Event-Based Security Control for Discrete-time Stochastic Systems

Derui Ding[1,*], Zidong Wang[2,3], Guoliang Wei[1], Fuad E. Alsaadi[3]

[1]Shanghai Key Lab of Modern Optical System, Department of Control Science and Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China
[2]Department of Computer Science, Brunel University London, Uxbridge, Middlesex UB8 3PH, U.K.
[3]Faculty of Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia.
[*]deruiding2010@usst.edu.cn

Abstract: This paper is concerned with the event-based security control problem for a class of discrete-time stochastic systems with multiplicative noises subject to both randomly occurring Denial-of-Service (DoS) attacks and randomly occurring deception attacks. An event-triggered mechanism is adopted with hope to reduce the communication burden, where the measurement signal is transmitted only when a certain triggering condition is violated. A novel attack model is proposed to reflect the randomly occurring behaviors of the DoS attacks as well as the deception attacks within a unified framework via two sets of Bernoulli distributed white sequences with known conditional probabilities. A new concept of mean-square security domain is put forward to quantify the security degree. We aim to design an output feedback controller such that the closed-loop system achieves the desired security. By using the stochastic analysis techniques, some sufficient conditions are established to guarantee the desired security requirement and the control gain is obtained by solving some linear matrix inequalities with nonlinear constraints. A simulation example is utilized to illustrate the usefulness of the proposed controller design scheme.

1. Introduction

It has been well recognized that some characteristics of nonlinear systems can be closely approximated by models with multiplicative noises rather than by linearized models [1]. In the past few decades, considerable research efforts have been made on the control issues for stochastic systems with multiplicative noises (also called bilinear systems or systems with state-dependent noises) and a rich body of literature has been available. Up to now, there have been mainly four approaches that shed insightful lights on the control design of stochastic systems with multiplicative noises, namely, the game-theoretic method [2], the linear matrix inequality (LMI) approach [3], the Riccati equation approach [4, 5] and the optimization method [6].

Owing to the ever-increasing popularity of communication networks, more and more control tasks are executed over communication links [7–13]. It should be mentioned that, in the interest of energy saving, the traditional time-based control scheme might be a conservative choice. According to the engineering practice, when the limited resource becomes a concern, the following three points should be taken into account when selecting communication protocols: 1) too frequent data interaction via networks is likely to overspend the depletable bandwidth and thus deteriorate communication quality; 2) it is often the case that only some vitally important measurement data should be transmitted for control/estimation purposes as long as the basic system performance can be maintained; and 3) unnecessary communications between the system components in an energy-limited environment (e.g. battery-operated wireless sensor networks) could lead to the waste of the limited resource. In this case, it is theoretically significant and practically important to develop some new control schemes that are capable of utilizing the network resource in an efficient way when transmitting measurement or control information. In response to the engineering need for emerge-saving, in the past few years, the event-based control issues have received much attention from the control community. Some initial yet inspiring results have been reported in [14–18] for the consensus control problems of multi-agent systems, in [19–22] for the sample-data control problems, and in [23] for the model predictive control problems. Note that the main characteristics of the event-based control scheme are that the control information is updated only when some function of the system state or measurement exceeds a certain threshold [24–26]. In comparison with the widely used time-based control scheme, such an event-based scheme could effectively reduce the communication burden and improve the resource utilization efficiency. As such, it makes practical sense to investigate the event-based control problem for stochastic systems with multiplicative noises.

As is well known, sensors, controllers and controlled plants are often connected over a common network medium for networked control systems (NCSs). In such an engineering setting, the exchanged data without security protection can be easily exploited by attackers (or adversaries) [27]. Nowadays, two types of attack models, namely, Denial-of-Service (DoS) attacks and deception attacks, are generally adopted in the performance analysis and synthesis when it comes to the security issue. It is worth noting that, by destroying certain significant data, the aim of the adversaries is often to destabilize the plant or steer the plant to the adversaries' expected operating point [28]. As such, the network security is of utmost importance in modern society that has been attracting considerable attention in recent years. Up to now, some preliminary results have been reported in the literature, see, e.g. [29–31] for the case of DoS attacks, [32,33] for the case of deception attacks and [34, 35] for the case of replay attacks. Furthermore, for the attacked systems with protection equipment or software, the attacks may occur in a *random* way since the successes of the attacks are largely dependent on the network conditions (e.g. network load, network congestion, network transmission rate) that are typically randomly fluctuated. Very recently, a Bernoulli process or Markov process with known statistical information has been employed in [36] to govern the randomly occurring DoS attacks. Nevertheless, the network-induced random nature of the deception attacks has been largely overlooked due probably to the difficulty in coming up with appropriate methodologies for the problem formulation and theoretical analysis. Furthermore, the attackers could adopt any type of attack at a particular time in order to increase their successful ratio. Therefore, to closely reflect the reality, it would be practically significant to look into the security issue when both the DoS deception attacks occur randomly within a unified framework.

Summarizing the discussion above, it can be concluded that the security control problems have attracted some initial research interest and most available results have been concerned with the single type of attacks (e.g. either DoS attacks or deception attacks). So far, the security control problem with both *randomly occurring DoS attacks and randomly occurring deception attacks* has not been properly investigated, not to mention the case where *the event-based communication scheme* is also utilized. It is, therefore, the purpose of this paper to shorten such a gap by examining the impact of mixed network attacks on the system security under an event-based mechanism. This appears to be a challenging task with two essential difficulties identified as follows: 1) how can we establish a model to describe randomly occurring DoS attacks and randomly occurring deception attacks within a unified framework? 2) what kind of methods can be developed to quantify the influences from both the random nature and the interference signals transmitted by adversaries on the security performance?

In this paper, to handle the two identified challenges, an attack model is first proposed to simultaneously describe the randomly occurring DoS attacks and randomly occurring deception attacks via two sets of Bernoulli distributed white sequences, and a new concept of mean-square security domain is put forward to quantify the security degree. Then, by using the stochastic analysis techniques, some sufficient conditions are established to guarantee the security requirement of the addressed systems and the desired controller gain is obtained by solving certain linear matrix inequalities with nonlinear constraints. The main contribution of this paper is mainly threefold: *1) A novel attack model is established to account for the randomly occurring behaviors of the DoS attacks and the deception attacks; 2) the event-based mechanism is utilized to reduce the communication burden; and 3) based on the proposed attack model, the controller gain is obtained to ensure that the closed-loop system is secure with respect to the parameter set* $(\delta_1, \delta_2, \delta_3, \delta_4, R)$ *where each parameter does have its own engineering interpretation.*

Notation The notation used here is fairly standard except where otherwise stated. $\mathbb{R}^n$ and $\mathbb{R}^{n\times m}$ denote, respectively, the n dimensional Euclidean space and the set of all $n \times m$ real matrices. I denotes the identity matrix of compatible dimensions. The notation $X \geq Y$ (respectively, $X > Y$), where X and Y are symmetric matrices, means that $X - Y$ is positive semi-definite (respectively, positive definite). A^T represents the transpose of A. $\lambda_{max}(A)$ and $\lambda_{min}(A)$ denote the maximum and minimum eigenvalue of A, respectively. For matrices $A \in \mathbb{R}^{m\times n}$ and $B \in \mathbb{R}^{p\times q}$, their Kronecker product is a matrix in $\mathbb{R}^{mp\times nq}$ denoted as $A \otimes B$. $\mathbb{E}\{x\}$ stands for the expectation of the stochastic variable x. $||x||$ describes the Euclidean norm of a vector x. The shorthand $\mathrm{diag}\{M_1, M_2, \cdots, M_n\}$ denotes a block diagonal matrix with diagonal blocks being the matrices M_1, ..., M_n. In symmetric block matrices, the symbol $*$ is used as an ellipsis for terms induced by symmetry.

2. Problem Formulation and Preliminaries

In this paper, consider the following discrete-time stochastic system with multiplicative noises in both the system and measurement equations:

$$\begin{cases} x_{k+1} = \Big(A_0 + \sum_{i=1}^{r} \omega_{i,k} A_i\Big) x_k + B u_k \\ \tilde{y}_k = \Big(C_0 + \sum_{i=1}^{s} \varpi_{i,k} C_i\Big) x_k \end{cases} \tag{1}$$

where $x_k \in \mathbb{R}^{n_x}$, $\tilde{y}_k \in \mathbb{R}^{n_y}$ and $u_k \in \mathbb{R}^{n_u}$ are the state vector, the sensor measurement and the controller input, respectively. A_i ($i = 0, 1. \cdots, r$), B and C_i ($i = 0, 1. \cdots, s$) are known constant matrices with appropriate dimensions. $\omega_{i,k} \in \mathbb{R}$ ($i = 1, 2, \cdots, r$) and $\varpi_{i,k} \in \mathbb{R}$ ($i = 1, 2, \cdots, s$) are multiplicative noises with zero means and unity variances, and are mutually uncorrelated in k and i, r and s are known positive integers. It is assumed that the rank of B is n_u.

In this paper, an event-triggered communication mechanism is taken into consideration in order to reduce the communication burden. Define the event generator function $\psi(\cdot, \cdot) : \mathbb{R}^{n_y} \times \mathbb{R} \to \mathbb{R}$ as follows:

$$\psi(e_k, \delta) = e_k^T e_k - \delta_1^2 \tag{2}$$

where

$$e_k := \tilde{y}^t_{k_s} - \tilde{y}_k$$

with $\tilde{y}^t_{k_s}$ being the *transmitted* information at the *latest* event instant and δ_1 being a given positive scalar. The executions are triggered as long as the condition

$$\psi(e_k, \delta_1) > 0$$

is satisfied. Therefore, the sequence of event triggered instants

$$0 \leq s_0 < s_1 < \cdots < s_l < \cdots$$

is determined iteratively by

$$s_{l+1} = \inf\{k \in \mathbb{N} | k > s_l,\ \psi(e_k, \delta_1) > 0\}.$$

Furthermore, it is assumed that the attackers only destroy the transmitted data and have the ability to carry out both the Denial-of-Service (DoS) attacks and the deception attacks with certain success probabilities, in other words, both kinds of attack can be launched in a random way. To reflect such a situation that is of practical significance, a new attack model is proposed as follows:

$$y^t_{k_s} = \alpha^t_{k_s}(\tilde{y}^t_{k_s} + \beta^t_{k_s} v^t_{k_s}) + (1 - \alpha^t_{k_s}) y^t_{k_{s-1}} \tag{3}$$

where $y^t_{k_s}$ is the *register information* on the controller and $v^t_{k_s} \in \mathbb{R}^{n_y}$ stands for the signals sent by attackers. In addition, $v^t_{k_s}$ is modeled as

$$v^t_{k_s} = -\tilde{y}^t_{k_s} + \xi^t_{k_s}$$

for deception attacks where the non-zero $\xi^t_{k_s}$ satisfying

$$\|\xi^t_{k_s}\| \leq \delta_2$$

is an arbitrary bounded energy signal. The stochastic variables α_{k_s} and β_{k_s} are Bernoulli distributed white sequences taking values on 0 or 1 with the following probabilities

$$\begin{aligned} \text{Prob}\{\alpha_{k_s} = 0\} = 1 - \bar{\alpha}, \quad \text{Prob}\{\alpha_{k_s} = 1\} = \bar{\alpha}, \\ \text{Prob}\{\beta_{k_s} = 0\} = 1 - \bar{\beta}, \quad \text{Prob}\{\beta_{k_s} = 1\} = \bar{\beta}, \end{aligned}$$

where $\bar{\alpha} \in [0, 1)$ and $\bar{\beta} \in [0, 1)$ are two known constants.

Remark 1. Generally speaking, network attacks can be divided into the Denial-of-Service (DoS) attacks and the deception attacks. For DoS attacks, the adversary prevents the controller from receiving sensor measurements. For deception attacks, the adversary sends false information to controllers. Due to the network-induced phenomena and the application of safety protection devices, there is a nonzero probability for each attack launched via networks to be unsuccessful at a certain time. The model proposed in (3) provides a novel unified framework to account for the phenomena of both randomly occurring DoS attacks and randomly occurring deception attacks.

Remark 2. Three cases can be observed from (3) as follows: a) the systems suffer from the deception attacks when $\alpha_{k_s}^t = 1$ and $\beta_{k_s}^t = 1$; b) the systems are subject to the DoS attacks when $\alpha_{k_s}^t = 0$ and the register information on controller cannot be updated in this case; and c) the controller receives the normal sensor measurements when $\alpha_{k_s}^t = 1$ and $\beta_{k_s}^t = 0$. Furthermore, it is worth mentioning that Case a) (with $\xi_{k_s}^t = 0$) describes the traditional phenomenon of packet dropouts and Case b) can also reflect the time-delays. Therefore, the proposed attack model covers time delays and packet dropouts as its special cases.

Remark 3. Due to limited energy, the adversaries could not arbitrarily launch the attacks and, from the defenders' perspective, the cyber-attack could be intermittent and the injected signal is bounded. Furthermore, the injected signal sent by adversaries is a kind of invalid information to achieve the control task and therefore it can be viewed as an energy bounded noise. The main purpose of the present research is to improve the security by enhancing the insensitivity to certain types of bounded and random cyber-attacks.

For $k \in [k_s, k_{s+1})$, the *register information* (3) can be rewritten as

$$y_k = \alpha_{k_s}^t (\tilde{y}_{k_s}^t + \beta_{k_s}^t v_{k_s}^t) + (1 - \alpha_{k_s}^t) y_{k-1} \tag{4}$$

with $y_{k_s} = y_{k_s}^t$. Furthermore, taking both the even-triggering condition and the attack bound into consideration, and applying the output-feedback control

$$u_k = K y_k$$

where K is the control parameter to be determined, one has the following closed-loop system

$$\begin{aligned} \tilde{x}_{k+1} = {} & \mathcal{A}_1 \tilde{x}_k + (\bar{\alpha} - \alpha_{k_s}^t) \mathcal{A}_2 \tilde{x}_k + ((\alpha_{k_s}^t - \bar{\alpha}) - \chi_{k_s}) \mathcal{A}_3 \tilde{x}_k \\ & + \mathcal{A}_{4,k_s} \tilde{x}_k + \bar{\alpha} \bar{\beta} \mathcal{A}_5 \xi_{k_s}^t + \bar{\alpha}(1 - \bar{\beta}) \mathcal{A}_5 e_k + \chi_{k_s} \mathcal{A}_5 \xi_{k_s}^t + ((\alpha_{k_s}^t - \bar{\alpha}) - \chi_{k_s}) \mathcal{A}_5 e_k. \end{aligned} \tag{5}$$

where

$$\begin{aligned} \tilde{x}_k &= \left[\begin{array}{cc} x_k^T & y_{k-1}^T \end{array} \right]^T, \\ \chi_{k_s} &= (\alpha_{k_s}^t - \bar{\alpha}) \bar{\beta} + (\beta_{k_s}^t - \bar{\beta}) \bar{\alpha} + (\alpha_{k_s}^t - \bar{\alpha})(\beta_{k_s}^t - \bar{\beta}) \\ \mathcal{A}_1 &= \left[\begin{array}{cc} A_0 + \bar{\alpha}(1 - \bar{\beta}) BKC_0 & (1 - \bar{\alpha}) BK \\ \bar{\alpha}(1 - \bar{\beta}) C_0 & (1 - \bar{\alpha}) I \end{array} \right], \\ \mathcal{A}_2 &= \left[\begin{array}{cc} 0 & BK \\ 0 & I \end{array} \right], \quad \mathcal{A}_3 = \left[\begin{array}{cc} BKC_0 & 0 \\ C_0 & 0 \end{array} \right], \quad \mathcal{A}_5 = \left[\begin{array}{c} BK \\ I \end{array} \right] \\ \mathcal{A}_{4,k_s} &= \left[\begin{array}{cc} \sum_{i=1}^r \omega_{i,k} A_i + \alpha_{k_s}^t (1 - \beta_{k_s}^t) \sum_{i=1}^s \varpi_{i,k} BKC_i & 0 \\ \alpha_{k_s}^t (1 - \beta_{k_s}^t) \sum_{i=1}^s \varpi_{i,k} C_i & 0 \end{array} \right] \end{aligned}$$

Remark 4. A schematic structure of the addressed control problem can be shown in Fig. 1. The adversary can detect the transmitted data from plants and then try to destroy them to attain certain goals. Furthermore, in order to increase the success ratio and enhance the covertness of attacks, the adversary could randomly adopt any type of attacks at each time. On the other hand, it is easy to find from (2) that the time interval (also called inter-event time) between adjacent event-triggering instants is generally not a constant, which is determined by the event generator function ψ. Therefore, the closed-loop system (5) cannot be regarded as a discrete-time expression with constant sampling interval.

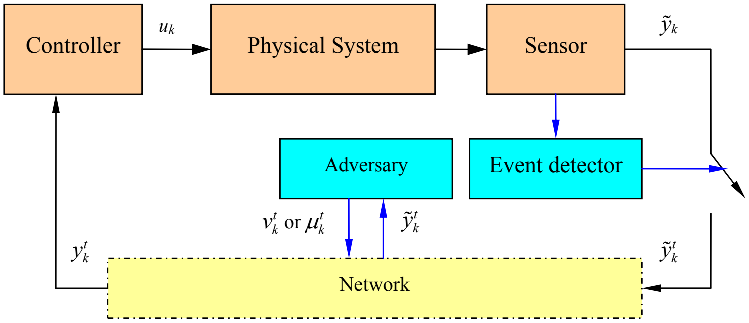

Fig. 1. *Attacks on an event-based control system.*

Before proceeding further, we introduce the following definitions.

Definition 1. For a given positive scalar δ_3 representing the desired security level, the set

$$\mathscr{D} = \left\{ \tilde{x}_0 \in \mathbb{R}^{n_x} : \mathbb{E}||\tilde{x}_k||^2 \leq \delta_3^2, \ \forall k \right\} \tag{6}$$

is said to be the mean-square security domain of the origin of the closed-loop system (5).

Definition 2. Let R be a positive definite matrix and δ_1, δ_2, δ_3 and δ_4 be given constants. The closed-loop system (5) is said to be secure with respect to $(\delta_1, \delta_2, \delta_3, \delta_4, R)$ if, when $\psi(e_k, \delta_1) \leq 0$, $||\xi_k|| \leq \delta_2$ and $\tilde{x}_0^T R \tilde{x}_0 \leq \delta_4^2$, one has $\mathbb{E}||\tilde{x}_k||^2 \leq \delta_3^2$ for all k.

Remark 5. The five parameters δ_1, δ_2, δ_3, δ_4 and R do have their own engineering insights. To be specific, δ_1 is the triggering threshold that governs the transmission frequency for the benefit of energy saving, δ_2 is the energy bound for the false signals that the adversary likes to impose on the measurement output from the attacked system, δ_3 is associated with the desired security level (i.e., the upper bound for the dynamics evolution of the attached system in the mean square sense), δ_4 is about the energy of the initial system state and R is the weighting matrix for the initial system state. Obviously, these five parameters play crucial roles for the system security performance evaluation and design.

Our aim in this paper is to design an output feedback controller for system (5) with the event-triggering communication mechanism and the randomly occurring cyber attacks. In other words, we are going to determine the controller gain K such that the closed-loop system (5) is secure with respect to $(\delta_1, \delta_2, \delta_3, \delta_4, R)$.

3. Main Results

In this section, the security is analyzed for the closed-loop system (5) with the event-triggering communication mechanism and the randomly occurring cyber attacks. A sufficient condition is provided to guarantee that the closed-loop system (5) is secure with respect to $(\delta_1, \delta_2, \delta_3, \delta_4, R)$. Then, the explicit expression of the desired controller gain is proposed in terms of the solution to certain matrix inequalities subject to nonlinear constraints.

Let us start with giving the following lemma that will be used in the proof of our main result in this paper.

Lemma 1. Given constant matrices Σ_1, Σ_2, Σ_3, where $\Sigma_1 = \Sigma_1^T$ and $\Sigma_2 = \Sigma_2^T > 0$. Then $\Sigma_1 + \Sigma_3^T \Sigma_2^{-1} \Sigma_3 < 0$ if and only if

$$\begin{bmatrix} \Sigma_1 & \Sigma_3^T \\ \Sigma_3 & -\Sigma_2 \end{bmatrix} < 0 \quad \text{or} \quad \begin{bmatrix} -\Sigma_2 & \Sigma_3 \\ \Sigma_3^T & \Sigma_1 \end{bmatrix} < 0.$$

Theorem 1. Let the positive scalars $\delta_1, \delta_2, \delta_3, \delta_4$, the positive definite matrix R and the controller gain K be given. The closed-loop system (5) is secure with respect to $(\delta_1, \delta_2, \delta_3, \delta_4, R)$ if there exist two positive definite matrices P_1 and P_2, and three positive scalars ε_1, ε_2 and π satisfying the following inequalities

$$\begin{cases} \Xi_1 = \begin{bmatrix} \Xi_{11} & \Xi_{12} & \Xi_{13} \\ * & \Xi_{22} & 0 \\ * & * & \Xi_{33} \end{bmatrix} < 0 & \text{(7a)} \\ \Xi_2 = \max\left\{ \dfrac{\lambda_{\max}(P_R)\delta_4^2}{\lambda_{\min}(P)}, \dfrac{\theta^2\gamma}{\lambda_{\min}(P)(\gamma-1)} \right\} \leq \delta_3^2 & \text{(7b)} \end{cases}$$

where

$$\begin{aligned} \mathcal{A}_4 &= \text{diag}\Big\{ \sum_{i=1}^{r} A_i^T P_1 A_i + \bar{\alpha}(1-\bar{\beta}) \sum_{i=1}^{s} \big((BKC_i)^T P_1 BKC_i + C_i^T P_2 C_i \big), 0 \Big\}, \\ P &= \text{diag}\{P_1, P_2\}, \quad \bar{\chi} = \tilde{\alpha}\bar{\beta}^2 + \tilde{\beta}\bar{\alpha}^2 + \tilde{\alpha}\tilde{\beta}, \;\; \theta = \sqrt{\varepsilon_1\delta_1^2 + \varepsilon_2\delta_2^2}, \\ \Xi_{11} &= \mathcal{A}_1^T P \mathcal{A}_1 + \tilde{\alpha}\mathcal{A}_2^T P \mathcal{A}_2 - 2(\tilde{\alpha} - \tilde{\alpha}\bar{\beta})\mathcal{A}_2^T P \mathcal{A}_3 \\ &\quad + (\tilde{\alpha} - 2\tilde{\alpha}\bar{\beta} + \bar{\chi})\mathcal{A}_3^T P \mathcal{A}_3 + \mathcal{A}_4 - P + \pi I, \\ \Xi_{12} &= \bar{\alpha}\bar{\beta}\mathcal{A}_1^T P \mathcal{A}_5 - \tilde{\alpha}\bar{\beta}\mathcal{A}_2^T P \mathcal{A}_5 + (\tilde{\alpha}\bar{\beta} - \bar{\chi})\mathcal{A}_3^T P \mathcal{A}_5, \\ \Xi_{13} &= \bar{\alpha}(1-\bar{\beta})\mathcal{A}_1^T P \mathcal{A}_5 - (\tilde{\alpha} - \tilde{\alpha}\bar{\beta})\mathcal{A}_2^T P \mathcal{A}_5 + (\tilde{\alpha} - 2\tilde{\alpha}\bar{\beta} + \bar{\chi})\mathcal{A}_3^T P \mathcal{A}_5, \\ \Xi_{22} &= ((\bar{\alpha}\bar{\beta})^2 + \bar{\chi})\mathcal{A}_5^T P \mathcal{A}_5 - \varepsilon_2 I, \quad \Xi_{23} = (\bar{\alpha}^2\tilde{\beta} + \tilde{\alpha}\bar{\beta} - \bar{\chi})\mathcal{A}_5^T P \mathcal{A}_5 \\ \Xi_{33} &= (\bar{\alpha}^2(1-\bar{\beta})^2 + \tilde{\alpha} - 2\tilde{\alpha}\bar{\beta} + \bar{\chi})\mathcal{A}_5^T P \mathcal{A}_5 - \varepsilon_1 I, \quad \tilde{\alpha} = \bar{\alpha}(1-\bar{\alpha}), \\ P_R &= R^{-1/2} P R^{-1/2}, \;\; \rho = \lambda_{\max}(P), \quad \gamma = \frac{\rho}{\rho - \pi}, \quad \tilde{\beta} = \bar{\beta}(1-\bar{\beta}). \end{aligned}$$

Proof: See the Appendix.

Having obtained the analysis results, we are now in a position to handle the design problem of the controller gain matrix K. First, in terms of Lemma 1 and the inequality

$$2(\mathcal{A}_2 - \mathcal{A}_3)^T P \mathcal{A}_3 \leq (\mathcal{A}_2 - \mathcal{A}_3)^T P (\mathcal{A}_2 - \mathcal{A}_3) + \mathcal{A}_3^T P \mathcal{A}_3,$$

(7a) is true if the following holds

$$\Pi_1 = \begin{bmatrix} \Pi_{11} & * & * \\ \bar{\Pi}_{12} & -\bar{P}^{-1} & * \\ \Pi_{17} & 0 & -I \otimes P_1^{-1} \end{bmatrix} < 0 \tag{8}$$

where

$$\begin{aligned}
\mathcal{B}_1 &= [\ \mathcal{A}_3 \quad -\mathcal{A}_5 \quad \mathcal{A}_5\ ], \quad \mathcal{B}_2 = [\ \mathcal{A}_2 - \mathcal{A}_3 \quad \mathcal{A}_5 \quad \mathcal{A}_5\ ],\\
\mathcal{S}_1 &= \text{diag}\{I, 0, -I\}, \quad \mathcal{S}_2 = \text{diag}\{I, -I, I\},\\
\bar{P} &= \text{diag}\big\{P, P, P, P, P\big\}, \quad \Upsilon = [\ C_1^T \quad C_2^T \quad \cdots \quad C_s^T\ ]^T,\\
\Pi_{00} &= \sum_{i=1}^{r} A_i^T P A_i + \bar{\alpha}(1-\bar{\beta}) \sum_{i=1}^{s} C_i^T P_2 C_i - P_1 + \pi I,\\
\Pi_{11} &= \text{diag}\Big\{\Pi_{00}, -P_2 + \pi I,\ -\varepsilon_2 I,\ -\varepsilon_1 I\Big\},\\
\bar{\Pi}_{12} &= [\ \Pi_{12}^T \quad \Pi_{13}^T \quad \Pi_{14}^T \quad \Pi_{15}^T \quad \Pi_{16}^T\ ]^T,\\
\Pi_{12} &= [\ \mathcal{A}_1 \quad \bar{\alpha}\bar{\beta}\mathcal{A}_5 \quad \bar{\alpha}(1-\bar{\beta})\mathcal{A}_5\ ], \quad \Pi_{13} = \sqrt{\bar{\chi}}\mathcal{B}_1,\\
\Pi_{14} &= \sqrt{\tilde{\alpha}}\mathcal{B}_2\mathcal{S}_1, \quad \Pi_{15} = \sqrt{\tilde{\alpha}\bar{\beta}}\mathcal{B}_2\mathcal{S}_2, \quad \Pi_{16} = \sqrt{\tilde{\alpha}\bar{\beta}}\mathcal{B}_1\mathcal{S}_1,\\
\Pi_{17} &= \Big[\ \sqrt{\bar{\alpha}(1-\bar{\beta})}(I \otimes BK)\Upsilon \quad 0 \quad 0 \quad 0\ \Big].
\end{aligned}$$

In what follows, we introduce a free matrix

$$\Theta = \begin{bmatrix} \Theta_{11} & \Theta_{12} \\ 0 & \Theta_{22} \end{bmatrix}$$

and denote

$$\begin{aligned}
W =& [\ B((B^T B)^{-1})^T \quad B^{\perp}\ ]^T,\\
\bar{K} =& \Theta_{11} K,\ \mathcal{K} = [\bar{K}^T \ \ 0]^T,\\
\Gamma =& \Theta W + W^T \Theta^T - P_1,\ \Psi = \Theta W P_1^{-1} W^T \Theta^T,
\end{aligned}$$

where $\Theta_{11} \in \mathbb{R}^{n_x \times p}$, $\Theta_{12} \in \mathbb{R}^{n_x \times (n_x - p)}$ and $\Theta_{22} \in \mathbb{R}^{(n_x-p)\times(n_x-p)}$, $B^{\perp}$ stands for an orthogonal basis of the null space for B^T.

Pre- and post-multiplying the inequality (8) by

$$\text{diag}\{I, I_5 \otimes \text{diag}\{\Theta W, P_2\}, I \otimes (\Theta W)\}$$

and

$$\text{diag}\{I, I_5 \otimes \text{diag}\{(\Theta W)^T, P_2\}, I \otimes (\Theta W)^T\}$$

yields

$$\Pi_2 = \begin{bmatrix} \Pi_{11} & * & * \\ \tilde{\Pi}_{12}^* & -I_5 \otimes \text{diag}\{\Psi, P_2\} & * \\ \tilde{\Pi}_{17} & 0 & -I \otimes \Psi \end{bmatrix} \leq 0 \qquad (9)$$

where

$$\begin{aligned}
\tilde{\mathcal{B}}_1 &= \begin{bmatrix} \mathcal{K}C_0 & 0 & -\mathcal{K} & \mathcal{K} \\ P_2 C_0 & 0 & -P_2 & P_2 \end{bmatrix}, \quad \tilde{\mathcal{B}}_2 = \begin{bmatrix} -\mathcal{K}C_0 & \mathcal{K} & \mathcal{K} & \mathcal{K} \\ -P_2 C_0 & P_2 & P_2 & P_2 \end{bmatrix},\\
\tilde{\Pi}_{12} &= \begin{bmatrix} \Theta W A_0 + \bar{\alpha}(1-\bar{\beta})\mathcal{K}C_0 & (1-\bar{\alpha})\mathcal{K} & \bar{\alpha}\bar{\beta}\mathcal{K} & \bar{\alpha}(1-\bar{\beta})\mathcal{K} \\ \bar{\alpha}(1-\bar{\beta})P_2 C_0 & (1-\bar{\alpha})P_2 & \bar{\alpha}\bar{\beta}P_2 & \bar{\alpha}(1-\bar{\beta})P_2 \end{bmatrix},\\
\tilde{\Pi}_{13} &= \sqrt{\bar{\chi}}\tilde{\mathcal{B}}_1, \quad \tilde{\Pi}_{14} = \sqrt{\tilde{\alpha}}\tilde{\mathcal{B}}_2\mathcal{S}_1, \quad \tilde{\Pi}_{15} = \sqrt{\tilde{\alpha}\bar{\beta}}\tilde{\mathcal{B}}_2\mathcal{S}_2,\\
\tilde{\Pi}_{16} &= \sqrt{\tilde{\alpha}\bar{\beta}}\tilde{\mathcal{B}}_2\mathcal{S}_2, \quad \tilde{\Pi}_{17} = \Big[\ \sqrt{\bar{\alpha}(1-\bar{\beta})}(I \otimes \mathcal{K})\Upsilon \quad 0 \quad 0 \quad 0\ \Big],\\
\tilde{\Pi}_{12}^* &= [\ \tilde{\Pi}_{12}^T \quad \tilde{\Pi}_{13}^T \quad \tilde{\Pi}_{14}^T \quad \tilde{\Pi}_{15}^T \quad \tilde{\Pi}_{16}^T\ ]^T.
\end{aligned}$$

It is apparent from (9) that

$$\begin{aligned}\Pi_2 = & \begin{bmatrix} \Pi_{11} & * & * \\ \tilde{\Pi}_{12}^{*} & -I_5 \otimes \text{diag}\{\Gamma, P_2\} & * \\ \tilde{\Pi}_{17} & 0 & -I \otimes \Gamma \end{bmatrix} \\ & + \text{diag}\Big\{0, I_5 \otimes \text{diag}\{\Gamma - \Psi, 0\}, I \otimes (\Gamma - \Psi)\Big\}. \end{aligned} \tag{10}$$

Finally, in light of

$$\begin{aligned}\Theta W + (\Theta W)^T & - \Theta W P_1 (\Theta W)^T - P_1 \\ & = -(P_1 - \Theta W) P_1 (P_1 - \Theta W)^T \leq 0, \end{aligned}$$

one has

$$\Pi_2 \leq \Pi_3 := \begin{bmatrix} \Pi_{11} & * & * \\ \tilde{\Pi}_{12}^{*} & -I_5 \otimes \text{diag}\{\Gamma, P_2\} & * \\ \tilde{\Pi}_{17} & 0 & -I \otimes \Gamma \end{bmatrix}. \tag{11}$$

It should be pointed out that the matrix ΘW is invertible if $\Pi_2 \leq \Pi_3 < 0$. It can be seen that $\Pi_2 < 0$ is equivalent to (8), and therefore $\Pi_2 < 0$ is equivalent to (7a) in Theorem 1. Finally, according to the analysis conducted above, the following theorem is easily accessible from Theorem 1 and its proof is therefore omitted.

Theorem 2. Let the positive scalars $\delta_1, \delta_2, \delta_3, \delta_4$ and the positive definite matrix R be given. Assume that there exist two positive definite matrices P_1 and P_2, two matrices Θ and $\bar{K}$ and three positive scalars ε_1, ε_2 and π satisfying the matrix inequalities $\Pi_3 < 0$, and the condition (7b). In this case, with the controller gain matrix given by

$$K = \Theta_{11}^{-1} \bar{K}$$

the closed-loop system (5) is secure with respect to $(\delta_1, \delta_2, \delta_3, \delta_4, R)$.

Algorithm:

Step 1. Denote a positive scalar τ for linearly searching step size.

Step 2. Let $\pi = 0$ and then check the solvability of inequality (7a). If it is solvable, go to next step, else go to *Step 6*.

Step 3. Let $\pi = \pi + \tau$, solve the following optimal problem:

$$\textbf{OP}: \quad \min_{\pi, \tilde{\rho}_{\max}} \tilde{\rho}_{\max} + \varepsilon_1 + \varepsilon_2 \quad \text{s. t.} \ (7a) \ \text{ and } \ P < \tilde{\rho}_{\max} I.$$

Step 4. If the optimal problem **OP** is solvable, calculate ρ, γ, $\lambda_{\max}(P_R)$, $\lambda_{\min}(P)$ and θ^2. In what follows, obtain Ξ_2 and go to the next step. If it is not solvable, go to *Step 6*.

Step 5. Check the condition (7b). If $\Xi_2 \leq \delta_3^2$, $K = \Theta_{11}^{-1} \bar{K}$ is the desired controller gain, the calculation stops. Else go to *Step 3*.

Step 6. The algorithm is infeasible. Stop.

In the case that the threshold $\delta_1 = 0$, it is not difficult to see that the triggering rules are always fulfilled, that is, the event-based approach reduces to a time-driven one. Consequently, we have the following corollary.

Corollary 1. Let the positive scalars $\delta_2, \delta_3, \delta_4$ and the positive definite matrix R be given. Assume that there exist two positive definite matrices P_1 and P_2,, two matrices Θ and $\bar{K}$ and two positive scalars ε_1 and π satisfying the following inequalities

$$\begin{cases} \Xi_3 = \begin{bmatrix} \Xi_{11}^* & * & * \\ \tilde{\Xi}_{12}^* & -I_5 \otimes \bar{\Gamma} & * \\ \Xi_{17}^* & 0 & -I \otimes \Gamma \end{bmatrix} < 0 & \text{(12a)} \\ \Xi_4 = \max\left\{ \dfrac{\lambda_{\max}(P_R)\delta_4^2}{\lambda_{\min}(P)}, \dfrac{\theta^2\gamma}{\lambda_{\min}(P)(\gamma - 1)} \right\} \leq \delta_3^2 & \text{(12b)} \end{cases}$$

where

$$\begin{aligned}
&\bar{\mathcal{B}}_1 = \begin{bmatrix} \mathcal{K}C_0 & 0 & -\mathcal{K} \\ P_2C_0 & 0 & -P_2 \end{bmatrix}, \quad \bar{\mathcal{B}}_2 = \begin{bmatrix} -\mathcal{K}C_0 & \mathcal{K} & \mathcal{K} \\ -P_2C_0 & P_2 & P_2 \end{bmatrix}, \\
&\Xi_{11}^* = \text{diag}\Big\{\Pi_{00}, -P_2 + \pi I, \ -\varepsilon_1 I\Big\}, \quad \theta = \sqrt{\varepsilon_1}\delta_2, \\
&\Xi_{12}^* = \begin{bmatrix} \Theta W A_0 + \bar{\alpha}(1-\bar{\beta})\mathcal{K}C_0 & (1-\bar{\alpha})\mathcal{K} & \bar{\alpha}\bar{\beta}\mathcal{K} \\ \bar{\alpha}(1-\bar{\beta})P_2C_0 & (1-\bar{\alpha})P_2 & \bar{\alpha}\bar{\beta}P_2 \end{bmatrix}, \\
&\Xi_{13}^* = \sqrt{\bar{\chi}}\bar{\mathcal{B}}_1, \quad \Xi_{14}^* = \sqrt{\tilde{\alpha}}\bar{\mathcal{B}}_2\bar{\mathcal{S}}_1, \quad \Xi_{15}^* = \sqrt{\tilde{\alpha}\bar{\beta}}\bar{\mathcal{B}}_2\bar{\mathcal{S}}_2, \\
&\Xi_{16}^* = \sqrt{\tilde{\alpha}\bar{\beta}}\bar{\mathcal{B}}_1\bar{\mathcal{S}}_1, \quad \Pi_{17}^* = \begin{bmatrix} \sqrt{\bar{\alpha}(1-\bar{\beta})}(I \otimes \mathcal{K})\Upsilon & 0 & 0 \end{bmatrix}, \\
&\tilde{\Xi}_{12}^* = \begin{bmatrix} \Xi_{12}^{*T} & \Xi_{13T}^* & \Xi_{14}^{*T} & \Xi_{15}^{*T} & \Xi_{16}^{*T} \end{bmatrix}^T, \\
&\bar{\mathcal{S}}_1 = \text{diag}\{I, 0\}, \quad \bar{\mathcal{S}}_2 = \text{diag}\{-I, I\}.
\end{aligned}$$

In this case, with the controller gain matrix given by $K = \Theta_{11}^{-1}\bar{K}$, the closed-loop system (5) is secure with respect to $(0, \delta_2, \delta_3, \delta_4, R)$.

Remark 6. In this paper, the event-based security control problem is investigated for a class of discrete-time stochastic systems with multiplicative noises and cyber attacks. By utilizing two sets of Bernoulli distributed white sequences, a novel attack model is proposed to account for the phenomenon of both randomly occurring DoS attacks and randomly occurring deception attacks. Based on such a model, the result established in Theorem 2 contains all the information about the threshold of the event-triggered communication mechanism, the security requirements and the statistical information of cyber attacks. It is worth mentioning that the research methodology developed in this paper is quite general that can be applied to a variety of systems. For example, the obtained results can been easily extended to more complicated cases such as the case where the attacks occur in the channel between controllers and physical systems as well as the channel between sensors and controllers.

4. Illustrative example

Following [37], we consider the security control problem for a geared DC motor, which is a component of the MS150 modular servo system. Setting the sampling time $T = 0.01s$, we obtain the following discretized nominal system matrix and measurement matrix:

$$A_0 = \begin{bmatrix} 1 & 0.0098 \\ 0 & 0.9653 \end{bmatrix}, \quad C_0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}^T.$$

In the MS150 modular servo system, the control input u_k is a voltage and the measurement output $\tilde{y}_k$ is a rotary angle of the extended shaft, which is also called the position of the shaft. The movement of the motor is affected by the stochastic disturbance $\omega_{i,k}$ ($i = 1$). To this end, other parameters are given as

$$A_1 = \begin{bmatrix} 0.0120 & 0 \\ 0 & 0.0900 \end{bmatrix},$$
$$B = \begin{bmatrix} 1.50 \\ 0.01 \end{bmatrix}, \quad C_1 = \begin{bmatrix} 0.12 \\ -0.14 \end{bmatrix}^T.$$

Assume that the attack probabilities are $\bar{\alpha} = 0.90$ and $\bar{\beta} = 0.25$. Moreover, the parameters δ_1, δ_2, δ_3, δ_4 and R are, respectively, 0.004, 0.10, 0.32, 0.30 and diag$\{0.95, 0.95\}$.

By using the Matlab software (with the YALMIP 3.0 [38]) where the solver is selected as 'solvesdp', a set of feasible solutions of Theorem 2 is obtained as follows:

$$\varepsilon_1 = 24.8338, \quad \varepsilon_2 = 22.3623, \quad \pi = 0.4044, \quad \bar{K} = -5.6703, P_2 = 5.0861$$
$$P_1 = \begin{bmatrix} 9.6681 & -0.1235 \\ -0.1235 & 9.9088 \end{bmatrix}, \Theta = \begin{bmatrix} 15.6750 & 0.3023 \\ 0 & -16.5272 \end{bmatrix}.$$

Furthermore, the desired control parameter is obtained as $K = -0.3617$.

In the simulation, the disturbance signal of attackers ξ_k^t is selected as $\delta_2 \sin(k)$ and the initial value is set as $x_0 = [0.20 \ \ -0.18]^T$. The simulation results are shown in Figs. 2-4, where Fig. 2 plots the norm of states for the open-loop system and the closed-loop system without attacks. Since the spectral radius of the matrix $A_0 \otimes A_0 + \sum_{i=1}^{p} A_i \otimes A_i$ is 1.0015, we can see that the open-loop system is unstable.

Fig. 3 depicts the norm of states for the closed-loop system with attacks. The curve experiences three unexpected jumps at $k = 75$, 78, 81 and 114 since the system suffers from deception attacks at $k = 73$, 74, 77, 80 and 113. In comparison with the dotted line in Fig. 2, the control performance is degraded by attacks.

The event-triggered time and the successful time of attacks are shown in Fig. 4, from which we can easily find that the number of event-triggered communication is quite small and the communication burden is effectively reduced. In Table 1 and Table 2, we further examine the effect on the security level from the increased attack probability of DoS attacks (or deception attacks) and we can conclude that the security performance deteriorates as the attack probability increases.

Table 1 The minimum security level with different $1 - \bar{\alpha}$ for $\bar{\beta} = 0.001$

$1 - \bar{\alpha}$	0.380	0.385	0.390	0.395	0.400	0.405	0.410
Security level δ_3^2	0.5899	0.6065	0.6254	0.6457	0.6680	0.6937	0.7213
$1 - \bar{\alpha}$	0.415	0.420	0.425	0.430	0.435	0.440	0.445
Security level δ_3^2	0.753	0.7894	0.8305	0.8784	0.9359	1.0034	1.0851

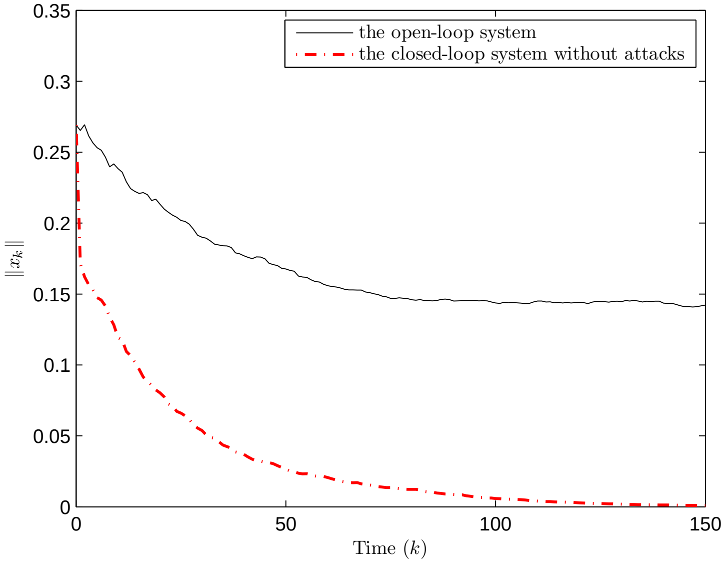

Fig. 2. *The norm of states for the open-loop system and the closed-loop system without attacks.*

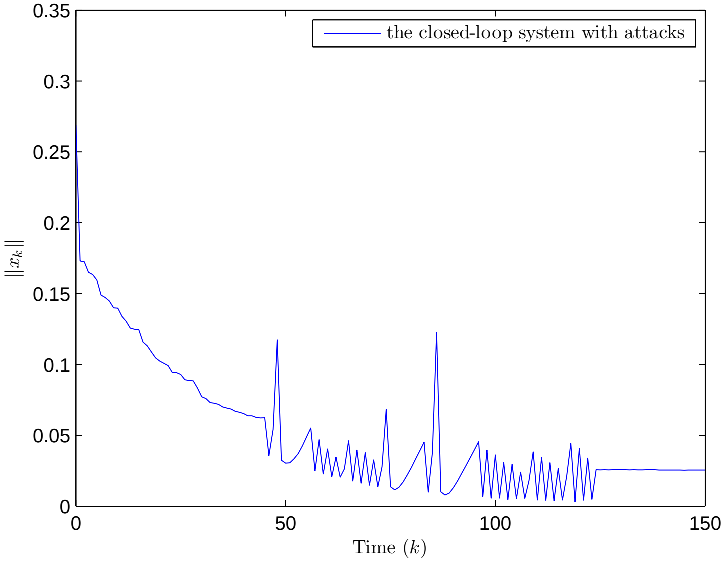

Fig. 3. *The norm of states for the closed-loop system with attacks.*

Table 2 The minimum security level with different $\bar{\beta}$ for $\bar{\alpha} = 0.999$

β	0.26	0.29	0.32	0.35	0.38	0.41	0.44
Security level δ_3^2	1.8650	1.8664	1.8676	1.8686	1.8716	1.8743	1.8778
β	0.47	0.50	0.53	0.56	0.59	0.62	0.65
Security level δ_3^2	1.8842	1.8905	1.8990	1.9093	1.9221	1.9395	2.1790

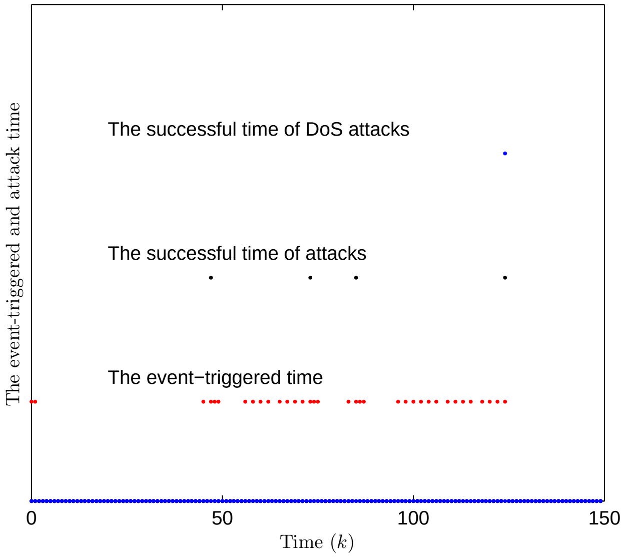

Fig. 4. *The event-triggered time and the attack time*

5. Conclusion

In this paper, the event-based security control problem has been discussed for a class of discrete-time stochastic systems with multiplicative noises. The plant under consideration is subject to randomly occurring DoS attacks and randomly occurring deception attacks. First, a novel attack model has been provided to describe such two attacks within a unified framework. Then, an event-based communication mechanism has been utilized to reduce the communication burden. Furthermore, the output feedback controller gain matrix has been obtained by solving a linear matrix inequality with nonlinear constraints. Finally, a simulation example has been exploited to show the effectiveness of the event-triggered security control scheme proposed in this paper.

6. Acknowledgments

This work was supported in part by Royal Society of the UK, the National Natural Science Foundation of China under Grants 61329301, 61573246 and 61374039, the Shanghai Rising-Star Programme of China under Grant 16QA1403000, the Program for Capability Construction of Shanghai Provincial Universities under Grant 15550502500 and the Alexander von Humboldt Foundation of Germany.

Appendix: Proof of Theorem 1

Construct the Lyapunov function

$$V_k = \tilde{x}_k^T P \tilde{x}_k.$$

By calculating the difference of V_k along the trajectory of system (5) and taking the mathematical expectation on $\omega_{i,k}$, $\varpi_{j,k}$ ($i = 1, 2, \cdots, r$, $j = 1, 2, \cdots, s$), $\alpha_{k_s}^t$ and $\beta_{k_s}^t$, one has

$$\begin{aligned}
\mathbb{E}\{\Delta V_k | \tilde{x}_k\} &= \mathbb{E}\big\{\tilde{x}_{k+1}^T P \tilde{x}_{k+1} - \tilde{x}_k^T P \tilde{x}_k | \tilde{x}_k\big\} \\
&= \mathbb{E}\Big\{\mathbb{E}\big\{\tilde{x}_{k+1}^T P \tilde{x}_{k+1} - \tilde{x}_k^T P \tilde{x}_k \big| \alpha_{k_s}^t, \beta_{k_s}^t\big\}\Big| \tilde{x}_k\Big\} \\
&= \mathbb{E}\Big\{\tilde{x}_k^T \Big(\mathcal{A}_1^T P \mathcal{A}_1 + \tilde{\alpha}\mathcal{A}_2^T P \mathcal{A}_2 - 2(\tilde{\alpha} - \tilde{\alpha}\bar{\beta})\mathcal{A}_2^T P \mathcal{A}_3 \\
&\quad + (\tilde{\alpha} - 2\tilde{\alpha}\bar{\beta} + \bar{\chi})\mathcal{A}_3^T P \mathcal{A}_3 + \mathcal{A}_4 - P\Big)\tilde{x}_k \\
&\quad + \tilde{x}_k^T \big(2\bar{\alpha}\bar{\beta}\mathcal{A}_1^T P \mathcal{A}_5 - 2\tilde{\alpha}\bar{\beta}\mathcal{A}_2^T P \mathcal{A}_5 + 2(\tilde{\alpha}\bar{\beta} - \bar{\chi})\mathcal{A}_3^T P \mathcal{A}_5\big)\xi_{k_s}^t \\
&\quad + \tilde{x}_k^T \big(2\bar{\alpha}(1 - \bar{\beta})\mathcal{A}_1^T P \mathcal{A}_5 - 2(\tilde{\alpha} - \tilde{\alpha}\bar{\beta})\mathcal{A}_2^T P \mathcal{A}_5 \\
&\quad + 2(\tilde{\alpha} - 2\tilde{\alpha}\bar{\beta} + \bar{\chi})\mathcal{A}_3^T P \mathcal{A}_5\big)e_k + (\xi_{k_s}^t)^T \big(((\bar{\alpha}\bar{\beta})^2 + \bar{\chi})\mathcal{A}_5^T P \mathcal{A}_5\big)\xi_{k_s}^t \\
&\quad + 2(\xi_{k_s}^t)^T \big((\bar{\alpha}^2\tilde{\beta} + \tilde{\alpha}\bar{\beta} - \bar{\chi})\mathcal{A}_5^T P \mathcal{A}_5\big)e_k \\
&\quad + e_k^T \big((\bar{\alpha}^2(1 - \bar{\beta})^2 + \tilde{\alpha} - 2\tilde{\alpha}\bar{\beta} + \bar{\chi})\mathcal{A}_5^T P \mathcal{A}_5\big)e_k \Big| \tilde{x}_k\Big\} \\
&= \eta_k^T \tilde{\Xi} \eta_k
\end{aligned} \tag{13}$$

where

$$\eta_k = [\ \tilde{x}_k^T \quad (\xi_{k_s}^t)^T \quad e_k^T\ ]^T,$$

$$\tilde{\Xi} = \begin{bmatrix} \Xi_{11} - \pi I & \Xi_{12} & \Xi_{13} \\ * & \Xi_{22} + \varepsilon_2 I & 0 \\ * & * & \Xi_{33} + \varepsilon_1 I \end{bmatrix}.$$

Subsequently, taking $\psi(e_k, \delta_1) \leq 0$ and $\|\xi_k^t\| \leq \delta_2$ into consideration, one has

$$\begin{aligned}
&\mathbb{E}\{\Delta V(k)\} \\
&\leq \mathbb{E}\big\{\eta_k^T \tilde{\Xi}\eta_k + \varepsilon_1(\delta_1^2 - e_k^T e_k) + \varepsilon_2(\delta_2^2 - (\xi_{k_s}^t)^T \xi_{k_s}^t)\big\} \\
&= \mathbb{E}\big\{\eta_k^T \Xi_1 \eta_k - \eta_k^T \text{diag}\{\pi I,\ 0,\ 0\}\eta_k\big\} + \varepsilon_1\delta_1^2 + \varepsilon_2\delta_2^2 \\
&\leq\ - \mathbb{E}\big\{\eta_k^T \text{diag}\{\pi I,\ 0,\ 0\}\eta_k\big\} + \theta^2
\end{aligned} \tag{14}$$

which implies

$$\mathbb{E}\{\Delta V_k\} \leq -\pi\mathbb{E}\{\|\tilde{x}_k\|^2\} + \theta^2. \tag{15}$$

For any scalar $\gamma > 1$, it follows from the above inequality that

$$\begin{aligned}
&\mathbb{E}\{\gamma^{k+1} V_{k+1}\} - \mathbb{E}\{\gamma^k V_k\} \\
&= \gamma^{k+1}\mathbb{E}\{V_{k+1} - V_k\} + \gamma^k(\gamma - 1)\mathbb{E}\{V_k\} \\
&\leq \gamma^k((\gamma - 1)\rho - \gamma\pi)\mathbb{E}\{\|\tilde{x}_k\|^2\} + \gamma^{k+1}\theta^2.
\end{aligned} \tag{16}$$

Selecting $\gamma = \frac{\rho}{\rho - \pi}$ and one has from (16) that

$$\mathbb{E}\{\gamma^k V_k\} - \mathbb{E}\{V_0\} \leq (\gamma^k + \gamma^{k-1} + \cdots + \gamma)\theta^2 \tag{17}$$

which implies

$$\begin{aligned}\mathbb{E}\{V_k\} &\le \gamma^{-k}\mathbb{E}\{V_0\} + (1+\gamma^{-1}+\cdots+\gamma^{-k+1})\theta^2 \\ &= \gamma^{-k}\mathbb{E}\{V_0\} + \frac{[1-(1/\gamma)^k]\theta^2}{1-1/\gamma} \\ &= \gamma^{-k}\Big[\mathbb{E}\{V_0\} - \frac{\theta^2\gamma}{\gamma-1}\Big] + \frac{\theta^2\gamma}{\gamma-1} \\ &\le \gamma^{-k}\Big(\lambda_{\max}(R^{-1/2}PR^{-1/2})\delta_4^2 - \frac{\theta^2\gamma}{\gamma-1}\Big) + \frac{\theta^2\gamma}{\gamma-1} \\ &\le \max\Big\{\lambda_{\max}(R^{-1/2}PR^{-1/2})\delta_4^2, \frac{\theta^2\gamma}{\gamma-1}\Big\}.\end{aligned} \tag{18}$$

Finally, it can be concluded from (7b) that the closed-loop system (5) is secure with respect to $(\delta_1, \delta_2, \delta_3, \delta_4, R)$, which completes the proof.

7. References

[1] Hu, J., Wang, Z., Shen, B., Gao, H.: ‘Quantised recursive filtering for a class of nonlinear systems with multiplicative noises and missing measurements’, *International Journal of Control*, 2013, 86, (4), pp. 650-663

[2] Hou, T., Zhang, W., Ma, H.: ‘Finite horizon $\mathcal{H}_2/\mathcal{H}_\infty$ control for discrete-time stochastic systems with Markovian jumps and multiplicative noise’, *IEEE Transactions on Automatic Control*, 2010, 55, (5), pp. 1185-1191

[3] Wen, S., Zeng, Z., Huang, T.: ‘Observer-based H_∞ fuzzy control for discrete-time Takagi-Sugeno fuzzy mixed delay systems with random packet losses and multiplicative noises’, *International Journal of Systems Science*, 2015, 46, (1), pp. 159-169

[4] Gershon, E., Shaked, U., Yaesh, I.: ‘$\mathcal{H}_\infty$ control and filtering of discrete-time stochastic systems with multiplicative noise’, *Automatica*, 2001, 37, (3), pp. 409-417

[5] Yang, F., Wang, Z., Hung, Y. S.: ‘Robust Kalman filtering for discrete time-varying uncertain systems with multiplicative noises’, *IEEE Transactions on Automatic Control*, 2002, 47, (7), pp. 1179-1183

[6] Yang, Z., Shi, X., Chen, J.: ‘Optimal coordination of mobile sensors for target tracking under additive and multiplicative noises’, *IEEE Transactions on Industrial Electronics*, 2014, 61, (7), pp. 3459-3468

[7] Caballero-Aguila, R., Hermoso-Carazo, A., Jimenez-Lopez, J. D., Linares-Perez, J., Nakamori, S.: ‘Signal estimation with multiple delayed sensors using covariance information’, *Digital Signal Processing*, 2010, 20, (2), pp. 528-540

[8] Ding, D., Wang, Z., Alsaadi, F. E., Shen, B.: ‘Receding horizon filtering for a class of discrete time-varying nonlinear systems with multiple missing measurements’, *International Journal of General Systems*, 2015, 44, (2), pp. 198-211

[9] Ding, D., Wang, Z., Shen, B., Dong, H.: ‘Event-triggered distributed $\mathcal{H}_\infty$ state estimation with packet dropouts through sensor networks’, *IET Control Theory & Applications*, 2015, 9, (13), pp. 1948-1955

[10] Dong, H., Wang, Z., Ding, S. X., Gao, H.: 'Finite-horizon estimation of randomly occurring faults for a class of nonlinear time-varying systems', *Automatica*, 2014, 50, (12), pp. 3182-3189

[11] Liu, S., Wei, G., Song, Y., Liu, Y.: 'Error-constrained reliable tracking control for discrete time-varying systems subject to quantization effects', *Neurocomputing*, 2016, 174, pp. 897-905

[12] Chen, B.,cZhang, W.-A., Li, Y., Hu, G., Song, H.: 'Distributed fusion estimation with communication bandwidth constraints', *IEEE Transactions on Automatic Control*, 2015, 60, (5), pp. 1398-1403

[13] Liang, J., Shen, B., Dong, H., Lam, J.: 'Robust distributed state estimation for sensor networks with multiple stochastic communication delays', *International Journal of Systems Science*, 2011, 42, (9), pp. 1459-1471

[14] Seyboth, G. S., Dimarogonas, D. V., Johansson, K. H.: 'Event-based broadcasting for multi-agent average consensus', *Automatica*, 2013, 49, (1), pp. 245-252

[15] Fan, Y., Feng, G., Wang, Y., Song, C.: 'Distributed event-triggered control of multi-agent systems with combinational measurements', *Automatica*, 2013, 49, (2), pp. 671-675

[16] Ding, D., Wang, Z., Shen, B.: 'Event-triggered consensus control for discrete-time stochastic multi-agent systems: The input-to-state stability in probability', *Automatica*, 2015, 62, pp. 284-291

[17] Meng, X., Chen, T.: 'Event based agreement protocols for multi-agent networks', *Automatica*, 2013, 49, (7), pp. 2125-2132

[18] Cao, M., Xiao, F., Wang, L.: 'Second-order leader-following consensus based on time and event hybrid-driven control', *Systems & Control Letters*, 2014, 74, pp. 90-97

[19] Donkers, M. C. F., Heemels, W. P. M. H.: 'Output-based event-triggered control with guaranteed $\mathcal{L}_\infty$-gain and improved and decentralized event triggering', *IEEE Transactions on Automatic Control*, 2012, 57, (6), pp. 1362-1367

[20] Tabuada, P.: 'Event-triggered real-time scheduling of stabilizing control tasks', *IEEE Transactions on Automatic Control*, 2007, 52, (9), pp. 1680-1685

[21] Zhang, J., Feng, G.: 'Event-driven observer-based output feedback control for linear systems', *Automatica*, 2014, 50, (7), pp. 1852-1859

[22] Wei, G., Wang, L., Liu, Y.: '$\mathcal{H}_\infty$ control for a class of multi-agent systems via a stochastic sampled-data method', *IET Control Theory & Applications*, 2015, 9, (14), pp. 2057-2065

[23] Li, H., Shi, Y.: 'Event-triggered robust model predictive control of continuous-time nonlinear systems', *Automatica*, 2014, 50, (5), pp. 1507-1513

[24] Peng, C., Han, Q.-L.: 'A novel event-triggered transmission scheme and L_2 control Co-design for sampled-data control systems', *IEEE Transactions on Automatic Control*, 2013, 58, (10), pp. 2620-2626

[25] Anta, A., Tabuada, P.: 'To sample or not to sample self-triggered control for nonlinear systems', *IEEE Transactions on Automatic Control*, 2010, 55, (9), pp. 2030-2042

[26] Shi, D., Chen, T., Shi, L.: ‘Event-triggered maximum likelihood state estimation’, *Automatica*, 2014, 50, (1), pp. 247-254

[27] Chen, J., Li, J., Lai, T. H.: ‘Energy-efficient intrusion detection with a barrier of probabilistic sensors: global and local’, *IEEE Transactions on Wireless Communications*, 2013, 12, (9), pp. 4742-4755

[28] Clark, A., Bushnell, L., Poovendran, R.: ‘A passivity-based framework for composing attacks on networked control systems’, *Proc. 50th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, Oct. 2012, pp. 1814-1821

[29] Foroush, H., Martínez, S.: ‘On event-triggered control of linear systems under periodic Denial-of-Service jamming attacks’, *IEEE 51st Annual Conference on Decision and Control (CDC)*, Maui, HI, USA, Dec. 2012, pp. 2551-2256

[30] Befekadu, G. K., Gupta, V., Antsaklis, P. J.: ‘Risk-sensitive control under a class of denial-of-service attack models’, *American Control Conference (ACC)*, San Francisco, CA, USA, Jun.-Jul. 2011, pp. 643-648

[31] Long, M., Wu, C.-H., Hung, J. Y.: ‘Denial of service attacks on network-based control systems: impact and mitigation’, *IEEE Transactions on Industrial Informatics*, 2005, 1, (2), p-p. 85-96

[32] Pang, Z.-H., Liu, G.-P.: ‘Design and implementation of secure networked predictive control systems under deception attacks’, *IEEE Transactions on Control Systems Technology*, 2012, 20, (5), pp. 1334-1342

[33] Teixeira, A., Sandberg, H., Johansson, K. H.: ‘Networked control systems under cyber attacks with applications to power networks’, *American Control Conference (ACC)*, Baltimore, MD, USA, Jun.-Jul. 2010, pp. 3690-3696

[34] Mo, Y., Sinopoli, B.: ‘Secure control against replay attacks’, *Proc. 47th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, Sept.-Oct. 2009, pp. 911-918

[35] Zhu, M., Martinez, S.: ‘On the performance analysis of resilient networked control systems under replay attacks’, *IEEE Transactions on Automatic Control*, 2014, 59, (3), pp. 804-808

[36] Amin, S., Cárdenas, A. A., Sastry, S. S.: ‘Safe and secure networked control systems under denial-of-service attacks’, *HSCC 2009*, 2009, pp. 31-45

[37] Zhang, H., Shi, Y., Mehr, A.: ‘Robust static output feedback control and remote PID design for networked motor systems’, *IEEE Transactions on Industrial Electronics*, 2011, 58, (12), pp. 5396-5405

[38] Löfberg, J.: ‘YALMIP : A toolbox for modeling and optimization in MATLAB’. *IEEE International Symposium on Computer Aided Control Systems Design*, Taipei, Taiwan, Sept. 2004, pp. 284-289