A Stochastic Cyber-Attack Detection Scheme for Stochastic Control Systems Based on Frequency-Domain Transformation Technique

Yumei Li[1,⋆], Holger Voos[1], Albert Rosich[1], and Mohamed Darouach[2]

[1] Interdisciplinary Centre for Security Reliability and Trust (SnT), University of Luxembourg, Luxembourg
[2] Centre de la Recherche en Automatique de Nancy (CRAN), Universite de Lorraine, France
{yumei.li@uni.lu,Holger.Voos@uni.lu,albert.rosich@uni.lu, mohamed.darouach@univ-lorraine.fr}

Abstract. Based on frequency-domain transformation technique, this paper proposes an attack detection scheme for stochastic control systems under stochastic cyber-attacks and disturbances. The focus is on designing an anomaly detector for the stochastic control systems. First, we construct a model of stochastic control system with stochastic cyber-attacks which satisfy the Markovian stochastic process. And we also introduced the stochastic attack models that a control system is possibly exposed to. Next, based on the frequency-domain transformation technique and linear algebra theory, we propose an algebraic detection scheme for a possible stochastic cyber-attack. We transform the detector error dynamic equation into an algebraic equation. By analyzing the rank of the stochastic matrix $E(Q(z_0))$ in the algebraic equation, residual information is obtained and anomalies in the stochastic system are detected. In addition, sufficient and necessary conditions guaranteeing the detectability of the stochastic cyber-attacks are obtained. The presented detection approach in this paper is simple, straightforward and more ease to implement. Finally, the results are applied to some physical systems that are respectively subject to a stochastic data denial-of-service (DoS) attack and a stochastic data deception attack on the actuator. The simulation results underline that the detection approach is efficient and feasible in practical application.

Keywords: Cyber-attacks detection, Stochastic control system, Stochastic DoS attack, Stochastic data deception attack.

1 Introduction

As networks become ubiquitous and more and more industrial control systems are also connected to open public networks, control systems are increasingly exposed to cyber-attacks [1]-[4]. Some well-known examples are the Nimda attack [2], the SQL Slammer attack [3], the July 2009 cyber-attacks [4]. A control system is vulnerable to these

⋆ This work was supported by the Fonds National de la Recherche, Luxembourg, under the project CO11/IS/1206050 (SeSaNet)

M.H. Au et al. (Eds.): NSS 2014, LNCS 8792, pp. 209–222, 2014.

threats and successful attacks on control systems can cause serious consequences which may lead to the loss of vital societal function, financial loss and even loss of life [5]. Therefore, these attacks should be detected as soon 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. [6]-[21]). For example, S. Amin [6] and D. G. Eliades [13] did research on the cyber security of water systems. A.R. Metke [14], S. Sridhar [15], A.H. Mohsenian-Rad [16] and F. Pasqualetti [21] focus on cyber-attacks on smart grid systems. While cyber-attacks in conventional IT systems are only influencing information, cyber-attacks on control systems are changing physical processes and hence the real world [17]. Previous methods and tools used to protect traditional information technology against cyber-attacks might finally not completely prevent successful intrusion of malware in the control system. Therefore, new approaches are needed. Although networked control systems are protected by information technology (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 [17]-[20]. However, the existing detection approaches [17]-[20] are not yet sufficient to cope with complex cyber-attacks on a control process, which motivates our research in this area.

This paper presents an algebraic detection approach for a stochastic control system under stochastic cyber-attacks and disturbances. 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 the stochastic system under stochastic cyber-attacks is derived. The main contributions in the paper are as follows. First, we construct a model of stochastic control system with stochastic cyber-attacks which satisfy the Markovian stochastic process. And we also introduced the stochastic attack models that a control system is possibly exposed to. Next, based on the frequency-domain transformation technique and linear algebra theory, we propose an algebraic attack detection scheme for the control system subject to stochastic cyber-attacks and disturbances. F. Hashim [18] also use a frequency domain analysis in the detection of DoS attacks, he proposes the detection algorithm by investigating the frequency spectrum distribution of the network traffic. However, we transform the detector error dynamic equation into an algebraic equation, which make the discussion of the problem simpler and more straightforward. Moreover, we extend the idea in [22] to control systems with stochastic disturbances and apply it to detect a possible stochastic attack. Here, we consider the possible cyber-attacks as the non-zero solutions of the algebraic equation and the residual as its constant vector. By analyzing the rank of stochastic matrix $E\left(Q(z_0)\right)$ in the algebraic equation, the residual information is obtained. Further, based on the rank of $E(Q(z_0))$ and the obtained residual information, we are able to determine the detectability of the possible cyber-attacks. Some sufficient

and necessary conditions are obtained, which guarantee that a stochastic cyber-attack is detectable or undetectable. In addition, by using the linear matrix inequation (LMI) algorithm, we also propose an approach for determining the detector gain matrix. Finally, the obtained results are applied to some physical systems that are respectively subject to stochastic data DoS attacks and stochastic data deception attacks on the actuator. Two simulation examples are given to illustrate the effectiveness of the obtained results. In example 1, we discuss a control system that is subjected to a stochastic data deception attack and disturbance. In example 2, we use the laboratory process in [23] that consists of four interconnected water tanks (QTP). Simulation results underline that the proposed attack detection approach is effective and feasible in practical application.

The paper is organized as follows. In section II, the system models and the models of stochastic attacks are introduced. In section III, the main results and proofs are presented. We design an anomaly detector for a control system under stochastic cyber-attacks and disturbances. Some sufficient and necessary conditions guaranteeing the detectability of cyber-attacks are obtained. In section IV, we provide two simulation examples to demonstrate the effectiveness and feasibility of the obtained results. Finally, some conclusions are discussed in Section V.

2 Problem Formulation

Consider the following stochastic control system:

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) + \alpha(t)F_1 a_k^a(t) + E_1\omega(t) \\ x(0) &= x_0 \\ y(t) &= Cx(t) + \beta(t)F_2 a_k^s(t) + E_2\nu(t) \end{aligned} \tag{1}$$

where $x(t) \in R^n$ is the state vector. x_0 is the initial state, $y(t) \in R^m$ is the measurement output, $u(t) \in R^r$ is the known input vector. $a_k^a(t) \in R^r$ denotes the actuator cyber-attack or the physical attack and $a_k^s(t) \in R^m$ denotes the sensor cyber-attack. $\omega(t)$ and $\nu(t)$ are systems noise and process noise, respectively. A, B, F_1, E_1,and C, F_2, 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

$$\begin{aligned} E\{\alpha(t)\} &= \Pr ob\{\alpha(t) = 1\} = \rho \\ E\{\beta(t)\} &= \Pr ob\{\beta(t) = 1\} = \sigma. \end{aligned} \tag{2}$$

Where 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 $\beta(t) = 0$) implies 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. Assuming $\alpha(t)$ and $\beta(t)$ are independent stochastic variables and satisfy

$$E\{\alpha(t)\beta(t)\} = E\{\alpha(t)\}E\{\beta(t)\}. \tag{3}$$

Further, assuming $\alpha(t)$ and $\beta(t)$ are independent of measurement noises $\omega(t), \nu(t)$ and the initial state x_0. Generally, cyber-attacks targeting control systems mainly include denial-of-service (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 (1).

2.1 Modeling Stochastic Data Denial-of-Service Attacks

In stochastic data DoS attacks, the objective of the adversary is to prevent the actuator from receiving control commands or the controller from receiving sensor measurements. Therefore, by jamming the communication channels, compromising devices and preventing them from sending data, attacking the routing protocols, flooding the communication network with random data and so on, the adversary can launch a stochastic data DoS attack that satisfies Markovian stochastic processes. Using the general framework (1), a stochastic DoS attack on the actuator and on the sensors can be respectively modelled as

$$\begin{cases} \alpha(t) \in \{0,1\}, t \geq t_0 \\ F_1 = B \\ a_k^a(t) = -u(t) \end{cases} \text{(I)} \quad \text{and} \quad \begin{cases} \beta(t) \in \{0,1\}, t \geq t_0 \\ F_2 = C \\ a_k^s(t) = -x(t) \end{cases} \text{(II)}$$

2.2 Modeling Stochastic Data Deception Attacks

In stochastic data deception attacks, the adversary attempts to prevent the actuator or the sensor from receiving an integrity data, therefore, he sends false information $\widetilde{u}(t) \neq u(t)$ or $\widetilde{y}(t) \neq y$ from controllers or sensors. The false information can include: a wrong sender identity, an incorrect sensor measurement or an incorrect control input; an incorrect time when a measurement was observed, or inject a bias data that cannot be detected in the system. The adversary can launch these attacks by obtaining the secret keys or by compromising some controllers or sensors. A stochastic data deception attack on the actuator and on the sensors can be modelled as

$$\begin{cases} \alpha(t) \in \{0,1\}, t \geq t_0 \\ F_1 = B \\ a_k^a(t) = -u(t) + b_k^a(t) \end{cases} \text{(III)} \quad \text{and} \quad \begin{cases} \beta(t) \in \{0,1\}, t \geq t_0 \\ F_2 = C \\ a_k^s(t) = -x(t) + b_k^s(t) \end{cases} \text{(IV)}$$

where $b_k^a(t)$ and $b_k^s(t)$ are deceptive data that the adversary attempts to launch on the actuator and the sensor, respectively.

Especially, when the adversary attempts to launch a detective data $b_k^a(t)$ (or $b_k^s(t)$) that makes the transfer function $G_{b_k^a r}(s)$ (or $G_{b_k^s r}(s)$) is zero, a zero dynamic attack occurs. Where $G_{b_k^a r}(s)$ (or $G_{b_k^s r}(s)$) is the transfer function from the zero attack signal to residual signal. Obviously, a zero dynamic attack is undetectable. A stochastic zero dynamic attack on the actuator and sensor can be respectively modelled as

$$\begin{cases} \alpha(t) \in \{0,1\}, t \geq t_0 \\ F_1 = B \\ a_k^a(t) = b_k^a(t) \\ G_{b_k^a r}(s) = 0 \end{cases} \text{(V)} \quad \text{and} \quad \begin{cases} \beta(t) \in \{0,1\}, t \geq t_0 \\ F_2 = C \\ a_k^s(t) = b_k^s(t) \\ G_{b_k^s r}(s) = 0 \end{cases} \text{(VI)}$$

3 Stochastic Cyber-Attack Detection Scheme Based on Frequency-Domain Description

In this section, our objective is the anomaly detection. We assume 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 sequel of the paper because they do not affect to the residual when there are no modeling errors in the system transfer matrix. Therefore, the system can be rewritten (1) as follows

$$\begin{aligned} \dot{x}(t) &= Ax(t) + \alpha(t)F_1 a_k^a(t) + E_1\omega(t) \\ x(0) &= x_0 \\ y(t) &= Cx(t) + \beta(t)F_2 a_k^s(t) + E_2\nu(t). \end{aligned} \tag{4}$$

We assume the following anomaly detector

$$\begin{aligned} \dot{\widetilde{x}}(t) &= A\widetilde{x}(t) + \widetilde{B}r(t) \\ \widetilde{x}(0) &= 0 \\ r(t) &= y(t) - C\widetilde{x}(t) \end{aligned} \tag{5}$$

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

We consider system (4) and detector (5). Let

$$e(t) = x(t) - \widetilde{x}(t)$$

then we obtain the following anomaly detector error dynamic

$$\begin{aligned} \dot{e}(t) &= \overline{A}e(t) + \overline{B}a_k(t) + \overline{E}_1 d(t) \\ r(t) &= Ce(t) + \overline{D}a_k(t) + \overline{E}_2 d(t) \end{aligned} \tag{6}$$

with the following matrices

$$\begin{aligned} &\overline{A} = (A - \widetilde{B}C),\ \overline{B} = \left[F_1\alpha(t)\ -\beta(t)\widetilde{B}F_2\right],\ \overline{E}_1 = \left[E_1\ -\widetilde{B}E_2\right] \\ &\overline{D} = \left[0\ F_2\beta(t)\right],\ \overline{E}_2 = \left[0\ E_2\right] \end{aligned} \tag{7}$$

and the vectors

$$a_k(t) = \begin{bmatrix} a_k^a(t) \\ a_k^s(t) \end{bmatrix}, d(t) = \begin{bmatrix} w(t) \\ v(t) \end{bmatrix}, d_1(t) = \begin{bmatrix} a_k(t) \\ d(t) \end{bmatrix}. \tag{8}$$

First, we give the definition of an undetectable cyber-attack on control systems which will be used in the sequel of the paper.

Definition 1. For the stochastic control system (4) and the detector (5), if a cyber-attack $a_k(t)$ on the system (4) leads to the residual $r(t)$ of the measurement output equal to zero, then the attack is undetectable.

Before presenting the main results, we first give the following lemmas that can be used to determine the detector gain matrix.

Lemma 1. [8] The error dynamic (6) with $d_1(t) = 0$ is asymptotically stable, if there exists symmetric positive definite matrix $P > 0$ and matrix X such that the following LMI holds

$$\Lambda = A^T P + PA - C^T X^T - XC < 0. \tag{9}$$

When the LMI is solvable, the detector gain matrix is given by $\widetilde{B} = PX$.

Next, based on a frequency-domain description, we transform the error dynamic (6) into the following algebraic equation

$$Q(s)X(s) = B(s) \tag{10}$$

where

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

Remark 1. Here, due to the cyber-attack $a_k(t)$ is a stochastic signal, matrices $\overline{B}$ and $\overline{D}$ are the resulting stochastic matrices, correspondingly, the system matrix $Q(s)$ is a stochastic matrix. In order to obtain effective results, we introduce $E(Q(s))$ that is a mathematical expectation of the stochastic matrix $Q(s)$ and

$$\begin{aligned} E\left(Q(s)\right) &= E\begin{bmatrix} (A - \widetilde{B}C) - sI & F_1\alpha(t) & -\beta(t)\widetilde{B}F_2 & E_1 & -\widetilde{B}E_2 \\ C & 0 & \beta(t)F_2 & 0 & E_2 \end{bmatrix} \\ &= \begin{bmatrix} (A - \widetilde{B}C) - sI & \rho F_1 & -\sigma\widetilde{B}F_2 & E_1 & -\widetilde{B}E_2 \\ C & 0 & \sigma F_2 & 0 & E_2 \end{bmatrix}. \end{aligned}$$

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

Theorem 1. For the system (4), assume that the expectation of the stochastic matrix $E(Q(s))$ has full column normal rank. The cyber-attack $a_k(t)$ $(0 \neq a_k(t) \in \overline{G})$ as $t = z_0$ is undetecable, if and only if there exists $z_0 \in \mathbb{C}$, such that

$$E\left(Q(z_0)\right)Y(z_0) = 0. \tag{11}$$

Where

$$\begin{aligned} E\left(Q(z_0)\right) &= \begin{bmatrix} (A - \widetilde{B}C) - z_0 I & \rho F_1 & -\sigma\widetilde{B}F_2 & E_1 & -\widetilde{B}E_2 \\ C & 0 & \sigma F_2 & 0 & E_2 \end{bmatrix} \\ Y^T(z_0) &= \left(e(z_0) \; a_k^a(z_0) \; a_k^s(z_0) \; w(z_0) \; v(z_0) \right)^T \end{aligned}$$

$\overline{G}$ is a set of undetectable cyber-attacks and the detector gain matrix $\widetilde{B} = PX$ is given by Lemma 1.

Proof. (if) The proof of the sufficiency is obvious. If there is a $z_0 \in \mathbb{C}$ such that (11) holds for all $a_k(z_0) \in \overline{G}$, it becomes obvious that the equation (10) is homogeneous.

Therefore, the output residual $r(z_0) = 0$ and the cyber-attack $a_k(t)$ as $t = z_0$ is undetectable.

(only if) Assume that the cyber-attack $a_k(t)$ as $t = z_0$ is undetectable and since

$$E(Q(s)) = E\begin{bmatrix} \overline{A} - sI & \overline{B} & \overline{E}_1 \\ \overline{C} & \overline{D} & \overline{E}_2 \end{bmatrix}$$

has full column normal rank, then by the definition 1, there must exist a $z_0 \in \mathbb{C}$ such that the residual $r(z_0) = 0$ and

$$E\left(Q(z_0)\right)X(z_0) = 0. \tag{12}$$

Substituting (7) into (12), we obtain (11). The proof of Theorem is completed.

From Theorem 1, we can obtain the following corollary:

Corollary 1. For the system (4), assume that the expectation of the stochastic matrix $E(Q(s))$ has full column normal rank. The cyber-attack $a_k(t)$ $(0 \neq a_k(z_0) \in \overline{G})$ as $t = z_0$ is an undetectable zero dynamic attack, if there exists $z_0 \in \mathbb{C}$ and $e_0 \neq 0$, such that

$$\begin{bmatrix} (A - \widetilde{B}C) - z_0 I & \rho F_1 & -\sigma\widetilde{B}F_2 \\ C & 0 & \sigma F_2 \end{bmatrix} \begin{pmatrix} e_0 \\ a_0^a \\ a_0^s \end{pmatrix} = 0. \tag{13}$$

Where $e_0 = e(0)$ is an error state zero direction associated with z_0, a_0^a and a_0^s are zero dynamics attack directions on the actuator and the sensor, respectively. Under this condition, we can obtain the zero attack policy as $a_k(t) = \begin{pmatrix} a_0^a \\ a_0^s \end{pmatrix} e^{z_0 t}$ such that the transfer function $G_{a_k^a r}(s) = 0$ and $G_{a_k^s r}(s) = 0$.

Corollary 1 is a consequence of Theorem 1.

Theorem 2. For the system (4), assume that the expectation of the stochastic matrix $E\left(Q(s)\right)$ has full column normal rank. The cyber-attack $a_k(t)$ $(0 \neq a_k(t) \in \overline{G})$ as $t = z_0$ is undetectable, if and only if there exists $z_0 \in \mathbb{C}$ such that

$$rankE(Q(z_0)) < dim(Y(z_0)). \tag{14}$$

Where $dim(Y(z_0))$ is the dimension of vector $Y(z_0)$.

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

$$rankE(Q(z_0)) < dim(Y(z_0)).$$

It becomes obvious that z_0 is an invariant zero [22] of the detector error dynamic(6). Then by Theorem 1, the cyber-attack $a_k(t)$ as $t = z_0$ is undetectable.

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

$$E(Q(z_0))Y(z_0) = B(z_0) \tag{15}$$

is a homogeneous equation, i.e.

$$E(Q(z_0))Y(z_0) = 0. \tag{16}$$

If we assume

$$rankE(Q(z_0)) = dim(Y(z_0))$$

then the homogeneous equation (16) has a zero as its unique solution. However, this is contradictory to the condition that

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

is a solution of (16). Therefore the assumption is false, only

$$rankQ(z_0) < dim(Y(z_0))$$

is true. This finally completes the proof of Theorem 2.

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

Theorem 3. For the system (4), assume that the expectation of stochastic matrix $E(Q(s))$ has full column normal rank. The cyber-attack $a_k(t)$ $(0 \neq a_k(t) \in G)$ is detectable, if and only if the following condition

$$rankE(Q(z_0)) = dim(Y(z_0)) \tag{17}$$

always holds for any $z_0 \in \mathbb{C}$. Where G is a set of detectable cyber-attacks, $dim(Y(z_0))$ is the dimension of vector $Y(z_0)$.

Proof. The proof of the Theorem 3 is similar to that of the Theorem 2, therefore, we omit it.

Actually, the Theorem 3 is equivalent to the following corollary.

Corollary 2. For the system (4), assume that the expectation of stochastic matrix $E(Q(s))$ has full column normal rank. The cyber-attack $a_k(t)$ $(0 \neq a_k(t) \in G)$ is detectable, if and only if no $z_0 \in \mathbb{C}$ exists such that

$$rankE(Q(z_0)) < dim(Y(z_0)) \tag{18}$$

4 Simulation Results

In this section, we provide two simulation examples to illustrate the effectiveness of the obtained results.

Example 1. Consider the following system that is subjected to a stochastic data deception attack (III)

$$\begin{aligned} \dot{x}(t) &= Ax(t) + \alpha(t)Ba_k^a(t) + E_1\omega(t) \\ x(0) &= x_0 \\ y(t) &= Cx(t). \end{aligned} \tag{19}$$

and with the following parameters:

$$A = \begin{bmatrix} -0.9 & 0 & 0.1 & 0 \\ 0 & -0.2 & 0 & -0.1 \\ 0 & 0 & -0.4 & 0 \\ 0 & 0 & 0 & -0.3 \end{bmatrix}, B = \begin{bmatrix} 0.03 \\ 0 \\ 0 \\ 0.09 \end{bmatrix}, E_1 = \begin{bmatrix} 0 \\ 0.04545 \\ 0.09090 \\ 0 \end{bmatrix}, C = \begin{bmatrix} 0.5 & 0 & 0 & 0 \\ 0 & 0.5 & 0 & 0 \end{bmatrix}.$$

Applying the Lemma 1, the corresponding detector gain matrix is obtained as follows

$$\widetilde{B} = \begin{bmatrix} 0.58890 & 0 \\ 0 & 3.5714 \\ 0.0981 & 0 \\ 0 & -0.7143 \end{bmatrix}.$$

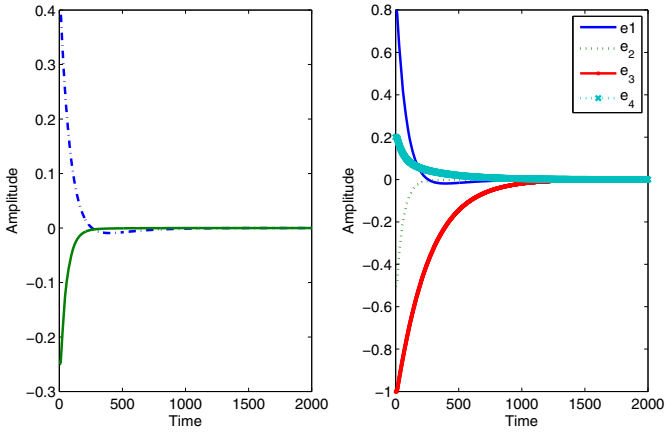

Fig. 1. The time response of residual and error dynamic under $a_k^a(t) = 0$ and $\omega(t) = 0$

Set the initial conditions as $x(0) = [0.8, -0.5, -1, 0.2]^T$ and $\widetilde{x}(0) = [0, 0, 0, 0]^T$. When the stochastic event $\alpha(t) = 0$, the system is not subject to a cyber-attack, i.e. $a_k^a(t) = 0$. The error dynamic without stochastic attacks and noises should be asymptotically stable according to Lemma 1. Fig.1. displays the time response of the residual signal and the error dynamic under $a_k^a(t) = 0$ and $\omega(t) = 0$. Fig.2. displays the time response of the system states and the residual signal under noise $\omega(t) \neq 0$ and attack $a_k^a(t) = 0$. These simulation results show that the system (19) is stable when the attack signal $a_k^a(t) = 0$.

When the stochastic event $\alpha(t) = 1$ and the attacked probability $\rho = 0.8$, the stochastic matrix $rank(E(Q(s))) = 6$, and no z_0 exists such that $rank(E(Q(z_0))) < 6$, that is to say, for any z_0, $rank(E(Q(z_0)))$ has always full column rank. According to Theorem 3, the deception signal $a_k^a(t)$ is detectable. Fig.3. shows the deception signal $a_k^a(t)$ and stochastic noise signal, respectively. Fig.4. shows the time response of the residual and

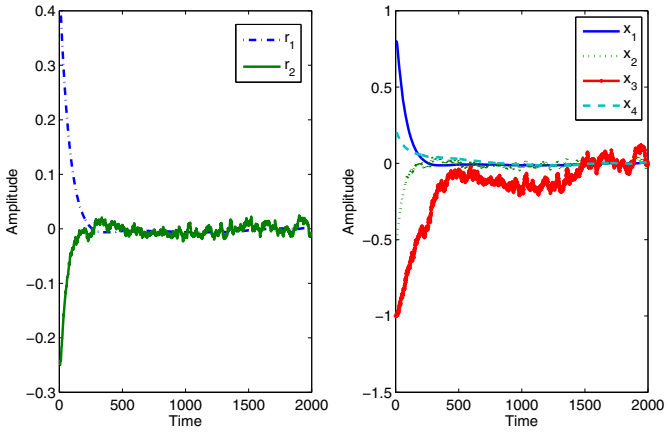

Fig. 2. The time response of residual and system states under $\omega(t) \neq 0$ and $a_k^a(t) = 0$

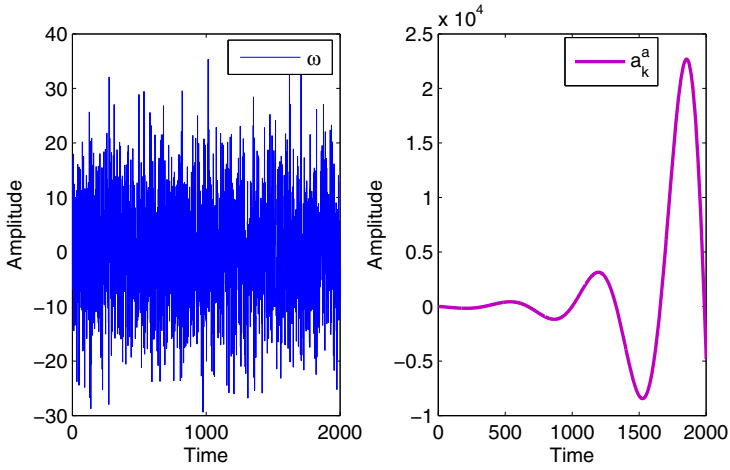

Fig. 3. The noise signal ω (t) and deception attack signal $a_k^a(t)$

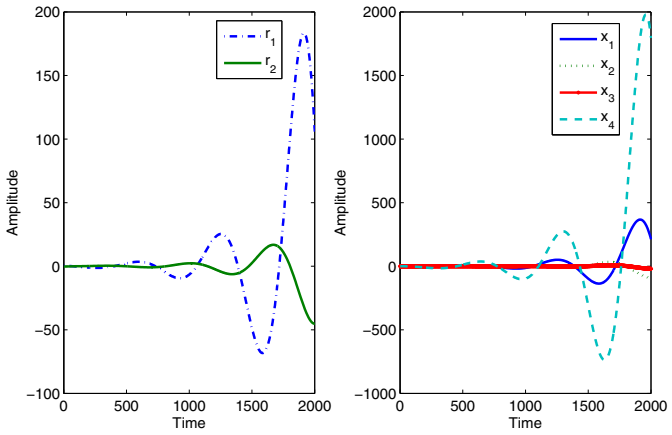

Fig. 4. The time response of residual and plant states under deception signal $a_k^a(t)$

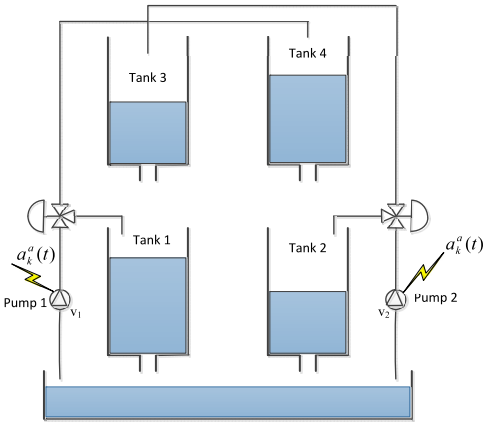

Fig. 5. Quadruple-tank water system

system (19) under the deception signal $a_k^a(t)$. Fig.4. also demonstrates the system can not be work normally under the cyber-attack. Simulation results underline that a cyber-attack can be effectively detected if the condition in the Theorem 3 is satisfied.

Example 2. Consider the model of the QTP (see [23]):

$$\begin{aligned} \dot{x} &= Ax + Bu \\ y &= Cx. \end{aligned} \tag{20}$$

The QTP controlled through a wireless communication network, which is depicted in Fig.5. In order to detect the attacks on the actuators Pump 1 and Pump 2, we consider

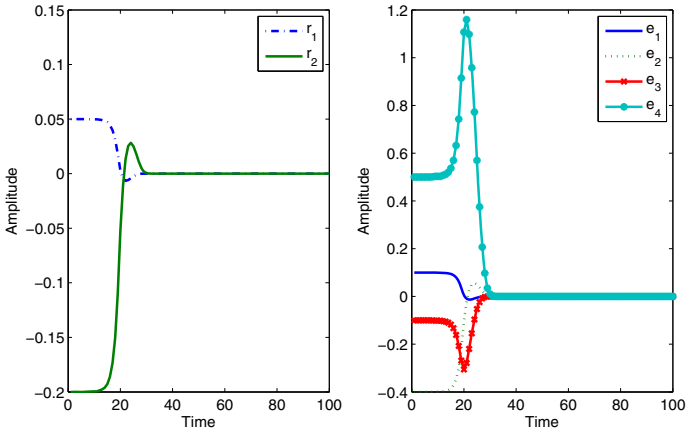

Fig. 6. The time response of residual and error dynamic without attack

the operating points P_+ [23] with the following parameters:

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

Assume that the system (20) is subject to a zero dynamic attack (V) on the actuator, the corresponding detector gain matrix can be obtained as follows

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

When the stochastic event $\alpha(t)=0$, i.e. $a_k^a(t)=0$, Fig.6. displays the error dynamic is asymptotically stable. When the stochastic event $\alpha(t)=1$ and the attacked probability $\rho=0.5$, the stochastic matrix $rank(E(Q(s)))=6$, however, there exists a $z_0=0.0127$ such that $rank(E(Q(z_0)))=5<6$. According to Theorem 2, the cyber-attacks signal is undetectable, because it is possible for the adversary to launch a stochastic zero attack signal $a_k^a(t)$ as the following:

$$a_k^a(t)=\begin{bmatrix} -1.074 \\ 1 \end{bmatrix} e^{0.0127t}$$

such that the transfer function $G_{a_k^a r}(s)$ is zero. Fig.7. displays the attack signal $a_k^a(t)$ and the time response of the residual and the QTP under the attack, respectively. It is clear that the QTP can not work normally under the stochastic attack. Simulation results demonstrate that a cyber-attack on the control system is undetectable if the condition in the Theorem 2 is satisfied.

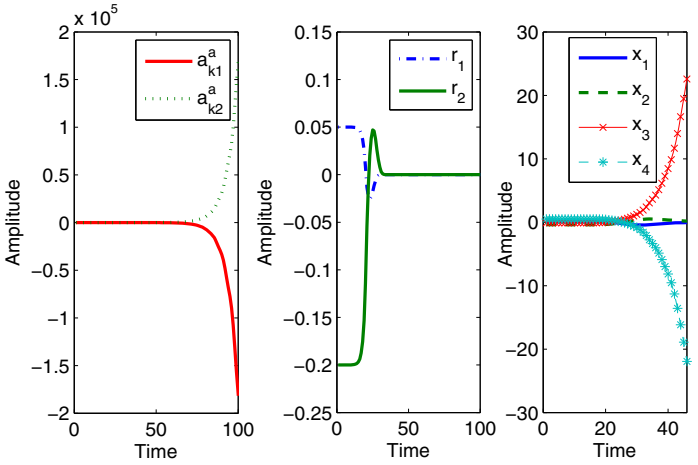

Fig. 7. The attack signal and the time response of residual and plant states under zero dynamic attack $a_k^a(t)$

5 Conclusion

This paper presents an algebraic detection scheme for control systems under stochastic cyber-attacks and disturbances. It is a relatively simple and straightforward detection approach. Based on the frequency-domain transformation technique and linear algebra theory, an effective anomaly detector is derived. Further, some sufficient and necessary conditions are obtained, which guarantee that a stochastic cyber-attack is detectable or undetectable. The main work focuses on stochastic cyber-attacks detection approach on control systems and we mention the stochastic attacks model that control systems are possibly exposed to. The proposed scheme is applied to some physical systems that are subject to the stochastic data DoS attack and data deception attack, respectively. Simulation results underline that the proposed attack detection approach is effective and feasible in practical application. Before the cyber intruders are removed and the security branches are closed, or operators start the repair or exchange of faulty components, the physical process must be kept in a safe state as long as possible. Therefore, next steps that are urgent for us to consider are the cyber-attacks fault-tolerant control and fault estimation on control systems.

References

1. Wolf, M., Daly, P.W.: Security Engineering for Vehicular IT Systems. Vieweg-Teubner (2009)
2. Nimda worm, `http://www.cert.org/advisories/CA-2001-26.html`
3. Moore, D., Paxson, V., Savage, S., Shannon, C., Staniford, S., Weaver, N.: Inside the Slammer worm. IEEE Security & Privacy 1(4) (2003)
4. New "cyber attacks" hit S Korea, `http://news.bbc.co.uk/2/hi/asia-pacific/8142282.stm`

5. Slay, J., Miller, M.: Lessons learned from the Maroochy water breach. Critical Infrastructure Protection 253, 73–82 (2007)
6. Amin, S., Galina, A., Schwartz, S., Sastry, S.: Security of Interdependent and Identical Networked Control Systems. Automatica 49(1), 186–192 (2013)
7. Andersson, G., Esfahani, P.M., et al.: Cyber-Security of SCADA Systems. Session: Cyber -Physical System Security in A Smart Grid Enviroment (2011)
8. Li, Y.M., Voos, H., Darouach, M.: Robust H_∞ fault estimation for control systems under stochastic cyber-attacks. In: 33rd China Control Conference, Nanjing, China (accepted, 2014)
9. Rosich, A., Voos, H., Li, Y.M., Darouach, M.: A Model Predictive Approach for Cyber-Attack Detection and Mitigation in Control Systems. In: 52nd IEEE Annual Conference on Decision and Control, Italy, pp. 6621–6626 (2013)
10. Teixeira, A., Pérez, D., Sandberg, H., Johansson, K.H.: Attack Models and Scenarios for Networked Control Systems. In: HiCoNS 2012, Beijing, China, pp. 55–64 (2012)
11. Mo, Y., Sinopoli, B.: False data injection attacks in control systems. In: First Workshop on Secure Control Systems, Stockholm, Sweden (2010)
12. Amin, S., Litrico, X., Sastry, S.S., Bayen, A.M.: Cyber Security of Water SCADA Systems: (I) Analysis and Experimentation of Stealthy Deception Attacks. IEEE Transactions on Control Systems Technology 21(5), 1963–1970 (2013)
13. Eliades, D.G., Polycarpou, M.M.: A fault diagnosis and security framework for water systems. IEEE Transactions on Control Systems Technology 18(6), 1254–1265 (2010)
14. Metke, A.R., Ekl, R.L.: Security technology for smart grid networks. IEEE Transactions on Smart Grid 1(1), 99–107 (2010)
15. Sridhar, S., Hahn, A., Govindarasu, M.: Cyber–physical system security for the electric power grid. Proceedings of the IEEE 99(1), 1–15 (2012)
16. Mohsenian-Rad, A.H., Garcia, A.L.: Distributed internet-based load altering attacks against smart power grids. IEEE Transactions on Smart Grid 2(4), 667–674 (2011)
17. Anjali, S., Ramesh, C.J.: Dual-Level Attack Detection and Characterization for Networks under DDoS. In: International Conference on Availability, Reliability and Security (2010)
18. Hashim, F., Kibria, M.R., Jamalipour, A.: Detection of DoS and DDoS Attacks in NGMN Using Frequency Domain Analysis. In: Proceedings of APCC 2008, copyright(c) 2008 IEICE 08 SB 0083 (2008)
19. Weimer, J., Kar, S., Johansson, K.H.: Distributed Detection and Isolation of Topology Attacks in Power Networks. In: HiCoNS 2012, Beijing, China, pp. 65–71 (2012)
20. Liu, Y., Reiter, M.K., Ning, P.: False data injection attacks against state estimation in electric power grids. In: ACM Conference on Computer and Communications Security, Chicago, USA, pp. 21–32 (2009)
21. Pasqualetti, F.: Secure Control Systems: A Control-Theoretic Approach to Cyber-Physical Security. A Dissertation for the degree of Doctor of Philosophy in Mechanical Engineering (2012)
22. Zhou, K., Doyle, J.C., Glover, K.: Robust and Optimal Control. Prentice-Hall, Inc., Upper Saddle River (1996)
23. Johansson, K.H.: The Quadruple-Tank Process: A Multivariable Laboratory Process with an Adjustable Zero. IEEE Transactions on Control Systems Technology 8(3), 456–465 (2000)