Encryption-Decryption-Based Consensus Control for Multi-agent Systems: Handling Actuator Faults ⋆

Chen Gao [a], Zidong Wang [b], Xiao He [a,*], Hongli Dong [c]

[a] Department of Automation, BNRist (Beijing National Research Center for Information Science and Technology), Tsinghua University, Beijing 100084, China.

[b] Department of Computer Science, Brunel University London, Uxbridge, Middlesex, UB8 3PH, United Kingdom.

[c] Artificial Intelligence Energy Research Institute, Northeast Petroleum University, Daqing 163318, China.

Abstract

This paper deals with the encryption-decryption-based passive fault-tolerant consensus control problem for a class of linear multi-agent systems subject to loss-of-effectiveness and additive actuator faults. Both the secure communication and fault tolerance issues are investigated, and their impacts on the consensus are examined. To ensure the communication security, two encryption-decryption-based fault-tolerant consensus control schemes are proposed, with which the original state of the local agent is first encrypted into a series of codewords and then decrypted by other agents to realize data privacy preserving. The necessary and sufficient condition is established for the addressed consensus problem under the adopted controller structure. A series of numerical examples are given to verify the effectiveness of the developed consensus control strategy.

Key words: Actuator faults; Encryption-decryption; Multi-agent system; Fault-tolerant consensus control.

1 Introduction

A multi-agent system (MAS) consists of multiple interacting intelligent agents that can work cooperatively to achieve coordinated tasks such as cooperative estimation [16, 24, 33], containment and consensus control [13, 25–27, 38, 40], search and attack [10, 19, 36, 37]. Consensus control for MASs aims at designing distributed controllers with information of neighbors to achieve consensus on a quantity of interests. In the past decade, the consensus control algorithms have been rapidly developed for various MASs and a rich body of literature has been available, see e.g. [4, 11, 30] for summaries of the latest progress.

With the ever-increasing complexity with the MASs, the cyber-security has become a technology/business issue attracting tremendous research attention from both industry and academy. Briefly speaking, a risk exists as long as there is a certain vulnerability exposed to the attacker [5, 42, 43]. For MASs, the vulnerability may result from a communication-link weakness (e.g. bandwidth constraints [35]) or a potential component fault (e.g. an actuator fault [32]). Moreover, the interconnection among agents through the communication networks exhibits obvious vulnerabilities to potential attackers, and this may cause performance degradation or even entire damage of the overall MAS. In this sense, it is of practical significance to look into the security issues of MASs from the perspectives of 1) secure communication scheme design to realize congestion mitigation and data protection; and 2) fault-tolerant consensus controller design to enhance individual reliability of the system components.

In the context of secure communication, the encryption-decryption algorithms (EDAs) have been commonly deployed to protect the data confidentiality [44, 45], and two popular algorithms are the Advanced-Encryption-Standard-based (AES) algorithm [5] and the Data-Encryption-Standard-based (DES) algorithm [29]. While traditional EDAs are for cryptography, there has been a recent trend to combine EDAs with the dynamics of the MAS itself so that the transmitted data can be further compressed to facilitate the congestion-free transmission. Relevant results can be found in [18, 20] for single-integrator MASs, [21, 23] for double-integrator MASs and [9, 17, 34] for general linear MASs, where the encryption process can be divided into the transformation and the quantization steps. More specifically, in the transformation step, the original data (state/output

⋆ This work was supported in part by the National Natural Science Foundation of China under Grants 61733009, 61873148, 61873058 and 61933007, the National Key Research and Development Program of China under Grant 2017YFA0700300, the Natural Science Foundation of Guangdong Province of China under Grant 2018B030311054, the Shuimu Tsinghua Scholar Program of China under Grant 2021SM040, the Royal Society of the UK, and the Alexander von Humboldt Foundation of Germany.

* Corresponding author.

Email addresses: Zidong.Wang@brunel.ac.uk (Zidong Wang), hexiao@tsinghua.edu.cn (Xiao He), shiningdhl@vip.126.com (Hongli Dong).

variable) is transformed into new data by using the dynamics of the system in order to reduce the size of the data to be sent. During the quantization step, the new data is converted into codewords on the basis of different quantization algorithms. It is worth noting that the introduction of the quantization will inevitably cause data distortion, which gives rise to technical challenges on the corresponding stability/consensus analysis.

On the other hand, agents may experience faults due to various reasons such as abnormal wear of components and abnormal working conditions. The fault, if not dealt with in time, could propagate to neighboring agents, thereby affecting the performance of the entire MAS, which imposes reliability requirements on the design of consensus controllers. In view of this, the fault-tolerant consensus control (FTCC) issue becomes vitally important. In this paper, both loss-of-effectiveness (LoE) faults and additive faults are investigated. In a sense, additive faults only affect the steady-state performance while LoE faults may affect the ability of achieving consensus [3], and hence we focus our attention on the LoE fault. There have been a number of excellent results for LoE faults by using the adaptive controller [1, 7], the robust controller [2, 8], the slide-mode-based controller [31, 41] and the backstepping-based controller [14, 39]. To be more specific, the adaptive controller can be adjusted online without needing a priori information about the bounds on faults, but its rather complicated structure increases the difficulty for the controller design and implementation. The robust controller is different from the adaptive one in that it is designed offline to tolerant all considered faults and, no matter the actuator is healthy or faulty, the control law remains the same and is therefore easy to implement.

When it comes to the secure communication, the existing FTCC methods cannot be directly applied to MASs since the data distortion may result in unsatisfactory performance and even instability, which brings about additional yet substantial challenges. To this end, we aim to investigate the FTCC problem for MASs within an encryption-decryption framework, and two challenges we are facing here are the strong couplings of the controller design and the EDA design as well as the impact from the fault. To be more specific, we need to take into the following three facts that contribute to the analysis/design complexities, that is, 1) the fault of the actuator seriously affects the exact execution of the controller; 2) the dynamics of the closed-loop system plays a major impact on the design of the encryption-decryption algorithm; and 3) the data distortion caused by the EDA influences, in turn, the design of the desired controller.

Based on the above discussions, the main purpose of this paper is to cope with the FTCC problem subject to actuator faults under an encryption-decryption scheme. *The main contributions of this paper are summarized as follows: 1) two encryption-decryption-based FTCC schemes are proposed to enhance the security of MASs from two aspects, i.e., individual reliability and interconnection security; 2) under the given controller structure, the necessary and sufficient condition for the existence of the EDA is derived by constructing a novel matrix norm as well as its compatible vector norm; and 3) two novel methods are proposed to deal with the fault-induced heterogeneity, especially for the LoE fault.*

The rest of this paper is structured as follows. Section 2 introduces the preliminaries of graphs, and Section 3 provides the model of MASs subject to actuator faults and two kinds of encryption-decryption-based FTCC schemes. Section 4 provides the main results and Section 5 presents numerical simulation examples. Section 6 concludes this paper.

Notations. Let $\mathbf{1}_n$ (or $\mathbf{0}_n$) denote the n-dimensional column vector whose entries are all ones (or all zeros). $\mathbf{0}_{m\times n}$ denotes the $m \times n$ matrix with all zeros. I_n represents the n-dimensional identity matrix. $\text{diag}\{d_0, \ldots, d_n\}$ stands for a diagonal matrix with $d_0, \ldots, d_n$ as its diagonal elements. $\rho(A)$ and $\lambda_{\max}(A)$ ($\lambda_{\min}(A)$) denote the spectral radius and the maximum (minimum) eigenvalue of the square matrix A, respectively. $\|\cdot\|_2$ and $\|\cdot\|_\infty$ stand for, respectively, the 2-norm and the ∞-norm of a vector or a matrix. $\|\cdot\|_\star$ and $\|\cdot\|_*$ denote the introduced matrix norm (to be proposed later) and its compatible vector norm, respectively. For a given real number x, $\lceil x \rceil$ means the minimum integer not smaller than x. $\otimes$ represents the Kronecker product.

2 Preliminaries on Graph Theory

Considering an MAS comprising N agents, we use a graph $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E}, \mathcal{A})$ to describe the interconnection among agents, where $\mathcal{V} = \{\mathcal{V}_1, \mathcal{V}_2, \ldots, \mathcal{V}_N\}$ denotes the set of nodes (i.e. agents), $\mathcal{E}$ denotes the set of edges and $\mathcal{A} = \begin{bmatrix} a_{ij} \end{bmatrix} \in \mathbb{R}^{N\times N}$ denotes the adjacency matrix. Node j is said to be the neighbor of node i ($j \in \mathcal{N}_i$) if node i can directly obtain the information from node j (i.e. $\mathcal{E}_{ji} \in \mathcal{E}$). For node i, the number of its neighbors is denoted by d_i. In addition, the weight $a_{ij} = 1$ if and only if $\mathcal{E}_{ji} \in \mathcal{E}$, otherwise $a_{ij} = 0$. $d_i \triangleq \sum_{j=1}^{N} a_{ij}$ denotes the degree of node i and $d_{\max} \triangleq \max_i d_i$. If $\mathcal{A}^T = \mathcal{A}$, then the graph represents an undirected graph. A directed graph $\mathcal{G}$ is said to have a spanning tree (or an undirected graph is said to be connected) if there exist paths from one node to every other nodes. Let $L = \begin{bmatrix} l_{ij} \end{bmatrix} \in \mathbb{R}^{N\times N}$ denote the Laplacian matrix of the graph $\mathcal{G}$ with $l_{ii} = \sum_{j\neq i} a_{ij},\ l_{ij} = -a_{ij}, i \neq j$.

In this paper, we focus on the undirected graph with $L^T = L$. It is well known that, if the undirected graph $\mathcal{G}$ is connected, then there exists an orthogonal matrix $T = \begin{bmatrix} T_0\ T_1 \end{bmatrix}$ with $T_0 = \sqrt{\frac{1}{N}}\mathbf{1}_N$ such that $T^T L T = \text{diag}\{0, \Phi\}$, where $\Phi = \text{diag}\{\lambda_2, \ldots, \lambda_N\}$ is a positive-definite matrix, and $0 = \lambda_1 < \lambda_2 \leq \ldots \lambda_{N-1} \leq \lambda_N$ are the real eigenvalues of L [6].

3 Problem Formulation

3.1 Actuator faults

Consider an MAS consisting of N agents subject to actuator LoE faults, i.e. multiplicative faults, and additive faults:

$$x_i(k+1) = Ax_i(k) + B\big((I - \varrho_i(k))u_i(k) + \vartheta_i(k)\big), \tag{1}$$

where $x_i \in \mathbb{R}^n$, $u_i \in \mathbb{R}^m$, $\varrho_i \in \mathbb{R}^{m\times m}$ and $\vartheta_i \in \mathbb{R}^m$ are, respectively, the state variable, the input variable, the multiplicative fault and the additive fault, respectively. ϱ_i is defined as $\varrho_i \triangleq \mathrm{diag}\{\varrho_{i1}, \varrho_{i2}, \dots, \varrho_{im}\} \in \mathbb{R}^{m\times m}$, where ϱ_{ih} $(h = 1, 2, \dots, m)$ represents the unknown failure factor of the h-th actuator of the agent i. $\vartheta_i \triangleq \begin{bmatrix}\vartheta_{i1}, \ \vartheta_{i2}, \cdots, \vartheta_{im}\end{bmatrix}^T$. Assume that $0 \le \varrho_{ih}(k) \le \varrho_{\max} < 1$ and $\|\vartheta_i(k)\|_\infty \le \vartheta_{\max}$ for any k. $\varrho_{\max}$ and $\vartheta_{\max}$ are the known upper bounds.

3.2 Encryption-decryption-based FTCC scheme I

Suppose that the state of the system is fully available. The proposed encryption-decryption-based FTCC scheme I is shown in Fig. 1. The designed encryption algorithm, the decryption algorithm and the controller are shown as follows.

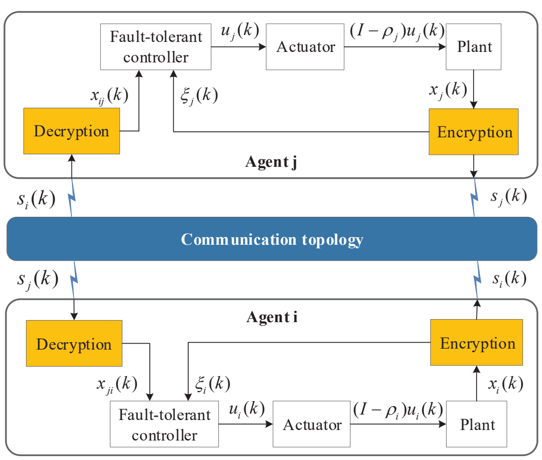

Fig. 1. Encryption-decryption-based FTCC scheme I.

Encryption algorithm of agent i:

$$\begin{cases} s_i(k) = Q_t\left(\dfrac{x_i(k) - A\xi_i(k-1)}{g(k-1)}\right) \\ \xi_i(k) = A\xi_i(k-1) + g(k-1)s_i(k) \\ \xi_i(0) = \mathbf{0}_n, \end{cases} \tag{2}$$

where $\xi_i(k) \in \mathbb{R}^n$ and $s_i(k) \in \mathbb{R}^n$. $g(k)$ is the dynamic encryption key to be designed. For a vector $v = \begin{bmatrix}v_1, v_2, \cdots, v_n\end{bmatrix}^T$, the quantization function is $Q_t(v) \triangleq \begin{bmatrix}q_t(v_1), q_t(v_2), \cdots, q_t(v_n)\end{bmatrix}^T$ with

$$q_t(v_i) = \begin{cases} d\hbar, & (d-\frac{1}{2})\hbar \le v_i < (d+\frac{1}{2})\hbar \\ -q_t(-v_i), & v_i \le -\frac{1}{2}\hbar, \end{cases} \tag{3}$$

where $\hbar$ is a given quantization parameter and $|v_i - q_t(v_i)| \le \hbar/2$. The upper bound of $|q_t(v_i)|$ is $M\hbar$ with $M \triangleq \max_{i,k} \|s_i(k)/\hbar\|_\infty$.

Decryption algorithm of agent i:

$$\begin{cases} x_{ji}(k) = Ax_{ji}(k-1) + g(k-1)s_j(k) \\ x_{ji}(0) = \mathbf{0}_n, \quad j \in \mathcal{N}_i, \end{cases} \tag{4}$$

where $x_{ji}(k)$ is the state obtained after decryption. The decryption key is identical to the encryption key and hence $x_{ji}(k) = \xi_j(k)$.

Fault-tolerant controller of agent i:

$$u_i(k) = -cK\sum_{j=1}^{N} a_{ij}(\xi_i(k) - x_{ji}(k)), \tag{5}$$

where c and K are the coupling gain and the feedback gain, respectively.

By defining the encryption error as $e_i(k) \triangleq \xi_i(k) - x_i(k)$ and the quantization error as $\delta_i(k-1) \triangleq s_i(k) - (x_i(k) - A\xi_i(k-1))/g(k-1)$, we have

$$\begin{cases} e_i(k) = g(k-1)\delta_i(k-1), \quad k \ge 1 \\ e_i(0) = -x_i(0). \end{cases} \tag{6}$$

Remark 1 *The auxiliary variable $\xi_i(k)$ is introduced to reduce the size of the transmitted data, which can be demonstrated later by the simulation results that $\|s_i(k)\|_\infty$ is maintained below a threshold even if $x_i(k)$ tends to diverge. Besides, different from the common uniform quantization scheme (for which $g(k) \equiv 1$), the quantization scheme associated with appropriately selected encryption-decryption key $g(k)$ will not introduce additional steady-state error.*

Remark 2 *In case that the EDA is obtained by eavesdroppers, we provide a possible remedy to ensure that the state of all agents is kept secret from others (including their neighbors). Note that the contribution from agent j in the controller (5), denoted by $c_{ij}(k) \triangleq a_{ij}(\xi_i(k) - x_{ji}(k))$, can be obtained according to*

$$\begin{cases} c_{ij}(k) = Ac_{ij}(k-1) + a_{ij}g(k-1)(s_i(k) - s_j(k)) \\ c_{ij}(0) = \mathbf{0}_n, \quad j \in \mathcal{N}_i, \end{cases}$$

which implies that the value of $a_{ij}(\xi_i(k) - x_{ji}(k))$ can be derived from that of $a_{ij}(s_i(k) - s_j(k))$. Besides, a_{ij} can be calculated according to $a_{ij} = a_i \times a_j$ with a_i and a_j generated by agents i and j, respectively. Then, by exploiting the Paillier encryption algorithm (PEA), agent i can obtain $a_j(s_i(k) - s_j(k))$ without knowing the values of a_j and $s_j(k)$, and this is made achievable due to the homomorphic property of the PEA [28].

3.3 Encryption-decryption-based FTCC scheme II

In what follows, we provide a modified encryption-decryption-based FTCC scheme, where a new auxiliary system is introduced to generate ζ_i.

Auxiliary states of agent i:

$$\begin{cases} \zeta_i(k+1) = A\zeta_i(k) + Bu_{i2}(k) \\ \zeta_i(0) = x_i(0). \end{cases} \tag{7}$$

Encryption algorithm of agent i:

$$\begin{cases} s_i(k) = Q_t\left(\dfrac{\zeta_i(k) - A\xi_i(k-1)}{g(k-1)}\right) \\ \xi_i(k) = A\xi_i(k-1) + g(k-1)s_i(k) \\ \xi_i(0) = \mathbf{0}_n. \end{cases} \tag{8}$$

Decryption algorithm of agent i:

$$\begin{cases} x_{ji}(k) = Ax_{ji}(k-1) + g(k-1)s_j(k) \\ x_{ji}(0) = \mathbf{0}_n, \quad j \in \mathcal{N}_i. \end{cases} \tag{9}$$

Internal state-tracking controller of agent i:

$$u_{i1}(k) = -c_1K_1(x_i(k) - \zeta_i(k)). \tag{10}$$

External consensus controller of agent i:

$$u_{i2}(k) = -c_2K_2\sum_{j=1}^{N} a_{ij}(\xi_i(k) - x_{ji}(k)). \tag{11}$$

Total controller of agent i:

$$u_i(k) = u_{i1}(k) + u_{i2}(k). \tag{12}$$

Remark 3 *It is worth mentioning that the structure of Scheme I leads to a coupling between the fault-tolerant controller (5) and the EDA. This coupling, if not appropriately dealt with, could largely affect the performance of the MAS. As such, we propose a novel analysis method capable of quantitatively analyzing the coupling to facilitate the decoupling design. On the other hand, by introducing an additional healthy system (7), Scheme II could be naturally used to realize the decoupling design of the EDA and the fault-tolerant controller (10). Nevertheless, under Scheme II, the design of the external-consensus loop does not really consider the internal state-tracking loop. This kind of open-loop structure cannot deal with the situation where agents fail to track the healthy system, and this constitutes one of our future research focuses.*

In the following, we will give the definition of consensus.

Definition 1 *(Consensus [26]) For the system (1), if*

$$\lim_{k\to\infty} \|x_i(k) - x_j(k)\| = 0 \tag{13}$$

is satisfied for any given matrix norm and $i, j \in \mathfrak{N} \triangleq \{1, 2, \ldots, N\}$, then we say that the consensus is reached asymptotically.

Definition 2 *(Bounded consensus) For the system (1), if there exists a positive constant $\mathcal{B}$ such that*

$$\lim_{k\to\infty} \|x_i(k) - x_j(k)\| \le \mathcal{B} \tag{14}$$

is satisfied for any given matrix norm and $i, j \in \mathfrak{N}$, then the bounded consensus is said to be reached.

This paper aims to choose the appropriate encryption-decryption-based FTCC scheme and design appropriate encryption-decryption algorithms and fault-tolerant controllers to guarantee the consensus or bounded consensus of the MAS (1) subject to actuator faults through secure communication.

4 Main Results

In this section, we provide a series of executable algorithms to design encryption-decryption-based FTCC schemes with respect to LoE faults and additive faults.

4.1 Handling LoE faults

Considering the MAS subject to LoE faults, we design a fault-tolerant controller under the structure of encryption-decryption-based FTCC scheme I, and then discuss the size of the transmitted data.

By denoting

$$\begin{aligned} &x = \left[x_1^T, x_2^T, \cdots, x_N^T\right]^T, \ e = \left[e_1^T, e_2^T, \cdots, e_N^T\right]^T \\ &\xi = \left[\xi_1^T, \xi_2^T, \cdots, \xi_N^T\right]^T, \ s = \left[s_1^T, s_2^T, \cdots, s_N^T\right]^T, \\ &u = \left[u_1^T, u_2^T, \cdots, u_N^T\right]^T, \ \delta = \left[\delta_1^T, \delta_2^T, \cdots, \delta_N^T\right]^T, \\ &\varrho = \mathrm{diag}\{\varrho_1, \varrho_2, \ldots, \varrho_N\}, \end{aligned}$$

the consensus problem of the MAS can be transform ed into a stability analysis problem of a MIMO system through the following steps, where $\vartheta_{\max} = 0$.

s1) From (1) and (5), we obtain the closed-loop system:

$$\begin{aligned} &x(k+1) \\ &= (I_N \otimes A)x(k) - c(I_N \otimes B)(I - \varrho)(L \otimes K)\xi(k) \\ &= \big(I_N \otimes A - c(I_N \otimes B)(I - \varrho)(L \otimes K)\big)x(k) \\ &\quad - c(I_N \otimes B)(I - \varrho)(L \otimes K)e(k). \end{aligned} \tag{15}$$

s2) Letting $z \triangleq (T_1^T \otimes I_n)x$, then we obtain

$$\begin{aligned} &z(k+1) \\ &= \big(I_{N-1} \otimes A - c(T_1^T \otimes B)(I - \varrho)(T_1\Phi \otimes K)\big)z(k) \\ &\quad - c(T_1^T \otimes B)(I - \varrho)(L \otimes K)e(k). \end{aligned} \tag{16}$$

Before providing the main results, we give the following assumptions and lemmas.

Assumption 1 *The undirected graph $\mathcal{G}$ is connected.*

Assumption 2 *There exists a known positive constant χ_0 such that $\|x_i(0)\|_\infty \le \chi_0$, $\forall i \in \mathfrak{N}$, which means that the initial state deviations between agents are bounded.*

Lemma 1 *Under Assumption 1, for any give positive semi-definite matrix $P \geq 0$, we have*

$$\lambda_2 L \otimes P \leq L^2 \otimes P \leq \lambda_N L \otimes P.$$

Proof: The result can be directly obtained from $L = T_1 \Phi T_1^T$ and $T_1^T T_1 = I_{N-1}$.

As an important mathematical tool, the modified discrete algebraic Riccati equation (MDARE) is introduced:

$$P = A^T PA - \kappa A^T PB(B^T PB + I)^{-1} B^T PA + Q, \tag{17}$$

where $\kappa \triangleq 1 - \kappa_0^2$. For $\kappa_0 = 0$, the MDARE (17) is reduced to the traditional discrete algebraic Riccati equation.

Lemma 2 *([15, 22]) Assume that (A, B) is stabilizable. Then, the following statements are true.*

a) If A has no eigenvalues with magnitude larger than 1, then the MDARE (17) has a unique positive-definite solution P for any $0 < \kappa_0 < 1$.

b) For the case where the rank of B is 1, if A has at least one eigenvalue with magnitude larger than 1, then the MDARE (17) has a unique positive-definite solution if $0 \leq \kappa_0 < 1/\prod_i |\lambda_i^u(A)|$, where $\lambda_i^u(A)$ denotes the unstable eigenvalue of A.

c) If the MDARE (17) has a unique positive-definite solution P, then $P = \lim_{k\to\infty} P(k)$ for any given initial $P(0) \geq 0$, where

$$\begin{aligned} P(k) = Q + A^T P(k-1)A - \kappa A^T P(k-1)B \\ \times (B^T P(k-1)B + I)^{-1} B^T P(k-1)A. \end{aligned}$$

Next, we propose a novel method that enables us to establish the *necessary and sufficient* condition for the existence of the EDA.

Theorem 1 *Under Assumption 1 and the encryption-decryption-based FTCC scheme I, if and only if*

$$\rho(\tilde{\Lambda}) < 1,$$

where $\tilde{\Lambda} \triangleq I_{N-1} \otimes A - c(T_1^T \otimes B)(I - \varrho)(T_1\Phi \otimes K)$, then there exists an encryption-decryption key $g(k) > 0$ such that the consensus of the MAS with agents (1) can be reached for any given initial states.

Proof: *Sufficiency.* From (16), for $k \geq 2$, we have

$$\begin{aligned} &z(k) \\ &= \tilde{\Lambda} z(k-1) - \tilde{K} e(k-1) \\ &= \tilde{\Lambda}^{k-1} z(1) - \sum_{l=1}^{k-1} \tilde{\Lambda}^{k-l-1} \tilde{K} e(l) \\ &= \tilde{\Lambda}^{k-1} z(1) - \sum_{l=1}^{k-1} \tilde{\Lambda}^{k-l-1} \tilde{K} g(l-1)\delta(l-1), \end{aligned} \tag{18}$$

where $\tilde{K} \triangleq c(T_1^T \otimes B)(I - \varrho)(L \otimes K)$ and $z(1) = \tilde{\Lambda} z(0) - \tilde{K} e(0)$. It follows Assumption 2 that $z(1)$ is bounded.

Noting that $\rho(\tilde{\Lambda}) < 1$, we can find a matrix norm $\|\cdot\|_\star$ such that $\rho(\tilde{\Lambda}) \leq \|\tilde{\Lambda}\|_\star = \eta \leq \rho(\tilde{\Lambda}) + \varepsilon < 1$ for any given $0 < \varepsilon < 1 - \rho(\tilde{\Lambda})$. According to [12], for any given matrix norm, there is a vector norm that is compatible with it. To be more specific, for any vector $x \in \mathbb{R}^n$, its vector norm can be chosen as:

$$\|x\|_* = \|xv^T\|_\star, \tag{19}$$

where $v \in \mathbb{R}^n$ can be any non-zero vector.

Therefore, for $\forall k \geq 2$, we have

$$\begin{aligned} \|z(k)\|_* &\leq \eta^{k-1} \|z(1)\|_* \\ &\quad + \|\tilde{K}\|_\star \sum_{l=1}^{k-1} g(l-1)\eta^{k-l-1} \|\delta(l-1)\|_*, \end{aligned} \tag{20}$$

where $\|z(1)\|_*$ is bounded.

Denoting $f(k) = \sum_{l=1}^{k-1} g(l-1)\eta^{k-l-1}\|\delta(l-1)\|_*$ with $k \geq 2$ and $h(k) = f(k)/g(k)$, we obtain

$$\begin{cases} h(k+1) = \dfrac{\eta g(k) h(k)}{g(k+1)} + \dfrac{g(k-1)}{g(k+1)} \|\delta(k-1)\|_* \\ h(2) = \dfrac{g(0)}{g(2)} \|\delta(0)\|_*. \end{cases} \tag{21}$$

If $g(k)$ satisfies

$$\begin{cases} \sup\limits_k g(k)/g(k+1) = \mu \\ \lim\limits_{k\to\infty} g(k) = 0 \\ 0 < \eta\mu < 1, \end{cases} \tag{22}$$

then we conclude that

$$h(k) \leq \frac{2\mu^2}{1 - \eta\mu} \max_k \|\delta(k)\|_* \tag{23}$$

and $\lim\limits_{k\to\infty} f(k) = 0$ which, together with (20), yields

$$\lim_{k\to\infty} \|z(k)\|_* = 0, \tag{24}$$

that is, $\lim_{k\to\infty} z(k) = \mathbf{0}_{n(N-1)}$.

By denoting $y_1 \triangleq (T_0^T \otimes I_n)x$, then it follows from $z(k) = \mathbf{0}_{n(N-1)}$ that

$$x(k) = (T \otimes I_n) \left[y_1^T, z^T \right]^T = \sqrt{1/N} (\mathbf{1}_N \otimes I_n) y_1(k),$$

which means that the consensus is reached.

Necessity. It is known that $\lim_{k\to\infty} \tilde{\Lambda}^k = \mathbf{0}$ if and only if $\rho(\tilde{\Lambda}) < 1$. If $\rho(\tilde{\Lambda}) \geq 1$, $z(k)$ will not converge to zero unless $z(0) = \mathbf{0}$, which means that the consensus of the MAS cannot be achieved unless the MAS is consensus at initial time. The necessity is now proved and the proof is complete.

Remark 4 *The motivation for introducing the matrix norm $\|\cdot\|_\star$ is to overcome the unsuitability of the standard norms for the problem addressed in this paper. We take the analysis method employed in [17] as a comparison* *for further illustration. In [17], the Euclidean norm $\|\cdot\|_2$ of a vector/matrix is employed to derive the results. It should be noted that, for a given matrix A with $\rho(A)<1$, its Euclidean norm may be larger than 1. For the case $\|A\|_2>1$, the analysis method with Euclidean norm will no longer be applicable. In view of this, we construct a new matrix norm as well as its compatible vector norm in this paper.*

So far, with the help of the proposed norm, we have derived the necessary and sufficient condition for the existence of the EDA in Theorem 1, that is, $\rho(\tilde{\Lambda})<1$. In what follows, we will provide two executable algorithms based on Lemma 3 to design the controller gains such that $\rho(\tilde{\Lambda})<1$ is satisfied.

Lemma 3 *Under Assumption 1, for the single-input case, i.e. $u_i\in\mathbb{R}$, if there exist a positive constant c and a positive-definite matrix P satisfying*

$$P=A^TPA-\kappa A^TPB(B^TPB+I)^{-1}B^TPA+Q \tag{25}$$

with a given positive-definite matrix Q and $\kappa\triangleq 2c\lambda_2(1-\varrho_{\max})-c^2\lambda_N^2$, then we have $\rho(\tilde{\Lambda})<1$ by choosing $K=(B^TPB+I)^{-1}B^TPA$.

Proof: For any vector $v_1\in\mathbb{R}^{n(N-1)}$, by denoting

$$v_2\triangleq(T_1\otimes I_n)v_1,\ \tilde{A}\triangleq T_1^T\otimes A,\ \tilde{P}\triangleq\Phi\otimes P,$$

we have

$$\begin{aligned}&v_1^T(\tilde{\Lambda}^T\tilde{P}\tilde{\Lambda}-\tilde{P})v_1\\&=v_2^T(\tilde{A}-\tilde{K})^T\tilde{P}(\tilde{A}-\tilde{K})v_2-v_2^T(L\otimes P)v_2.\end{aligned} \tag{26}$$

By virtue of Lemma 1 and $K^TB^TPBK=A^TPBK-K^TK$, we obtain that

$$\begin{aligned}&v_2^T(\tilde{A}-\tilde{K})^T\tilde{P}(\tilde{A}-\tilde{K})v_2\\&=v_2^T\big(c^2(L\otimes K^T)(I-\varrho)(L\otimes B^TPB)(I-\varrho)(L\otimes K)\\&\quad+L\otimes A^TPA-2c(L\otimes A^TPB)(I-\varrho)(L\otimes K)\big)v_2\\&\le v_2^T\big(L\otimes A^TPA-2c\lambda_2(1-\varrho_{\max})(L\otimes A^TPBK)\\&\quad+c^2\lambda_N^2(L\otimes K^TB^TPBK)\big)v_2\\&=v_2^T\Big(L\otimes\big(A^TPA-\kappa A^TPB(B^TPB+I)^{-1}B^TPA\big)\\&\quad-c^2\lambda_N^2(L\otimes K^TK)\Big)v_2\\&\le v_2^T\Big(L\otimes\big(-\kappa A^TPB(B^TPB+I)^{-1}B^TPA\\&\quad+A^TPA\big)\Big)v_2.\end{aligned} \tag{27}$$

which, together with (25) and (26), leads to

$$\begin{aligned}v_1^T\left(\tilde{\Lambda}^T\tilde{P}\tilde{\Lambda}-\tilde{P}\right)v_1&\le -v_2^T(L\otimes Q)v_2\\&=-v_1^T(\Phi\otimes Q)v_1\\&\le 0.\end{aligned} \tag{28}$$

Furthermore, $v_1^T(\tilde{\Lambda}^T\tilde{P}\tilde{\Lambda}-\tilde{P})v_1=0$ holds if and only if $v_1=\mathbf{0}$ holds, which yields $\tilde{\Lambda}^T\tilde{P}\tilde{\Lambda}-\tilde{P}<0$. Letting v denote the corresponding eigenvector of the eigenvalue $\lambda(\tilde{\Lambda})$, we have

$$\begin{aligned}v^*\tilde{\Lambda}^T\tilde{P}\tilde{\Lambda}v&=|\lambda(\tilde{\Lambda})|^2v^*\tilde{P}v\\&<v^*\tilde{P}v,\end{aligned} \tag{29}$$

where v^* is the conjugate transpose of v, and $\bar{\lambda}(\tilde{\Lambda})$ and $\lambda(\tilde{\Lambda})$ are two conjugate complex numbers. Then, it follows that $\rho(\tilde{\Lambda})<1$, and the proof is complete.

It is worth noting that, (28), together with (29), implies

$$\begin{aligned}v^*\left(\tilde{\Lambda}^T\tilde{P}\tilde{\Lambda}-\tilde{P}\right)v&=\left(|\lambda(\tilde{\Lambda})|^2-1\right)v^*(\Phi\otimes P)v\\&<-v^*(\Phi\otimes Q)v.\end{aligned} \tag{30}$$

Therefore, we have $\rho(\tilde{\Lambda})<\eta_0$ with

$$\eta_0\triangleq\sqrt{1-\lambda_{\min}(Q)/\lambda_{\max}(P)}. \tag{31}$$

Algorithm 1. For the single-input case, the controller gains c and $K=(B^TPB+I)^{-1}B^TPA$ can be designed by solving the MDARE (25) with a given positive-definite matrix Q.

Algorithm 2. For the multi-input case, first, we can obtain a series of controller gains c and $K=(B^TPB+I)^{-1}B^TPA$ by solving the MDARE (25) with different $\varrho_{\max}\ge 0$. Then for each pair of controller gains c and K, calculate the admissible range of ϱ such that $\rho(\tilde{\Lambda})<1$. Choose the controller gains that maximize the admissible range of ϱ.

Remark 5 *In Lemma 3, each agent is supposed to be a single-input system, that is, $B\in\mathbb{R}^n$ and thus $(B^TPB+I)^{-1}\in\mathbb{R}$. Therefore, in the derivation of (27), the following inequality holds:*

$$\begin{aligned}&v_2^T(L\otimes A^TPB)(I-\varrho)(L\otimes K)v_2\\&\ge(1-\varrho_{\max})v_2^T(L^2\otimes A^TPBK)v_2.\end{aligned} \tag{32}$$

It should be noted that for the multi-input case, if $(B^TPB+I)^{-1}$ is not a diagonal matrix, the above derivation may fails. In this case, Algorithm 2 will be an alternative. Algorithm 2 is reasonable due to the fact that the eigenvalue of a matrix is a continuous function on its entries, that is, for each pair of obtained c and K, there exists an admissible set $\mathcal{S}\triangleq\{\varrho|0\le\varrho_{ih}<\bar{\varrho}_{ih}\}$ such that $\rho(\tilde{\Lambda})<1$ for any $\varrho\in\mathcal{S}$.

Remark 6 *Recalling that $\kappa=2c\lambda_2(1-\varrho_{\max})-c^2\lambda_N^2$, we have $\kappa\le\frac{\lambda_2^2}{\lambda_N^2}(1-\varrho_{\max})^2\le 1$. Suppose that (A,B) is stabilizable. Then, it follows from Lemma 2 that the controller derived by Algorithms 1-2 can solve the consensus problem with respect to any of the following graphs:*

c1) Arbitrary connected undirected graphs for the case where A has no unstable eigenvalues. The coupling gain c can be arbitrary value satisfying

$$0<c<\frac{2\lambda_2}{\lambda_N^2}(1-\varrho_{\max}).$$

c2) The specific connected undirected graphs satisfying

$$1-\frac{1}{\prod_i|\lambda_i^u(A)|^2}<\frac{\lambda_2^2}{\lambda_N^2}(1-\varrho_{\max})^2$$

for the case where A has at least one unstable eigenvalue and rank$(B)=1$. Meanwhile, the coupling gain c can be chosen from the set

$$\left\{c\middle|2c\lambda_2(1-\varrho_{\max})-c^2\lambda_N^2>1-\frac{1}{\prod_i|\lambda_i^u(A)|^2}\right\}.$$

Next, we will turn our attention to analyze the requirement on the bandwidth, which can be reflected by the size of transmitted data M. Recalling the definition of Q_t in (3), we have

$$M=\left\lceil\max_{i,k}\left\|\frac{x_i(k)-A\xi_i(k-1)}{\hbar g(k-1)}\right\|_\infty-\frac{1}{2}\right\rceil. \tag{33}$$

Based on Theorem 1, we obtain the following result.

Theorem 2 *Under Assumptions 1 and 2, if the following conditions are satisfied:*

$$\begin{cases}\rho(\tilde{\Lambda})<1 & \text{(34a)}\\ \sup\limits_k\dfrac{g(k)}{g(k+1)}=\mu,\quad 1<\mu<\frac{1}{\rho(\tilde{\Lambda})} & \text{(34b)}\\ \lim\limits_{k\to\infty}g(k)=0, & \text{(34c)}\end{cases}$$

then M is bounded.

Proof: For $\forall i\in\mathfrak{N}$, at time instant $k+1$, we obtain

$$\begin{aligned}&\left\|\frac{x_i(k+1)-A\xi_i(k)}{g(k)}\right\|_\infty\\ \le&\frac{g(k-1)\|A\|_\infty}{g(k)}\left\|\frac{x_i(k)-A\xi_i(k-1)}{g(k-1)}-s_i(k)\right\|_\infty\\ &+\left\|\frac{B(I-\varrho_i)u_i(k)}{g(k)}\right\|_\infty\\ \le&\frac{g(k-1)\hbar\|A\|_\infty}{2g(k)}+\frac{\|Bu_i(k)\|_\infty}{g(k)}.\end{aligned} \tag{35}$$

For $j\in\mathcal{N}_i$, we have

$$\begin{aligned}\|Bu_i(k)\|_\infty\le&\, cd_{\max}\|BK\|_\infty\max_j\|\xi_i(k)-x_i(k)\\ &+x_i(k)-x_j(k)+x_j(k)-\xi_j(k)\|_\infty\\ \le&\, cd_{\max}\|BK\|_\infty(g(k-1)\hbar\\ &+\max_j\|x_i(k)-x_j(k)\|_\infty),\end{aligned} \tag{36}$$

Note that

$$\begin{aligned}&\max_j\|x_i(k)-x_j(k)\|_\infty\\ \le&\sqrt{x(k)^T(L\otimes I_n)x(k)}\\ =&\sqrt{z(k)^T(\Phi\otimes I_n)z(k)}\\ \le&\sqrt{n(N-1)\lambda_N}\|z(k)\|_\infty.\end{aligned} \tag{37}$$

Moreover, combining (20) and (23) leads to

$$\|z(k)\|_*\le\eta^{k-1}\|z(1)\|_*+\|\tilde{K}\|_\star\frac{2\mu^2g(k)}{1-\eta\mu}\max_k\|\delta(k)\|_*. \tag{38}$$

According to the equivalence property of matrix norms, we can find two positive constants k_1 and k_2 such that $k_1\|\cdot\|_\infty\le\|\cdot\|_\star\le k_2\|\cdot\|_\infty$ holds. This, together with the definition of the compatible vector norm (19) with $v=\begin{bmatrix}1,\ 0,\ \cdots,\ 0\end{bmatrix}^T$, leads to

$$\|z(k)\|_\infty\le\frac{k_2}{k_1}\eta^{k-1}\|z(1)\|_\infty+\frac{\mu^2\hbar k_2^2g(k)}{k_1(1-\eta\mu)}\|\tilde{K}\|_\infty. \tag{39}$$

Recalling the introduction of η and (34b), we know that there exists a constant ε such that $\eta\mu<1$, and thus $\eta^{k-1}/g(k)<\mu/g(0)$. Finally, we arrive at

$$\begin{aligned}&\left\|\frac{x_i(k+1)-A\xi_i(k)}{g(k)}\right\|_\infty\\ \le&\frac{ck_2d_{\max}\|BK\|_\infty\sqrt{n(N-1)\lambda_N}}{k_1}\left(\frac{\mu^2\hbar k_2}{1-\eta\mu}\|\tilde{K}\|_\infty\right.\\ &\left.+\frac{\mu\|z(1)\|_\infty}{g(0)}\right)+\frac{\mu\hbar\|A\|_\infty}{2}+c\mu\hbar d_{\max}\|BK\|_\infty.\end{aligned} \tag{40}$$

Then, the result follows from (33), which ends the proof.

Remark 7 *Theorem 1 emphasizes the existence of $g(k)$ and then Theorem 2 provides a feasible method to design $g(k)$. To be more specific, 1) Theorem 1 means that, if there exists a controller such that $\rho(\tilde{\Lambda})<1$, then we can always find a corresponding encryption-decryption key $g(k)$ to ensure the consensus, that is, the fault-tolerant controller design can be decoupled from the EDA design; and 2) Theorem 2 reveals that the choice of $g(k)$ depends on the fault, and gives a feasible form of $g(k)$. $\rho(\tilde{\Lambda})$ in Theorem 2 can be replaced by η_0 for the single-input case as shown in* (31). *For the multi-input case, the maximum of $\rho(\tilde{\Lambda})$ can be calculated off-line according to the known $\varrho_{\max}$.*

4.2 Handling LoE and additive faults

Considering the MAS subject to LoE and additive faults, we adopt the encryption-decryption-based FTCC scheme II and provide the following design method.

Theorem 3 *Under Assumption 1 and the encryption-decryption-based FTCC scheme II, the bounded consensus can be reached if there exist c_1, c_2, K_1 and K_2 such that $\rho(\tilde{\Lambda}_1)<1$ and $\rho(\tilde{\Lambda}_2)<1$, where $\tilde{\Lambda}_1\triangleq A-c_1B(I-\varrho_i)K_1$ and $\tilde{\Lambda}_2\triangleq I_{N-1}\otimes A-c_2(\Phi\otimes BK_2)$. In addition, the encryption-decryption key $g(k)>0$ can be designed according to*

$$\begin{cases}\sup\limits_k\dfrac{g(k)}{g(k+1)}=\mu,\quad 1<\mu<\frac{1}{\rho(\tilde{\Lambda}_2)} & \text{(41a)}\\ \lim\limits_{k\to\infty}g(k)=0, & \text{(41b)}\end{cases}$$

such that the size of the transmitted data is bounded.

Proof: The bounded consensus can be proved through two steps: 1) by introducing $\tilde{z} = (T_1^T \otimes I_n)\zeta$, where $\zeta = \left[\zeta_1^T, \zeta_2^T, \cdots, \zeta_N^T\right]^T$, we can prove that the consensus with respect to the state ζ can be reached, i.e. $\lim_{k\to\infty} \|\zeta_i(k) - \zeta_j(k)\| = 0$; and 2) by introducing the internal state error $\bar{e}_i \triangleq x_i - \zeta_i$, we can prove that $\lim_{k\to\infty} \|x_i(k) - \zeta_i(k)\|$ is bounded. As for the size of the transmitted data, its boundedness can be directly derived from Theorem 2. Now, the proof is complete.

Finally, we provide two algorithms to design the controller gains.

Algorithm 3 For the single-input case, the internal state-tracking controller gains c_1 and $K_1 = (B^T P_1 B + I)^{-1} B^T P_1 A$ can be designed by solving the following M-DARE:

$$P_1 = A^T P_1 A - \kappa_1 A^T P_1 B (B^T P_1 B + I)^{-1} B^T P_1 A + Q_1$$

where $\kappa_1 \triangleq 2c_1(1 - \varrho_{\max}) - c_1^2$ and Q_1 is a given positive-definite matrix.

Algorithm 4 The consensus controller gains c_2 and $K_2 = (B^T P_2 B + I)^{-1} B^T P_2 A$ can be designed by solving the following MDARE:

$$P_2 = A^T P_2 A - \kappa_2 A^T P_2 B (B^T P_2 B + I)^{-1} B^T P_2 A + Q_2$$

where $\kappa_2 \triangleq 2c_2\lambda_2 - c_2^2\lambda_N^2$ and Q_2 is a given positive-definite matrix.

5 Simulations

Consider a network of five agents described by (1) with

$$A = \begin{bmatrix} 1 & 0.1 \\ 0.15 & 0.5 \end{bmatrix}, \quad B = \begin{bmatrix} 0.2 \\ 0.25 \end{bmatrix},$$

where A has an unstable eigenvalue 1.0284. The undirected topology among agents is represented by an adjacency matrix $\mathcal{A}$ with $a_{12} = a_{23} = a_{34} = a_{45} = a_{51} = a_{21} = a_{32} = a_{43} = a_{54} = a_{15} = 1$ and other elements being 0. $\lambda_2 = 1.3820$ and $\lambda_N = 3.6180$. Let $\varrho_{\max} = 0.2$ and $\vartheta_{\max} = 0.6$. Then, we can figure out the controller gains $c_1 = 0.7$, $c_2 = 0.1056$, $K_1 = \begin{bmatrix} 3.2554 & 1.0947 \end{bmatrix}$ and $K_2 = \begin{bmatrix} 3.8489 & 0.8924 \end{bmatrix}$ according to Algorithms 3 and 4. The relevant parameters are set as $Q_1 = Q_2 = I_2$ and $\hbar = 1$. The initial state is set as $x(0) = \begin{bmatrix} 10 & 0 & 20 & 2 & 3 & 0 & 4 & 1 & 5 & 3 \end{bmatrix}^T$. Suppose that $\varrho = \mathrm{diag}\{0.1, 0.2, 0.15, 0.1, 0.2\}$ and $\vartheta = \begin{bmatrix} 0.5 & 0.2 & 0.45 & 0.6 & 0.23 \end{bmatrix}^T$.

We conduct the simulations in the following two cases:

1) Without any encryption-decryption scheme (Fig. 2);
2) With encryption-decryption-based FTCC scheme II (Fig. 3):
   $g(k) = 0.89^k$ and $\hbar = 1$.

The trajectories of $\|x_1(k) - x_i(k)\|_2$ and the size of transmitted data are provided in Figs. 2-3, where $s_{\max}(k)$ is defined as $s_{\max}(k) \triangleq \max_i \|x_i(k)\|_\infty$ in Case 1, and $s_{\max}(k) \triangleq \max_i \|s_i(k)\|_\infty$ in Case 2. From these simulation results, we conclude that: 1) compared with the scheme in Case 1, the introduction of the quantization in Case 2 leads to the discontinuity of the input variables, and affects the transient performance of the system accordingly; 2) the proposed encryption-decryption scheme will not affect the steady-state performance of the system, i.e., the steady-state error will converge to zero; 3) compared with the result in Case 1, the size of the transmitted data in Case 2 is bounded; and 4) the proposed fault-tolerant consensus controller can tolerate the LoE fault and the additive fault.

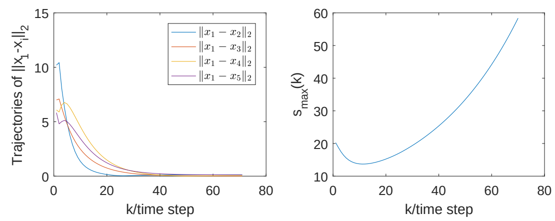

Fig. 2. Simulation results under Case 1.

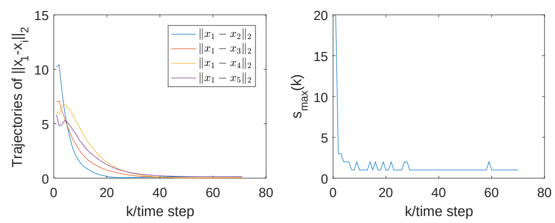

Fig. 3. Simulation results under Case 2.

6 Conclusion

In this paper, we have proposed two kinds of encryption-decryption-based FTCC schemes, where the encryption-decryption mechanism has been introduced to facilitate the secure communication and the fault-tolerant controller has been designed to improve individual reliability. The derived necessary and sufficient condition could serve as an index in controllers and EDAs design, and help to obtain low-conservatism results. In a sense, additive faults lead to the bounded consensus of MASs, while LoE faults may affect the ability of MASs to reach consensus. As for the LoE fault, MDARE-based design algorithms have been provided to deal with the fault-induced heterogeneity. One of the future research topics would be the consideration of the encryption-decryption-based FTCC for continuous systems. Besides, we are interested in the fault-diagnosis-based control method, especially in the context of encryption-decryption issues.

References

[1] C. Chen, K. Xie, F. L. Lewis, S. Xie and A. Davoudi, Fully distributed resilience for adaptive exponential

synchronization of heterogeneous multi-agent systems against actuator faults, *IEEE Transactions on Automatic Control*, vol. 64, no. 8, pp. 3347–3354, 2019.

[2] J. Chen, W. Zhang, Y.-Y. Cao and H. Chu, Observer-based consensus control against actuator faults for linear parameter-varying multiagent systems, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 47, no. 7, pp. 1336–1347, 2017.

[3] C. A. Desoer and Y.-T. Wang, On the generalized Nyquist stability criterion, *IEEE Transactions on Automatic Control*, vol. 25, no. 2, pp. 187–196, 1980.

[4] L. Ding, Q.-L. Han, X. Ge and X.-M. Zhang, An overview of recent advances in event-triggered consensus of multiagent systems, *IEEE transactions on Cybernetics*, vol. 48, no. 4, pp. 1110–1123, 2018.

[5] D. Dzung, M. Naedele, T. P. Von Hoff and M. Crevatin, Security for industrial communication systems, *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1152–1177, 2005.

[6] J. A. Fax and R. M. Murray, Information flow and cooperative control of vehicle formations, *IEEE Transactions on Automatic Control*, vol. 49, no. 9, pp. 1465–1476, 2004.

[7] Z. Feng and G. Hu, Connectivity-preserving flocking for networked Lagrange systems with time-varying actuator faults, *Automatica*, vol. 109, pp. 108509, 2019.

[8] C. Gao and X. He, Fault-tolerant consensus control for multi-agent systems with actuator saturation, In: *Proc. 33rd Youth Academic Annual Conference of Chinese Association of Automation (YAC)*, pp. 484–488, 2018.

[9] C. Gao, Z. Wang, X. He and H. Dong, Fault-tolerant consensus control for multi-agent systems: An encryption-decryption scheme, *IEEE Transactions on Automatic Control*, in press, DOI: 10.1109/TAC.2021.3079407.

[10] C. Gao, Z. Zhen and H. Gong, A self-organized search and attack algorithm for multiple unmanned aerial vehicles, *Aerospace Science and Technology*, vol. 54, pp. 229–240, 2016.

[11] X. Ge and Q.-L. Han, Consensus of multiagent systems subject to partially accessible and overlapping Markovian network topologies, *IEEE Transactions on Cybernetics*, vol. 47, no. 8, pp. 1807–1819, Aug. 2017.

[12] R. A. Horn and C. R. Johnson, *Matrix analysis*, United Kingdom: Cambridge University Press, 1985.

[13] M. Ji, G. Ferrari-Trecate, M. Egerstedt and A. Buffa, Containment control in mobile networks, *IEEE Transactions on Automatic Control*, vol. 53, no. 8, pp. 1972–1975, 2008.

[14] X. Jin, Adaptive iterative learning control for high-order nonlinear multi-agent systems consensus tracking, *Systems & Control Letters*, vol. 89, pp. 16–23, 2016.

[15] T. Katayama, On the matrix Riccati equation for linear systems with random gain, *IEEE Transactions on Automatic Control*, vol. 21, no. 5, pp. 770–771, 1976.

[16] C. Kwon and I. Hwang, Sensing-based distributed state estimation for cooperative multiagent systems, *IEEE Transactions on Automatic Control*, vol. 64, no. 6, pp. 2368–2382, 2019.

[17] H. Li, G. Chen, X. Liao and T. Huang, Leader-following consensus of discrete-time multiagent systems with encoding-decoding, *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 63, no. 4, pp. 401–405, 2016.

[18] H. Li, C. Huang, G. Chen, X. Liao and T. Huang, Distributed consensus optimization in multiagent networks with time-varying directed topologies and quantized communication, *IEEE Transactions on Cybernetics*, vol. 47, no. 8, pp. 2044–2057, 2017.

[19] P. Li and H. Duan, A potential game approach to multiple UAV cooperative search and surveillance, *Aerospace Science and Technology*, vol. 68, pp. 403–415, 2017.

[20] T. Li and L. Xie, Distributed consensus over digital networks with limited bandwidth and time-varying topologies, *Automatica*, vol. 47, no. 9, pp. 2006–2015, 2011.

[21] T. Li and L. Xie, Distributed coordination of multi-agent systems with quantized-observer based encoding-decoding, *IEEE Transactions on Automatic Control*, vol. 57, no. 12, pp. 3023–3037, 2012.

[22] Z. Li and Z. Duan, *Cooperative control of multi-agent systems: A consensus region approach*, Boca Raton: CRC Press, 2017.

[23] K. Liu, X. Mu and T. Li, Sampled-data-based consensus of continuous-time systems with limited data rate, *IET Control Theory Applications*, vol. 11, no. 14, pp. 2328–2335, 2017.

[24] Q. Liu, Z. Wang, X. He and D. H. Zhou, On Kalman-consensus filtering with random link failures over sensor networks, *IEEE Transactions on Automatic Control*, vol. 63, no. 8, pp. 2701–2708, 2018.

[25] X. Liu, J. Lam, W. Yu and G. Chen, Finite-time consensus of multiagent systems with a switching protocol, *IEEE Transactions on Neural Networks and Learning Systems*, vol. 27, no. 4, pp. 853–862, 2016.

[26] R. Olfati-Saber and R. M. Murray, Consensus protocols for networks of dynamic agents, In: *Proc. 2003 American Control Conference*, pp. 951–956, 2003.

[27] R. Olfati-Saber and R. M. Murray, Consensus problems in networks of agents with switching topology and time-delays, *IEEE Transactions on Automatic Control*, vol. 49, no. 9, pp. 1520–1533, 2004.

[28] P. Paillier, Public-key cryptosystems based on composite degree residuosity classes, In: *Proc. International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 223–238, 1999.

[29] Z.-H. Pang and G.-P. Liu, Design and implementation of secure networked predictive control systems under deception attacks, *IEEE Transactions on Control Systems Technology*, vol. 20, no. 5, pp.1334–1342, 2012.

[30] J. Qin, Q. Ma, Y. Shi and L. Wang, Recent advances in consensus of multi-agent systems: A brief survey, *IEEE Transactions on Industrial Electronics*, vol. 64, no. 6, pp. 4972–4983, 2016.

[31] J. Qin, G. Zhang, W. X. Zheng and Y. Kang, Adaptive sliding mode consensus tracking for second-order nonlinear multiagent systems with actuator faults, *IEEE Transactions on Cybernetics*, vol. 49, no. 5, pp. 1605–1615, 2019.

[32] R. Sakthivel, B. Kaviarasan, C. K. Ahn and H. R. Karimi, Observer and stochastic faulty actuator-based reliable consensus protocol for multiagent system, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 12, pp. 2383–2393, 2018.

[33] W. Song, J. Wang, S. Zhao and J. Shan, Event-triggered cooperative unscented Kalman filtering and its application in multi-UAV systems, *Automatica*, vol. 105, pp. 264–273, 2019.

[34] L. Wang, Z. Wang, G. Wei and F. E. Alsaadi, Observer-based consensus control for discrete-time multiagent systems with coding-decoding communication protocol, *IEEE Transactions on Cybernetics*, vol. 49, no. 12, pp. 4335–4345, 2019.

[35] Z. Wang, L. Wang, S. Liu and G. Wei, Encoding-decoding-based control and filtering of networked systems: Insights, developments and opportunities, *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 1, pp. 3–18, 2018.

[36] H. Xiao, R. Cui and D. Xu, A sampling-based Bayesian approach for cooperative multiagent online search with resource constraints, *IEEE Transactions on Cybernetics*, vol. 48, no. 6, pp. 1773–1785, 2018.

[37] W. Xu, D. W. C. Ho, J. Zhong and B. Chen, Event/self-triggered control for leader-following consensus over unreliable network with DoS attacks, *IEEE Transactions on Neural Networks and Learning Systems*, vol. 30, no. 10, pp. 3137–3149, 2019.

[38] D. Yang, W. Ren, X. Liu and W. Chen, Decentralized event-triggered consensus for linear multi-agent systems under general directed graphs, *Automatica*, vol. 69, pp. 242–249, 2016.

[39] Y. Yang and D. Yue, Distributed adaptive fault-tolerant control of pure-feedback nonlinear multi-agent systems with actuator failures, *Neurocomputing*, vol. 221, pp. 72–84, 2017.

[40] H. Zhang, D. Yue, C. Dou, W. Zhao and X. Xie, Data-driven distributed optimal consensus control for unknown multiagent systems with input-delay, *IEEE Transactions on Cybernetics*, vol. 49, no. 6, pp. 2095–2105, 2019.

[41] B. Zhou, W. Wang and H. Ye, Cooperative control for consensus of multi-agent systems with actuator faults, *Computers & Electrical Engineering*, vol. 40, no. 7, pp. 2154–2166, 2014.

[42] K. Zhu, J. Hu, Y. Liu, N. D. Alotaibi and F. E. Alsaadi, On ℓ_2-ℓ_∞ output-feedback control scheduled by stochastic communication protocol for two-dimensional switched systems, *International Journal of Systems Science*, in press, DOI: 10.1080/00207721.2021.1914768.

[43] L. Zou, Z. Wang, J. Hu, Y. Liu and X. Liu, Communication-protocol-based analysis and synthesis of networked systems: Progress, prospects and challenges, *International Journal of Systems Science*, in press, DOI: 10.1080/00207721.2021.1917721.

[44] L. Zou, Z. Wang, Q.-L. Han and D. H. Zhou, Moving horizon estimation of networked nonlinear systems with random access protocol, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 5, pp. 2937–2948, 2021.

[45] L. Zou, Z. Wang, H. Geng and X. Liu, Set-membership filtering subject to impulsive measurement outliers: A recursive algorithm, *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 2, pp. 377–388, 2021.