An Algebraic Detection Approach for Control Systems under Multiple Stochastic Cyber-attacks

Yumei Li, Holger Voos, Mohamed Darouach, and Changchun Hua

***Abstract*—In order to compromise a target control system successfully, hackers possibly attempt to launch multiple cyber-attacks aiming at multiple communication channels of the control system. However, the problem of detecting multiple cyber-attacks has been hardly investigated so far. Therefore, this paper deals with the detection of multiple stochastic cyber-attacks aiming at multiple communication channels of a control system. Our goal is to design a detector for the control system under multiple cyber-attacks. Based on frequency-domain transformation technique and auxiliary detection tools, an algebraic detection approach is proposed. By applying the presented approach, residual information caused by different attacks is obtained respectively and anomalies in the control system are detected. Sufficient and necessary conditions guaranteeing the detectability of the multiple stochastic cyber-attacks are obtained. The presented detection approach is simple and straightforward. Finally, two simulation examples are provided, and the simulation results show that the detection approach is effective and feasible.**

***Index Terms*—Cyber-attack detection, control system, multiple stochastic cyber-attacks.**

I. INTRODUCTION

As networks become ubiquitous and more and more industrial control systems are connected to open public networks, control systems are increased the risk of exposure to cyber-attacks. Control systems are vulnerable to cyber-threats, and successful attacks on them can cause serious consequences$^{[1-3]}$. Therefore, the security and safety issues in controlled systems have been recently realized and they are currently attracting considerable attention$^{[4-20]}$. Some researchers focused on the cyber security of water systems$^{[3,6-7]}$. Further works considered cyber-attacks on smart grid systems$^{[4,8-10,12]}$. In order to detect as well as identify and isolate these cyber-attacks as early as possible, different detection approaches were presented. For example [13] investigated the problem of false data injection attacks against state estimation in electric power grids$^{[14]}$ proposed a model predictive approach for cyber-attack detection$^{[15]}$. presented a stochastic cyber-attack detection scheme based on frequency-domain transformation technique$^{[16]}$. considered robust H_∞ cyber-attacks estimation for control systems$^{[17]}$. proposed a detection algorithm by investigating the frequency spectrum distribution of the network traffic. References [18−20] used consensus dynamics in networked multi-agent systems including malicious agents. As far as we know, no existing literatures deal with the problem of multiple cyber-attacks. In practice, however, 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 succeed. 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. The fact that no research currently deals with the detection of multiple cyber-attacks on a control process motivates our research in detection of multiple cyber-attacks.

This paper deals with the problem to detect multiple stochastic cyber-attacks aiming at multiple communication channels of a control system. We present an algebraic detection approach based on the frequency-domain transformation. The basic idea is to use appropriate observers to generate residual information related to cyber-attacks. An anomaly detector for the control system under multiple stochastic cyber-attacks and stochastic disturbances is derived. The main contributions in the paper are as follows. We first propose a control system with multiple stochastic cyber-attacks that satisfy a Markovian stochastic process. In addition, we also introduce the stochastic attack models that are aiming at a specific controller command input channel or sensor measurement output channel. Second, based on the frequency-domain transformation technique and auxiliary detection tools, the error dynamics of the control system is transformed into algebraic equations. We consider possible cyber-attacks as non-zero solutions of the algebraic equations and the residuals as their constant vectors. By analyzing the ranks of the stochastic system matrix and the auxiliary stochastic system matrices, the residual information caused by attacks from different communication channel is obtained, respectively. Furthermore, based on the obtained residual information, we are able to determine the detectability of these cyber-attacks. The sufficient and necessary conditions guaranteeing that these attacks are detectable or undetectable are obtained. Finally, we provide two simulation examples to illustrate the effectiveness of our results. In Example 1, we consider a control system with stochastic noises. We detect possible stochastic cyber-attacks, which are aiming at three different controller command input channels on the actuator. In Example 2, we use the quadruple-tank process (QTP) as described in [21]. We also detect two possible cyber-attacks on the QTP. These simulation results show that the proposed attack detection approach is effective and feasible.

For convenience, we adopt the following notations: $\mathrm{E}\{\cdot\}$ is the mathematical expectation operator; $\dim(\cdot)$ denotes the di-

Manuscript received September 30, 2014; accepted January 24, 2015. This work was supported by the Fonds National de la Recherche, Luxembourg (CO11/IS/1206050 (SeSaNet)) and National Natural Science Foundation of China (61273222). Recommended by Associate Editor Xinping Guan.

Citation: Yumei Li, Holger Voos, Mohamed Darouach, Changchun Hua. An algebraic detection approach for control systems under multiple stochastic cyber-attacks. *IEEE/CAA Journal of Automatica Sinica*, 2015, **2**(3): 258−266

Yumei Li and Holger Voos are with the Interdisciplinary Centre for Security Reliability and Trust (SnT), University of Luxembourg, Luxembourg L-2721, Luxembourg (e-mail: yumei.li@uni.lu; holger.voos@uni.lu).

Mohamed Darouach is with the Centre de la Recherche en Automatique de Nancy (CRAN), Universite de Lorraine, Longwy 54400, France (e-mail: modar@pt.lu).

Changchun Hua is with the Institute of Electrical Engineering, Yanshan University, Qinhuangdao 066004, China (e-mail: cch@ysu.edu.cn).

mension of given vector; $L_{\mathcal{F}}^2([0,\ \infty);\ \mathbf{R}^n)$ is the space of nonanticipative stochastic processes.

II. Problem statement

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

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

where $x(t) \in \mathbf{R}^r$ is the state vector, $u(t) \in \mathbf{R}^m$ is the control input, $y(t) \in \mathbf{R}^p$ is the measurement output, $a_i^a(t) \in \mathbf{R}$, $i = 1, \ldots, n_1$ and $a_j^s(t) \in \mathbf{R}$, $j = 1, \ldots, n_2$ denote the actuator cyber-attack aiming at the i-th controller command input channel and the sensor cyber-attack aiming at the j-th sensor measurement output channel, respectively. A, B, C, E_1 and E_2 are known constant matrices. $w(t)$ and $v(t)$ are stochastic noises ($w(t), v(t) \in L_{\mathcal{F}}^2([0,\infty); \mathbf{R}^n)$). f_i and h_j are the attacked coefficients. $\alpha_i(t)$ and $\beta_i(t)$ are Markovian stochastic processes with the binary state (0 or 1), which satisfy the following probability

$$\begin{aligned} &\mathrm{E}\{\alpha_i(t)\} = \mathrm{Prob}\{\alpha_i(t) = 1\} = \rho_i,\\ &\mathrm{E}\{\beta_j(t)\} = \mathrm{Prob}\{\beta_j(t) = 1\} = \sigma_j,\\ &\qquad i = 1, \ldots, n_1 \le m, \quad j = 1, \ldots, n_2 \le r. \end{aligned} \tag{2}$$

Herein, the event $\alpha_i(t) = 1$ (or $\beta_j(t) = 1$) shows that the i-th controller command input channel on the actuator (or the j-th 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 i-th (or the j-th)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 $a_j^s(t)$). $\alpha_i(t)$ and $\beta_j(t)$ are independent from each other, they are also independent from the stochastic noises $w(t), v(t)$ and the initial state x_0.

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

$$\begin{aligned} B &= \begin{bmatrix} b_1 & \ldots & b_i & \ldots & b_m \end{bmatrix},\\ C &= \begin{bmatrix} c_1 & \ldots & c_j & \ldots & c_r \end{bmatrix}, \end{aligned} \tag{3}$$

where b_i is the i-th column vector of matrix B and c_j is the j-th column vector of matrix C. And the control input $u(t)$ and the system state $x(t)$ are written as

$$u(t) = \begin{bmatrix} u_1(t) \\ u_2(t) \\ \vdots \\ u_m(t) \end{bmatrix}, \quad x(t) = \begin{bmatrix} x_1(t) \\ x_2(t) \\ \vdots \\ x_r(t) \end{bmatrix}. \tag{4}$$

A. Modeling a Stochastic Cyber-attacks on a Specified Communication Channel

In order to increase the success 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 a control system. In a stochastic data denial-of-service (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 by sending false information $\widetilde{u}(t) \neq u(t)$ or $\widetilde{y}(t) \neq y(t)$ from controllers or sensors. The false information includes: injection of a bias data that cannot be detected in the system, or an incorrect time of observing a measurement; 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.

In this work, we model stochastic data DoS attacks and stochastic data deception attacks, which hackers possibly launch on a control system aiming at a specific controller command input channel or sensor measurement output channel.

1) A stochastic DoS attack preventing the actuators from receiving control command of the i-th control channel can be modelled as

$$\begin{aligned} &\alpha_i(t) \in \{0, 1\}, \qquad t \ge t_0, \ \ i = 1, \ldots, n_1 \le m,\\ &f_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}_{m \times 1},\\ &a_i^a(t) = -u_i(t). \end{aligned} \tag{5}$$

2) A stochastic DoS attack preventing the sensors from receiving sensor measure of the j-th output channel can be modelled as

$$\begin{aligned} &\beta_j(t) \in \{0, 1\}, \qquad t \ge t_0, \ \ j = 1, \ldots, n_2 \le r,\\ &h_j = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}_{r \times 1},\\ &a_j^s(t) = -x_j. \end{aligned} \tag{6}$$

Moreover, if the following conditions are satisfied:

$$\sum_{i=1}^{m} \alpha_i(t) f_i a_i^a(t) = -u(t), \tag{7}$$

and

$$\sum_{j=1}^{r} \beta_j(t) h_j a_j^s(t) = -x(t), \tag{8}$$

these stochastic attacks mentioned above completely deny the services on the actuator and on the sensors, respectively.

3) A stochastic data deception attack preventing the actuator from a correct control input of the i-th control channel can be modelled as

$$\begin{aligned}&\alpha_i(t) \in \{0,1\}, \qquad t \geq t_0,\ \ i=1,\ldots,n_1 \leq m,\\ &f_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}_{m\times 1}, \\ &a_i^a(t) = -u_i(t) + d_i^a(t) \text{ or } a_i^a(t) = d_i^a(t).\end{aligned} \tag{9}$$

4) A stochastic data deception attack preventing the sensor from a correct sensor measurement of the j-th output channel can be modelled as

$$\begin{aligned}&\beta_j(t) \in \{0,1\}, \qquad t \geq t_0,\ \ j=1,\ldots,n_2 \leq r,\\ &h_j = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}_{r\times 1}, \\ &a_j^s(t) = -x_j + d_j^s(t) \text{ or } a_j^s(t) = d_j^s(t),\end{aligned} \tag{10}$$

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

Now, let $T_{d_i^a y}(s) = C(sI-A)^{-1}b_i$ which is the transfer function from the attack $d_i^a(t)$ to output measure $y(t)$. When hackers launch a data deception attack $a_i^a(t) = d_i^a(t)$ on the actuator to make $T_{d_i^a y}(s) = 0$, 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 $d_j^s(t)$ to output $y(t)$ is $T_{d_j^s y}(s) = c_j \neq 0$.

Remark 1. In the stochastic attack models (5)$-$(10), the attacked coefficients f_i and h_j are column vectors. Herein only the element in the i-th row is 1 and the rest elements are 0 in f_i, which implies that only the i-th control channel of a control system is attacked. Similarly, only the element in the j-th row is 1 and the rest elements are 0 in h_j, which implies that only the j-th output channel of a control system is attacked.

Remark 2. 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 a 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.

III. Main results

In this section, we present the approach to the anomaly detection. We assume that the following conditions are satisfied: 1) the pair (A,B) is controllable; 2) (A,C) is observable. For simplification of the 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 modeling errors in the system transfer matrix. Therefore, system (1) can be rewritten as follows:

$$\begin{aligned}&\dot{x}(t) = Ax(t) + \sum_{i=1}^{n_1} \alpha_i(t)Bf_i a_i^a(t) + E_1 w(t),\\ &x(0) = x_0,\\ &y(t) = Cx(t) + \sum_{j=1}^{n_2} \beta_j(t)Ch_j a_j^s(t) + E_2 v(t).\end{aligned} \tag{11}$$

We set up the following anomaly detector:

$$\begin{aligned}&\dot{\widetilde{x}}(t) = A\widetilde{x}(t) + \widetilde{B}r(t),\\ &\widetilde{x}(0) = 0,\\ &r(t) = y(t) - C\widetilde{x}(t),\end{aligned} \tag{12}$$

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

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

$$\begin{aligned}&\dot{e}(t) = \overline{A}e(t) + \sum_{i=1}^{n} \overline{F}_i a_i(t) + \overline{E}_1 d(t),\\ &r(t) = Ce(t) + \sum_{i=1}^{n} \overline{H}_i a_i(t) + \overline{E}_2 d(t),\end{aligned} \tag{13}$$

with the matrices

$$\begin{aligned}&\overline{A} = (A - \widetilde{B}C),\\ &\overline{H}_i = \left[\begin{array}{cc} 0 & \beta_i(t)Ch_i, \end{array}\right],\\ &\overline{F}_i = \left[\begin{array}{cc} \alpha_i(t)Bf_i & -\beta_i(t)\widetilde{B}Ch_i, \end{array}\right],\\ &\overline{E}_1 = \left[\begin{array}{cc} E_1 & -\widetilde{B}E_2 \end{array}\right],\\ &\overline{E}_2 = \left[\begin{array}{cc} 0 & E_2 \end{array}\right],\end{aligned} \tag{14}$$

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

$$n \leq \max\{n_1, n_2\},$$

$$\begin{cases} a_{n_1+1}^a(t) = a_{n_1+2}^a(t) = \cdots = a_n^a(t) = 0, & n = n_2 > n_1,\\ a_{n_2+1}^s(t) = a_{n_2+2}^s(t) = \cdots = a_n^s(t) = 0, & n = n_1 > n_2,\end{cases}$$

and

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

Before presenting the main results, we give the following definition and lemma.

Definition 1. For anomaly detector error dynamics, if a cyber-attack on a control system leads to zero output residual, then the cyber-attack is undetectable.

If $T_{dr}(s) = C(sI - \overline{A})^{-1}\overline{E}_1 + \overline{E}_2$ denotes the transfer function from stochastic disturbance $d(t)$ to output residual $r(t)$, the robust stability condition of error dynamic (13) is given in term of the following lemma.

Lemma 1[16]**.** When all stochastic events $\alpha_i(t) = \beta_i(t) = 0$ $(i = 1, \ldots, n)$, there are the following conclusions:

1) The error dynamics (13) without disturbances is asymptotically stable, if there exists a symmetric positive definite matrix $P > 0$ and a matrix X such that the following linear matrix inequality (LMI) holds

$$\Psi = A^{\mathrm{T}}P + PA - C^{\mathrm{T}}X^{\mathrm{T}} - XC + C^{\mathrm{T}}C < 0. \qquad (15)$$

2) The error dynamics (13) with disturbances $d(t)$ $(0 \neq d(t) \in L_{\mathcal{F}}^2([0,\infty); \mathbf{R}^n))$ is robustly stable, if $\|T_{dr}(s)\|_\infty < 1$ and if there exists a symmetric positive definite matrix $P > 0$ and a matrix X such that the following LMI holds

$$\begin{bmatrix} \Psi & PE_1 & -XE_2 + C^{\mathrm{T}}E_2 \\ * & -I & 0 \\ * & * & -I + E_2^{\mathrm{T}}E_2 \end{bmatrix} < 0. \qquad (16)$$

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

A. Algebraic Detection Scheme for Multiple Stochastic Cyber-attacks Aiming at Multiple Communication Channels

In this section, using the frequency-domain description of the system, we transform the error dynamics (13) into the following equation:

$$Q(s)X(s) = B(s), \qquad (17)$$

where

$$Q(s) = \begin{bmatrix} \overline{A} - sI & \overline{F}_1 & \ldots & \overline{F}_n & \overline{E}_1 \\ C & \overline{H}_1 & \ldots & \overline{H}_n & \overline{E}_2 \end{bmatrix},$$

$$X(s) = \begin{pmatrix} e(s) \\ a_1(s) \\ \vdots \\ a_n(s) \\ d(s) \end{pmatrix}, \quad B(s) = \begin{pmatrix} 0 \\ r(s) \end{pmatrix}.$$

Further, in order to obtain effective results, we introduce the mathematical expectation of the stochastic matrix $Q(s)$ as follows:

$$\mathrm{E}(Q(s)) = \begin{bmatrix} \overline{A} - sI & \mathrm{E}(\overline{F}_1) & \ldots & \mathrm{E}(\overline{F}_n) & \overline{E}_1 \\ C & \mathrm{E}(\overline{H}_1) & \ldots & \mathrm{E}(\overline{H}_n) & \overline{E}_2 \end{bmatrix}, \qquad (18)$$

where

$$\begin{aligned} &\mathrm{E}(\overline{F}_i) = \begin{bmatrix} \rho_i B f_i & -\sigma_i \widetilde{B} C h_i \end{bmatrix}, \\ &\mathrm{E}(\overline{H}_i) = \begin{bmatrix} 0 & \sigma_i C h_i \end{bmatrix}, \qquad i = 1, \ldots, n. \end{aligned}$$

Then the system (17) can be described as

$$\mathrm{E}(Q(s))X(s) = B(s), \qquad (19)$$

and the equation (19) can be rewritten as

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

where

$$\mathrm{E}(\widetilde{Q}_i(s)) = \begin{bmatrix} \dfrac{\overline{A} - sI}{n} & \mathrm{E}(\overline{F}_i) & \dfrac{\overline{E}_1}{n} \\ \dfrac{\overline{C}}{n} & \mathrm{E}(\overline{H}_i) & \dfrac{\overline{E}_2}{n} \end{bmatrix},$$

$$X_i(s) = \begin{pmatrix} e(s) \\ a_i(s) \\ d(s) \end{pmatrix},$$

$$B_i(s) = \begin{pmatrix} 0 \\ r_i(s) \end{pmatrix},$$

$$r(s) = \sum_{i=1}^{n} r_i(s).$$

Consider the following stochastic matrix:

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

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

$$\begin{aligned} &\dot{e}(t) = \overline{A}e(t) + \overline{F}_i a_i(t) + \overline{E}_1 d(t), \\ &r(t) = Ce(t) + \overline{H}_i a_i(t) + \overline{E}_2 d(t), \\ &\qquad\qquad\qquad\qquad i = 1, \ldots, n, \end{aligned} \qquad (20)$$

and the auxiliary stochastic equations

$$\mathrm{E}(Q_i(s))X_i = B_i(s), \quad i = 1, \ldots, n. \qquad (21)$$

Remark 3. Here, since the matrices $\overline{F}_i$ and $\overline{H}_i$ include the stochastic parameters $\alpha_i(t)$ and $\beta_i(t)$, the system matrix $Q(s)$ correspondingly includes these stochastic parameters, and $\mathrm{E}(Q(s))$ and $\mathrm{E}(Q_i(s))$ include stochastic probabilities ρ_i and σ_i as well, which take values in $[0, 1]$. Therefore, they are stochastic matrices.

Remark 4. In this work, we introduce the auxiliary mathematical "tools" (20) and (21). The auxiliary error dynamics (20) represents the fact that the control system is only subjected to a stochastic cyber-attack $a_i(t)$ on the i-th communication channel. Applying the auxiliary equation (21), we can obtain the information of residual $r_i(t)$ that is caused by the cyber-attack $a_i(t)$. In addition, the detector gain matrix $\widetilde{B}$ can be determined according to Lemma 1.

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

Theorem 1. For system (11), we assume that all of these stochastic matrices $\mathrm{E}(Q(s))$ and $\mathrm{E}(Q_i(s))$ $(i = 1, \ldots, n)$ have full column normal rank. All of these cyber-attacks $a_i(s)$ $(i = 1, \ldots, n$, $(0 \neq a_i(s) \in \overline{G}))$ when $s = z_0$ are undetectable, if and only if there exists $z_0 \in$, such that

$$\mathrm{rank}\mathrm{E}(Q(z_0)) < \dim(X(z_0)), \qquad (22)$$

and

$$\mathrm{rank}\mathrm{E}(Q_i(z_0)) < \dim(X_i(z_0)), \quad i = 1, \ldots, n. \qquad (23)$$

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

Proof. (If) Assume that there exists $z_0 \in \mathbf{C}$ such that conditions (22) and (23) hold for all $a_i(z_0) \in \overline{G}$, it becomes obvious that z_0 is an invariant zero[22] of the detector error system (13) and the auxiliary system (20). Then all of the equations in (19) and (20) are homogeneous, i.e., $B(z_0) = 0$ and $B_i(z_0) = 0$. Therefore, the output residual $r_i(z_0) = 0$, $i = 1, \ldots, n$, and $r(z_0) = \sum_{i=1}^{n} r_i(z_0) = 0$ as well. By Definition 1, all of these cyber-attacks $a_i(s)$, $i \ldots, n$ when $s = z_0$ are undetectable.

(Only if) Assume that all of these cyber-attacks $a_i(s)$, $i = 1, \ldots, n$ when $s = z_0$ are undetectable, then there must exist a $z_0 \in \mathbf{C}$ such that the residual $r_i(z_0) = 0$ and $r(z_0) = \sum_{i=1}^{n} r_i(z_0) = 0$. Therefore, all of the equations in (19) and (21) are homogeneous. If we assume that all of matrices $\mathrm{E}(Q(z_0))$ and $\mathrm{E}(Q_i(z_0))$ have full column rank, then all of these homogeneous equations have and only have one zero solution. However, this contradicts with the conditions that

$$X\,|_{s=z_0} \neq 0, \quad X_i\,|_{s=z_0} \neq 0, \;\; i = 1, \ldots, n$$

are solutions to (19) and (21), respectively. Therefore the assumptions are false, only conditions (22) and (23) are true. □

Theorem 2. For system (11), we assume that all of stochastic matrices $\mathrm{E}(Q(s))$ and $\mathrm{E}(Q_i(s))$ $(i = 1, \ldots, n)$ have full column normal rank. 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 $z_0 \in \mathbf{C}$:

$$\mathrm{rank}\mathrm{E}(Q(z_0)) = \dim(X(z_0)), \tag{24}$$

and

$$\mathrm{rank}\mathrm{E}(Q_i(z_0)) = \dim(X_i(z_0)), \;\; i = 1, \ldots, n. \tag{25}$$

Herein G is a set of detectable cyber-attacks.

Proof. (If) Assuming that conditions (24) and (25) always hold for any $z_0 \in \mathbf{C}$, it is obvious that the stochastic matrices $\mathrm{E}(Q(z_0))$ and $\mathrm{E}(Q_i(z_0))$ $(i = 1, \ldots, n)$ have full column rank. Then the equation

$$\mathrm{E}(Q(z_0))X(z_0) = B(z_0), \tag{26}$$

and the auxiliary stochastic equations

$$\mathrm{E}(Q_i(z_0))X_i = B_i(z_0), \;\; i = 1, \cdots, n \tag{27}$$

have one and only one solution. In the following, we proof by contradiction. Assume that residual $r(z_0) = 0$ and $r_i(z_0) = 0$, $i = 1, \ldots, n$, then equations (26) and (27) has one and only one zero solution, i.e.,

$$X\,|_{s=z_0} = 0, \quad X_i\,|_{s=z_0} = 0, \;\; i = 1, \ldots, n.$$

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

$$X\,|_{s=z_0} \neq 0, \quad X_i\,|_{s=z_0} \neq 0, \;\; i = 1, \ldots, n.$$

Therefore $r(z_0) \neq 0$ and $r_i(z_0) \neq 0$, $i = 1, \ldots, n$, these cyber-attacks $a_i(s)$ $(0 \neq a_i(s) \in G)$, $i = 1, \ldots, n$, for any $s = z_0$ are detectable.

(Only if) Assume that there exists a $z_0 \in \mathbf{C}$ which satisfies conditions (22) and (23). Since all of the stochastic matrices $\mathrm{E}(Q(s))$ and $\mathrm{E}(Q_i(s))$ $(i = 1, \ldots, n)$ have full column ranks, according to Theorem 1, these cyber-attacks $a_i(s)$, $i = 1, \ldots, n$ are undetectable as $s = z_0$. However, this is in contradiction with the given condition that all of these cyber-attacks $a_i(s)$, $i = 1, \ldots, n$ are detectable for any $s = z_0$. Therefore the assumption is false, only

$$\mathrm{rank}\mathrm{E}(Q(z_0)) = \dim(X(z_0)),$$

and

$$\mathrm{rank}\mathrm{E}(Q_i(z_0)) = \dim(X_i(z_0)), \;\; i = 1, \ldots, n$$

are true. □

Furthermore, we can obtain the following corollary according to Theorem 1 and Theorem 2.

Corollary 1. For system (11), assume that all of stochastic matrices $\mathrm{E}(Q(s))$ and $\mathrm{E}(Q_i(s))$ $(i = 1, \ldots, n)$ have full column normal rank. If there exists $z_0 \in \mathbf{C}$, such that

$$\mathrm{rank}\mathrm{E}(Q(z_0)) < \dim(X(z_0)), \tag{28}$$

then there are the following conclusions.

1) The cyber-attack $a_i(z_0)$ $(0 \neq a_i(s) \in G)$ is detectable, if and only if

$$\mathrm{rank}\mathrm{E}(Q_i(z_0)) = \dim(X_i(z_0)). \tag{29}$$

2) The cyber-attack $a_j(z_0)$ $(0 \neq a_j(s) \in G)$ is undetectable, if and only if

$$\mathrm{rank}\mathrm{E}(Q_j(z_0)) < \dim(X_j(z_0)). \tag{30}$$

IV. Simulation results

In this section, we provide two simulation examples to illustrate the effectiveness of our results. In Example 1, we consider a control system under three stochastic cyber-attacks and a stochastic noise. We detect two possible stochastic data DoS attacks and a possible stochastic data deception attack, which are aiming at three controller command input channels on the actuator. In Example 2, we use the laboratory process as presented in [21], which consists of four interconnected water tanks. We will also detect possible cyber-attacks on QTP controlled through a wireless communication network.

Example 1. Consider the following system with a stochastic noise $w(t)$

$$\begin{aligned} &\dot{x}(t) = Ax(t) + Bu(t) + E_1 w(t), \\ &x(0) = x_0, \\ &y(t) = Cx(t), \end{aligned} \tag{31}$$

and with the following parameters:

$$A = \begin{bmatrix} -0.8 & 0 & 0.1 & 0 & 0 \\ 0 & -0.2 & 0 & -0.1 & 0 \\ 0 & 0 & -0.4 & 0 & 0 \\ 0 & 0 & 0 & -0.3 & 0 \\ 0.2 & 0 & 0.1 & 0 & -0.5 \end{bmatrix},$$

$$B = \begin{bmatrix} 0.03 & 0 & 0.3 \\ 0 & 0.04 & 0 \\ 0 & -0.08 & 0.45 \\ -0.21 & 0 & 0.1 \\ 0.09 & 0 & 0 \end{bmatrix},$$

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

Assume that it is subjected to two stochastic data DoS attacks and a stochastic data deception attack on the actuator aiming at three controller command input channels, i.e.,

$$\begin{aligned} &\alpha_1(t) \in \{0,1\}, \quad t \geq t_0, \\ &f_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \\ &a_1^a(t) = -u_1(t), \end{aligned} \tag{32}$$

and

$$\begin{aligned} &\alpha_2(t) \in \{0,1\}, \quad t \geq t_0, \\ &f_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \\ &a_2^a(t) = -u_2(t) + b_2^a(t), \end{aligned} \tag{33}$$

and

$$\begin{aligned} &\alpha_3(t) \in \{0,1\}, \quad t \geq t_0, \\ &f_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \\ &a_3^a(t) = -u_3(t). \end{aligned} \tag{34}$$

As mentioned before, we ignore the control input, since it does not affect the residual.

By applying Lemma 1, the robust detector gain matrix can be obtained as follows:

$$\widetilde{B} = \begin{bmatrix} 0.6316 & 0 & 0.0826 & 0 \\ 0 & 2.7474 & 0 & -0.6078 \\ 0.0961 & 0 & 1.2444 & 0 \\ 0 & -0.6325 & 0 & 1.7707 \\ 0.0251 & 0 & 0.0304 & 0 \end{bmatrix}.$$

Set the initial conditions as $\widetilde{x}(0) = [0,0,0,0,0]^{\mathrm{T}}$ and $x(0) = [-0.2, 0.4, 0.8, -1, 0.1]^{\mathrm{T}}$. When the stochastic events $\alpha_1(t) = \alpha_2(t) = \alpha_3(t) = 0$ occur, the system is not under any cyber-attacks. Fig. 1 displays the time responses of the residual and the system state under stochastic noise $w(t)$ only, which shows that the system is robustly stable. When the stochastic events $\alpha_1(t) = \alpha_2(t) = \alpha_3(t) = 1$ occur, the system is under multiple cyber-attacks. We take the attack probabilities $\rho_1 = \rho_2 = 0.8$ and $\rho_3 = 0.5$, the stochastic matrix $\operatorname{rank}(\mathrm{E}(Q(s))) = 9$, and $\operatorname{rank}(\mathrm{E}(Q(z_0))) = 9$, $\operatorname{rank}(\mathrm{E}(Q_i(z_0))) = 7$ $(i = 1,2,3)$, which shows that $\operatorname{rank}(\mathrm{E}(Q(z_0)))$, $\operatorname{rank}(\mathrm{E}(Q_i(z_0)))$ $(i = 1,2,3)$ have always full column rank for any z_0. According to Theorem 2, the three attacks are detectable. Fig. 2 displays the noise signal and the attack signals, while Fig. 3 shows the time responses of the residual and the system state under three attacks and noise. Fig. 4, Fig. 5 and Fig. 6 give the time responses of the residual under the attack $a_1^a(t)$, $a_2^a(t)$ and $a_3^a(t)$, respectively. Simultaneously, they show the corresponding attack signals. The simulation results underline that these cyber-attacks can be effectively detected if the conditions in Theorem 2 are satisfied.

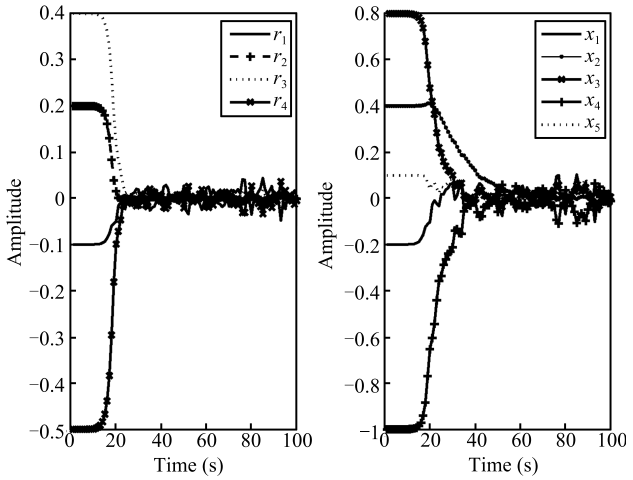


Fig. 1. The time responses of the residual and the system state under the noise.

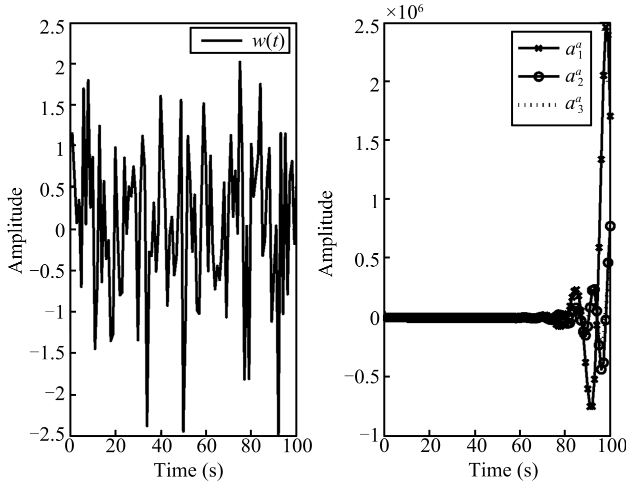


Fig. 2. The noise signal and the attack signals.

Example 2. Consider the model of the QTP in [21].

$$\begin{aligned} \dot{x} &= Ax + Bu, \\ y &= Cx, \end{aligned} \tag{35}$$

with the following parameters:

$$A = \begin{bmatrix} -0.0158 & 0 & 0.0256 & 0 \\ 0 & -0.0109 & 0 & 0.0178 \\ 0 & 0 & -0.0256 & 0 \\ 0 & 0 & 0 & -0.0178 \end{bmatrix},$$

$$C = \begin{bmatrix} 0.5 & 0 & 0 & 0 \\ 0 & 0.5 & 0 & 0 \end{bmatrix},$$

$$B = \begin{bmatrix} 0.0482 & 0 \\ 0 & 0.0350 \\ 0 & 0.0775 \\ 0.0559 & 0 \end{bmatrix}.$$

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

$$\begin{aligned} &\alpha_1(t) \in \{0,1\}, \quad t \geq t_0, \\ &f_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \\ &a_1^a(t) = b_1^a(t), \end{aligned} \tag{36}$$

and

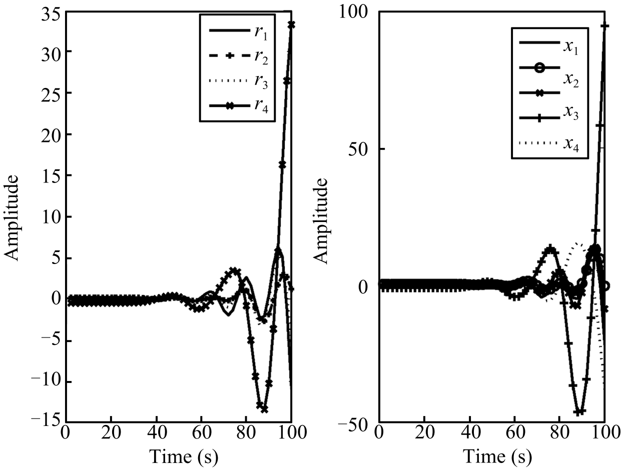


Fig. 3. The time responses of the residual and the system state under three attacks and noise.

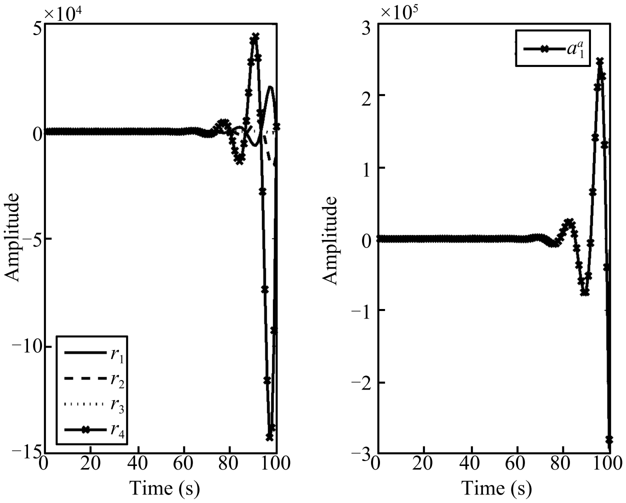


Fig. 4. The time responses of the residual under attack $a_1^a(t)$ and the attack signal $a_1^a(t)$.

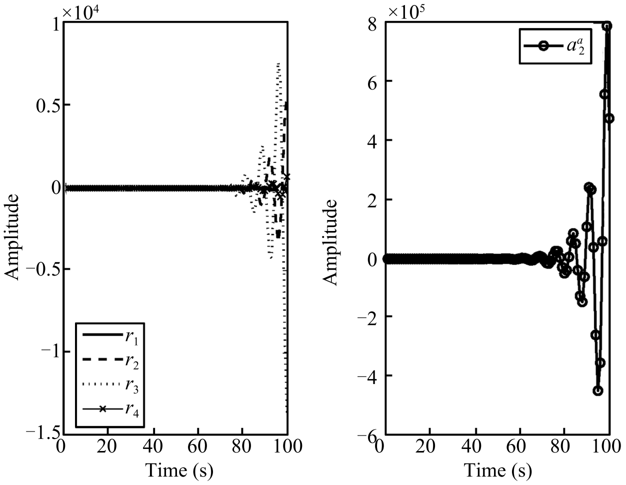


Fig. 5. The time responses of the residual under attack $a_2^a(t)$ and the attack signal $a_2^a(t)$.

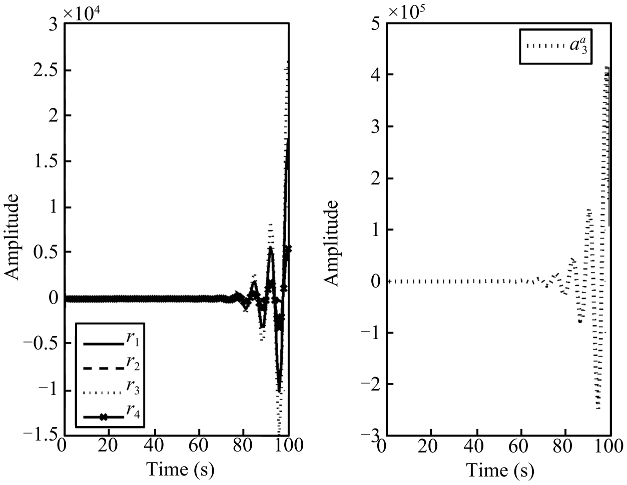


Fig. 6. The time responses of the residual under attack $a_3^a(t)$ and the attack signal $a_3^a(t)$.

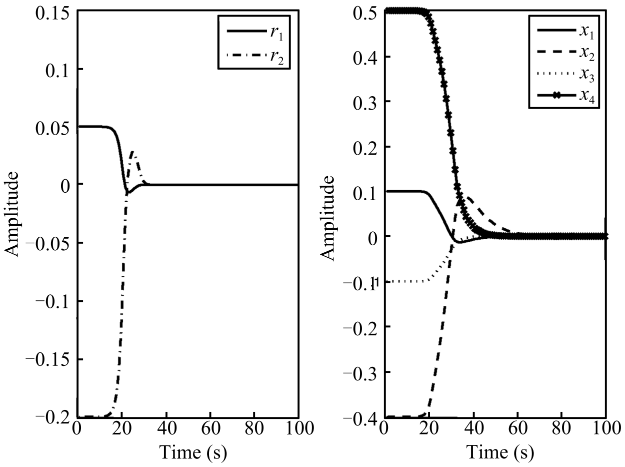


Fig. 7. The time responses of the residual and the system state without attacks.

$$\begin{aligned} &\alpha_2(t) \in \{0, 1\}, \quad t \geq t_0, \\ &f_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \\ &a_2^a(t) = b_2^a(t). \end{aligned} \tag{37}$$

The detector gain matrix can be obtained as follows:

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

We set the initial conditions as $\widetilde{x}(0) = [0, 0, 0, 0]^{\rm T}$ and $x(0) = [0.1, -0.4, -0.1, 0.5]^{\rm T}$. When the stochastic events $\alpha_1(t) = \alpha_2(t) = 0$ occur, Fig. 7 visualizes that the system (35) is asymptotically stable. When the stochastic events $\alpha_1(t) = \alpha_2(t) = 1$ occur and the attack probabilities are $\rho_1 = 0.8$, $\rho_2 = 0.5$, we have stochastic matrix ${\rm rank}({\rm E}(Q(s))) = 6$, however, there exists a $z_0 = 0.0127$ such that ${\rm rank}({\rm E}(Q(z_0))) = 5$ and ${\rm rank}({\rm E}(Q_i(z_0))) = 5$ $(i = 1, 2)$. Aiming at two different control channels, it is possible for the hacker to launch two stochastic data deception attacks as follows:

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

$$b_2^a(t) = \mathrm{e}^{0.0127t},$$

such that the transfer function from attacks to residual is zero. Therefore, it is difficult to detect these stealthy attacks. Fig. 8 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 when $s = z_0 = 0.0127$ could not be detected by original model. However, applying the auxiliary tools (20), (21) and according to Corollary 1, these attacks can also be detected. Fig. 9 displays the attack signal $a_1^a(t)$ and the responses of the residual under this attack. Fig. 10 shows the attack signal $a_2^a(t)$ and the responses of residual under this attack. Obviously, applying Corollary 1, the two stochastic data deception attacks can be detected effectively.

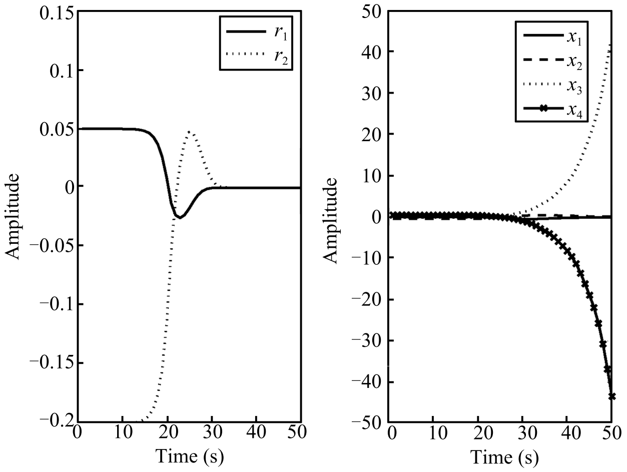


Fig. 8. The time responses of the residual and the system state under attacks $a_1^a(t)$ and $a_2^a(t)$.

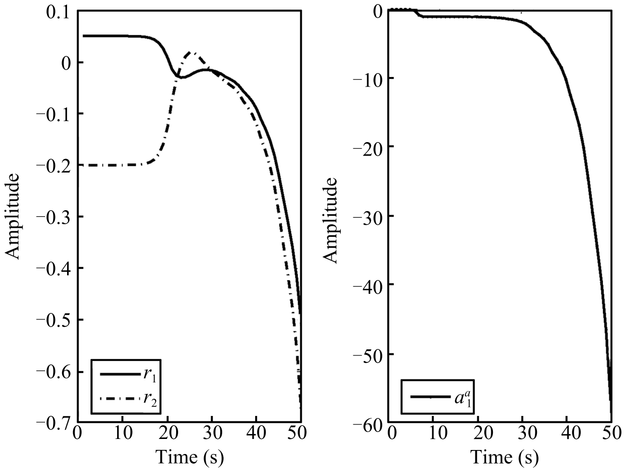


Fig. 9. The time responses of residual under the attack $a_1^a(t)$ and the attack signal $a_1^a(t)$.

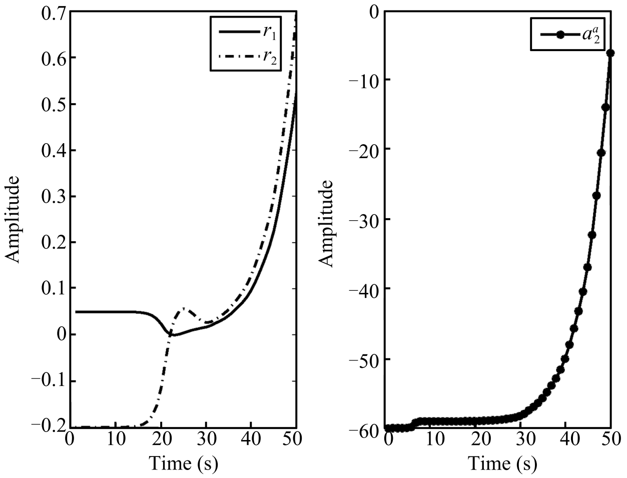


Fig. 10. The time responses of residual under the attack $a_2^a(t)$ and the attack signal $a_2^a(t)$.

V. Conclusion

This paper presents a cyber-attack detection approach for control systems under multiple stochastic cyber-attacks and disturbances. The proposed problem is significant in practice, because hackers might launch multiple attacks aiming at one target so that the aggression opportunities are increased and the attack target can be compromised, more stealthily and successfully. For example, the hacker is able to simultaneously launch DoS attacks, deception attacks and replay attacks that are respectively aiming at different communication channels of a control system. The main work here is focused on novel cyber-attack detection schemes that allow the detection of multiple stochastic attacks in order to protect control systems against a wide range of possible attack models. We give two simulation examples the results of which demonstrate that the detection approaches proposed in this paper are feasible and effective.

References

[1] Bier V, Oliveros S, Samuelson L. Choosing what to protect: strategic defensive allocation against an unknown attacker. *Journal of Public Economic Theory*, 2007, **9**(4): 563−587

[2] Amin S, Schwartz G A, Sastry S S. Security of interdependent and identical networked control systems. *Automatica*, 2013, **49**(1): 186−192

[3] Slay J, Miller M. Lessons learned from the Maroochy water breach. *Critical Infrastructure Protection*, 2007, **253**: 73−82

[4] Andersson G, Esfahani P M, Vrakopoulou M, Margellos K, Lygeros J, Teixeira A, Dan G, Sanderg H, Johansson K H. Cyber-security of SCADA systems. *Session: Cyber-Physical System Security in a Smart Grid Environment*, 2011.

[5] Mo Y L, Sinopoli B. False data injection attacks in control systems. In: Proceedings of the 1st Workshop on Secure Control Systems. Stockholm, Sweden, 2010.

[6] Amin S, Litrico X, Sastry S, Bayen A M. Cyber security of water SCADA systems: (I) analysis and experimentation of stealthy deception attacks. *IEEE Transactions on Control Systems Technology*, 2013, **21**(5): 1963−1970

[7] Eliades D G, Polycarpou M M. A fault diagnosis and security framework for water systems. *IEEE Transactions on Control Systems Technology*, 2010, **18**(6): 1254−1265

[8] Metke A R, Ekl R L. Security technology for smart grid networks. *IEEE Transactions on Smart Grid*, 2010, **1**(1): 99−107

[9] Sridhar S, Hahn A, Govindarasu M. Cyber-physical system security for the electric power grid. *Proceedings of the IEEE*, 2012, **100**(1): 210−224

[10] Mohsenian-Rad A H, Leon-Garcia A. Distributed internet-based load altering attacks against smart power grids. *IEEE Transactions on Smart Grid*, 2011, **2**(4): 667−674

[11] Sardana A, Joshi R C. Dual-level attack detection and characterization for networks under DDoS. In: Proceedings of the 2010 International Conference on Availability, Reliability and Security. Krakow: IEEE, 2010. 9−16

[12] Weimer J, Kar S, Johansson K H. Distributed detection and isolation of topology attacks in power networks. In: Proceedings of the 2012 HiCoNS′12. Beijing, China, 2012. 17−18

[13] Liu Y, Reiter M K, Ning P. False data injection attacks against state estimation in electric power grids. In: Proceedings of the 2009 ACM Conference on Computer and Communications Security. Chicago, IL, USA: ACM, 2009. 21−32

[14] Rosich A, Voos H, Li Y M, Darouach M. A model predictive approach for cyber-attack detection and mitigation in control systems. In: Proceedings of the 52nd Annual Conference on Decision and Control. Firenze: IEEE, 2013. 6621−6626

[15] Li Y M, Voos H, Rosich A, Darouach M. A stochastic cyber-attack detection scheme for stochastic control systems based on frequency-domain transformation technique. In: Proceedings of the 8th International Conference on Network and System Security. Xi′an, China: Springer, 2014. 209−222

[16] Li Y M, Voos H, Darouach M. Robust H_∞ fault estimation for control systems under stochastic cyber-attacks. In: Proceedings of the 33rd Chinese Control Conference. Nanjing, China: ORBilu, 2014. 3124−3129

[17] Hashim F, Kibria M R, Jamalipour A. Detection of DoS and DDoS attacks in NGMN using frequency domain analysis. In: Proceedings of the 14th Asia-Pacific Conference on Communications. Tokyo: IEEE, 2008. 1 −5

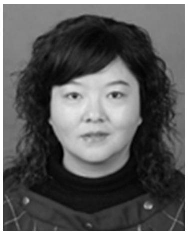
[18] Sundaram S, Hadjicostis C N. Distributed function calculation via linear iterative strategies in the presence of malicious agents. *IEEE Transactions on Automatic Control*, 2011, **56**(7): 1495−1508

[19] Teixeira A, Sandberg H, Johansson K H. Networked control systems under cyber attacks with applications to power networks. In: Proceedings of the 2010 American Control Conference. Baltimore, MD: IEEE, 2010. 3690−3696

[20] Pasqualetti F, Bichi A, Bullo F. Consensus computation in unreliable networks: a system theoretic approach. *IEEE Transactions on Automatic Control*, 2012, **57**(1): 90−104

[21] Johansson K H. The quadruple-tank process: a multivariable laboratory process with an adjustable zero. *IEEE Transactions on Control Systems Technology*, 2000, **8**(3): 456−465

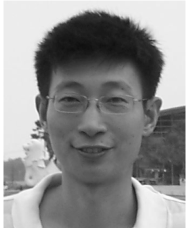
[22] Zhou K M, Doyle J C, Glover K. *Robust and Optimal Control*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1996.



Yumei Li received her Ph. D. degree in control theory and control engineering from Yanshan University, China, in 2009. She is currently a research associate at the Interdisciplinary Centre of Security, Reliability and Trust (SnT) at the University of Luxembourg. Her research interests include intelligent control and stochastic systems, secure and resilient automation control systems, distributed control, and cooperative control of multiagent system. Corresponding author of this paper.

Holger Voos studied electrical engineering at Saarland University, Germany, and received his Ph. D. degree in automatic control from the Technical University of Kaiserslautern, Germany, in 2002. He is currently a professor at the University of Luxembourg in the Faculty of Science, Technology and Communication, Research Unit of Engineering Sciences. He is the head of the Automatic Control Research Group and of the Automation and Robotics Research Group at the Interdisciplinary Centre of Security, Reliability and Trust (SnT) at the University of Luxembourg. His research interests include distributed and networked control, model predictive control, and safe and secure automation systems with applications in mobile and space robotics, energy systems and biomedicine.

Mohamed Darouach graduated from Ecole Mohammadia d'Ingnieurs, Rabat, Morocco, in 1978, and received the Docteur Ingnieur and Doctor of Sciences degrees from Nancy University, France, in 1983 and 1986, respectively. From 1978 to 1986 he was associate professor and professor of automatic control at Ecole Hassania des Travaux Publics, Casablanca, Morocco. Since 1987 he is a professor at University de Lorraine. He has been a vice director of the Research Center in Automatic Control of Nancy (CRAN UMR 7039, Nancy-University, CNRS) from 2005 to 2013. He obtained a degree Honoris Causa from the Technical University of IASI and Since in 2010. He is a member of the Scientific Council of Luxembourg University. Since 2013 he is a vice director of the University Institute of Technology of Longwy (University de Lorraine). He held invited positions at University of Alberta, Edmonton. His research interests include span theoretical control, observers design, and control of large-scale uncertain systems with applications.



Changchun Hua received his Ph. D. degree from Yanshan University, China, in 2005. He was a research fellow in National University of Singapore Carleton University, Canada and University of Duisburg-Essen, Germany. Now he is a professor at Yanshan University, China. His research interests include nonlinear control systems, control systems design over network, teleoperation systems, and intelligent control.