Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Stochastic stability analysis of networked control systems with random cryptographic protection under random zero-measurement attacks*

Meng-zhou GAO[1,2,3], Dong-qin FENG‡[1]

[1]*State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou 310027, China*

[2]*School of Cyberspace, Hangzhou Dianzi University, Hangzhou 310018, China*

[3]*Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, Shanghai 200240, China*

E-mail: mzgao@hdu.edu.cn; dongqinfeng@zju.edu.cn

Received May 25, 2017; Revision accepted Aug. 9, 2017; Crosschecked Sept. 15, 2018

Abstract: Security issues in networked control systems (NCSs) have received increasing attention in recent years. However, security protection often requires extra energy consumption, computational overhead, and time delays, which could adversely affect the real-time and energy-limited system. In this paper, random cryptographic protection is implemented. It is less expensive with respect to computational overhead, time, and energy consumption, compared with persistent cryptographic protection. Under the consideration of weak attackers who have little system knowledge, ungenerous attacking capability and the desire for stealthiness and random zero-measurement attacks are introduced as the malicious modification of measurements into zero signals. NCS is modeled as a stochastic system with two correlated Bernoulli distributed stochastic variables for implementation of random cryptographic protection and occurrence of random zero-measurement attacks; the stochastic stability can be analyzed using a linear matrix inequality (LMI) approach. The proposed stochastic stability analysis can help determine the proper probability of running random cryptographic protection against random zero-measurement attacks with a certain probability. Finally, a simulation example is presented based on a vertical take-off and landing (VTOL) system. The results show the effectiveness, robustness, and application of the proposed method, and are helpful in choosing the proper protection mechanism taking into account the time delay and in determining the system sampling period to increase the resistance against such attacks.

Key words: Networked control systems; Security; Cyber attacks; Stochastic stability; Cryptographic protection
https://doi.org/10.1631/FITEE.1700334 **CLC number:** TP273

1 Introduction

The upgrade of proprietary network protocols to open protocols and the accessibility of remote users to sensor-control data via corporate networks and the Internet increase the efficiency of networked control systems (NCSs), but create cyber vulnerabilities in NCSs at the same time (Amin et al., 2013; Teixeira et al., 2015; Wang YN et al., 2016).

NCS cyber vulnerabilities, especially to deception attacks that compromise integrity (Teixeira

‡ Corresponding author

* Project supported by the National Natural Science Foundation of China (No. 61433006), the Key Research Project of Zhejiang Province, China (No. 2017C01062), the Open Research Project of the State Key Laboratory of Industrial Control Technology, Zhejiang University, China (No. ICT1800422), the Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, China (No. AGK2018003), the Department of Education of Zhejiang Province, China (No. Y201840611), and the Zhejiang Provincial Natural Science Foundation of China (No. LY16F020019)

ORCID: Meng-zhou GAO, https://orcid.org/0000-0003-2250-2127

et al., 2012), have received considerable attention in recent years. Following a carefully designed attack strategy, deception attacks are launched by compromising control packets or measurements (Pasqualetti et al., 2013) and changing correct data into designed incorrect data to cause the system to make incorrect decisions. In particular, stealthy deception attacks can be implemented without being discovered by traditional anomaly detectors, such as bad data detection schemes. The failure to give an alarm about an abnormal situation can cause serious control issues, such as stability problems. However, it has been overlooked largely that cyber attacks can be understood as intermittent or random implementations for the following reasons: (1) Success of adversary attacks is highly dependent on the network circumstances (e.g., network load, network congestion, and network transmission rate); (2) Attacks cannot be (or are arbitrarily) launched persistently if attackers have limited resources (e.g., energy) (Ding et al., 2017a, 2017b).

Recent research addresses intermittent or randomly occurring cyber attacks. The malicious modification of sensor data is characterized statistically by a set of unknown probability transition matrices and the distributed estimation problem is studied using quantized data in the presence of attacks (Zhang et al., 2015). Sensor measurements that may have been corrupted by a cyber attacker are estimated based on a binary random variable by new game-theoretic approaches (Vamvoudakis et al., 2014). Cyber attacks are modeled by a random Markov process in multiagent systems to study a distributed secure consensus tracking control problem (Feng et al., 2017). Deception attacks on commands and measurements are introduced intelligently and with intermittent behaviors to produce the most damage without being discovered (Muradore and Quaglia, 2015). The filter and fault estimator against randomly occurring nonlinearities and deception attacks are co-designed (Hu et al., 2016). Nevertheless, protection against such attacks is not considered simultaneously.

To protect the networked control system against deception attacks, cryptographic protection can be applied to an NCS that attempts to refuse well-designed attacks and deceives attackers by hiding information within a confusing string of seemingly random symbols. Moreover, stealthy deception attacks on encrypted data during transmission would be revealed and lose the stealthiness advantage eventually when the compromised data fail to derive the original plain data and turn into messy code during decryption. There have already been various applications of cryptographic protection to secure systems. Muradore and Quaglia (2015) proposed the application of a cryptographic algorithm on a short digest of a commonly known hash function between senders and receivers, so that the message signature is generated to ensure message integrity during transmission. A new concept of encrypting a linear controller using the modified homomorphic encryption schemes based on the public-key Rivest–Shamir–Adleman (RSA) and ElGamal encryption systems has been presented by Kogiso and Fujita (2015). A privacy-preserving protocol based on the Pallier additive homomorphic cryptosystem where each agent encrypts its own information before sending it to an untrusted cloud computing infrastructure was proposed by Shoukry et al. (2016). Symmetric cryptography and one-way encryption keys were used to protect sensitive data in networked critical infrastructures by Cao et al. (2013). Pang and Liu (2012) presented a secure transmission mechanism between the controller side and the plant side, involving the integrated data encryption standard (DES) algorithm, the message digest (MD5) algorithm, the timestamp strategy, and the recursive networked predictive control method. Some vendors have incorporated the AES-128 and AES-256 encryption algorithms into their meter design to protect confidentiality (Bennett and Wicker, 2010) and integrity in some cases. The IEC 62 351 protocol standard specifies the security requirements of data authentication, data confidentiality, access control, and intrusion detection (Wang et al., 2011).

However, cryptographic protection requires extra computational overhead, time, and energy consumption. It often makes security objectives conflict with real-time dynamic performance due to limited computation capacity, energy resources, and time and communication constraints (Wang D et al., 2016). Excessive cryptographic protection is wasteful and may even be harmful to the system. Therefore, cryptographic protection needs to be designed properly.

Qiu et al. (2012) balanced security strength and energy for a phasor measurement unit (PMU)

monitoring system in a smart grid. The tradeoff between the system's dynamic performance and its security was analyzed in a distributed networked control system (NCS) against various network attacks (Zeng and Chow, 2013). Muradore and Quaglia (2015) proposed a packet-based selective encryption mechanism which is designed to be active only when needed to reduce energy consumption, and to detect when an attack starts and ends. Jiang et al. (2016) proposed a unified framework to tackle energy, security, reliability, and timing requirements for security- and safety-critical systems.

In this paper, we propose a random implementation of cryptographic protection. This approach reduces the number of times that the protection is implemented, and therefore reduces computational overhead, time delays, and energy consumption compared with continuous cryptographic protection. We also introduce random zero-measurement attacks, which require less system knowledge, possess stealthiness well against the basic abnormal detection, and study the stochastic stability of NCS with random cryptographic protection under random zero-measurement attacks. The proposed theorem for stochastic stability considers the running probability of protection and attacks as two correlated Bernoulli distributed random variables. Simulations are carried out in a vertical take-off and landing (VTOL) aircraft system to show the effectiveness and application of random cryptographic protection against random measurement attacks and the robustness of the method in the presence of measurement noise. The theorem can be used to determine the proper probability of random cryptographic protection against random zero-measurement delays if the attack probability is known previously and the result is meaningful for an energy-limited or energy-constrained real-time system.

To facilitate the following discussions, a list of mathematical notations used in this study is given in Table 1.

Table 1 Notation list

Notation	Meaning
τ	The delay caused by the added security protection
T	Sampling period
k	Sequence number of the sampling instant
t_k	The k^{th} sampling instant
$\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$	System matrices
$\boldsymbol{K}$	Fixed feedback control gain
$\boldsymbol{x}(t)$	The state vector at time t
$\boldsymbol{y}(t)$	The measurement output with no attacks at time t
$\boldsymbol{x}_0$	Initial state vector
$\boldsymbol{x}_k$	The state vector at the k^{th} sampling instant
$\boldsymbol{y}_k$	The measurement output without attacks at the k^{th} sampling instant
α_k	The stochastic variable followed by random cryptographic protection at the k^{th} sampling instant
β'_k	The stochastic variable followed by random zero-measurement attacks with no protection at the k^{th} sampling instant
β_k	The stochastic variable followed by random zero-measurement attacks, in practice considering random cryptographic protection at the k^{th} sampling instant
$\bar{\alpha}$	Protection probability, which is the probability distribution of α_k
$\bar{\beta}$	Attack probability, which is the probability distribution of β'_k
$\boldsymbol{\xi}_k$	The malicious sampled measurement signals modified by adversaries at the k^{th} sampling instant
$\boldsymbol{y}_k^a$	The measurements considering both attacks and protection at the k^{th} sampling instant
$\boldsymbol{u}_k^a$	The control input considering both attacks and protection at the k^{th} sampling instant

2 Problem description

In this section, random cryptographic protection and random zero-measurement attacks are formulated and introduced. The linear time-invariant control system with a sampled controller under random cryptographic protection and random zero-measurement attacks is also presented.

2.1 Random cryptographic protection

To protect integrity and confidentiality, data (e.g., measurements and control commands) are encrypted before transmission through the network and then decrypted at the destination to obtain the original data. Specifically, unauthorized modification of encrypted transmitted data will cause incorrect decryption and result in messy code, which can be used as the evidence of data attacks. Compromised malicious signals can be discovered, discarded, and even trigger an alarm easily. Integrated cryptographic protection, however, inevitably causes additional delays and power consumption (Qiu et al., 2011).

Considering the limited computational ability and sacrificed performance of NCSs, random cryptographic protection is used to decrease the number of implementations and reduce implementation costs. In random cryptographic protection, communicated measurements are protected stochastically at different instants. Specifically, after measurements are sampled at sampling instant t_k, random cryptographic protection is implemented following stochastic variable $\alpha_k \in \{1, 0\}$, which is the Bernoulli distributed white sequence. If $\alpha_k = 1$, security protection is running and protection delays occur between the sensor and controller; if $\alpha_k = 0$, security protection is not running and protection delays do not occur between the sensor and controller. The protection probability of α_k is given as

$$\begin{cases} \text{Prob}\{\alpha_k = 1\} = \mathbb{E}\{\alpha_k\} = \bar{\alpha}, \\ \text{Prob}\{\alpha_k = 0\} = 1 - \mathbb{E}\{\alpha_k\} = 1 - \bar{\alpha}. \end{cases} \tag{1}$$

Thus, the energy consumption and resource savings as a result of random cryptographic protection are $(1-\bar{\alpha})\times 100\%$ of the energy consumption and resources that are needed for continuous cryptographic protection, respectively. Note that with random cryptographic protection, an encryption check will be launched before decryption to decide whether to decrypt the data.

2.2 Random zero-measurement attacks

Consider careful attackers who wish to be stealthy but have little capacity to design tricky attacking methods that can bypass basic detection of abnormalities. For example, if the injected attack value is too small or too large, and is beyond the allowable state threshold, the system will recognize the anomaly and can possibly raise an alarm to the system operator. Furthermore, the deviations caused by attacks will accumulate when the number of attacks increases if the expectancy value of the injected attacks is not equal to the true measurement value (Ding et al., 2017c). Under such considerations, zero-measurement attacks are designed by changing all sampled measurement signals into zeros ($\boldsymbol{\xi}_k = \mathbf{0}, k \in \mathbb{Z}$) which are mostly normal and expected (sometimes the nominal states are used as zeros) to spoof NCS with no need for external inputs.

Moreover, attackers who do not have a correct cryptographic key are unable to tamper with encrypted data without being discovered. According to Muradore and Quaglia (2015), the attacker cannot touch the encrypted messages if they expect to avoid being discovered. Assume that attackers have the ability to determine if messages are protected. This is reasonable because encrypted messages will be gibberish and unreadable. Facing unencrypted signals, attackers randomly launch zero-measurement attacks, which can be called 'random zero-measurement attacks', in light of their specific ability to follow a stochastic binary variable $\beta'_k \in \{0, 1\}$. In particular, when random cryptographic protection is not implemented, $\beta'_k = 1$ means that zero-measurement attacks are injected; $\beta'_k = 0$ means that zero-measurement attacks are not launched. When random cryptographic protection is implemented, zero-measurement attacks will not run and β'_k is always equal to zero. The probability distribution of β'_k is

$$\begin{cases} \text{Prob}\{\beta'_k = 1 | \alpha_k = 0\} = \mathbb{E}\{\beta'_k | \alpha_k = 0\} = \bar{\beta}, \\ \text{Prob}\{\beta'_k = 0 | \alpha_k = 0\} = 1 - \mathbb{E}\{\beta'_k | \alpha_k = 0\} = 1 - \bar{\beta}, \\ \text{Prob}\{\beta'_k = 1 | \alpha_k = 1\} = \mathbb{E}\{\beta'_k | \alpha_k = 1\} = 0, \\ \text{Prob}\{\beta'_k = 0 | \alpha_k = 1\} = 1 - \mathbb{E}\{\beta'_k | \alpha_k = 1\} = 1. \end{cases} \tag{2}$$

If the attackers are powerful, zero-measurement attacks can be launched frequently and even constantly; however, if the attackers have limited attacking energy, they might be unable to launch frequent zero-measurement attacks. As we can see, binary variables α_k and β'_k are correlated so that security protection affects the implementation of attacks. Considering the correlation with random cryptographic protection, the implementation of random zero-measurement attacks, in practice, follows probability β_k, which is formulated as

$$\beta_k = \beta'_k(1 - \alpha_k). \tag{3}$$

Note that α_k and β'_{k-1} are independent. Similarly, α_k and β_{k-1} are independent. β_k is also a binary variable. Because α_k, β'_k, and β_k are binary variables, we can obtain $\alpha_k\alpha_k = \alpha_k$, $\beta'_k\beta'_k = \beta'_k$, and $\beta_k\beta_k = \beta_k$. Moreover, the binary variables follow the distributive law of multiplication, and the following equalities can be derived:

$$\begin{cases}(1-\beta_k')(1-\alpha_k)=1-\alpha_k-\beta_k'(1-\alpha_k)=1-\alpha_k-\beta_k,\\ \alpha_k\beta_k=\alpha_k\beta_k'(1-\alpha_k)=0,\\ \alpha_k(1-\beta_k)=\alpha_k-\alpha_k\beta_k'(1-\alpha_k)=\alpha_k.\end{cases} \tag{4}$$

2.3 Networked control system model with random cryptographic protection under random zero-measurement attacks

The NCS model is shown in Fig. 1. System states are sensed under fixed sampling period T, and then sent to controllers via a communication network. Assume that time delay τ caused by cryptographic protection is smaller than sampling period T. In the case of random cryptographic protection, the system dynamics at sampling instant t_k becomes

$$\begin{aligned}\boldsymbol{x}_{k+1}&=\overline{\boldsymbol{A}}\boldsymbol{x}_k+\overline{\boldsymbol{B}}_2\boldsymbol{u}_k+\alpha_k\overline{\boldsymbol{B}}_3\boldsymbol{u}_{k-1}+(1-\alpha_k)\overline{\boldsymbol{B}}_3\boldsymbol{u}_k\\&=\overline{\boldsymbol{A}}\boldsymbol{x}_k+\overline{\boldsymbol{B}}_1\boldsymbol{u}_k+\alpha_k\overline{\boldsymbol{B}}_3(\boldsymbol{u}_{k-1}-\boldsymbol{u}_k),\end{aligned} \tag{5}$$

where

$$\boldsymbol{x}_k=\boldsymbol{x}(t_k),\boldsymbol{u}_k=\boldsymbol{u}(t_k),\overline{\boldsymbol{A}}=\mathrm{e}^{\boldsymbol{A}T},$$

$$\begin{cases}\overline{\boldsymbol{B}}_1=\displaystyle\int T_0\mathrm{e}^{\boldsymbol{A}\theta}\mathrm{d}\theta\boldsymbol{B}=(\mathrm{e}^{\boldsymbol{A}T}-\boldsymbol{I})\boldsymbol{A}^{-1}\boldsymbol{B},\\ \overline{\boldsymbol{B}}_2=\displaystyle\int_0^{T-\tau_0}\mathrm{e}^{\boldsymbol{A}\theta}\mathrm{d}\theta\boldsymbol{B}=[\mathrm{e}^{\boldsymbol{A}(T-\tau_0)}-\boldsymbol{I}]\boldsymbol{A}^{-1}\boldsymbol{B},\\ \overline{\boldsymbol{B}}_3=\overline{\boldsymbol{B}}_1-\overline{\boldsymbol{B}}_2.\end{cases}$$

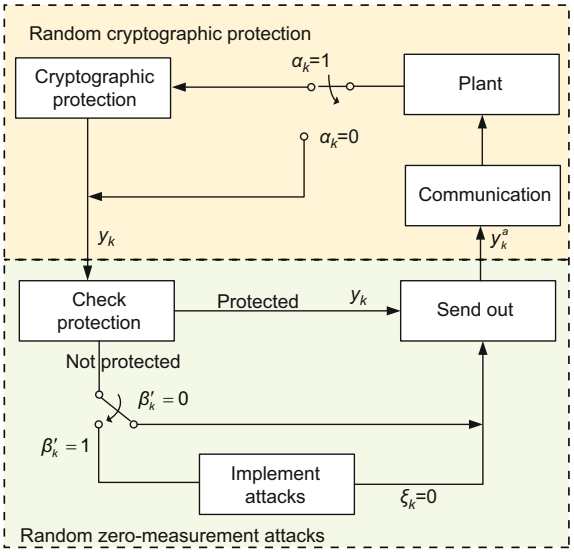


Fig. 1 The networked control system model under random zero-measurement attacks and random cryptographic protection

The discrete controller can be modeled as

$$\boldsymbol{u}(t)=\begin{cases}\boldsymbol{u}_0,0\le t<T+\tau,\\ \boldsymbol{u}_k,kT+\tau\le t<(k+1)T+\tau,k\in\mathbb{Z}^+,\end{cases} \tag{6}$$

where $\boldsymbol{u}_k=\boldsymbol{K}\boldsymbol{y}_k$. In the case of random zero-measurement attacks, the measurement of sampling instant $t_k=kT$ ($k\in\mathbb{Z}^+$) becomes

$$\begin{aligned}\boldsymbol{y}_k^a&=\alpha_k\boldsymbol{y}_k+(1-\alpha_k)[\beta_k'\boldsymbol{\xi}_k+(1-\beta_k')\boldsymbol{y}_k]\\&=\boldsymbol{y}_k+\beta_k(\boldsymbol{\xi}_k-\boldsymbol{y}_k),\end{aligned} \tag{7}$$

where $\boldsymbol{y}_k=\boldsymbol{C}\boldsymbol{x}_k$ is the normal measurement without being compromised. Then, the control input under a random attacking strategy turns into

$$\boldsymbol{u}_k^a=\boldsymbol{K}\boldsymbol{y}_k^a. \tag{8}$$

Substituting Eqs. (7) and (8) into Eq. (5), the formulation of the closed-loop system considering both the possible attacks and protection becomes

$$\begin{aligned}\boldsymbol{x}_{k+1}=&(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k+\beta_k\overline{\boldsymbol{B}}_1\boldsymbol{K}(\boldsymbol{\xi}_k-\boldsymbol{C}\boldsymbol{x}_k)\\&-\alpha_k\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_k+\alpha_k\overline{\boldsymbol{B}}_3\boldsymbol{K}[\boldsymbol{C}\boldsymbol{x}_{k-1}\\&+\beta_{k-1}(\boldsymbol{\xi}_{k-1}-\boldsymbol{C}\boldsymbol{x}_{k-1})],\end{aligned} \tag{9}$$

where if $\boldsymbol{\xi}_k=\boldsymbol{0}$, the NCS under random zero-measurement attacks and random cryptographic protection is formulated as

$$\begin{aligned}\boldsymbol{x}_{k+1}=&(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k-\beta_k\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_k\\&-\alpha_k\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_k+\alpha_k(1-\beta_{k-1})\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_{k-1}.\end{aligned} \tag{10}$$

3 Main results

In this section, some sufficient conditions are provided based on stochastic analysis. The following preliminaries are used to derive our main results:

Definition 1 (Stochastic stability (Xu et al., 2004)) The stochastic system (Eq. (10)) is said to be stochastically stable if there exists a scalar $\delta>0$ such that

$$\mathbb{E}\left\{\sum_{k=0}^{\infty}\boldsymbol{x}_k^2\right\}\le\delta\mathbb{E}\left\{\boldsymbol{x}_0^2\right\}. \tag{11}$$

Lemma 1 (Tarn and Rasis, 1976) Let $V(\boldsymbol{x}_k)$ be a Lyapunov functional. If there exist real scalars

$\psi_1 \geq 0, \mu > 0, \nu > 0$, and $0 < \psi_2 < 1$ such that

$$\mu \boldsymbol{x}_k^2 \leq V(\boldsymbol{x}_k) \leq \nu \boldsymbol{x}_k^2 \tag{12}$$

and

$$\mathbb{E}\{V(\boldsymbol{x}_{k+1})|\boldsymbol{x}_k\} - V(\boldsymbol{x}_k) \leq \psi_1 - \psi_2 V(\boldsymbol{x}_k), \tag{13}$$

then sequence $\boldsymbol{x}_k$ satisfies

$$\mathbb{E}\{\boldsymbol{x}_k^2\} \leq \frac{\nu}{\mu}\boldsymbol{x}_0^2(1-\psi_2)^k + \frac{\psi_1}{\mu\psi_2}. \tag{14}$$

Lemma 2 (Schur's complements) Given constant symmetric matrices $\boldsymbol{\Sigma}_1$, $\boldsymbol{\Sigma}_2$, and $\boldsymbol{\Sigma}_3$, where $\boldsymbol{\Sigma}_1 = \boldsymbol{\Sigma}_1^{\mathrm{T}}$ and $\boldsymbol{\Sigma}_2 = \boldsymbol{\Sigma}_2^{\mathrm{T}}$, the following conditions are equivalent:

$$\boldsymbol{\Sigma}_2 > 0, \boldsymbol{\Sigma}_1 + \boldsymbol{\Sigma}_3^{\mathrm{T}}\boldsymbol{\Sigma}_2^{-1}\boldsymbol{\Sigma}_3 < 0 \tag{15}$$

and

$$\begin{bmatrix} \boldsymbol{\Sigma}_1 & \boldsymbol{\Sigma}_3^{\mathrm{T}} \\ \boldsymbol{\Sigma}_3 & -\boldsymbol{\Sigma}_2 \end{bmatrix} < 0 \text{ or } \begin{bmatrix} -\boldsymbol{\Sigma}_2 & \boldsymbol{\Sigma}_3 \\ \boldsymbol{\Sigma}_3^{\mathrm{T}} & \boldsymbol{\Sigma}_1 \end{bmatrix} < 0. \tag{16}$$

We shall focus on the stochastic stability analysis for system (10). The two stochastic variables are considered correlated, and the correlation makes our stochastic stability different from those in previous studies. Now, we provide the main results in the following theorems:

Theorem 1 For a given controller gain matrix $\boldsymbol{K}$, closed-loop system (10) with random cryptographic protection of probability $\bar{\alpha}$ is stochastically stable under random zero-measurement attacks of probability $\bar{\beta}$, if there exist positive-definite matrices $\boldsymbol{P}_1$ and $\boldsymbol{P}_2$ satisfying

$$\begin{bmatrix} \boldsymbol{\Lambda}_1 & * & * & * \\ \boldsymbol{0} & \boldsymbol{\Lambda}_2 & * & * \\ \rho\boldsymbol{P}_1(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C}) & \rho\boldsymbol{P}_1\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C} & -\boldsymbol{P}_1 & * \\ \rho\boldsymbol{P}_1\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C} & \rho\boldsymbol{P}_1\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C} & \boldsymbol{0} & -\boldsymbol{P}_1 \end{bmatrix} < 0, \tag{17}$$

where ρ, $\boldsymbol{\Lambda}_1$, and $\boldsymbol{\Lambda}_2$ are denoted in Eq. (18), shown on the top of the next page.

Proof We define the following Lyapunov function for system (10):

$$\boldsymbol{V}_k = \boldsymbol{x}_k^{\mathrm{T}}\boldsymbol{P}_1\boldsymbol{x}_k + \boldsymbol{x}_{k-1}^{\mathrm{T}}\boldsymbol{P}_2\boldsymbol{x}_{k-1},$$

where $\boldsymbol{P}_1, \boldsymbol{P}_2$ are positive-definite matrices. Then we can derive Eq. (19), shown on the top of the next page.

Note that

$$\begin{aligned}\mathbb{E}\{\alpha_k(1-\beta_{k-1})\} &= \mathbb{E}\{\alpha_k - \alpha_k\beta_{k-1}^{'} - \alpha_k\beta_{k-1}^{'}\alpha_{k-1})\} \\ &= \bar{\alpha}(1-\bar{\beta}+\bar{\alpha}\bar{\beta}),\end{aligned} \tag{20}$$

$$\begin{aligned}\mathbb{E}\{\beta_k\} &= \mathbb{E}\{\beta_k|\alpha_k = 0\} = \sum_{i=1}^{2} x_i\mathbb{P}(\beta_k = x_i|\alpha_k = 0) \\ &= \mathbb{P}\{\beta_k = 1|\alpha_k = 0\} = (1-\bar{\alpha})\bar{\beta}.\end{aligned} \tag{21}$$

Then we have Eq. (22), shown on the top of the next page, where

$$\begin{aligned}\boldsymbol{\eta}_k &= [\boldsymbol{x}_k, \boldsymbol{x}_{k-1}]^{\mathrm{T}}, \\ \boldsymbol{\Lambda} &= \begin{bmatrix} \overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C} & \overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C} \\ \overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C} & -\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C} \end{bmatrix}^{\mathrm{T}} \\ &\quad \cdot \begin{bmatrix} \bar{\alpha}(1-\bar{\beta}+\bar{\alpha}\bar{\beta})\boldsymbol{P}_1 & \boldsymbol{0} \\ \boldsymbol{0} & \bar{\alpha}(1-\bar{\beta}+\bar{\alpha}\bar{\beta})\boldsymbol{P}_1 \end{bmatrix} \\ &\quad \cdot \begin{bmatrix} \overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C} & \overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C} \\ \overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C} & -\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C} \end{bmatrix} + \begin{bmatrix} \boldsymbol{\Lambda}_1 & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{\Lambda}_2 \end{bmatrix}.\end{aligned} \tag{23}$$

By Schur's complement, inequality (17) implies $\boldsymbol{\Lambda} < 0$. Thus, we have

$$\begin{aligned}&\mathbb{E}\{\boldsymbol{V}_{k+1}|\boldsymbol{x}_k, \boldsymbol{x}_{k-1}, \cdots, \boldsymbol{x}_0\} - \boldsymbol{V}_k = \boldsymbol{\eta}_k^{\mathrm{T}}\boldsymbol{\Lambda}\boldsymbol{\eta}_k \\ &\quad \leq -\lambda_{\min}(-\boldsymbol{\Lambda})\boldsymbol{\eta}_k^{\mathrm{T}}\boldsymbol{\eta}_k < -\alpha\boldsymbol{\eta}_k^{\mathrm{T}}\boldsymbol{\eta}_k,\end{aligned} \tag{24}$$

where

$$0 < \alpha < \min\{\lambda_{\min}(-\boldsymbol{\Lambda}), \sigma\}. \tag{25}$$

Define $\sigma := \max\{\lambda_{\max}(\boldsymbol{P}_1), \lambda_{\max}(\boldsymbol{P}_2)\}$. From inequality (24), we have

$$\begin{aligned}&\mathbb{E}\{\boldsymbol{V}_{k+1}|\boldsymbol{x}_k, \boldsymbol{x}_{k-1}, \cdots, \boldsymbol{x}_0\} - \boldsymbol{V}_k \\ &\quad < -\alpha\boldsymbol{\eta}_k^{\mathrm{T}}\boldsymbol{\eta}_k < -\frac{\alpha}{\sigma}\boldsymbol{V}_k := -\psi\boldsymbol{V}_k.\end{aligned} \tag{26}$$

Therefore, by Definition 1, it can be verified from Lemma 1 that closed-loop system (10) is stochastically stable by $\psi_2 = \psi$ and $\psi_1 = 0$.

This completes the proof.

Similarly, we can conduct the stochastic analysis of NCS without random cryptographic protection under random zero-measurement attacks as a special case of Theorem 1, to understand the impact of random zero-measurement attacks on NCS. The NCS under random zero-measurement attacks without random cryptographic protection is formulated as

$$\begin{aligned}\rho =&\sqrt{\bar{\alpha}(1-\bar{\beta}+\bar{\alpha}\bar{\beta})},\\ \boldsymbol{\Lambda}_1 =&(1-2\bar{\alpha}+2\bar{\alpha}\bar{\beta}-\bar{\beta}-\bar{\alpha}^2\bar{\beta})(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C})^{\mathrm{T}}\boldsymbol{P}_1(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C})+(\bar{\beta}-\bar{\alpha}\bar{\beta})\bar{\boldsymbol{A}}\mathrm{T}\boldsymbol{P}_1\bar{\boldsymbol{A}}\\ &+\bar{\alpha}(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C}-\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C})^{\mathrm{T}}\boldsymbol{P}_1(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C}-\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C})\\ &-\bar{\alpha}(1-\bar{\beta}+\bar{\alpha}\bar{\beta})(\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C})^{\mathrm{T}}\boldsymbol{P}_1(\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C})+\boldsymbol{P}_2-\boldsymbol{P}_1,\\ \boldsymbol{\Lambda}_2 =&-\bar{\alpha}(1-\bar{\beta}+\bar{\alpha}\bar{\beta})(\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C})^{\mathrm{T}}\boldsymbol{P}_1(\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C})-\boldsymbol{P}_2.\end{aligned}\tag{18}$$

$$\begin{aligned}&\mathbb{E}\{\boldsymbol{V}_{k+1}|\boldsymbol{x}_k,\boldsymbol{x}_{k-1},\cdots,\boldsymbol{x}_0\}-\boldsymbol{V}_k\\ &=\mathbb{E}\{\boldsymbol{x}_{k+1}^{\mathrm{T}}\boldsymbol{P}_1\boldsymbol{x}_{k+1}\}+\boldsymbol{x}_k^{\mathrm{T}}(\boldsymbol{P}_2-\boldsymbol{P}_1)\boldsymbol{x}_k-\boldsymbol{x}_{k-1}^{\mathrm{T}}\boldsymbol{P}_2\boldsymbol{x}_{k-1}\\ &=\mathbb{E}\{\alpha_k(1-\beta_{k-1})\}[(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k+\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_{k-1}]^{\mathrm{T}}\boldsymbol{P}_1[(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k+\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_{k-1}]\\ &\quad+\mathbb{E}\{\alpha_k(1-\beta_{k-1})\}(\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_k-\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_{k-1})^{\mathrm{T}}\boldsymbol{P}_1(\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_k-\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_{k-1})\\ &\quad+\mathbb{E}\{\beta_k\}(\overline{\boldsymbol{A}}\boldsymbol{x}_k)^{\mathrm{T}}\boldsymbol{P}_1\overline{\boldsymbol{A}}\boldsymbol{x}_k+\mathbb{E}\{\alpha_k\}[(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C}-\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k]^{\mathrm{T}}\boldsymbol{P}_1[(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C}-\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k]\\ &\quad-\mathbb{E}\{\alpha_k(1-\beta_{k-1})\}\{[(\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k]^{\mathrm{T}}\boldsymbol{P}_1[(\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k]+[(\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_{k-1}]^{\mathrm{T}}\boldsymbol{P}_1[(\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_{k-1}]\}\\ &\quad+(1-\mathbb{E}\{\alpha_k\}-\mathbb{E}\{\beta_k\}-\mathbb{E}\{\alpha_k(1-\beta_{k-1})\})[(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k]^{\mathrm{T}}\boldsymbol{P}_1[(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k]\\ &\quad+\boldsymbol{x}_k^{\mathrm{T}}(\boldsymbol{P}_2-\boldsymbol{P}_1)\boldsymbol{x}_k-\boldsymbol{x}_{k-1}^{\mathrm{T}}\boldsymbol{P}_2\boldsymbol{x}_{k-1}.\end{aligned}\tag{19}$$

$$\begin{aligned}&\mathbb{E}\{\boldsymbol{V}_{k+1}|\boldsymbol{x}_k,\boldsymbol{x}_{k-1},\cdots,\boldsymbol{x}_0\}-\boldsymbol{V}_k\\ &=\bar{\alpha}(1-\bar{\beta}+\bar{\alpha}\bar{\beta})[(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k+\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_{k-1}]^{\mathrm{T}}\boldsymbol{P}_1[(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k+\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_{k-1}]\\ &\quad+\bar{\alpha}(1-\bar{\beta}+\bar{\alpha}\bar{\beta})(\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_k-\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_{k-1})^{\mathrm{T}}\boldsymbol{P}_1(\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_k-\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_{k-1})\\ &\quad+(1-\bar{\alpha})\bar{\beta}(\overline{\boldsymbol{A}}\boldsymbol{x}_k)^{\mathrm{T}}\boldsymbol{P}_1\overline{\boldsymbol{A}}\boldsymbol{x}_k+\bar{\alpha}[(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C}-\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k]^{\mathrm{T}}\boldsymbol{P}_1[(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C}-\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k]\\ &\quad-\bar{\alpha}(1-\bar{\beta}+\bar{\alpha}\bar{\beta})\{[(\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k]^{\mathrm{T}}\boldsymbol{P}_1[(\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k]+[(\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_{k-1}]^{\mathrm{T}}\boldsymbol{P}_1[(\overline{\boldsymbol{B}}_3\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_{k-1}]\}\\ &\quad+[1-2\bar{\alpha}+2\bar{\alpha}\bar{\beta}-\bar{\beta}-\bar{\alpha}^2\bar{\beta})][(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k]^{\mathrm{T}}\boldsymbol{P}_1[(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k]\\ &\quad+\boldsymbol{x}_k^{\mathrm{T}}(\boldsymbol{P}_2-\boldsymbol{P}_1)\boldsymbol{x}_k-\boldsymbol{x}_{k-1}^{\mathrm{T}}\boldsymbol{P}_2\boldsymbol{x}_{k-1}\\ &=\boldsymbol{\eta}_k^{\mathrm{T}}\boldsymbol{\Lambda}\boldsymbol{\eta}_k.\end{aligned}\tag{22}$$

$$\boldsymbol{x}_{k+1}=\overline{\boldsymbol{A}}\boldsymbol{x}_k+(1-\beta_k)\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C}\boldsymbol{x}_k.\tag{27}$$

Theorem 2 For a given controller gain matrix $\boldsymbol{K}$, closed-loop system (27) without random cryptographic protection is stochastically stable under random zero-measurement attacks with probability $\bar{\beta}$, if there exists positive-definite matrix $\boldsymbol{P}$ satisfying

$$\begin{bmatrix}-\boldsymbol{P} & * & *\\ \rho_1\boldsymbol{P}(\bar{\boldsymbol{A}}+\bar{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C}) & -\boldsymbol{P} & *\\ \rho_2\boldsymbol{P}\bar{\boldsymbol{A}} & 0 & -\boldsymbol{P}\end{bmatrix}<0,\tag{28}$$

where $\rho_1=\sqrt{1-\bar{\beta}}$, and $\rho_2=\sqrt{\bar{\beta}}$.

Proof We define the following Lyapunov function for system (27):

$$\boldsymbol{V}_k=\boldsymbol{x}_k^{\mathrm{T}}\boldsymbol{P}\boldsymbol{x}_k,$$

and $\boldsymbol{P}$ is a positive-definite matrix. Then we can derive

$$\begin{aligned}&\mathbb{E}\{\boldsymbol{V}_{k+1}|\boldsymbol{x}_k,\boldsymbol{x}_{k-1},\cdots,\boldsymbol{x}_0\}-\boldsymbol{V}_k\\ &=\mathbb{E}\{\boldsymbol{x}_{k+1}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{x}_{k+1}\}-\boldsymbol{x}_k^{\mathrm{T}}\boldsymbol{P}\boldsymbol{x}_k\\ &=\mathbb{E}\{(1-\beta_k)\}[(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k]^{\mathrm{T}}\\ &\quad\cdot\boldsymbol{P}[(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k]+\mathbb{E}\{\beta_k\}(\overline{\boldsymbol{A}}\boldsymbol{x}_k)^{\mathrm{T}}\boldsymbol{P}\overline{\boldsymbol{A}}\boldsymbol{x}_k\\ &\quad-\boldsymbol{x}_k^{\mathrm{T}}\boldsymbol{P}\boldsymbol{x}_k\\ &=(1-\bar{\beta})[(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k]^{\mathrm{T}}\boldsymbol{P}[(\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C})\boldsymbol{x}_k]\\ &\quad+\bar{\beta}(\overline{\boldsymbol{A}}\boldsymbol{x}_k)^{\mathrm{T}}\boldsymbol{P}\overline{\boldsymbol{A}}\boldsymbol{x}_k-\boldsymbol{x}_k^{\mathrm{T}}\boldsymbol{P}\boldsymbol{x}_k\\ &=\boldsymbol{x}_k^{\mathrm{T}}\boldsymbol{\Lambda}_1\boldsymbol{x}_k,\end{aligned}\tag{29}$$

where

$$\begin{aligned}\boldsymbol{\Lambda}_1=&\begin{bmatrix}\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C}\\ \overline{\boldsymbol{A}}\end{bmatrix}^{\mathrm{T}}\begin{bmatrix}(1-\bar{\beta})\boldsymbol{P} & \boldsymbol{0}\\ \boldsymbol{0} & \bar{\beta}\boldsymbol{P}\end{bmatrix}\\ &\cdot\begin{bmatrix}\overline{\boldsymbol{A}}+\overline{\boldsymbol{B}}_1\boldsymbol{K}\boldsymbol{C}\\ \overline{\boldsymbol{A}}\end{bmatrix}-\boldsymbol{P}.\end{aligned}\tag{30}$$

By Schur's complement, inequality (28) implies that $\boldsymbol{\Lambda}_1<0$. Thus, we have

$$\begin{aligned}\mathbb{E}\{\boldsymbol{V}_{k+1}|\boldsymbol{x}_k,\boldsymbol{x}_{k-1},\cdots,\boldsymbol{x}_0\}-\boldsymbol{V}_k&=\boldsymbol{x}_k^{\mathrm{T}}\boldsymbol{\Lambda}_1\boldsymbol{x}_k\\&\leq-\lambda_{\min}(-\boldsymbol{\Lambda}_1)_k^{\mathrm{T}}\boldsymbol{x}_k<-\alpha_1\boldsymbol{x}_k^{\mathrm{T}}\boldsymbol{x}_k,\end{aligned}\tag{31}$$

where

$$0<\alpha_1<\min\{\lambda_{\min}(-\boldsymbol{\Lambda}_1),\sigma_1\}.\tag{32}$$

Define $\sigma_1:=\lambda(\boldsymbol{P})$. From inequality (31), we have

$$\begin{aligned}&\mathbb{E}\{\boldsymbol{V}_{k+1}|\boldsymbol{x}_k,\boldsymbol{x}_{k-1},\cdots,\boldsymbol{x}_0\}-\boldsymbol{V}_k\\&<-\alpha_1\boldsymbol{x}_k^{\mathrm{T}}\boldsymbol{x}_k<-\frac{\alpha_1}{\sigma_1}\boldsymbol{V}_k:=-\psi_3\boldsymbol{V}_k.\end{aligned}\tag{33}$$

Therefore, by Definition 1, it can be verified from Lemma 1 that closed-loop system (27) is stochastically stable by $\psi_2=\psi_3$ and $\psi_1=0$.

This completes the proof.

4 Simulation examples

The aim of random zero-measurement attacks is to make the system unstable, whereas the goal of random protection is to maintain stability. In this section, we demonstrate the effectiveness and applicability of the proposed method using a VTOL aircraft system as an example. The robustness of this method in the presence of measurement noise is also shown. The following is the linearized dynamic equation of the VTOL aircraft system (Keel et al., 1988):

$$\begin{aligned}\dot{\boldsymbol{x}}(t)=&\begin{bmatrix}-0.0366&0.0271&0.0188&-0.4555\\0.0482&-1.01&0.0024&-4.0208\\0.1002&0.3681&-0.707&1.42\\0&0&1&0\end{bmatrix}\boldsymbol{x}(t)\\&+\begin{bmatrix}0.4422&0.1761\\3.5446&-7.5922\\-5.52&4.49\\0&0\end{bmatrix}\boldsymbol{u}(t),\\\boldsymbol{y}(t)=&[0,\ \ 1,\ \ 0,\ \ 0]\boldsymbol{x}(t),\\\boldsymbol{u}(t)=&\begin{bmatrix}-0.9963\\1.8018\end{bmatrix}\boldsymbol{y}(t),\end{aligned}\tag{34}$$

where $\boldsymbol{x}=[x_1,x_2,x_3,x_4]^{\mathrm{T}}$ and $\boldsymbol{u}=[u_1,u_2]^{\mathrm{T}}$. Specifically, x_1,x_2,x_3, and x_4 denote the horizontal velocity, vertical velocity, pitch rate, and pitch angle, respectively. u_1 and u_2 denote the collective and longitudinal cyclic pitch control, respectively.

4.1 Stability analysis of the networked control system without random cryptographic protection under random zero-measurement attacks

In this case, the impact of random zero-measurement attacks on stability is analyzed without implementation of random cryptographic protection. Specifically, we can obtain the maximum attack probability $\bar{\beta}$ that NCS, without random cryptographic protection, can maintain its stability by solving the corresponding stability problem based on Theorems 1 and 2 using the LMI toolbox. For Theorem 1, this case is a special situation with $\alpha_k=0$. The results under various sampling periods T's derived from Theorem 1 (with $\alpha_k=0,k\in\mathbb{Z}$) and Theorem 2 are presented in Tables 2 and 3, respectively.

Table 2 Maximum allowable attack probability for the stochastic stability of the networked control system without random cryptographic protection based on Theorem 1

T (s)	$\bar{\beta}$	T (s)	$\bar{\beta}$
0.01	0.827	0.07	0.787
0.02	0.821	0.08	0.777
0.03	0.815	0.09	0.764
0.04	0.809	0.10	0.747
0.05	0.803	0.11	0.719
0.06	0.795	0.12	–

Table 3 Maximum allowable attack probability for the stochastic stability of the networked control system without random cryptographic protection based on Theorem 2

T (s)	$\bar{\beta}$	T (s)	$\bar{\beta}$
0.01	0.826	0.07	0.787
0.02	0.821	0.08	0.777
0.03	0.815	0.09	0.764
0.04	0.809	0.10	0.748
0.05	0.803	0.11	0.719
0.06	0.795	0.12	0

According to Tables 2 and 3, we can determine that the maximum allowable attack probability decreases as the sampling period increases. It means that NCS is more resistant against random zero-measurement attacks with a lower sampling period without random cryptographic protection. The reason could be that a system that samples more frequently may have less dependence on every discretely updated control and be more tolerant of

attacked measurements of the same attack probability $\bar{\beta}$, while a system that has a larger sampling period may rely more on individual measurements. Therefore, for the NCS without random cryptographic protection, a smaller sampling period is recommended to protect against random zero-measurement attacks of the larger attack probability.

Moreover, as we can see, the results derived from Theorem 1 are the same as those derived from Theorem 2, except for the circumstances where the sampling periods are equal to 0.01, 0.10, and 0.12 s, proving the effectiveness of Theorems 1 and 2. Based on Theorem 1, we can see that the system without random cryptographic protection is unstable when $T >$ 0.12 s, even if random zero-measurement attacks are not implemented. Based on Theorem 2, the system without random cryptographic protection is stochastically stable only if random zero-measurement attacks are not implemented ($\bar{\beta} = 0$) when $T = 0.12$ s, and is not stochastically stable when $T > 0.12$ s.

There is little difference between the results derived from Theorems 1 and 2. As for the difference between the results derived from Theorems 1 and 2, larger differences are determined as the final result of the maximum allowable attack probability for stochastic stability of the NCS without random cryptographic protection, because Theorems 1 and 2 are both sufficient but unnecessary conditions.

4.2 Stability analysis of the networked control system with random cryptographic protection under random zero-measurement attacks

In this case, assume that the probability of random zero-measurement attacks is known to system operators; this probability may be determined by vulnerability analysis or quantification of the system security state considering the attackers' capability. Following the proposed Theorem 1, the proper probability that random protection of the system maintains its stability against random zero-measurement attacks can be derived. Let sampling time T be 0.10 s and the time cost on security protection τ be 0.01 s. The simulation results of the stability analysis are shown in Fig. 2; the dot means that NCS with the corresponding protection probability $\bar{\alpha}$ and attack probability $\bar{\beta}$ is stable.

As shown in Fig. 2, the NCS without random cryptographic protection ($\bar{\alpha} = 0$) can be determined as stable based on Theorem 1 when attack probability $\bar{\beta}$ of random zero-measurement attacks is in the range of $[0, 0.748]$. When $\bar{\beta} > 0.748$, the NCS with random cryptographic protection of certain protection probability $\bar{\alpha}$ can be determined as stable based on Theorem 1, and the minimum required protection probability $\bar{\alpha}$ for stability increases with the increase of the attack probability. For example, when $\bar{\beta} = 1$, NCS can be determined as stable for protection probability $\bar{\alpha} \in [0.279, 1]$. The trajectories of the system states under random zero-measurement attacks of probability $\bar{\beta} = 1$ with random cryptographic protection of two different probabilities $\bar{\alpha} = 0$ and 0.279 are provided in Figs. 3 and 4, respectively. Specifically, the trajectory is derived as the mean values of the system states after 1000 individual trials. As shown in Fig. 3, the trajectory of the system states diverges. This represents the instability of NCS under such circumstances and is consistent with the result derived from Theorem 2 (Fig. 2). In Fig. 4, the trajectory of system states converges and NCS is stable under random cryptographic protection of probability $\bar{\alpha} = 0.279$. This agrees with the result derived from Theorem 1 (Fig. 2). This is consistent with the fact that random cryptographic protection with a larger probability could decrease the chance of random zero-measurement attacks with the same $\bar{\beta}$, which reduces the impact of the attack on stability. Therefore, the results demonstrate that random zero-measurement attacks with a certain attack probability can determine the consequences of instability and can be protected effectively by the proposed random cryptographic protection. Also,

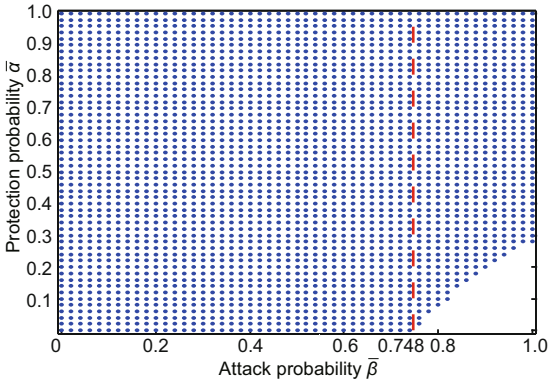


Fig. 2 Stability analysis of the networked control system with random cryptographic protection of various protection probabilities $\bar{\alpha}$'s under random zero-measurement attacks of various attack probabilities $\bar{\beta}$'s

References to color refer to the online version of this figure

the effectiveness of the proposed method in analyzing the stability of NCS with both random cryptographic protection and random zero-measurement attacks is proved.

4.3 Robustness of random protection in the presence of measurement noise

In this subsection, the robustness of random protection in the presence of measurement noise is studied based on simulations. Denote ω as the measurement noise, which follows the Gaussian distribution $\mathcal{N}(0,\sigma^2)$.

In the absence of measurement noise, the trajectory of the system states with random cryptographic protection of probability $\bar{\alpha}=0.279$ under random zero-measurement attacks of probability $\bar{\beta}=1$ is depicted in Fig. 4. Under the same protection and attack conditions, the same system is used to study the robustness of random protection in the presence of measurement noise. After 100 individual trials, the trajectories of the system states with the presence of different measurement noises are shown in Fig. 5. Specifically, simulations are performed under different values of σ^2 as $0.001, 0.01, 0.1$, and 1, as shown in Figs. 5a–5d.

As we can see, the system has certain robustness against measurement noise. In Fig. 5a, the system with measurement noise $\omega\sim\mathcal{N}(0,0.001)$ has a good robustness against the measurement noise. The fluctuations are small compared with the system without measurement noise (Fig. 4). In Fig. 5b, the fluctuation of the system with measurement noise $\omega\sim\mathcal{N}(0,0.01)$ is larger. In Fig. 5c, the system's robustness against measurement noise $\omega\sim\mathcal{N}(0,0.1)$ becomes worse; however, the system can remain stochastically stable. In Fig. 5d, the system with measurement noise $\omega\sim\mathcal{N}(0,1)$ tends to diverge, representing loss of robustness against measurement noise.

4.4 Impact of different delays for random protection on stability analysis

The time delay of random cryptographic protection is different with specific cryptographic

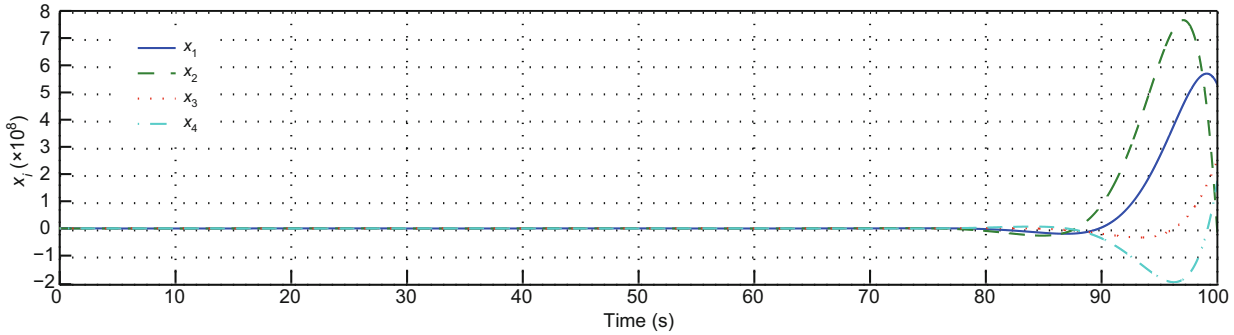


Fig. 3 Trajectories of system states without random cryptographic protection under random zero-measurement attacks of probability $\bar{\beta}=1$

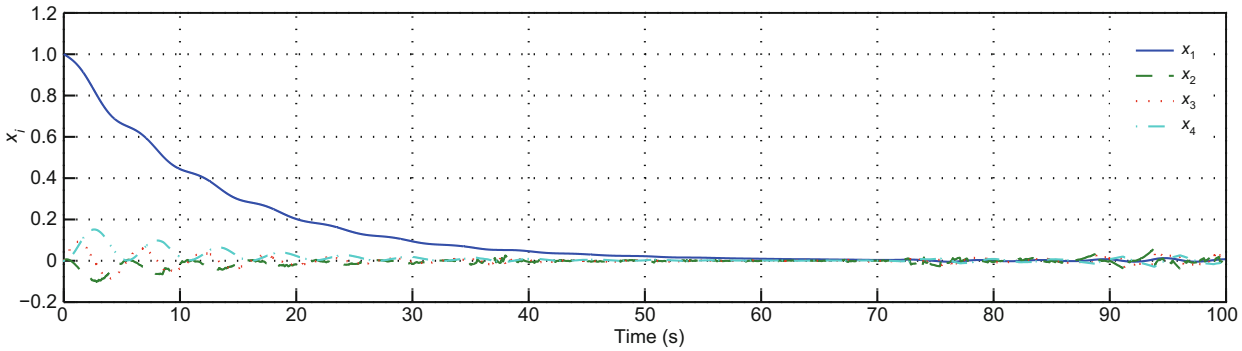
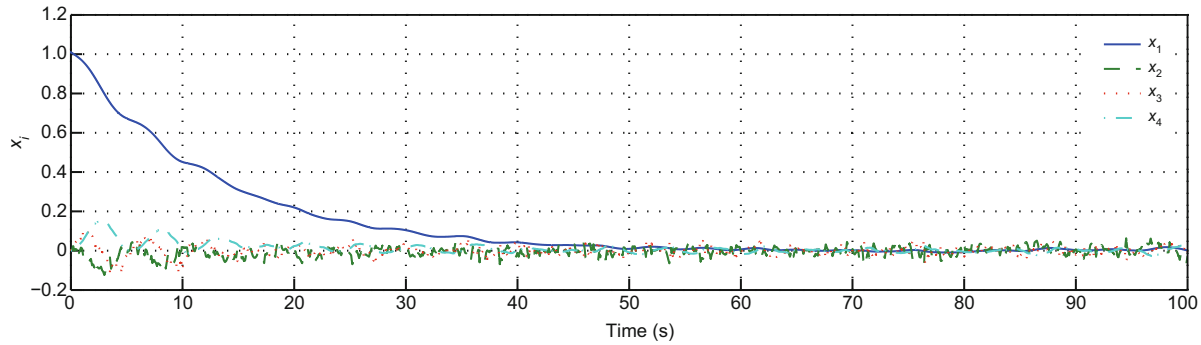
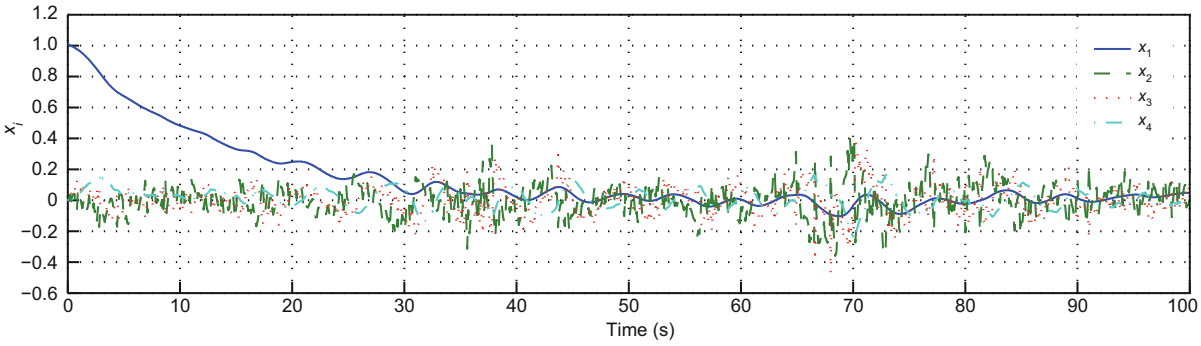


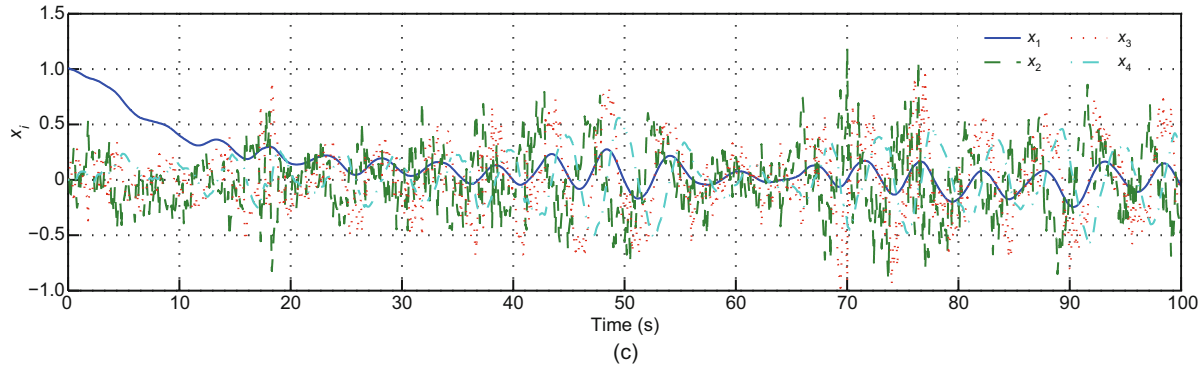
Fig. 4 Trajectories of system states with random cryptographic protection of probability $\bar{\alpha}=0.279$ under random zero-measurement attacks of probability $\bar{\beta}=1$



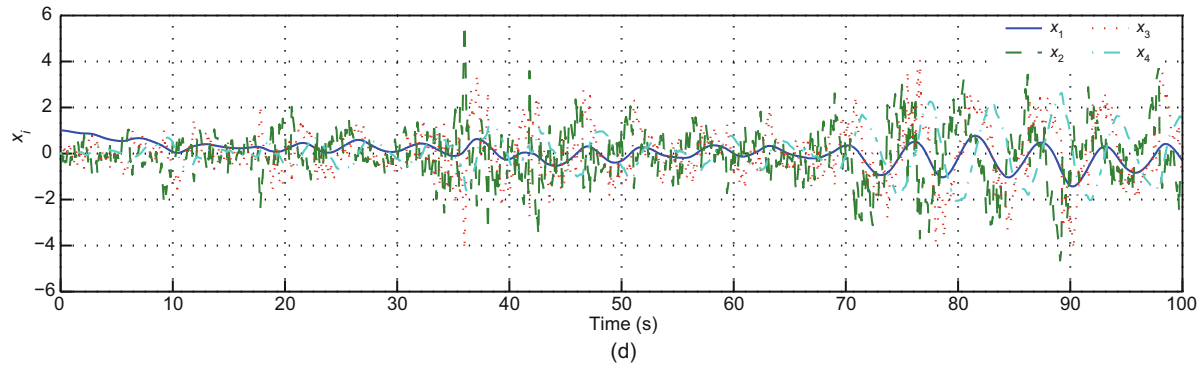
(a)



(b)



(c)



(d)

Fig. 5 Robustness of random cryptographic protection when measurement noises are $\omega \sim \mathcal{N}(0, 0.001)$ (a), $\omega \sim \mathcal{N}(0, 0.01)$ (b), $\omega \sim \mathcal{N}(0, 0.1)$ (c), and $\omega \sim \mathcal{N}(0, 1)$ (d)

algorithms, implementation platforms, and other factors. We analyzed the performance of random cryptographic protection for stability maintenance under different delays. Let sampling time T be 0.10 s. Simulations were performed for various cryptographic protection delays, such as 0.01, 0.03, 0.04, 0.05, and 0.09 s.

For these different delays, the stability regions of NCS with random cryptographic protection of $\bar{\alpha} \in [0,1]$ under random zero-measurement attacks of $\bar{\beta} \in [0,1]$ are depicted in Fig. 6. As we can see, the region decreases as the time delay increases. This is caused by random cryptographic protection. When the time delay is small (e.g., τ=0.01 or 0.03 s), feasible solutions of Theorem 1 always exist, and the system with random cryptographic protection of a certain protection probability is always stochastically stable for random zero-measurement attacks of any probability $\bar{\beta} \in [0,1]$. However, note that the minimum protection probability of random cryptographic protection which is required for NCS stability under random zero-measurement attacks increases as the time delay increases. Thus, Theorems 1 and 2 determine the minimum required protection probability under different attack probabilities to protect stability sufficiently but not too costly on energy consumption, computational overhead, and time delays.

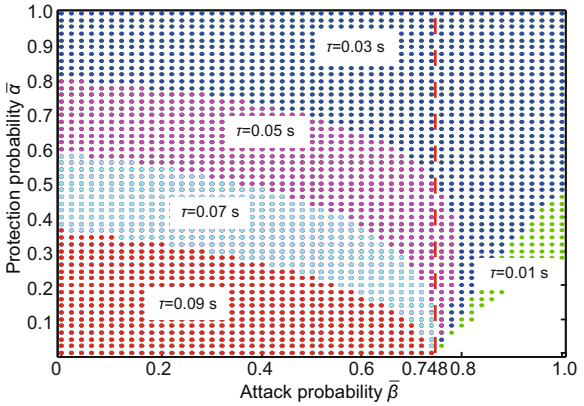


Fig. 6 Stability analysis of the networked control system with random zero-measurement attacks and random cryptographic protection for various protection delays τ

References to color refer to the online version of this figure

When the time delay becomes large, e.g., τ=0.05 or 0.09 s (Fig. 6), feasible stability analysis solutions cannot be determined by Theorem 1 for the NCS under random zero-measurement attacks of probability $\bar{\beta} > 0.748$. As discussed before, the random zero-measurement attacks of $\bar{\beta} \leq 0.748$ do not destabilize NCS. Thus, it is not guaranteed that random cryptographic protection can maintain the stability of NCS under random zero-measurement attacks when τ is large. In addition, there is no feasible solution for stochastic stability of NCS based on Theorem 1 under random zero-measurement attacks of a tolerable attack probability ($\bar{\beta} < 0.748$) when protection probability $\bar{\alpha}$ is large. In other words, random cryptographic protection might, in turn, aggravate the instability of the system under attacks. Also, it is interesting that the protection probability for the NCS stability under a certain attack probability could be piecewise. For example, when $\bar{\beta} = 0.78$, the system cannot be determined as stable via Theorem 1, with random cryptographic protection of probability $\bar{\alpha} \in [0, 0.16)$ and $\bar{\alpha} > 0.40$; however, it is stable with random cryptographic protection of probability $\bar{\alpha} \in [0.16, 0.40]$. These findings mean that the added security protection can protect the stochastic stability of NCS against random zero-measurement attacks; however, it can also have harmful effects on system stability and should, therefore, be designed carefully based on our proposed method.

4.5 Impact of the sampling period for random protection on stability analysis

In this subsection, the performance of random cryptographic protection in maintaining the stability of NCS with various sampling periods under random zero-measurement attacks is analyzed. Let τ=0.03 s and sampling period T be 0.03, 0.04, 0.06, 0.08, or 0.1 s. Fig. 7 shows the stability analysis of NCS with various sampling periods under random zero-measurement attacks and random cryptographic protection.

We can see that the stability region of protection probability $\bar{\alpha}$ and attack probability $\bar{\beta}$ increases with the increase of the sampling period. Specifically, when the NCS sampling period is small (e.g., $T = 0.08, 0.06, 0.04$, or 0.03 s), there is no feasible solution that can be derived from Theorem 1 if attack probability $\bar{\beta}$ is too large. Also, if protection probability $\bar{\alpha}$ is too large, the stochastic stability cannot be determined based on Theorem 1. This may be caused by the conservativeness of the proposed sufficient theorem, especially for protection probability

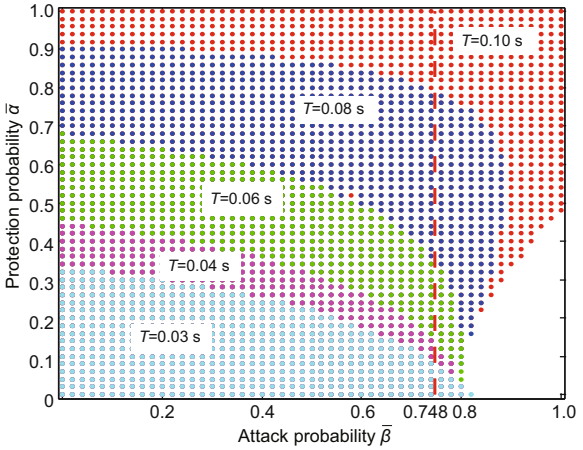


Fig. 7 Stability analysis of the networked control system with random zero-measurement attacks and random cryptographic protection for various sampling periods T

References to color refer to the online version of this figure

$\bar{\alpha}$ on the region boundary. However, another major reason could be that random cryptographic protection with a large protection probability $\bar{\alpha}$ is too intensive and may harm the NCS stability. This is obvious for the NCS with a lower sampling period. Therefore, the protection probability should be designed with consideration of the system sampling period. This could also be suggestive and considered during the design of the system's sampling period to enlarge the stability region of protection probability $\bar{\alpha}$ and attack probability $\bar{\beta}$, so that the protection can help NCS resist attacks with a large attack probability.

5 Conclusions

In this paper, random zero-measurement attacks have been introduced and formulated. To maintain stability of NCS under such attacks, random cryptographic protection was proposed, which requires less energy consumption, less computational overhead, and smaller time delays, compared with persistent cryptographic protection. Considering the attack and protection probabilities as two correlated Bernoulli distributed stochastic variables, sufficient conditions for the stochastic stability analysis were proposed and mathematically demonstrated. Based on the proposed theorem, the proper probability of random cryptographic protection for maintaining the stability of NCS under random zero-measurement attacks of certain attack probabilities can be determined by solving LMI. Finally, simulations were performed in a VTOL aircraft system. The results proved the effectiveness of our proposed method in determining the proper protection probability and robustness against measurement noise. The effects of the system sampling period and cryptographic delay on the stability analysis were provided.

This paper is useful in securing real-time NCSs with limited energy and computation resources. The proposed theorem is helpful in determining the proper time delay of the protection and the proper system sampling period to increase the system robustness against attacks, and can be considered as one corresponding factor of choosing the protection mechanism and designing the system sampling mechanism. In the future, the effect of random cryptographic protection on the dynamic performance of NCS will be studied, and a tradeoff model between security and energy cost, computation cost, and system dynamic performance will be analyzed.

References

Amin S, Litrico X, Sastry S, et al., 2013. Cyber security of water scada systems—part I: analysis and experimentation of stealthy deception attacks. *IEEE Trans Contr Syst Technol*, 21(5):1963-1970. https://doi.org/10.1109/tcst.2012.2211873

Bennett C, Wicker SB, 2010. Decreased time delay and security enhancement recommendations for AMI smart meter networks. Power & Energy Society Innovative Smart Grid Technologies Conf, p.1-6. https://doi.org/10.1109/isgt.2010.5434780

Cao HY, Zhu PD, Lu XC, et al., 2013. A layered encryption mechanism for networked critical infrastructures. *IEEE Netw*, 27(1):12-18. https://doi.org/10.1109/mnet.2013.6423186

Ding DR, Wang ZD, Ho DWC, et al., 2017a. Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks. *IEEE Trans Cybern*, 47(8):1936-1947. https://doi.org/10.1109/tcyb.2016.2582802

Ding DR, Wang ZD, Ho DWC, et al., 2017b. Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks. *Automatica*, 78:231-240. https://doi.org/10.1016/j.automatica.2016.12.026

Ding DR, Wei GL, Zhang SJ, et al., 2017c. On scheduling of deception attacks for discrete-time networked systems equipped with attack detectors. *Neurocomputing*, 219:99-106. https://doi.org/10.1016/j.neucom.2016.09.009

Feng Z, Wen GH, Hu GQ, 2017. Distributed secure coordinated control for multiagent systems under strategic attacks. *IEEE Trans Cybern*, 47(5):1273-1284. https://doi.org/10.1109/tcyb.2016.2544062

Hu J, Liu S, Ji DH, et al., 2016. On co-design of filter and fault estimator against randomly occurring nonlinearities and randomly occurring deception attacks. *Int J Gener Syst*, 45(5):619-632. https://doi.org/10.1080/03081079.2015.1106730

Jiang W, Pop P, Jiang K, 2016. Design optimization for security- and safety-critical distributed real-time applications. *Microprocess Microsyst*, 52:401-415. https://doi.org/10.1016/j.micpro.2016.08.002

Keel LH, Bhattacharyya SP, Howze JW, 1988. Robust control with structure perturbations. *IEEE Trans Autom Contr*, 33(1):68-78. https://doi.org/10.1109/9.362

Kogiso K, Fujita T, 2015. Cyber-security enhancement of networked control systems using homomorphic encryption. IEEE 54th Annual Conf on Decision and Control, p.6836-6843. https://doi.org/10.1109/cdc.2015.7403296

Muradore R, Quaglia D, 2015. Energy-efficient intrusion detection and mitigation for networked control systems security. *IEEE Trans Ind Inform*, 11(3):830-840. https://doi.org/10.1109/tii.2015.2425142

Pang ZH, Liu GP, 2012. Design and implementation of secure networked predictive control systems under deception attacks. *IEEE Trans Contr Syst Technol*, 20(5):1334-1342. https://doi.org/10.1109/tcst.2011.2160543

Pasqualetti F, Dörfler F, Bullo F, 2013. Attack detection and identification in cyber-physical systems. *IEEE Trans Autom Contr*, 58(11):2715-2729. https://doi.org/10.1109/tac.2013.2266831

Qiu MK, Gao WZ, Chen M, et al., 2011. Energy efficient security algorithm for power grid wide area monitoring system. *IEEE Trans Smart Grid*, 2(4):715-723. https://doi.org/10.1109/tsg.2011.2160298

Qiu MK, Su H, Chen M, et al, 2012. Balance of security strength and energy for a PMU monitoring system in smart grid. *IEEE Commun Mag*, 50(5):142-149. https://doi.org/10.1109/mcom.2012.6194395

Shoukry Y, Gatsis K, Alanwar A, et al., 2016. Privacy-aware quadratic optimization using partially homomorphic encryption. IEEE 55th Conf on Decision and Control, p.5053-5058. https://doi.org/10.1109/cdc.2016.7799042

Tarn TJ, Rasis Y, 1976. Observers for nonlinear stochastic systems. *IEEE Trans Autom Contr*, 21(4):441-448. https://doi.org/10.1109/tac.1976.1101300

Teixeira A, Pérez D, Sandberg H, et al., 2012. Attack models and scenarios for networked control systems. Proc 1st Int Conf on High Confidence Networked Systems, p.55-64. https://doi.org/10.1145/2185505.2185515

Teixeira A, Sou KC, Sandberg H, et al., 2015. Secure control systems: a quantitative risk management approach. *IEEE Contr Syst*, 35(1):24-45. https://doi.org/10.1109/mcs.2014.2364709

Vamvoudakis KG, Hespanha JP, Sinopoli B, et al., 2014. Detection in adversarial environments. *IEEE Trans Autom Contr*, 59(12):3209-3223. https://doi.org/10.1109/tac.2014.2351671

Wang D, Wang ZD, Shen B, et al., 2016. Recent advances on filtering and control for cyber–physical systems under security and resource constraints. *J Franklin Inst*, 353(11):2451-2466. https://doi.org/10.1016/j.jfranklin.2016.04.011

Wang WY, Xu Y, Khanna M, 2011. A survey on the communication architectures in smart grid. *Comput Netw*, 55(15):3604-3629. https://doi.org/10.1016/j.comnet.2011.07.010

Wang YN, Lin ZR, Liang X, et al., 2016. On modeling of electrical cyber-physical systems considering cyber security. *Front Inform Technol Electron Eng*, 17(5):465-478. https://doi.org/10.1631/fitee.1500446

Xu SY, Lam J, Chen TW, 2004. Robust H_∞ control for uncertain discrete stochastic time-delay systems. *Syst Contr Lett*, 51(3):203-215. https://doi.org/10.1016/j.sysconle.2003.08.004

Zeng WT, Chow M, 2013. Modeling and optimizing the performance–security tradeoff on D-NCS using the co-evolutionary paradigm. *IEEE Trans Ind Inform*, 9(1):394-402. https://doi.org/10.1109/tii.2012.2209662

Zhang JF, Blum RS, Lu XX, et al., 2015. Asymptotically optimum distributed estimation in the presence of attacks. *IEEE Trans Signal Process*, 63(5):1086-1101. https://doi.org/10.1109/tsp.2014.2386281