar{F}_i a_i(t) + \bar{E}_1 d(t), \\ r(t) &= Ce(t) + \sum_{i=1}^{n} \bar{H}_i a_i(t) + \bar{E}_2 d(t) \end{aligned} \tag{5.8}$$

with the matrices

$$\begin{aligned} &\bar{A} = (A - \tilde{B}C), \quad \bar{H}_i = [0 \quad \beta_i(t) C h_i], \\ &\bar{F}_i = [\alpha_i(t) B f_i \quad -\beta_i(t) \tilde{B} C h_i], \\ &\bar{E}_1 = [E_1 \quad -\tilde{B}E_2], \quad \bar{E}_2 = [0 \quad E_2] \end{aligned} \tag{5.9}$$

and the vectors

$$a_i(t) = \begin{bmatrix} a_i^a(t) \\ a_i^s(t) \end{bmatrix}, \quad d(t) = \begin{bmatrix} w(t) \\ v(t) \end{bmatrix},$$

where cyber-attacks $a_i^a(t)$, $a_i^s(t)$, $i=1,\ldots,n$ and the vectors describing the attacked coefficients f_i, h_i, $i=1,\ldots,n$ satisfy the following conditions:

$$\begin{aligned} &n \leqslant \max\{n_1, n_2\},\\ &a^a_{n_1+1}(t) = a^a_{n_1+2}(t) = \cdots = a^a_n(t) = 0 \quad \text{as } n = n_2 > n_1,\\ &a^s_{n_2+1}(t) = a^s_{n_2+2}(t) = \cdots = a^s_n(t) = 0 \quad \text{as } n = n_1 > n_2 \end{aligned}$$

and

$$\begin{aligned} &f_{n_1+1} = f_{n_1+2} = \cdots = f_n = 0 \quad \text{as } n = n_2 > n_1,\\ &h_{n_2+1} = h_{n_2+2} = \cdots = h_n = 0 \quad \text{as } n = n_1 > n_2. \end{aligned}$$

Using the frequency-domain description of the system, error dynamics (5.8) can be transformed into the following equation:

$$E(Q(s))X(s) = B(s), \tag{5.10}$$

where

$$E(Q(s)) = \begin{bmatrix} \bar{A} - sI & E(\bar{F}_1) & \cdots & E(\bar{F}_n) & \bar{E}_1 \\ C & E(\bar{H}_1) & \cdots & E(\bar{H}_n) & \bar{E}_2 \end{bmatrix}, \quad X(s) = \begin{pmatrix} e(s) \\ a_1(s) \\ \vdots \\ a_n(s) \\ d(s) \end{pmatrix}, \quad B(s) = \begin{pmatrix} 0 \\ r(s) \end{pmatrix}$$

and

$$E(\bar{F}_i) = [\rho_i B f_i \quad -\sigma_i \tilde{B} C h_i], \quad E(\bar{H}_i) = [0 \quad \sigma_i C h_i], \quad i = 1, \ldots, n.$$

Then equation (5.10) can be rewritten as

$$E(Q(s))X = \sum_{i=1}^{n} E(\tilde{Q}_i(s))X_i = \sum_{i=1}^{n} B_i(s),$$

where

$$E(\tilde{Q}_i(s)) = \begin{bmatrix} \dfrac{\bar{A} - sI}{n} & E(\bar{F}_i) & \dfrac{\bar{E}_1}{n} \\ \dfrac{\bar{C}}{n} & E(\bar{H}_i) & \dfrac{\bar{E}_2}{n} \end{bmatrix}, \quad X_i = \begin{pmatrix} e(s) \\ a_i(s) \\ d(s) \end{pmatrix}, \quad B_i(s) = \begin{pmatrix} 0 \\ r_i(s) \end{pmatrix}, \quad r(s) = \sum_{i=1}^{n} r_i(s).$$

Consider the following stochastic matrix:

$$E(Q_i(s)) = \begin{bmatrix} \bar{A} - sI & E(\bar{F}_i) & \bar{E}_1 \\ C & E(\bar{H}_i) & \bar{E}_2 \end{bmatrix}.$$

Since rank $E(\tilde{Q}_i(s)) = \text{rank}\, E(Q_i(s))$, we introduce the following auxiliary error dynamics:

$$\begin{aligned} \dot{e}(t) &= \bar{A}e(t) + \bar{F}_i a_i(t) + \bar{E}_1 d(t), \\ r(t) &= Ce(t) + \bar{H}_i a_i(t) + \bar{E}_2 d(t), \quad i = 1, \ldots, n \end{aligned} \tag{5.11}$$

and the auxiliary stochastic equations

$$E(Q_i(s))X_i = B_i(s), \quad i = 1, \ldots, n. \tag{5.12}$$

REMARK 5.4 In this work, we introduce the auxiliary mathematical 'tools' (5.11) and (5.12). Auxiliary error dynamics (5.11) represent the fact that the control system is only subjected to a stochastic cyber-attack $a_i(t)$ on the ith communication channel. Applying auxiliary equations (5.12), we can obtain the information of the residual $r_i(t)$ that is caused by the cyber-attack $a_i(t)$. In addition, the detector gain matrix $\tilde{B}$ can be obtained according to Lemma 4.1.

Now, applying the rank of the stochastic matrix, we obtain the following theorems.

THEOREM 5.1 For system (5.7), assume that all of these stochastic matrices $E(Q(s))$ and $E(Q_i(s))$ $(i = 1, \ldots, n)$ have full column normal ranks. All of these cyber-attacks $a_i(s)$ $(i = 1, \ldots, n,\ (0 \neq a_i(s) \in \bar{G}))$ as $s = z_0$ are undetectable, if and only if there exists $z_0 \in \mathbb{C}$, such that

$$\text{rank}\, E(Q(z_0)) < \dim(X(z_0)) \tag{5.13}$$

and

$$\text{rank}\, E(Q_i(z_0)) < \dim(X_i(z_0)), \quad i = 1, \ldots, n. \tag{5.14}$$

Herein, $\bar{G}$ is a set of undetectable cyber-attacks.

Proof. The proof of Theorem 5.1 straightforwardly follows the lines of the proof of Theorem 4.2. Therefore, the proof of Theorem 5.1 is omitted here. □

THEOREM 5.2 For system (5.7), assume that all of stochastic matrices $E(Q(s))$ and $E(Q_i(s))$ $(i = 1, \ldots, n)$ have full column normal ranks. All of these cyber-attacks $a_i(s)$ $(i = 1, \ldots, n,\ (0 \neq a_i(s) \in G))$ are detectable, if and only if the following conditions always hold for any $z_0 \in \mathbb{C}$:

$$\text{rank}\, E(Q(z_0)) = \dim(X(z_0)) \tag{5.15}$$

and

$$\text{rank}\, E(Q_i(z_0)) = \dim(X_i(z_0)), \quad i = 1, \ldots, n. \tag{5.16}$$

Herein, G is a set of detectable cyber-attacks.

Proof. The proof of Theorem 5.2 straightforwardly follows the lines of the proof of Theorem 4.3. Therefore, the proof of Theorem 5.2 is omitted here. □

According to Theorems 5.1 and 5.2, the following corollary can be obtained.

COROLLARY 5.1 For system (5.7), assume that all of stochastic matrices $E(Q(s))$ and $E(Q_i(s))$ $(i = 1, \ldots n)$ have full column normal ranks. If there exists $z_0 \in \mathbb{C}$, such that

$$\operatorname{rank} E(Q(z_0)) < \dim(X(z_0)), \tag{5.17}$$

then there are the following conclusions:

(1) the cyber-attack $a_i(z_0)$ $(0 \not\equiv a_i(s) \in G)$ is detectable, if and only if

$$\operatorname{rank} E(Q_i(z_0)) = \dim(X_i(z_0)); \tag{5.18}$$

(2) the cyber-attack $a_j(z_0)$ $(0 \not\equiv a_j(s) \in G)$ is undetectable, if and only if

$$\operatorname{rank} E(Q_j(z_0)) < \dim(X_j(z_0)). \tag{5.19}$$

6. Simulation results

In this section, we provide two simulation examples to illustrate the effectiveness of our results. In Example **??**, we consider an NCS under a stochastic cyber-attack and a stochastic noise. We detect the possible attack, which are launched on the actuator by hackers. In Example **??**, we consider a large-scale distributed networked water system that comprises of n identical connected subsystems. Moreover, each subsystem consists of four interconnected water tanks. We will also detect possible multiple cyber-attacks on a single subsystem.

EXAMPLE 6.1 Consider the following system that is subjected to a stochastic data deception attack on the actuator:

$$\begin{aligned} \dot{x}(t) &= Ax(t) + \alpha(t)Ba_k^a(t) + E_1 w(t), \\ x(0) &= x_0, \\ y(t) &= Cx(t). \end{aligned} \tag{6.1}$$

and with the following parameters:

$$A = \begin{bmatrix} -0.8 & 0 & 0.1 & 0 & 0 \\ 0 & -0.2 & 0 & -0.1 & 0 \\ 0 & 0 & -0.4 & 0 & 0 \\ 0 & 0 & 0 & -0.3 & 0 \\ 0.2 & 0 & 0.1 & 0 & -0.5 \end{bmatrix}, \quad B = \begin{bmatrix} 0.03 & 0.3 \\ 0 & 0 \\ 0 & 0.45 \\ -0.21 & 0.1 \\ 0.09 & 0 \end{bmatrix},$$

$$E_1 = \begin{bmatrix} 0.09 \\ -0.01 \\ 0.04 \\ -0.07 \\ 0.06 \end{bmatrix}, \quad C = \begin{bmatrix} 0.5 & 0 & 0 & 0 & 0 \\ 0 & 0.5 & 0 & 0 & 0 \\ 0 & 0 & 0.5 & 0 & 0 \end{bmatrix}.$$

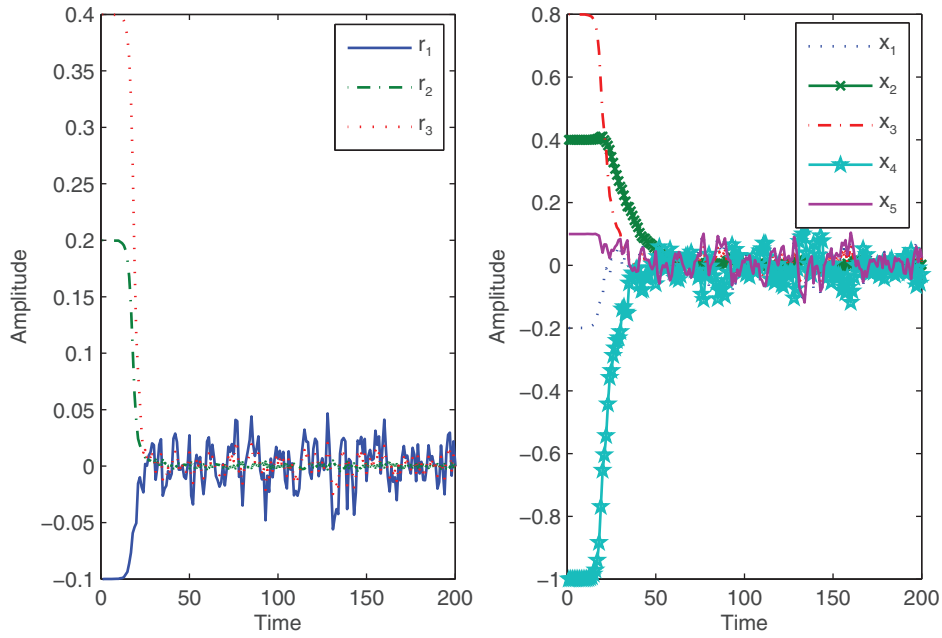

FIG. 2. The time responses of residual and system states under $w(t) \neq 0$ and $\alpha(t) = 0$.

Applying Lemma 4.1, the corresponding detector gain matrix is obtained as follows:

$$\tilde{B} = \begin{bmatrix} 0.6316 & 0 & 0.0826 \\ 0 & 3.5714 & 0 \\ 0.0961 & 0 & 1.2444 \\ 0 & -0.7143 & 0 \\ 0.0251 & 0 & 0.0304 \end{bmatrix}.$$

Set the initial conditions as $x(0) = [0.8, -0.5, -1, 0.2]^\top$ and $\tilde{x}(0) = [0, 0, 0, 0]^\top$. When the stochastic event $\alpha(t) = 0$ occur, the system is not subject to a cyber-attack. Figure 2 displays the time responses of the system states and the residual signal under the case of noise $w(t) \neq 0$ and $\alpha(t) = 0$, which shows that system (6.1) is robustly stable under the influence of noise $w(t)$ only. When the stochastic event $\alpha(t) = 1$ occur and the attacked probability $\rho = 0.8$, we can work out $\text{rank}(E(Q(s))) = 6$, and no z_0 exists such that $\text{rank}(E(Q(z_0))) < 6$, that is to say, for any z_0, $\text{rank}(E(Q(z_0)))$ has always full column rank. According to Theorem 4.3, the deception signal $a_k^a(t)$ is detectable. Figure 3(a) shows the deception signal $a_k^a(t)$ and stochastic noise signal, respectively. Figure 3(b) shows the time responses of the residual and system (6.1) under the deception signal $a_k^a(t)$. Figure 3(b) also demonstrates the system can not work normally under the cyber-attack. Simulation results underline that a cyber-attack can be effectively detected if the condition in Theorem 4.3 is satisfied.

EXAMPLE 6.2 Consider the large-scale distributed networked water system that comprises of n identical connected subsystems. Moreover, each subsystem consists of four interconnected water tanks, which is depicted in Fig. 4.

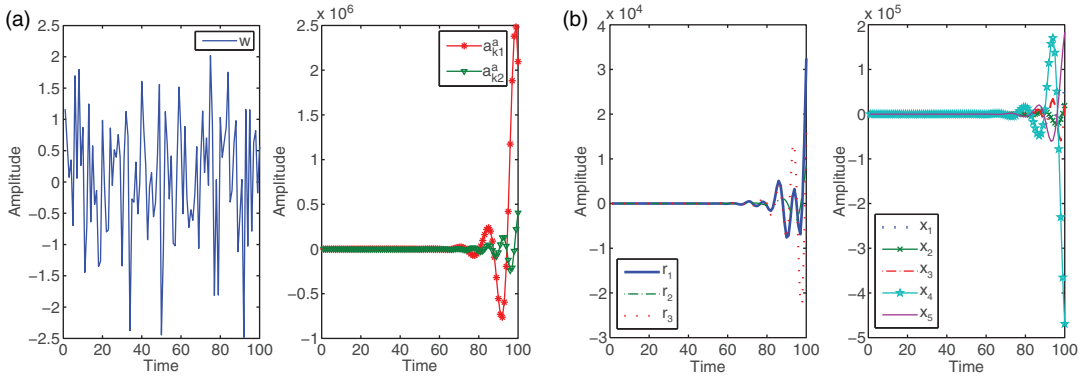

FIG. 3. The noise signal $w(t)$, deception attack signal $a_k^a(t)$ and the time responses of residual and plant states under deception signal $a_k^a(t)$.

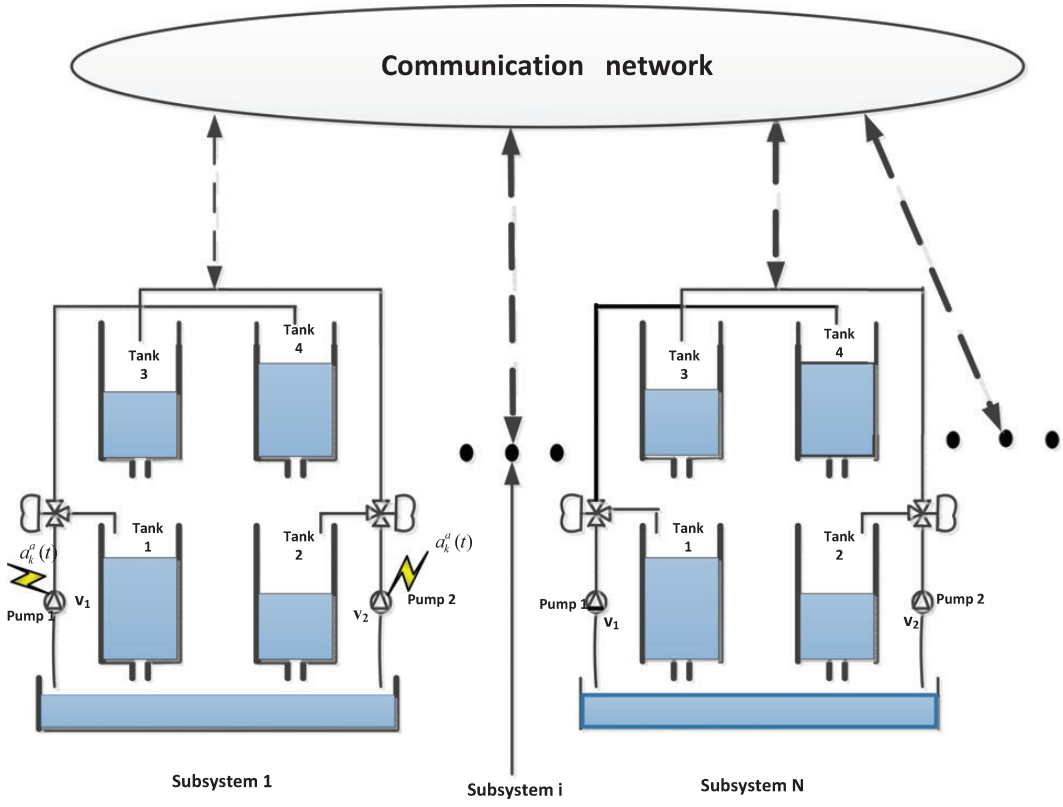

FIG. 4. A large-scale distributed networked water system.

Each subsystem in the large-scale distributed control system is used the model of the QTP in Johansson (2000). The dynamics of the QTP is the following non-linear model:

$$\begin{aligned}
\frac{\mathrm{d}h_1}{\mathrm{d}t} &= -\frac{a_1}{A_1}\sqrt{2gh_1} + \frac{a_3}{A_1}\sqrt{2gh_3} + \frac{\gamma_1 k_1}{A_1}\upsilon_1,\\
\frac{\mathrm{d}h_2}{\mathrm{d}t} &= -\frac{a_2}{A_2}\sqrt{2gh_2} + \frac{a_4}{A_2}\sqrt{2gh_4} + \frac{\gamma_2 k_2}{A_2}\upsilon_2,\\
\frac{\mathrm{d}h_3}{\mathrm{d}t} &= -\frac{a_3}{A_3}\sqrt{2gh_3} + \frac{(1-\gamma_2)k_2}{A_3}\upsilon_2,\\
\frac{\mathrm{d}h_4}{\mathrm{d}t} &= -\frac{a_4}{A_4}\sqrt{2gh_4} + \frac{(1-\gamma_1)k_1}{A_4}\upsilon_1,
\end{aligned} \tag{6.2}$$

where A_i is the cross-sectional area of Tank i; a_i is the cross-sectional area of the outlet hole of Tank i; h_i is the water level of Tank i; υ_i is the input voltage that is applied to Pump i; k_i is the proportional constant from the voltage υ_i to the corresponding flow. $\gamma_i \in (0,1)$ are related parameters that show if the flow to Tank 1 is $\gamma_1 k_1 \upsilon_1$, then the flow to Tank 4 is $(1-\gamma_1)k_1\upsilon_1$. Tank 2 and Tank 3 are treated in a similar way; g is the gravitational constant. The measured signals are $k_c h_1$ and $k_c h_2$. Applying linear transformation $x_i := h_i - h_i^0$ and $u_i = \upsilon_i - \upsilon_i^0$, the non-linear model of (6.2) is transformed into the following linear model:

$$\begin{aligned}
\dot{x} &= Ax + Bu,\\
y &= Cx.
\end{aligned} \tag{6.3}$$

In this example, we will detect possible cyber-attacks on the subsystem 1 that has the following parameters:

$$A = \begin{bmatrix} -0.0158 & 0 & 0.0256 & 0\\ 0 & -0.0109 & 0 & 0.0178\\ 0 & 0 & -0.0256 & 0\\ 0 & 0 & 0 & -0.0178 \end{bmatrix}, \quad B = \begin{bmatrix} 0.0482 & 0\\ 0 & 0.0350\\ 0 & 0.0775\\ 0.0559 & 0 \end{bmatrix},$$
$$C = \begin{bmatrix} 0.5 & 0 & 0 & 0\\ 0 & 0.5 & 0 & 0 \end{bmatrix}.$$

Assume that the subsystem 1 is subjected to two stochastic data deception attacks on the actuator, i.e.

$$\begin{cases} \alpha_1(t) \in \{0,1\}, \quad t \geqslant t_0,\\ f_1 = \begin{bmatrix} 1\\ 0 \end{bmatrix},\\ a_1^a(t) = b_1^a(t) \end{cases} \quad \text{and} \quad \begin{cases} \alpha_2(t) \in \{0,1\}, \quad t \geqslant t_0,\\ f_2 = \begin{bmatrix} 0\\ 1 \end{bmatrix},\\ a_2^a(t) = b_2^a(t) \end{cases} \tag{6.4}$$

the detector gain matrix can be obtained as follows:

$$\tilde{B} = \begin{bmatrix} 0.7852 & 0\\ 0 & 0.4766\\ 2.7432 & 0\\ 0 & 1.4367 \end{bmatrix}.$$

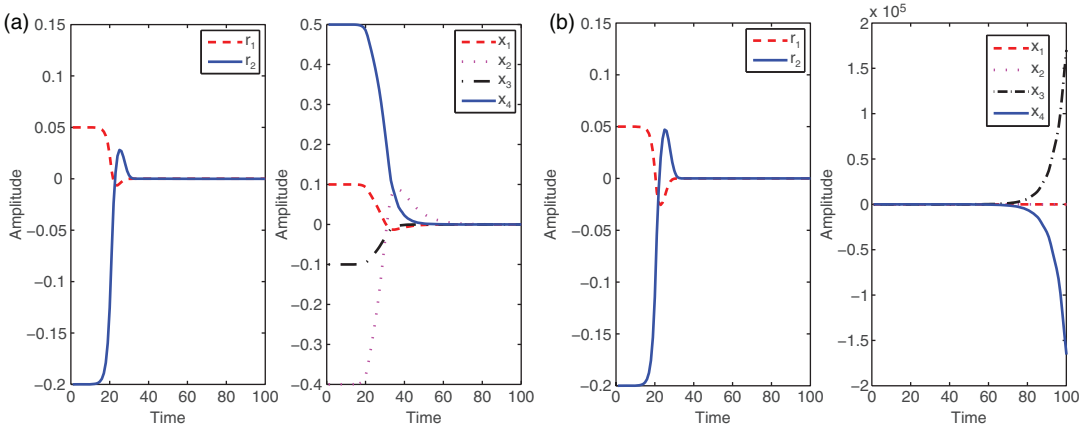

FIG. 5. (a) The time responses of residual and the system state without attacks and (b) the time responses of residual and the system state under attacks $a_1^a(t)$ and $a_2^a(t)$.

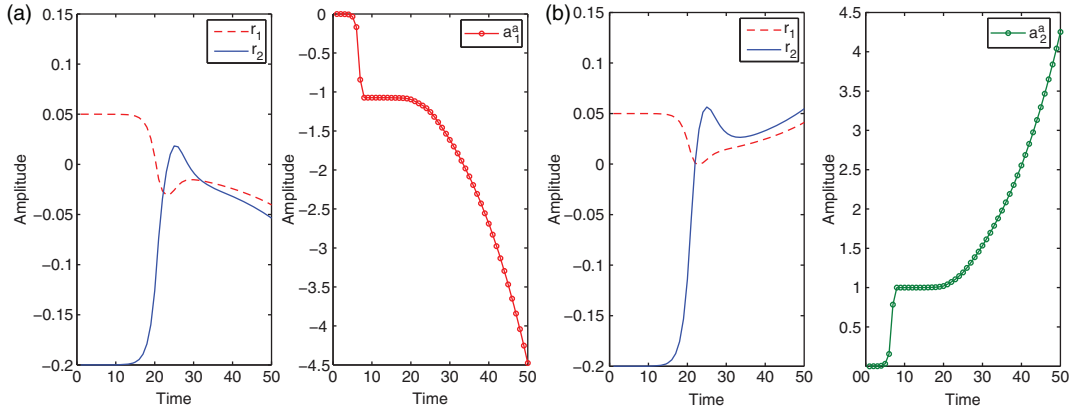

FIG. 6. The time responses of residual under the attack $a_1^a(t)$ and $a_2^a(t)$, respectively, and the attack signal $a_1^a(t)$ and $a_2^a(t)$.

We set the initial conditions to $\tilde{x}(0) = [0, 0, 0, 0]^\top$ and $x(0) = [0.1, -0.4, -0.1, 0.5]^\top$. When the stochastic events $\alpha_1(t) = \alpha_2(t) = 0$ occur, Fig. 5(a) displays that the system (6.3) is asymptotically stable. When the stochastic events $\alpha_1(t) = \alpha_2(t) = 1$ occur and the attacked probabilities are $\rho_1 = 0.8$, $\rho_2 = 0.5$, we have the stochastic matrix $\text{rank}(E(Q(s))) = 6$, however, there exists a $z_0 = 0.0127$ such that $\text{rank}\, E(Q(z_0)) = 5$ and $\text{rank}(E(Q_i(z_0))) = 5$ $(i = 1, 2)$. Aiming at two different control channels, it is possible for the hacker to launch two stochastic data deception attacks as follows:

$$b_1^a(t) = -1.074e^{0.0127t}, \quad b_2^a(t) = e^{0.0127t}$$

such that the transfer function from attacks to residual is zero. Therefore, it is difficult to detect these stealthy attacks. Figure 5(b) displays the time responses of the residual and the system state under the two attacks $a_1^a(t)$ and $a_2^a(t)$, which shows that these attacks as $s = z_0 = 0.0127$ originally could not be detected. However, applying auxiliary tools (5.11), (5.12) and according to Corollary 5.1, these attacks

now also can be detected. Figure 6(a) shows the response of the residual under attack $a_1^a(t)$ and the attack signal $a_1^a(t)$. Figure 6(b) shows the responses of residual under attack $a_2^a(t)$ and the attack signal $a_2^a(t)$. Obviously, applying Corollary 5.1, the two stochastic data deception attacks can be detected effectively.

7. Conclusion

This paper proposes algebraic detection schemes for NCSs under single stochastic cyber-attack and multiple stochastic cyber-attacks, respectively. It is a relatively simple and straightforward detection approach. Based on the frequency-domain transformation technique and traditional linear algebra theory, an effective anomaly detectors is derived. The main work is focused on novel cyber-attack detection schemes that allow the detection of single or multiple stochastic attacks in order to protect control systems against a wide range of possible attack models. The proposed schemes are applied to NCSs that are subject to the stochastic cyber-attacks. Simulation results underline that the proposed attack detection approaches are effective and feasible.

Funding

This work was supported by the Fonds National de la Recherche, Luxembourg, under the project CO11/IS/1206050 (SeSaNet) and the National Natural Science Foundation of China under Grant 61273222.

References

Amin, S., Galina, A, Schwartz, S. & Sastry, S. (2013) Security of interdependent and identical networked control systems. *Automatica*, **49**, 186–192.

Amin, S., Litrico, X., Sastry, S. S. & Bayen, A. M. (2013) Cyber security of water SCADA systems: (I) analysis and experimentation of stealthy deception attacks. *IEEE Trans. Control Syst. Technol.*, **21**, 1963–1970.

Andersson, G., Esfahani, P. M., Vrakopoulou, M., Margellos, K., Lygeros, J., Teixeira, A., Dán, G., Sandberg, H. & Johansson, K. H. (2011) Cyber-security of SCADA systems. *Sess. Cyber-Phys. Syst. Secur. A Smart Grid Environ.,* 1–2.

Anjali, S. & Ramesh, C. J. (2010) Dual-level attack detection and characterization for networks under DDoS. *International Conference on Availability, Reliability and Security*, Krakow, pp. 9–16.

Eliades, D. G. & Polycarpou, M. M. (2010) A fault diagnosis and security framework for water systems. *IEEE Trans. Control Syst. Technol.*, **18**, 1254–1265.

Hashim, F., Kibria, M. R. & Jamalipour, A. (2008) Detection of DoS and DDoS attacks in NGMN using frequency domain analysis. *Proceedings of APCC2008*.

Johansson, K. H. (2000) The quadruple-tank process: a multivariable laboratory process with an adjustable zero. *IEEE Trans. Control Syst. Technol.*, **8**, 456–465.

Li, Y. M., Voos, H. & Darouach, M. (2014a) Robust H_∞ fault estimation for control systems under stochastic cyber-attacks. *33rd China Control Conference*, Nanjing, China, pp. 3124–3129.

Li, Y. M., Voos, H., Darouach, M. & Hua, C. (2015) An algebraic detection approach for control systems under multiple stochastic cyber-attacks. *IEEE/CAA Journal of Automatica Sinica* (in press).

Li, Y. M., Voos, H., Rosich, A. & Darouach, M. (2014b) A stochastic cyber-attack detection scheme for stochastic control systems based on frequency-domain transformation technique. *The 8th International Conference on Network and System Security*, Xian, China, pp. 209–222.

Liu, Y., Reiter, M. K. & Ning, P. (2009) False data injection attacks against state estimation in electric power grids. *ACM Conference on Computer and Communications Security*, Chicago, USA, pp. 21–32.

METKE, A. R. & EKL, R. L. (2010) Security technology for smart grid networks. *IEEE Trans. Smart Grid*, **1**, 99–107.

MO, Y. & SINOPOLI, B. (2010) False data injection attacks in control systems. *First Workshop on Secure Control Systems*, Stockholm, Sweden.

MOHSENIAN-RAD, A. H. & GARCIA, A. L. (2011) Distributed internet-based load altering attacks against smart power grids. *IEEE Trans. Smart Grid*, **2**, 667–674.

MOORE, D., PAXSON, V., SAVAGE, S., SHANNON, C., STANIFORD, S. & WEAVER, N. (2003) Inside the Slammer worm. *IEEE Secur. Priv.*, **1**, 33–39.

New 'cyber attacks' hit S Korea, http://news.bbc.co.uk/2/hi/asia-pacific/8142282.stm.

NIMDA WORM. (2001) http://www.cert.org/advisories/CA-2001-26.html.

PASQUALETTI, F. (2012) Secure control systems: a control-theoretic approach to cyber-physical security. *A Dissertation for the degree of Doctor of Philosophy in Mechanical Engineering*.

PASQUALETTI, F., BICHI, A. & BULLO, F. (2012) Consensus computation in unreliable networks: a system theoretic approach. *IEEE Trans. Auto. Control*, **56**, 90–104.

ROSICH, A., VOOS, H., LI, Y. M. & DAROUACH, M. (2013) A model predictive approach for cyber-attack detection and mitigation in control systems. *IEEE 52nd Annual Conference on Decision and Control*, Italy, pp. 6621–6626.

SLAY, J. & MILLER, M. (2007) Lessons learned from the Maroochy water breach. *Critical Infrastructure Protection*, **253**, 73–82.

SRIDHAR, S., HAHN, A. & GOVINDARASU, M. (2012) Cyber-physical system security for the electric power grid. *Proc. IEEE*, **99**, 1–15.

SUNDARAM, S. & HADJICOSTIS, C. (2011) Distributed function calculation via linear iterative strategies in the presence of malicious agents. *IEEE Trans. Auto. Control*, **56**, 1495–1508.

TANG, Y., QIAN, F., GAO, H. & KURTHS, J. (2014) Synchronization in complex networks and its application—a survey of recent advances and challenges. *Ann. Rev. Control*, **38**, 184–198.

TEIXEIRA, A., PÉREZ, D., SANDBERG, H. & JOHANSSON, K. H. (2012) Attack models and scenarios for networked control systems. *HiCoNS'12*, Beijing, China, pp. 55–64.

TEIXEIRA, A., SANDBERG, H. & JOHANSSON, K. H. (2010) Networked control systems under cyber attacks with applications to power networks. *Proceedings of the American Control Conference*, pp. 3690–3696.

WEIMER, J., KAR, S. & JOHANSSON, K. H. (2012) Distributed detection and isolation of topology attacks in power networks. *HiCoNS 12*, Beijing, China, pp. 65–71.

WOLF, M. & DALY, P. W. (2009) *Security Engineering for Vehicular IT Systems*. Wiesbaden: Vieweg-Teubner/GWV Fachverlage GmbH.

ZHOU, K., DOYLE, J. C. & GLOVER, K. (1996) *Robust and Optimal Control*. Upper Saddle River, NJ, USA: Prentice-Hall Inc.