Fault-Tolerant Consensus Control for Multi-agent Systems: An Encryption-Decryption Scheme

Chen Gao, Zidong Wang, *Fellow, IEEE*, Xiao He, *Senior Member, IEEE*, and Hongli Dong, *Senior Member, IEEE*

***Abstract*—In this paper, the fault-tolerant consensus control problem is investigated for multi-agent systems with sensor faults. A first-order difference equation is utilized to describe the sensor fault, and an observer is designed to estimate the state and the fault simultaneously. For security enhancement and/or congestion mitigation purposes, the estimated state is first encrypted into a series of finite-level codewords by an encryption algorithm and then transmitted to other agents through a directed topology. After being received, the codewords are then decrypted by the corresponding decryption algorithm and subsequently utilized to design the consensus controller. By constructing a novel matrix norm along with its compatible vector norm, we obtain a necessary and sufficient condition, which serves as an index in the observer and the controller design. In the end, two simulation examples are given to demonstrate the validity of the results in this paper.**

***Index Terms*—Encryption-decryption scheme, multi-agent system, consensus, fault-tolerant control, sensor faults.**

I. Introduction

The consensus problem has long been a fundamental research topic with its root in distributed computing [3], [31]. In particular, the consensus control problem for multi-agent systems (MASs) has received considerable research attention ever since the seminal work in [9], where a directed graph has been used to model the local information exchange and the knowledge of the graph theory has been introduced to obtain stability conditions for the underlying MASs. Up to now, the consensus control problem for MASs has been extensively studied (see e.g. [6], [24]) with promising applications in a variety of domains such as formation control [8], [30], flocking control [5], [15], [16] and distributed estimation [26], [29].

As a research forefront, the security issue of MASs has attracted growing attention in response to the ever-increasing demand of safety and reliability. For MASs, the security issue may result from a communication-link weakness (logical security issue) or a potential component fault (physical security issue). As for the logical security issue in MASs, the interconnection among agents through the communication networks exhibits obvious vulnerabilities to potential attackers, and this may lead to unintended consequences. In general, data logical security includes three main security properties: confidentiality, integrity, and availability. Confidentiality prevents an unauthorized user from obtaining secret or private data. Integrity prevents an unauthorized user from modifying the data. Availability ensures that the data can be used when requested [28]. Compared with the integrity and availability against different attacks (e.g. Denial-of-Service attacks [10] and Byzantine agents attacks [35]), the confidentiality of MASs, not limited to the single- or double-integrator MASs, has only received initial research attention, which motivates us to shorten this gap.

Generally speaking, data confidentiality protection related technologies include two main types, namely cryptography-based encryption-decryption (CED) and private data release (PDR). CED aims to transmit data securely and correctly, which always requires heavy cryptographic calculations. On the other hand, PDR aims to perturb released data such that the original data can not be inferred from the perturbed data, and simultaneously, the perturbed data can still enable certain utilities [27], which is similar to the coding-decoding technology [33]. The coding-decoding technology has been investigated in the existing literature (see [4], [12], [21], [22] for single-integrator MASs, [23], [25] for double-integrator MASs, [17], [20], [32] for general linear MASs and [7] for nonlinear MASs) with the aim of designing a pair of encoder-decoder appropriately such that at each time instant, the decoding error is possibly small with the minimum size of the released data. Based on the above analysis, in this paper, we propose a novel encryption-decryption scheme combining CED and PDR technologies, where 1) the CED technology is employed to ensure the high security of the system; and 2) the PDR technology, realized by the coding-decoding technology, is employed to reduce the size of the released data, thereby reducing the heavy calculations that will be imposed on the CED algorithm.

Apart from enhancing the logical security, another effective way to improve the security of MASs is to guarantee the physical security, which refers to the protection of tangible items. In this paper, we concentrate on sensors and provide a feasible method to maintain certain availabilities of sensors even in the presence of faults. As is well known, sensors are used for obtaining information and thus provide the primary support for process monitoring and control. As for MASs, they usually perform tasks in harsh environments, which makes the sensors prone to faults. These faults may result from external environmental factors (e.g. temperature, humidity, pollution and corrosion) or internal factors (e.g. abnormal wear of components and over-heating). Moreover, due to the underlying interconnections among agents, these faults, if not dealt with in time, could propagate to the neighboring agents, thereby affecting the performance of the overall MAS. In addition, as compared with the actuator faults ([11], [34]) and the process faults ([18], [19]), the sensor faults need to gain more research attention because the embedded controller is not equipped with the fault-tolerant capability against sensor faults [38], and this motivates the research on the fault-tolerant control.

In general, the sensor fault is first estimated by constructing an augmented system as well as an observer, and a controller is then designed to compensate the effect from the sensor fault [13], [14], [39]. According to the prior knowledge about the faults, we can choose to construct an augmented descriptor system or an augmented

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 Beijing National Research Center for Information Science and Technology (BNRist) Program of China under Grant BNR2019TD01009, the Natural Science Foundation of Heilongjiang Province of China under Grant ZD2019F001, the Royal Society of the UK, and the Alexander von Humboldt Foundation of Germany. *(Corresponding author: Xiao He.)*

C. Gao and X. He are with the Department of Automation, Tsinghua University, Beijing 100084, China. (Email: hexiao@tsinghua.edu.cn)

Z. Wang is with the Department of Computer Science, Brunel University London, Uxbridge, Middlesex, UB8 3PH, United Kingdom. (Email: Zidong.Wang@brunel.ac.uk)

H. Dong is with the Artificial Intelligence Energy Research Institute, Northeast Petroleum University, Daqing 163318, China. She is also with the Heilongjiang Provincial Key Laboratory of Networking and Intelligent Control, Northeast Petroleum University, Daqing 163318, China. (Email: shiningdhl@vip.126.com)

non-descriptor system. Specifically, if we do not know any prior knowledge, an augmented descriptor system can be constructed [13], [14]. Nevertheless, it is worth noting that to obtain an accurate estimation, the detectability of the descriptor system is typically required and such a requirement is rather stringent. To get rid of the detectability requirement, an augmented non-descriptor system can be constructed by assuming the magnitude or the derivation/first-order difference of the fault is bounded [39]. Inspired by [39], where the continuous-time systems is considered, we construct an augmented non-descriptor system as well as its observer to deal with sensor faults for discrete-time systems. The novelty lies in that: 1) by introducing the first-order difference of the sensor fault, bias faults and drift faults can be estimated/tolerated simultaneously; and 2) a novel matrix norm along with its compatible vector norm is exploited so as to derive the necessary and sufficient condition for the observer and observer-based fault-tolerant controller design.

Motivated by the above discussion, in this paper, we strive to deal with the fault-tolerant consensus control problem for MASs subject to sensor faults under an encryption-decryption scheme. The main contributions of this paper are summarized as follows: 1) we have made one of the first attempts to deal with the data confidentiality issue through combining cryptographic computation algorithm and system dynamics, which could largely reduce the calculation burden and preserve certain control-theoretic performance of MASs; 2) a novel matrix norm along with its compatible vector norm is constructed (according to the property of the spectral radius) so as to obtain the necessary and sufficient condition to facilitate the design of the observer-based consensus controller; and 3) a novel analysis method is proposed based on the constructed norm to deal with the tight couplings of coding-decoding-based PDR algorithm, consensus controller and observer.

The rest of this paper is structured as follows. In Section II, fundamental concepts on graphs, the model of MASs subject to sensor faults and basic encryption-decryption ideas are introduced. In Section III, the encryption-decryption-based consensus is analyzed and the consensus controller is designed. In Section IV, two simulation examples are provided and Section V concludes this paper.

Notations. Let $\mathbf{1}_m$ and $\mathbf{0}_m$ denote the $m \times 1$ column vector with all ones and all zeros, respectively. $\mathbf{0}_{m\times n}$ stands for the $m \times n$ matrix with all zeros. I_n is a n-dimensional identity matrix. $\mathrm{diag}\{f_0, \ldots, f_n\}$ represents a diagonal matrix with $f_0, \ldots, f_n$ as its diagonal elements. $\rho(A)$ and $\lambda_{\max}(A)$ denote, respectively, the spectral radius and the maximum eigenvalue of the square matrix A. $\|\cdot\|_2$ and $\|\cdot\|_\infty$ denote, respectively, the 2-norm and the ∞-norm of a vector or a matrix. For a complex number s, $\mathrm{Re}(s)$ and $\bar{s}$ represent its real part and conjugate complex number, respectively. For a symmetric matrix P, $P > 0$ means P is positive definite. For a complex matrix $\mathcal{C}$, $\mathcal{C}^*$ denotes the conjugate transpose of $\mathcal{C}$. The symbol $\otimes$ represents the Kronecker product. For a given real number x, $\lceil x \rceil$ means the minimum integer not smaller than x.

II. Problem Formulation

For an MAS consisting of N agents, the information flow within the system forms a directed graph $\mathcal{G} \triangleq (v, \varepsilon, \mathcal{A}_\mathcal{G})$, where $v = \{v_1, v_2, \ldots, v_N\}$ is the set of nodes and each node represents an agent, $\varepsilon \subset v \times v$ is the set of edges and $\varepsilon_{ij} = (v_i, v_j) \in \varepsilon$ if there is an information flow from node v_i to node v_j, and $\mathcal{A}_\mathcal{G} = \left[a_{ij}\right]_{N\times N}$ is the adjacency matrix. The set of neighbors of node v_i is denoted by $\mathcal{N}_i = \{j | j \in v, j \neq i, \varepsilon_{ji} \in \varepsilon\}$ and the cardinality of $\mathcal{N}_i$ (i.e. the in-degree of node v_i) is denoted by d_i. $a_{ij} = 1/(d_i + 1)$ if and only if $\varepsilon_{ji} \in \varepsilon$, otherwise $a_{ij} = 0$. $L = \left[l_{ij}\right]_{N\times N}$ denotes the Laplacian matrix of the graph $\mathcal{G}$ with $l_{ii} = \sum_{j=1, j\neq i}^{N} a_{ij},\ l_{ij} = -a_{ij}, i \neq j$. The i-th eigenvalue of L is denoted by $\lambda_i(L)$. A directed graph $\mathcal{G}$ is said to contain a directed spanning tree if there exists a node that can reach any other nodes through paths.

In this paper, we consider the leaderless consensus of an MAS consisting of N agents. The dynamics of each agent is described by

$$\begin{cases} x_i(k+1) = Ax_i(k) + Bu_i(k) \\ \quad y_i(k) = Cx_i(k) + Ff_i(k) \end{cases} \tag{1}$$

where $x_i \in \mathbb{R}^n$, $u_i \in \mathbb{R}^m$ and $y_i \in \mathbb{R}^q$ are the state variable, the input variable and the output variable, respectively. $f_i(k) = \left[f_{i1}(k), \cdots, f_{ip}(k)\right]^T \in \mathbb{R}^p$ denotes the unknown sensor fault that evolves according to

$$f_i^{[1]}(k+1) = f_i^{[1]}(k) + \Delta f_i^{[1]}(k), \tag{2}$$

where $\Delta f_i^{[1]} \triangleq \left[\Delta f_{i1}^{[1]},\ \Delta f_{i2}^{[1]}, \cdots, \Delta f_{ip}^{[1]}\right]^T$ and $f_i^{[1]}(k) \triangleq f_i(k+1) - f_i(k)$. The form (2) can describe a variety of faults including bias faults (by letting $\Delta f_i^{[1]}(k) \equiv \mathbf{0}$ and $f_i^{[1]}(0) = \mathbf{0}$) and drift faults (by letting $\Delta f_i^{[1]}(k) \equiv \mathbf{0}$ and $f_i^{[1]}(0) \neq \mathbf{0}$).

Definition 1: (Consensus) The consensus is said to be reached asymptotically if

$$\lim_{k\to\infty} \|x_i(k) - x_j(k)\| = 0,\ i, j = 1, 2, \ldots, N \tag{3}$$

is satisfied for any given matrix norm.

By constructing the following augmented state

$$\zeta_i(k) \triangleq \left[x_i^T(k) \quad f_i^T(k) \quad \left(f_i^{[1]}(k)\right)^T\right]^T,$$

the augmented system can be established as follows:

$$\begin{cases} \zeta_i(k+1) = \bar{A}\zeta_i(k) + \bar{B}u_i(k) + \bar{D}\Delta f_i^{[1]}(k) \\ \quad y_i(k) = \bar{C}\zeta_i(k), \end{cases} \tag{4}$$

where

$$\bar{A} \triangleq \begin{bmatrix} A & \mathbf{0}_{n\times p} & \mathbf{0}_{n\times p} \\ \mathbf{0}_{p\times n} & I_p & I_p \\ \mathbf{0}_{p\times n} & \mathbf{0}_{p\times p} & I_p \end{bmatrix},\ \bar{B} \triangleq \begin{bmatrix} B \\ \mathbf{0}_{p\times m} \\ \mathbf{0}_{p\times m} \end{bmatrix},$$
$$\bar{C} \triangleq \begin{bmatrix} C & F & \mathbf{0}_{q\times p} \end{bmatrix},\ \bar{D} \triangleq \begin{bmatrix} \mathbf{0}_{n\times p} \\ \mathbf{0}_{p\times p} \\ I_p \end{bmatrix}.$$

Considering the augmented system (4), we propose an observer-based encryption-decryption fault-tolerant consensus control scheme for MASs, which is shown in Fig. 1. First, based on the augmented system (4), an observer is designed to estimate the state and the sensor fault simultaneously. Then, the estimated state variable is encrypted into codewords by a prescribed PDR algorithm as well as a CED algorithm, and subsequently transmitted to the specific agents according to the topology. The received codewords are decrypted and further utilized to design the distributed consensus controller.

In the following, the observer, the coding-decoding-based PDR scheme and the distributed consensus controller will be designed one by one.

Observer of agent i:

$$\begin{cases} \hat{\zeta}_i(k+1) = \bar{A}\hat{\zeta}_i(k) + \bar{B}u_i(k) + G(y_i(k) - \hat{y}_i(k)) \\ \quad \hat{y}_i(k) = \bar{C}\hat{\zeta}_i(k) \\ \quad \hat{\zeta}_i(0) = \mathbf{0}, \end{cases} \tag{5}$$

where $\hat{\zeta}_i(k) \triangleq \left[\hat{x}_i^T(k) \quad \hat{f}_i^T(k) \quad \left(\hat{f}_i^{[1]}(k)\right)^T\right]^T$ and G is the observer gain matrix to be designed.

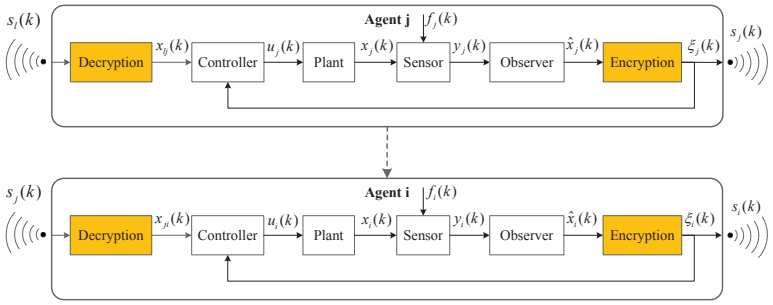

Fig. 1. Observer-based encryption-decryption control scheme.

PDR-coding algorithm of agent i:

$$\begin{cases} s_i(k) = Q_t\left(\dfrac{\hat{x}_i(k) - A\xi_i(k-1)}{g(k-1)}\right) \\ \xi_i(k) = A\xi_i(k-1) + g(k-1)s_i(k) \\ \xi_i(0) = \mathbf{0}, \end{cases} \tag{6}$$

where $\xi_i(k)$ is an auxiliary variable introduced to obtain $s_i(k)$, $s_i(k)$ is the codeword to be transmitted to agent j ($\varepsilon_{ij} \in \varepsilon$), $g(k)$ is a decaying scaling function to be determined, which can also be seen as a symmetric key in the process of PDR since one cannot decrypt the received information if $g(k)$ remains unknown. For $v = \left[v_1, \cdots, v_n\right]^T$, the quantization function is defined as $Q_t(v) \triangleq \left[q_t(v_1), \cdots, q_t(v_n)\right]^T$ with

$$q_t(v_i) = \begin{cases} d\beta, & (d-\frac{1}{2})\beta \le v_i < (d+\frac{1}{2})\beta \\ -q_t(-v_i), & v_i \le -\frac{1}{2}\beta, \end{cases} \tag{7}$$

where β is the given quantization parameter, $|v_i - q_t(v_i)| \le \beta/2$ and $d = 0, 1, 2, \ldots, M$ with $M = \max_{i,k} \|s_i(k)/\beta\|_\infty$. The communication channel of each agent is required to be capable of transmitting $\lceil \log_2(nM+1) + 1 \rceil$ bits of data at each time step.

PDR-decoding algorithm of agent i:

$$\begin{cases} x_{ji}(k) = Ax_{ji}(k-1) + g(k-1)s_j(k) \\ x_{ji}(0) = \mathbf{0}, \quad j \in \mathcal{N}_i, \end{cases} \tag{8}$$

where $x_{ji}(k)$ is the state obtained after decryption.

Controller of agent i:

$$u_i(t) = -cK\sum_{j=1}^{N} a_{ij}(\xi_i(k) - x_{ji}(k)), \tag{9}$$

where $c > 0$ is the coupling gain and K is the feedback gain matrix.

Remark 1: Under the PDR algorithm, agent j sends the codeword $s_j(k)$ to agent i ($\varepsilon_{ji} \in \varepsilon$). Agent i receives $s_j(k)$ and obtains the state $x_{ji}(k)$ according to the decryption algorithm (8). From (6) and (8), we have $x_{ji}(k) = \xi_j(k)$. Through the introduction of the quantization process, the coding-decoding algorithm works as a PDR technology to add uncertainties into the released data, which can be executed in conjunction with CED technology, e.g. Paillier encryption algorithm (PEA), to further enhance the security of the released data. To be more specific, we can transmit the first packet using PEA to ensure the initial state is secure and then let the PDR algorithm take over, which is sufficient to protect the state information of the MAS since the initial inferred error of eavesdroppers will lead to an exponential growing of the estimation error. The encryption-decryption scheme proposed in this paper can be summarized as: 1) the PDR algorithm, realized by introducing a dynamic coding-decoding algorithm, is exploited to add uncertainties into the released data; 2) the introduced coding-decoding algorithm is well designed to preserve control-theoretic performance of the MAS; 3) the CED algorithm, realized by a kind of homomorphic encryption algorithm, is introduced to ensure the high security of the released data; and 4) PDR and CED algorithms are executed cooperatively to greatly reduce the calculation burden.

Define the estimation error as $e_i(k) \triangleq x_i(k) - \hat{x}_i(k)$, the augmented estimation error as $\bar{e}_i(k) \triangleq \zeta_i(k) - \hat{\zeta}_i(k)$, the encryption error as $\tilde{e}_i(k) \triangleq \xi_i(k) - \hat{x}_i(k)$ and the quantization error as $\delta_i(k-1) \triangleq s_i(k) - (\hat{x}_i(k) - A\xi_i(k-1))/g(k-1)$. Then, we obtain

$$\begin{cases} \bar{e}_i(k+1) = (\bar{A} - G\bar{C})\bar{e}_i(k) + \bar{D}\Delta f_i^{[1]}(k) \\ e_i(k) = \begin{bmatrix} I_n & \mathbf{0}_{n\times 2p} \end{bmatrix}\bar{e}_i(k), \end{cases} \tag{10}$$

and

$$\begin{cases} \tilde{e}_i(k) = g(k-1)\delta_i(k-1), \quad k \ge 1 \\ \tilde{e}_i(0) = \mathbf{0}. \end{cases} \tag{11}$$

For notation simplicity, we denote

$$\begin{aligned} &x \triangleq \left[x_1^T, x_2^T, \cdots, x_N^T\right]^T,\ \hat{x} = \left[\hat{x}_1^T, \hat{x}_2^T, \cdots, \hat{x}_N^T\right]^T, \\ &y \triangleq \left[y_1^T, y_2^T, \cdots, y_N^T\right]^T,\ \zeta \triangleq \left[\zeta_1^T, \zeta_2^T, \cdots, \zeta_N^T\right]^T, \\ &e \triangleq \left[e_1^T, e_2^T, \cdots, e_N^T\right]^T,\ \bar{e} \triangleq \left[\bar{e}_1^T, \bar{e}_2^T, \cdots, \bar{e}_N^T\right]^T, \\ &\tilde{e} \triangleq \left[\tilde{e}_1^T, \tilde{e}_2^T, \cdots, \tilde{e}_N^T\right]^T,\ \xi \triangleq \left[\xi_1^T, \xi_2^T, \cdots, \xi_N^T\right]^T, \\ &s \triangleq \left[s_1^T, s_2^T, \cdots, s_N^T\right]^T,\ u \triangleq \left[u_1^T, u_2^T, \cdots, u_N^T\right]^T, \\ &\delta \triangleq \left[\delta_1^T, \delta_2^T, \cdots, \delta_N^T\right]^T. \end{aligned} \tag{12}$$

With the aid of the Kronecker product, the collective dynamics of the MAS can be represented as

$$\begin{cases} x(k+1) = (I_N \otimes A)x(k) + (I_N \otimes B)u(k) \\ y(k) = (I_N \otimes C)x(k). \end{cases} \tag{13}$$

Moreover, (6) and (10) can be written in the following compact form:

$$\begin{cases} s(k) = Q_t\left(\dfrac{\hat{x}(k) - (I_N \otimes A)\xi(k-1)}{g(k-1)}\right) \\ \xi(k) = (I_N \otimes A)\xi(k-1) + g(k-1)s(k) \\ \xi(0) = \mathbf{0}, \end{cases} \tag{14}$$

$$\begin{cases} \bar{e}(k+1) = (I_N \otimes (\bar{A} - G\bar{C}))\bar{e}(k) + \mathcal{D}\Delta f^{[1]}(k) \\ e(k) = (I_N \otimes \begin{bmatrix} I_n & \mathbf{0}_{n\times 2p} \end{bmatrix})\bar{e}(k). \end{cases} \tag{15}$$

where $\Delta f^{[1]} \triangleq \left[(\Delta f_1^{[1]})^T, (\Delta f_2^{[1]})^T, \cdots, (\Delta f_N^{[1]})^T\right]^T$ and $\mathcal{D} \triangleq I_N \otimes \bar{D}$.

In this paper, we investigate the fault-tolerant consensus control problem for MASs subject to sensor faults under the encryption-decryption scheme. In other words, we aim to design the PDR

algorithm (6)-(8), the observer (5) and the controller (9) such that:

1) the consensus of the MAS is reached asymptotically in the presence of the sensor fault (2);
2) the size of the transmitted data is bounded under the PDR algorithm (6)-(8).

III. Main Results

In this section, we first address the consensus problem of the addressed MAS and then analyze the size of the transmitted data. To start with, we give the following assumptions and lemmas, which will be used for deriving our main results in the sequel.

Assumption 1: The directed graph $\mathcal{G}$ contains a directed spanning tree.

Assumption 2: There exist known positive constants χ_c and χ_0 such that $\|x_c(0)\|_\infty \leq \chi_c$ and $\|\zeta(0)\|_\infty \leq \chi_0$, where $x_c(0) = x(0) - (\mathbf{1}_N \boldsymbol{r}^T \otimes I_n)x(0)$.

Lemma 1: [36] Under Assumption 1, 0 is a simple eigenvalue of L and all the other eigenvalues have positive real parts, i.e. $0 = \lambda_1(L) < \mathrm{Re}(\lambda_2(L)) \leq \ldots \leq \mathrm{Re}(\lambda_N(L))$. Moreover, $L\mathbf{1}_N = \mathbf{0}_N$ and there exists a vector $\boldsymbol{r} = \left[r_1, \cdots, r_N\right]^T$ such that $\boldsymbol{r}^T\mathbf{1}_N = 1$ and $\boldsymbol{r}^T L = \mathbf{0}_N^T$.

It follows from Lemma 1 that there exist matrix $T = \left[\frac{1}{\sqrt{N}}\mathbf{1}_N \ T_0\right]$ and $T^{-1} = \left[\sqrt{N}\boldsymbol{r} \ T_1^T\right]^T$ such that

$$T^{-1}LT = J = \begin{bmatrix} 0 & \mathbf{0} \\ \mathbf{0} & \Delta \end{bmatrix},$$

where Δ is a block diagonal matrix.

Lemma 2: Suppose that Assumption 1 holds. Let $P = P^T > 0$ be the solution of the following discrete Riccati equation:

$$A^TPA - P - A^TPB(B^TPB + I)^{-1}B^TPA + Q = 0. \quad (16)$$

Define $K = (B^TPB+I)^{-1}B^TPA$, $r_0 \geq \max_i |\lambda_i(L) - c_0|$ and $r = \left(\lambda_{\max}(Q^{-\frac{1}{2}}K^TB^TPBKQ^{-\frac{1}{2}})\right)^{-\frac{1}{2}}$. Let $c_0 \leq 2\min_i\{Re(\lambda_i(L))\}$. If there exist a matrix $Q = Q^T > 0$ and a scalar c_0 such that $r_0/c_0 < r$, then $\rho(A - \frac{1}{c_0}\lambda_i(L)BK) < 1$ for all $i = 2, \ldots, N$.

Proof: It follows from (16) and $K = (B^TPB + I)^{-1}B^TPA$ that

$$\begin{aligned} &A^TPA - P - A^TPB(B^TPB + I)^{-1}B^TPA + Q \\ &= (A - BK)^TP(A - BK) + K^TK - P + Q = 0. \end{aligned} \quad (17)$$

For a complex number $s = a + bj$, we know that

$$\begin{aligned} &(A - sBK)^*P(A - sBK) \\ &= (A - aBK)^TP(A - aBK) + b^2K^TB^TPBK. \end{aligned} \quad (18)$$

It follows from (17) and (18) that

$$\begin{aligned} &(A - sBK)^*P(A - sBK) - P \\ &= 2(1 - a)A^TPBK + (a^2 + b^2 - 1)K^TB^TPBK \\ &\quad - K^TK - Q \\ &= (1 - 2a + a^2 + b^2)K^TB^TPBK + (1 - 2a)K^TK - Q \\ &= |s - 1|^2K^TB^TPBK - Q + (1 - 2a)K^TK. \end{aligned} \quad (19)$$

Clearly, if $|s-1| < \left(\lambda_{\max}(Q^{-\frac{1}{2}}K^TB^TPBKQ^{-\frac{1}{2}})\right)^{-\frac{1}{2}} = r$ and $1 - 2a \leq 0$, then $(A - sBK)^*P(A - sBK) - P < 0$. Furthermore, notice that $r_0/c_0 < r$ implies

$$\max_i \left|\frac{\lambda_i(L)}{c_0} - 1\right| < r, \quad (20)$$

and $c_0 \leq 2\min_i\{Re(\lambda_i(L))\}$ implies

$$1 - 2Re\left(\frac{\lambda_i(L)}{c_0}\right) = 1 - \frac{2Re(\lambda_i(L))}{c_0} \leq 0. \quad (21)$$

Therefore, it can be inferred that $(A - \frac{1}{c_0}\lambda_i(L)BK)^*P(A - \frac{1}{c_0}\lambda_i(L)BK) < P$. Letting ν denote the corresponding eigenvector of the eigenvalue $\lambda(A - \frac{1}{c_0}\lambda_iBK)$, we have

$$\begin{aligned} &\nu^*(A - \frac{1}{c_0}\lambda_i(L)BK)^*P(A - \frac{1}{c_0}\lambda_i(L)BK)\nu \\ &= \nu^*\bar{\lambda}(A - \frac{1}{c_0}\lambda_iBK)P\lambda(A - \frac{1}{c_0}\lambda_iBK)\nu \\ &= |\lambda(A - \frac{1}{c_0}\lambda_iBK)|^2\nu^*P\nu < \nu^*P\nu, \end{aligned} \quad (22)$$

which further implies

$$\rho(A - \frac{1}{c_0}\lambda_iBK) < 1, \quad (23)$$

and the proof is complete. ■

Lemma 3: Let $P_1 = P_1^T > 0$ be the solution of the following discrete Riccati equation with a given matrix $Q_1 = Q_1^T > 0$:

$$\bar{A}P_1\bar{A}^T - P_1 - \bar{A}P_1\bar{C}^T(\bar{C}P_1\bar{C}^T + I)^{-1}\bar{C}P_1\bar{A}^T + Q_1 = 0. \quad (24)$$

Then, we have $\rho(\bar{A} - G\bar{C}) < 1$ and the observer gain matrix in (5) can be designed as $G = \bar{A}P_1\bar{C}^T(\bar{C}P_1\bar{C}^T + I)^{-1}$.

Proof: It follows from (24) and $G = \bar{A}P_1\bar{C}^T(\bar{C}P_1\bar{C}^T + I)^{-1}$ that

$$\begin{aligned} &(\bar{A} - G\bar{C})P_1(\bar{A} - G\bar{C})^T - P_1 \\ &= \bar{A}P_1\bar{A}^T - \bar{A}P_1\bar{C}^T(\bar{C}P\bar{C}^T + I)^{-1}\bar{C}P_1\bar{A}^T \\ &\quad - \bar{A}P_1\bar{C}^T(\bar{C}P\bar{C}^T + I)^{-2}\bar{C}P_1\bar{A}^T - P_1 \\ &= -Q_1 - \bar{A}P_1\bar{C}^T(\bar{C}P\bar{C}^T + I)^{-2}\bar{C}P_1\bar{A}^T < 0. \end{aligned} \quad (25)$$

With the similar procedure in Lemma 2, we can readily obtain $\rho(\bar{A} - G\bar{C}) < 1$. ■

Remark 2: The design of the consensus controller is dependent on the Laplacian matrix of the communication graph. Different from the undirected graph, the directed graph leads to complex eigenvalues of its Laplacian matrix, which complicates the controller design problem, and a conventional approach is to discuss the real and imaginary parts of the eigenvalue separately in order to obtain the controller gain, see e.g. [32]. In this paper, inspired by [20], we propose a novel Riccati-equation-based method as illustrated by Lemma 2, where the consensus controller gain is divided into two parts, namely, the coupling gain and the feedback gain. The coupling gain can be adjusted to handle the effect of the graph on the consensus and the feedback gain can be used to achieve the consensus. In addition, compared with the results in [20], the results derived by Lemma 2 has removed the full-rank assumption on the matrix B.

Combining (9), (13), (14) and (15), we obtain the closed-loop collective dynamics as follows:

$$\begin{aligned} x(k+1) &= (I_N \otimes A)x(k) - (cL \otimes BK)\xi(k) \\ &\quad \times (\xi(k) - x(k)) \\ &= (I_N \otimes A - cL \otimes BK)x(k) - (cL \otimes BK) \\ &\quad \times (\xi(k) - \hat{x}(k) + \hat{x}(k) - x(k)) \\ &= (I_N \otimes A - cL \otimes BK)x(t) - (cL \otimes BK) \\ &\quad \times (\tilde{e}(k) - e(k)) \\ &= (I_N \otimes A - cL \otimes BK)x(t) - (cL \otimes BK) \\ &\quad \times \left(\tilde{e}(k) - \left(I_N \otimes \begin{bmatrix} I_n & \mathbf{0}_{n\times 2p} \end{bmatrix}\right)\bar{e}(k)\right). \end{aligned} \quad (26)$$

Now, we are in a position to give the main results.

Theorem 1: Consider the case $\Delta f_i^{[1]}(k) \equiv \mathbf{0}$. Under Assumption 1 and the encryption-decryption-based fault-tolerant consensus control scheme (5)-(9), if and only if $\rho(A - c\lambda_i(L)BK) < 1$ for all $i = 2, \ldots, N$ and $\rho(\bar{A} - G\bar{C}) < 1$, 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. Letting $x_c(k) = x(k) - (\mathbf{1}_N \boldsymbol{r}^T \otimes I_n)x(k)$ and $z(k) = (T^{-1} \otimes I_n)x_c(k)$, we obtain from $(I_N - \mathbf{1}_N \boldsymbol{r}^T)L = L(I_N - \mathbf{1}_N \boldsymbol{r}^T) = L$ that

$$\begin{aligned} z(k+1) &= (I_N \otimes A - cJ \otimes BK)z(k) - (cJT^{-1} \otimes BK) \\ &\quad \times \left(\tilde{e}(k) - \left(I_N \otimes \begin{bmatrix} I_n & \mathbf{0}_{n\times 2p} \end{bmatrix}\right)\bar{e}(k)\right) \\ &\triangleq \begin{bmatrix} z_1^T(k+1) & z_{2-N}^T(k+1) \end{bmatrix}^T, \end{aligned} \tag{27}$$

where $z_1(k) \in \mathbb{R}^n$ and $z_{2-N}(k) \in \mathbb{R}^{(N-1)n}$. Noting that

$$z_1(k) = \left(\sqrt{N}\boldsymbol{r}^T(I_N - \mathbf{1}_N \boldsymbol{r}^T) \otimes I_n\right) x(k) \equiv 0, \tag{28}$$

we have

$$\begin{aligned} z_{2-N}(k+1) &= \Lambda z_{2-N}(k) - (c\Delta T_1 \otimes BK) \\ &\quad \times \left(\tilde{e}(k) - \left(I_N \otimes \begin{bmatrix} I_n & \mathbf{0}_{n\times 2p} \end{bmatrix}\right)\bar{e}(k)\right), \end{aligned} \tag{29}$$

where $\Lambda \triangleq I_{N-1} \otimes A - c\Delta \otimes BK$. Omitting the computation procedure, we arrive at

$$\begin{aligned} z_{2-N}(k) &= \Lambda^{k-1} z_{2-N}(1) - \sum_{l=1}^{k-1} \Lambda^{k-l-1}(c\Delta T_1 \otimes BK) \\ &\quad \times \left(\tilde{e}(l) - \left(I_N \otimes \begin{bmatrix} I_n & \mathbf{0}_{n\times 2p} \end{bmatrix}\right)\bar{e}(l)\right),\ k \geq 2. \end{aligned} \tag{30}$$

Denote $\rho = \max_i\{\rho(A - c\lambda_i(L)BK), \rho(\bar{A} - G\bar{C})\}$. Recalling that $\rho(A - c\lambda_i(L)BK) < 1$ and $\rho(\bar{A} - G\bar{C}) < 1$, we have $\rho < 1$. Using the property of the spectral radius, for any $0 < \varepsilon < 1 - \rho$, we can find a matrix norm such that $\rho(A - c\lambda_i(L)BK) = \rho(\Lambda) \leq \|\Lambda\| = \eta_1 \leq \rho + \varepsilon < 1$, $\rho(\bar{A} - G\bar{C}) = \rho(I_N \otimes (\bar{A} - G\bar{C})) \leq \|I_N \otimes (\bar{A} - G\bar{C})\| = \eta_2 \leq \rho + \varepsilon < 1$ and $\eta_2 < \eta_1$. Then, (30) further leads to

$$\begin{aligned} &\|z_{2-N}(k)\| \\ &\leq \eta_1^{k-1}\|z_{2-N}(1)\| + \|c\Delta T_1 \otimes BK\| \\ &\quad \times \sum_{l=1}^{k-1} g(l-1)\eta_1^{k-l-1}\|\delta(l-1)\| + \|c\Delta T_1 \otimes BK\| \\ &\quad \times \left\|I_N \otimes \begin{bmatrix} I_n & \mathbf{0}_{n\times 2p} \end{bmatrix}\right\| \sum_{l=1}^{k-1} \eta_1^{k-l-1}\|\bar{e}(l)\|, \quad k \geq 2, \end{aligned} \tag{31}$$

with

$$z_{2-N}(1) = \Lambda z_{2-N}(0) + \left(c\Delta T_1 \otimes \left(BK \begin{bmatrix} I_n & \mathbf{0}_{n\times 2p} \end{bmatrix}\right)\right)\bar{e}(0).$$

Denoting $f_1(k) = \sum_{l=1}^{k-1} g(l-1)\eta_1^{k-l-1}\|\delta(l-1)\|$ for $k \geq 2$ and $h(k) = f_1(k)/g(k)$, we obtain

$$h(k+1) = \frac{\eta_1 g(k)}{g(k+1)}h(k) + \frac{g(k-1)}{g(k+1)}\|\delta(k-1)\|. \tag{32}$$

If $\sup_k g(k)/g(k+1) = \mu$, $0 < \eta_1\mu < 1$ and $\lim_{k\to\infty} g(k) = 0$, then $h(k)$ satisfies

$$h(k) \leq \frac{2\mu^2}{1 - \eta_1\mu} \max_k \|\delta(k)\|, \tag{33}$$

and $\lim_{k\to\infty} f_1(k) = 0$.

Moreover, defining $f_2(k) = \sum_{l=1}^{k-1} \eta_1^{k-l-1}\|\bar{e}(l)\|$, we obtain

$$f_2(k) \leq \sum_{l=1}^{k-1} \eta_1^{k-l-1}\eta_2^{l-1}\|\bar{e}(1)\| \leq \frac{\eta_1^{k-2}}{1 - \eta_2/\eta_1}\|\bar{e}(1)\| \tag{34}$$

and furthermore $\lim_{k\to\infty} f_2(k) = 0$. Thus, we have

$$\lim_{k\to\infty} \|z_{2-N}(k)\| = 0, \tag{35}$$

which, together with $z(k) = (T^{-1} \otimes I_n)x_c(k)$, finally concludes that

$$\lim_{k\to\infty} \|x_c(k)\| = 0, \tag{36}$$

and the consensus is therefore achieved.

Necessity. We know that $\lim_{k\to\infty} \Lambda^k = \mathbf{0}$ if and only if $\rho(A - c\lambda_i(L)BK) < 1$, and $\lim_{k\to\infty}(\bar{A} - G\bar{C})^k = \mathbf{0}$ if and only if $\rho(\bar{A} - G\bar{C}) < 1$. If $\rho(A - c\lambda_i(L)BK) \geq 1$ or $\rho(\bar{A} - G\bar{C}) \geq 1$, $z_{2-N}(k)$ will not converge to zero unless $z_{2-N}(0) = \mathbf{0}$. The necessity is directly proved and the proof of Theorem 1 is now complete. ■

Remark 3: Based on the foregoing analysis, we know that $g(k)$ can be arbitrary forms satisfying $\sup_k g(k)/g(k+1) = \mu$, $0 < \eta_1\mu < 1$ and $\lim_{k\to\infty} g(k) = 0$, and two simple examples are $g_0\mu^{-k}$ and $g_0/(k+p)$. For the form $g(k) = g_0\mu^{-k}$, μ can be any values satisfying $1 < \mu < 1/(\rho + \varepsilon)$. Nevertheless, we prefer to choose a larger μ so as to have a higher convergence rate of $z(k)$.

Corollary 1: Consider the more general case where $\Delta f_i^{[1]}(k) \neq \mathbf{0}$ and $\|\Delta f_i^{[1]}(k)\|_\infty \leq f_{\max}$ for any i and k. Under Assumption 1 and the encryption-decryption-based fault-tolerant consensus control scheme (5)-(9), if $\rho(A - c\lambda_i(L)BK) < 1$ for all $i = 2, \ldots, N$ and $\rho(\bar{A} - G\bar{C}) < 1$, then there exists an encryption-decryption key $g(k) > 0$ such that the bounded consensus of the MAS with agents (1) can be reached for any given initial states.

Proof: It follows from (15) that

$$\|\bar{e}(k)\| \leq \eta^{k-1}\|\bar{e}(1)\| + \frac{k_2\|\mathcal{D}\|f_{\max}}{1 - \eta}, \tag{37}$$

where $0 < \eta < 1$ and $k_2 > 0$. This, together with (34), concludes that there exists a positive constant $\mathcal{B}$ such that $\lim_{k\to\infty} \|x_i(k) - x_j(k)\| \leq \mathcal{B}$, i.e., the bounded consensus can be reached. ■

In Theorem 1, we have derived the *necessary and sufficient* condition for the existence of the PDR algorithm. Meanwhile, we have provided a specific design method for the consensus controller gain and the observer gain in Lemma 2 and Lemma 3, respectively. In the following, we will discuss the size of the transmitted data.

From the definition of the quantization function Q_t in (7), it can be calculated that

$$M = \left\lceil \max_{i,k} \left\| \frac{\hat{x}_i(k) - A\xi_i(k-1)}{\beta g(k-1)} \right\|_\infty - \frac{1}{2} \right\rceil. \tag{38}$$

Theorem 2: Consider the case $\Delta f_i^{[1]}(k) \equiv \mathbf{0}$. Under Assumptions 1-2, suppose that the following conditions are satisfied:

$$\begin{cases} \rho(\bar{A} - G\bar{C}) < 1, & \text{(39a)} \\ \rho(A - c\lambda_i(L)BK) < 1, \quad i = 2, \ldots, N, & \text{(39b)} \\ \sup\limits_k \dfrac{g(k)}{g(k+1)} = \mu, \quad 1 < \mu < \frac{1}{(\rho+\varepsilon)}, & \text{(39c)} \\ \lim\limits_{k\to\infty} g(k) = 0, & \text{(39d)} \end{cases}$$

where ε and ρ are defined in Theorem 1. Then, M is bounded.

Proof: At time instant $k+1$, we obtain

$$\begin{aligned} &\left\| \frac{\hat{x}_i(k+1) - A\xi_i(k)}{g(k)} \right\|_\infty \\ &\leq \left\| \frac{\hat{x}_i(k+1) - x_i(k+1)}{g(k)} \right\|_\infty + \left\| \frac{x_i(k+1) - A\xi_i(k)}{g(k)} \right\|_\infty \\ &\leq \left\| \frac{\begin{bmatrix} I_n & \mathbf{0}_{n\times 2p} \end{bmatrix}\bar{e}_i(k)}{g(k)} \right\|_\infty + \left\| \frac{Bu_i(k)}{g(k)} \right\|_\infty \\ &\quad + \frac{g(k-1)\|A\|_\infty}{g(k)} \left\| \frac{x_i(k) - A\xi_i(k-1)}{g(k-1)} - s_i(k) \right\|_\infty \\ &\leq \frac{\|\bar{e}(k)\|_\infty + \|Bu_i(k)\|_\infty + \|A\|_\infty\|\bar{e}(k)\|_\infty}{g(k)} \end{aligned}$$

$$+\frac{g(k-1)\|A\|_\infty}{g(k)}\left\|\frac{\hat{x}_i(k)-A\xi_i(k-1)}{g(k-1)}-s_i(k)\right\|_\infty \le \frac{(1+\|A\|_\infty)\|\bar{e}(k)\|_\infty+\|Bu_i(k)\|_\infty}{g(k)}+\frac{g(k-1)\beta\|A\|_\infty}{2g(k)}. \tag{40}$$

Since $a_{ij}=1/(d_i+1)$, we have $\sum_{j=1}^N a_{ij}<1$ and

$$\begin{aligned}&\|Bu_i(k)\|_\infty\\ &< c\|BK\|_\infty \max_j \|\xi_i(k)-\hat{x}_i(k)+\hat{x}_i(k)-x_i(k)\\ &\quad-(\xi_j(k)-\hat{x}_j(k))-(\hat{x}_j(k)-x_j(k))\\ &\quad+(x_i(k)-x_j(k))\|_\infty\\ &\le c\|BK\|_\infty(g(k-1)\beta+2\|(T\otimes I_n)z(k)\|_\infty\\ &\quad+2\|\bar{e}_i(k)\|_\infty).\end{aligned} \tag{41}$$

Substituting (40) into (41) yields

$$\begin{aligned}&\left\|\frac{\hat{x}_i(k+1)-A\xi_i(k)}{g(k)}\right\|_\infty\\ &<\frac{2c\|BK\|_\infty\|T\otimes I_n\|_\infty\|z(k)\|_\infty}{g(k)}\\ &\quad+(1+\|A\|_\infty)\frac{\|\bar{e}(k)\|_\infty}{g(k)}+\frac{g(k-1)\beta}{2g(k)}\|A\|_\infty\\ &\quad+\frac{c\beta\|BK\|_\infty g(k-1)}{g(k)}+\frac{2c\|BK\|_\infty\|\bar{e}(k)\|_\infty}{g(k)}.\end{aligned} \tag{42}$$

Moreover, combining (31), (33) and (34), we obtain

$$\begin{aligned}&\|z(k)\|\\ &\le \eta_1^{k-1}\|z(1)\|+\|c\Delta T_1\otimes BK\|\frac{\mu^2\beta g(k)}{1-\eta_1\mu}\\ &\quad+\|c\Delta T_1\otimes BK\|\left\|I_N\otimes\begin{bmatrix}I_n & \mathbf{0}_{n\times 2p}\end{bmatrix}\right\|\frac{\eta_1^{k-2}\|\bar{e}(1)\|}{1-\eta_2/\eta_1}.\end{aligned} \tag{43}$$

From the equivalence property of the matrix norm, we know that there exist positive constants k_1 and k_2 such that $k_1\|\cdot\|_\infty\le\|\cdot\|\le k_2\|\cdot\|_\infty$. As a result, we have

$$\begin{aligned}\|z(k)\|_\infty &\le \frac{k_2}{k_1}\eta_1^{k-1}\|z(1)\|_\infty\\ &\quad+\frac{k_2}{k_1}\frac{\mu^2\beta g(k)}{1-\eta_1\mu}\|c\Delta T_1\otimes BK\|_\infty\\ &\quad+\frac{k_2^3\|c\Delta T_1\otimes BK\|_\infty\eta_1^{k-2}}{k_1(1-\eta_2/\eta_1)}\|\bar{e}(1)\|_\infty,\end{aligned} \tag{44}$$

and

$$\|\bar{e}(k)\|_\infty\le\frac{\|\bar{e}(k)\|}{k_1}\le\frac{\eta_2^k\|\bar{e}(0)\|}{k_1}\le\frac{k_2\eta_2^k\|\bar{e}(0)\|_\infty}{k_1}. \tag{45}$$

Finally, we obtain

$$\begin{aligned}&\left\|\frac{\hat{x}_i(k+1)-A\xi_i(k)}{g(k)}\right\|_\infty\\ &<\mu\beta c\|BK\|_\infty+\frac{1+\|A\|_\infty+2c\|BK\|_\infty}{g(0)}\frac{k_2\chi_0}{k_1}\\ &\quad+\frac{ck_2\|BK\|_\infty\|T\|_\infty}{k_1}\left(\frac{2k_2^3\eta_2\chi_0\|c\Delta T_1\otimes BK\|_\infty}{g(0)k_1\eta_1(\eta_1-\eta_2)}\right.\\ &\quad\left.+\frac{2\mu^2\beta\|c\Delta T_1\otimes BK\|_\infty}{1-\eta_1\mu}+\frac{2\chi_c\|T^{-1}\|_\infty\|A\|_\infty}{g(0)\eta_1}\right)\\ &\quad+\frac{\mu\beta\|A\|_\infty}{2},\end{aligned} \tag{46}$$

which implies that M is bounded. The proof is complete. ■

Remark 4: The condition $\eta_1\mu<1$ is utilized to prove the boundedness of M, but this condition is not necessary in ensuring the convergence of $z_{2-N}(k)$. This can be demonstrated by the following example: choosing $g(k)=g_0\mu^{-k}$ with $\eta_1\mu>1$ and $\mu>1$, then we obtain from (32) that $f_1(k)\le g_0\big(\eta_1^{k-2}+\frac{\eta_1^{k-2}-\mu^{2-k}}{\eta_1\mu-1}\big)\max_k\|\delta(k)\|,\forall k\ge 3$. Thus, $\lim_{k\to\infty}f_1(k)=0$, which implies that $z_{2-N}(k)$ is convergent. Moreover, it is worth noting that the derived bounded consensus in Corollary 1 will lead to the infinite size of the transmitted data under the proposed scheme (5)-(9), which is undesirable. In this case, we would like to provide a feasible scheme to reduce the size of the transmitted data. To be more specific, 1) a healthy system can be introduced for each agent as a reference system to deal with the external consensus; and 2) an internal observer-based controller can be designed to track the reference system.

Remark 5: Compared with existing results (e.g. [20]), the technical novelties of this paper can be summarized as follows:

1) The observer-based PDR algorithm is constructed, hence the state is no longer required to be fully available.
2) A general sensor fault model is considered that includes the commonly investigated bias faults and drift faults as special cases.
3) A novel matrix norm along with its compatible vector norm is exploited so as to derive the necessary and sufficient condition for the desired consensus.
4) The full-rank assumption on the matrix B is removed when designing the gain of the controller.

IV. Simulations

Consider an MAS consisting of six agents described by (1) with

$$A=\begin{bmatrix}1 & 0.1\\ 0.15 & 0.5\end{bmatrix},\ B=\begin{bmatrix}0.2\\ 0.25\end{bmatrix},C=\begin{bmatrix}1 & 0\end{bmatrix},\ F=1,$$

where A is unstable but (A,B) is stabilizable. The augmented system with $(\bar{A},\bar{C})$ is detectable. The initial state is set as $x(0)=\begin{bmatrix}1\ 0\ 2\ 2\ 3\ 0\ 4\ 1\ 5\ 3\ 6\ 4\end{bmatrix}^T$.

The directed topology among agents is shown in Fig. 2 and the Laplacian matrix of the graph is

$$L=\begin{bmatrix}0.75 & 0 & 0 & -0.25 & -0.25 & -0.25\\ -0.5 & 0.5 & 0 & 0 & 0 & 0\\ -0.33 & -0.33 & 0.67 & 0 & 0 & 0\\ -0.5 & 0 & 0 & 0.5 & 0 & 0\\ 0 & 0 & 0 & -0.5 & 0.5 & 0\\ 0 & 0 & 0 & 0 & -0.5 & 0.5\end{bmatrix}.$$

The eigenvalues of L are 0, 0.5, 0.6667, 1 and $0.625\pm 0.3307i$. The decaying scaling function is chosen as $g(k)=0.98^k$ and the quantization parameter is $\beta=1$. According to Lemma 2, the controller parameters in (9) are designed as $K=\begin{bmatrix}0.9457 & 0.2602\end{bmatrix}$ and $c=1.0526$. Other parameters are $c_0=0.95$, $r_0=0.4637$, $r=1.7013$, $r_0/c_0=0.4881<r$ and $Q=I$. Letting $Q_1=0.01I$, we obtain the observer gain as $G=\begin{bmatrix}6.4430 & 1.8283 & -5.9331 & -0.0769\end{bmatrix}^T$.

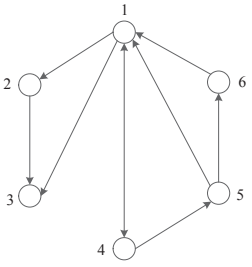

Fig. 2. Topology of the multi-agent system.

We consider the case where the bias fault and the drift fault occur simultaneously with $f_1^{[1]}(k) \equiv 1$, $f_2^{[1]}(k) \equiv 0$, $f_3^{[1]}(k) \equiv 3$, $f_4^{[1]}(k) \equiv 4$, $f_5^{[1]}(k) \equiv 0$, $f_6^{[1]}(k) \equiv 6$, $f_1(0) = 0$, $f_2(0) = 7$, $f_3(0) = 1$, $f_4(0) = 2$, $f_5(0) = 4$, $f_6(0) = 5$. Simulation results are shown in Figs. 3-7. Figs. 3-4 depict the trajectories of $x_c(k)$ and $u(k)$. Figs. 5-6 illustrate that the estimation error $\|e_i(k)\|_2$ of the designed observer approaches zero asymptotically and the bias/drift fault can be estimated. By denoting $s_{\max}(k) \triangleq \max_i \|s_i(k)\|_\infty$, we have Fig. 7 showing that the size of the encrypted data is indeed bounded. Therefore, this simulation example with offset faults has confirmed the theoretical results.

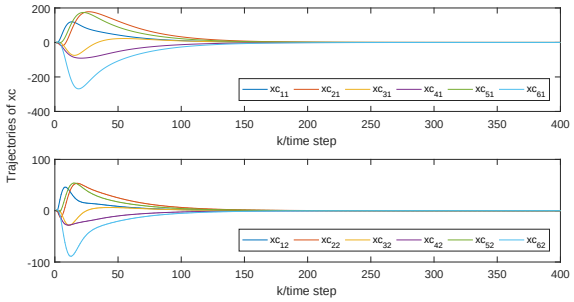

Fig. 3. Trajectories of $x_c(k)$.

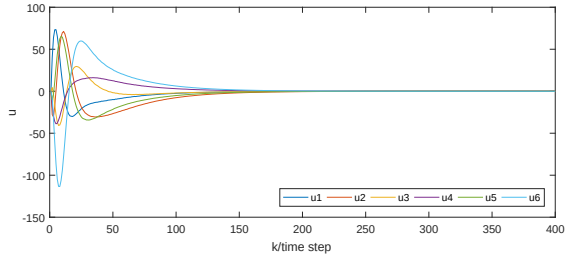

Fig. 4. Trajectories of the input variable $u_i(k)$.

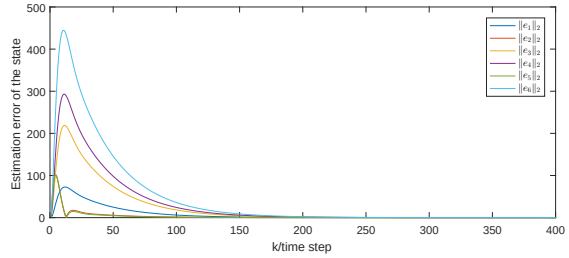

Fig. 5. State estimation errors $\|e_i(k)\|_2$.

V. Conclusion

In this paper, we make one of the first attempts to deal with the security issue of MASs (from the perspective of logical security and physical security) through developing a new cryptographic computation algorithm with system dynamics. Our focus is to discover the underlying fundamental properties by investigating linear systems, which can be extended to nonlinear systems. The main contributions include the design of the coding-decoding-based PDR algorithm and the design of the consensus controller under the directed topology. By employing and designing a decaying scale factor, the introduced PDR

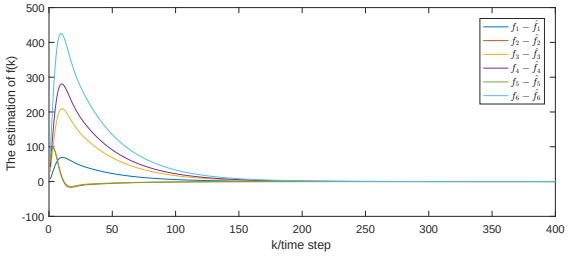

Fig. 6. Estimated fault $\hat{f}_i(k)$.

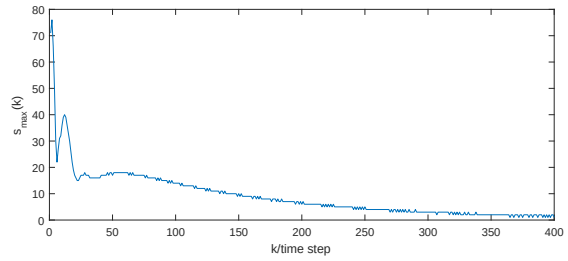

Fig. 7. Trajectory of $s_{\max}(k)$.

algorithm will not affect the steady-state performance of the system, i.e., the steady-state error will converge to zero. By introducing a novel matrix norm, the necessary and sufficient condition has been derived for the desired consensus. With the merits of enhancing the data security and facilitating the data compression, the proposed encryption-decryption scheme has potential applications in networked control systems [37], sensor networks [2], etc. As a future research topic, the encryption-decryption-based distributed estimation problem deserves further investigation especially in the presence of measurement noise or outliers [1].

References

[1] A. Alessandri and L. Zaccarian, Stubborn state observers for linear time-invariant systems, *Automatica*, vol. 88, pp. 1–9, 2018.
[2] X. Bai, Z. Wang, L. Sheng and Z. Wang, Reliable data fusion of hierarchical wireless sensor networks with asynchronous measurement for greenhouse monitoring, *IEEE Transactions on Control Systems Technology*, vol. 27, no. 3, pp. 1036–1046, 2019.
[3] V. Borkar and P. Varaiya, Asymptotic agreement in distributed estimation, *IEEE Transactions on Automatic Control*, vol. 27, no. 3, pp. 650–655, 1982.
[4] J. Chen and Q. Ling, Robust quantized consensus of discrete multi-agent systems in the input-to-state sense, *IEEE Access*, vol. 7, pp. 35699–35709, 2019.
[5] F. Cucker and S. Smale, Emergent behavior in flocks, *IEEE Transactions on Automatic Control*, vol. 52, no. 5, pp. 852–862, 2007.
[6] D. Ding, Z. Wang, B. Shen and G. Wei, Event-triggered consensus control for discrete-time stochastic multi-agent systems: The input-to-state stability in probability, *Automatica*, vol. 62, pp. 284–291, 2015.
[7] W. Dong, Consensus of high-order nonlinear continuous-time systems with uncertainty and limited communication data rate, *IEEE Transactions on Automatic Control*, vol. 64, no. 5, pp. 2100–2107, 2019.
[8] H. Du, W. Zhu, G. Wen, Z. Duan and J. Lü, Distributed formation control of multiple quadrotor aircraft based on nonsmooth consensus algorithms, *IEEE Transactions on Cybernetics*, vol. 49, no. 1, pp. 342–353, 2019.
[9] J. A. Fax and R. M. Murray, Graph laplacians and stabilization of vehicle formations, In: *Proc. 15th IFAC World Congress*, pp. 283–288, 2002.
[10] Z. Feng and G. Hu, Distributed secure average consensus for linear multi-agent systems under DoS attacks, In: *2017 American Control Conference*, pp. 2261–2266, 2017.
[11] C. Gao, Z. Wang, X. He and Q.-L. Han, Consensus control of linear multi-agent systems under actuator imperfection: When saturation meets fault, *IEEE Transactions on Systems, Man and Cybernetics: Systems*, 2021, early access, doi: 10.1109/TSMC.2021.3050370.

[12] L. Gao, X. Liao, H. Li and G. Chen, Event-triggered control for multi-agent network with limited digital communication, *Nonlinear Dynamics*, vol. 82, no. 4, pp. 1659–1669, 2015.

[13] M. Gao, S. Yang and L. Sheng, Distributed fault estimation for time-varying multi-agent systems with sensor faults and partially decoupled disturbances, *IEEE Access*, vol. 7, pp. 147905–147913, 2019.

[14] Z. Gao and H. Wang, Descriptor observer approaches for multivariable systems with measurement noises and application in fault detection and diagnosis, *Systems & Control Letters*, vol. 55, no. 4, pp. 304–313, 2006.

[15] S. Ghapani, J. Mei, W. Ren and Y. Song, Fully distributed flocking with a moving leader for Lagrange networks with parametric uncertainties, *Automatica*, vol. 67, pp. 67–76, 2016.

[16] Y. He and X. Mu, Cucker-Smale flocking subject to random failure on general digraphs, *Automatica*, vol. 106, pp. 54–60, 2019.

[17] S. Jadhav, A. Datar and H. Werner, Distributed approach to dynamic quantization for multi-agent systems, In: *Proc. 2018 Annual American Control Conference (ACC)*, pp. 2473–2478, 2018.

[18] M. Khalili, X. Zhang, M. A. Gilson and Y. Cao, Distributed fault-tolerant formation control of cooperative mobile robots, *IFAC-PapersOnLine*, vol. 51, no. 24, pp. 459–464, 2018.

[19] M. Khalili, X. Zhang, M. M. Polycarpou, T. Parisini and Y. Cao, Distributed adaptive fault-tolerant control of uncertain multi-agent systems, *Automatica*, vol. 87, pp. 142–151, 2018.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] Z. Li, W. Ren, X. Liu and L. Xie, Distributed consensus of linear multi-agent systems with adaptive dynamic protocols, *Automatica*, vol. 49, no. 7, pp. 1986–1995, 2013.

[25] 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.

[26] Q. Liu, Z. Wang, X. He and D. H. Zhou, Event-based distributed filtering over Markovian switching topologies, *IEEE Transactions on Automatic Control*, vol. 64, no. 4, pp. 1595–1602, 2019.

[27] Y. Lu and M. Zhu, A control-theoretic perspective on cyber-physical privacy: Where data privacy meets dynamic systems, *Annual Reviews in Control*, vol. 47, pp. 423–440, 2019.

[28] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig and B. Sinopoli, Cyber-physical security of a smart grid infrastructure, *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2011.

[29] 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.

[30] J. Thunberg, J. Goncalves and X. Hu, Consensus and formation control on $SE(3)$ for switching topologies, *Automatica*, vol. 66, pp. 109–121, 2016.

[31] J. Tsitsiklis, D. Bertsekas and M. Athans, Distributed asynchronous deterministic and stochastic gradient optimization algorithms, *IEEE Transactions on Automatic Control*, vol. 31, no. 9, pp. 803–812, 1986.

[32] 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*, pp. 1–11, 2018.

[33] 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.

[34] W. Wang, C. Wen, J. Huang and J. Zhou, Adaptive consensus of uncertain nonlinear systems with event triggered communication and intermittent actuator faults, *Automatica*, vol. 111, pp. 108667, 2020.

[35] Y. Wu and X. He, Secure consensus control for multi-agent systems with attacks and communication delays, *IEEE/CAA Journal of Automatica Sinica*, vol. 4, no. 1, pp. 136–142, 2017.

[36] 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.

[37] D. Zhao, Z. Wang, D. Ding and G. Wei, H_∞ PID control with fading measurements: The output-feedback case, *IEEE Transactions on Systems, Man, and Cybernetics-Systems*, vol. 50, no. 6, pp. 2170–2180, 2020.

[38] D. H. Zhou and P. M. Frank, Fault diagnostics and fault tolerant control, *IEEE Transactions on Aerospace and Electronic Systems*, vol. 34, no. 2, pp. 420–427, 1998.

[39] J.-W. Zhu, G.-H. Yang, W.-A. Zhang and L. Yu, Cooperative fault tolerant tracking control for multiagent systems: An intermediate estimator-based approach, *IEEE Transactions on Cybernetics*, vol. 48, no. 10, pp. 2972–2980, 2018.