Distributed Anti-Eavesdropping Fusion Estimation under Energy Constraints

Daxing Xu, Bo Chen, *Member, IEEE*, Yuchen Zhang, Li Yu, *Member, IEEE*

***Abstract*—This paper studies the distributed fusion estimation problem with energy-constrained sensors in the presence of eavesdroppers, where smart sensors send their local estimates to a remote fusion center (FC). To enhance privacy level, a novel encryption strategy is proposed by establishing an optimization problem, where the optimization objective is constructed by maximizing a combination of the fusion terminal estimation error covariance and the cost of encryption process in finite time domain. Meanwhile, the established problem is decomposed into several independent sub-optimization problems under a relaxation condition, and a sufficient condition that depends on the system parameters is derived such that the sub-optimization problems have optimal solutions. In this case, an optimal encryption strategy is designed with an analytical solution. Finally, a simulation example is given to show the effectiveness of the proposed methods.**

***Index Terms*—Secure fusion estimation; Eavesdropping; Privacy protection; Power allocation; Networked multi-sensor fusion systems.**

I. Introduction

Since networked multi-sensor fusion systems (NMFSs) have the advantages of simpler installation, easier maintenance and lower cost, a wide range of applications of NMFSs have been found in cyber-physical systems and networked target tracking [1], [2]. Real-time state estimation based on sensor measurements is one of the important issues in NMFSs. It has been shown that state estimation can improve the estimation accuracy while increasing reliability and robustness [3], [4]. However, due to the distributed structure of NMFSs and its openness to network, it is vulnerable to various malicious attacks. Typical attacks include denial-of-service (DoS) attacks [5], [6], false data injection (FDI) attacks [7], [8], and eavesdropping attacks [9], etc. For the eavesdropping attacks, an adversary can unconsciously monitor the packets transmitted on the channel. The leakage of key information, such as the destination of military aircraft, important privacy of customers, etc., will lead to severe consequences. At the same time, the sensors are often powered by batteries, which will cause another crucial issue on sensor energy limitation [10], [11]. Therefore, it is of great significance to study the anti-eavesdropping problem in fusion estimation under sensor energy constraints.

Generally, there are two basic fusion estimation structures in the existing literatures, namely, centralized fusion and distributed fusion [12]. Compared with the former, the latter has better reliability, robustness and system feasibility [1], [8], [12]. Therefore, this paper will pay more attention to security issue under distributed fusion. In recent years, to defend the DoS and FDI attacks in NMFSs, some works have been done in secure fusion estimation [6], [8], [13]–[18]. Particularly, a suboptimal secure dimensionality reduction fusion method was proposed against DoS attacks, while an effective attack strategy was designed for the attacker [6]. A recursive distributed Kalman fusion estimator was proposed in [8] by constructing a compensation strategy. However, these works were based on the premise that the attacker could obtain system information through eavesdropping attacks in advance, and then launched a strategic attack. Most of these works focused on how to reduce the damage of the attack to ensure the performance of fusion estimation, which was a passive defense method. In this case, active defense methods are of great significance to prevent system privacy data from being eavesdropped at the source and improve the security of NMFSs.

Notice that, defending against eavesdropping attacks in NMFSs means protecting the privacy of the transmitted system state data. Some works about the encryption of a message against eavesdroppers have been presented in privacy preserving [19]–[29]. From the perspective of sensor data scheduling, an optimal transmission scheduling against eavesdroppers was proposed in [19] to obtain the perfect secrecy, where the user's expected error remained bounded while the eavesdropper's expected error grew unbounded. Meanwhile, similar results were derived in [20] with feedback by minimizing the expected error covariance. Then, an event-triggered scheduling strategy and optimal transmission policy were provided to resist eavesdropper in [21], [22]. Moreover, state-secrecy coding scheme was introduced in [23]–[25] to achieve perfect secrecy by exploiting the system dynamics, physical model and the properties of process noises. Particularly, an optimal encryption schedule in presence of an eavesdropper with operation cost was proposed in [26], [27] to enhance the system privacy level. Recently, the distributed secure fusion estimation problem against eavesdroppers was discussed in [28] for perfect secrecy. Under the limited communication bandwidth, an insertion method of artificial noise (AN) based on the physical processes and local estimation error covariance was developed in [29] such that only eavesdropper's fusion error covariance became worse. However, all of these works have not considered the constraints of sensor energy that are unavoidable. Notice that the security of system state data increases as the sensor energy consumption increases [29]. In this case, the energy constraints of sensors become one important issue when designing the confidentiality method against eavesdroppers.

Motivated by the above-analysis, we shall study the distributed secure fusion estimation problem against eaves-

This work was supported by the National Natural Science Foundation of China under Grant 61973277 and Grant 62073292, and in part by the Zhejiang Provincial Natural Science Foundation of China under Grant LR20F030004. This paper was recommended by Associate Editor XX. (Corresponding author: Bo Chen)

D. Xu is with the Department of Automation, Zhejiang University of Technology, Hangzhou 310023, China and also with the College of Electrical and Information Engineering, Quzhou University, Quzhou 324000, China (daxingxu@163.com).

B. Chen, Y. Zhang and L. Yu are with the Department of Automation, Zhejiang University of Technology, Hangzhou 310023, China and also with the Zhejiang Provincial United Key Laboratory of Embedded Systems, Hangzhou 310023, China (bchen@aliyun.com, YuchenZhang95@163.com, lyu@zjut.edu.cn).

droppers under sensor energy constraints. To protect the state privacy, we need to impair the eavesdropper's fusion estimation performance. To achieve this goal, the transmitted data is encrypted with AN, where AN is the zero-mean Gaussian white noise generated by the sensor. Particularly, the variance of AN represents the noise energy, which is also the power consumed when the sensor generates AN. However, limited sensor energy is a natural constraint for each local sensor, and the sensor cannot always encrypt data every moment or encrypt with large AN energy. Under this case, each sensor needs to decide "when to encrypt the transmitted data" and "how much AN energy should be encrypted" to make the eavesdropper's fusion estimation performance be the worst. This is the main objective of this paper, and the contributions are summarized as follows: i) An energy optimization problem for privacy protection is formulated over a finite-time horizon, which is proved to be transformed into unrelated sub-optimization problems for each sensor under a relaxation condition; ii) A sufficient condition that depends on the system parameters is derived such that the sub-problems have optimal solutions. Then, an efficient encryption strategy with optimal encryption level and encryption sequence is obtained by solving the transformed sub-optimization problems.

Notations: The maximum eigenvalue of the matrix A is denoted by $\lambda_{\max}\{A\}$. The identity matrix with dimension n is represented by "I_n ". $\mathrm{diag}\{\cdot\}$ stands for the block diagonal matrix, while "$\mathrm{Tr}\{\cdot\}$ " represents the trace operator. $\lfloor\cdot\rfloor$ stands for floor operation. $\mathrm{E}\{\cdot\}$ denotes the mathematical expectation, and $\|\cdot\|$ stands for matrix norm. $\mathbb{C}$ represents complex number, and $\dagger$ denotes Hermitian transpose.

II. System Model and Preliminaries

Consider discrete-time systems with the following state-space model:

$$x(t+1) = Ax(t) + w(t)\ , \tag{1}$$

$$y_i(t) = C_i x(t) + v_i(t) \quad (i = 1, 2, ..., L)\ , \tag{2}$$

where $x(t) \in R^n$ is the system state in Fig.1, $y_i(t) \in R^{q_i}$ is the measurement of the ith sensor, and L is the number of sensors. $w(t)$ and $v_i(t)$ are mutually uncorrelated Gaussian white noises with zero mean and variances Q and R_i, respectively. A and C_i are constant matrices. It is assumed that the pair (C_i, A) is detectable and $(A, Q^{1/2})$ is controllable.

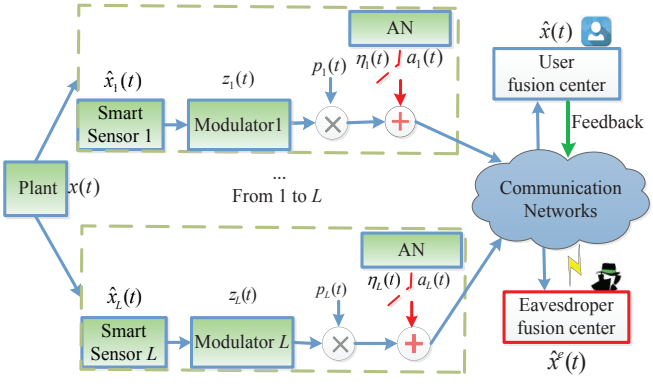

Fig. 1. Distributed fusion estimation with injected AN

The ith smart sensor in Fig.1, which has computation capability [30], collects the measurement $y_i(t)$ at time t. Then, each local estimate at the sensor is given by the Kalman filter [31]:

$$\begin{cases} \hat{x}_i^-(t) = A\hat{x}_i(t-1),\ P_i^-(t) = AP_i(t-1)A^{\mathrm{T}} + Q \\ K_i(t) = P_i^-(t)C_i{}^{\mathrm{T}}(C_iP_i^-(t)C_i^{\mathrm{T}} + R_i)^{-1} \\ \hat{x}_i(t) = \hat{x}_i^-(t) + K_i(t)(y_i(t) - C_i\hat{x}_i^-(t)) \\ P_i(t) = [I_n - K_i(t)C_i]P_i^-(t) \end{cases} \tag{3}$$

where $\hat{x}_i^-(t)$ and $\hat{x}_i(t)$ are the *apriori* and the *aposteriori* minimum mean square error estimates of the state $x(t)$ at time t, while $P_i^-(t)$ and $P_i(t)$ are the corresponding estimation error covariance matrices. Moreover, it follows from (3) that the estimation error cross-covariance matrix between the ith and the jth local estimates, which is denoted by $P_{ij}(t)$ ($i \neq j$), is computed by [12]:

$$\begin{aligned} P_{ij}(t) = [I_n - K_i(t)C_i][AP_{ij}(t-1)A^{\mathrm{T}} + Q] \\ \times[I_n - K_j(t)C_j]^{\mathrm{T}} \end{aligned} \tag{4}$$

At the sensor side, since the observation of sensor can be guaranteed in real time, $P_{ii}(t)$ and $P_{ij}(t)$ converge exponentially to steady-state values $\bar{P}_{ii}$ and $\bar{P}_{ij}$ with few steps [32]–[34]. Thus, we set the initial estimation error covariances as $P_{ii}(0) = \bar{P}_{ii}$, and $P_{ij}(0) = \bar{P}_{ij}$, then it can be concluded that $P_{ii}(t) = \bar{P}_{ii}$ and $P_{ij}(t) = \bar{P}_{ij}$ as t goes to ∞. Define $h(X) \triangleq AXA^{\mathrm{T}} + Q$, $h^k(X) \triangleq \underbrace{h \circ \cdots \circ h}_{k \text{ times}}(X)$, and $\mathrm{H}^k(X) \triangleq h^k(X) - h^{k-1}(X)$. It is concluded from [35], [36] that, if $k_1 \leq k_2, k_1, k_2 \in Z^+$, then $\bar{P}_{ii} < h^{k_1}(\bar{P}_{ii}) \leq h^{k_2}(\bar{P}_{ii})$.

A. Encryption Method with Artificial Noise

To prevent the transmitted information from being eavesdropped, encryption method based on AN is introduced. Particularly, before the local estimate $\hat{x}_i(t)$ is sent, a known mapping $\mathcal{F}_i(\hat{x}_i(t))$ is applied to generate a one-dimensional complex signal $z_i(t) \in \mathbb{C}$, which depends on the modulation scheme. We assume that the signal $z_i(t)$ is transmitted by multiple-input single-output communication with N_T transmission antennas. Then the channel gain matrix from the ith smart sensor to the FC for the user is $H_i^u(t) \in \mathbb{C}^{1\times N_T}$. Furthermore, considering the injected AN, the transmitted signal has the following form [37]:

$$\bar{z}_i(t) = p_i(t)z_i(t) + a_i(t) \tag{5}$$

where $p_i(t) \in \mathbb{C}^{N_T\times 1}$ is a zero-mean Gaussian random vector, which is satisfied with $\mathrm{E}\{p_i(t)p_i^{\dagger}(t)\} = I_{N_T}$. $a_i(t) \in \mathbb{C}^{N_T\times 1}$ is the AN vector.

B. Distributed Fusion Estimation

At the FC side, the FC tries to decode the signals received from the local sensors to get the local estimates. In this case, the distributed matrix-weighted fusion filter $\hat{x}(t)$ at the FC is given by

$$\hat{x}(t) = \sum\nolimits_{i=1}^{L} W_i(t)\hat{x}_i(t) \tag{6}$$

where $\sum_{i=1}^{L} W_i(t) = I_n$.

Then, define $\sum(t) \triangleq \begin{bmatrix} P_{11}(t) \dots P_{1L}(t) \\ \vdots \quad\quad \vdots \\ P_{L1}(t) \dots P_{LL}(t) \end{bmatrix}$. Under the linear minimum variance criterion, according to the result in [12], the optimal weighting matrices $W_1(t)$, $W_2(t)$,...,$W_L(t)$ in (6) can be calculated by:

$$[W_1(t), \dots, W_L(t)] = (I_a^{\mathrm{T}}\Sigma^{-1}(t)I_a)^{-1}I_a^{\mathrm{T}}\Sigma^{-1}(t) \tag{7}$$

where $I_a = [I_n, I_n, \ldots, I_n]^{\mathrm{T}} \in R^{nL\times n}$. Then, the fusion estimation error covariance matrix $P(t) \triangleq \mathrm{E}\{(x(t)-\hat{x}(t))(x(t)-\hat{x}(t))^{\mathrm{T}}\}$ is given by

$$P(t) = (I_a^{\mathrm{T}}\Sigma^{-1}(t)I_a)^{-1} \tag{8}$$

For the eavesdropper, according to (6)-(8), define $\Sigma^e(t) \triangleq \begin{bmatrix} P^e_{11}(t)\ldots P^e_{1L}(t) \\ \vdots \quad\quad \vdots \\ P^e_{L1}(t)\ldots P^e_{LL}(t) \end{bmatrix}$ and the eavesdropper's estimation error covariance matrix $P^e(t) = (I_a^{\mathrm{T}}(\Sigma^e(t))^{-1}I_a)^{-1}$.

III. Problem Formulations

First, let the orthogonal basis for the null space of $H_i^u(t)$ be denoted by $\Phi_i(t) \in \mathbb{C}^{N_T\times(N_T-1)}$, which satisfies $\Phi_i^{\mathrm{T}}(t)\Phi_i(t) = I_{N_T-1}$. Then the AN vector $a_i(t)$ is chosen from the null space of $H_i^u(t)$. This means that $H_i^u(t)a_i(t) = 0$. In this case, the AN is proposed to be given by

$$a_i(t) = \Phi_i(t)\varsigma_i(t) \tag{9}$$

where $\varsigma_i(t) \in \mathbb{C}^{(N_T-1)\times 1}$ is zero-mean Gaussian white noise with variance $\mathrm{E}\{\varsigma_i(t)\varsigma_i^{\dagger}(t)\} = \sigma_i I_{N_T-1}$. Notice that the quantity σ_i is designed at the FC and fed back to the ith sensor. At the same time, let $H_i^e(t)$ be the channel gain matrix of eavesdropper from the ith sensor to the FC of eavesdropper. Then, the signal received from the ith sensor by the user $s_i^u(t)$ and eavesdropper $s_i^e(t)$ at the FC can be described as follows:

$$\begin{cases} s_i^u(t) = H_i^u(t)(p_i(t)z_i(t) + a_i(t)) \\ \quad\quad = H_i^u(t)p_i(t)z_i(t), \quad i = 1, 2, \ldots, L \\ s_i^e(t) = H_i^e(t)p_i(t)z_i(t) + H_i^e(t)a_i(t) \end{cases} \tag{10}$$

Remark 1. To conveniently show the effect of the designed AN on the performance of fusion estimation, we assume that the channels are ideal, and they do not contain channel noise. The user can obtain the channel gain $H_i^u(t)$ by using channel estimation algorithms with blind estimation, pilot-based estimation and semi-blind estimation [38]. This kind of scheme is also used in [39]–[41]. Since the channel gain is affected by physical factors such as signal scattering, multipath fading and power decay of distance, the channel gains of user and eavesdroppers must be different (i.e., $H_i^u(t) \neq H_i^e(t)(\forall t)$) in practical systems.

According to [42], the probability of successful decoding primarily relies on the signal-to-noise ratio (SNR). When the ith sensor encrypts a message with the AN power σ_i, it sends a packet to the FC with the emission power δ_i. In this case, combining the fact $\Phi_i(t)\Phi_i^{\mathrm{T}}(t) = I_{N_T}$, the SNR of the eavesdroppers are defined by

$$\varepsilon_i^e(t) = \frac{\delta_i \mathrm{E}\{|H_i^e(t)p_i(t)|^2\}}{\mathrm{E}\{|H_i^e(t)a_i(t)|^2\}} = \frac{\delta_i}{\sigma_i} \tag{11}$$

Notice that the successful decoding probability of the received signal is related to the SNR $\varepsilon_i(t)$, and the decoding probability has the following form [42]:

$$p\{\theta_i(t) = 1|\varepsilon_i(t)\} = f(\varepsilon_i(t)) = [1 - \xi(\sqrt{2\varepsilon_i(t)})]^m \tag{12}$$

where $\xi(x) = \int_x^{\infty} \frac{1}{\sqrt{2\pi}} \exp(-\frac{t^2}{2})dt$, and m is the transmitted data packet length and assumes that the transmission error is of bit-to-bit independent. $\theta_i(t)$ is a binary variable that denotes whether the received data is successfully decoded or not. Then, we can get $\theta_i(t) = 1$ only when every bit is received correctly.

Next, we analyze the fusion estimation performance of user when AN is injected into the transmitted signal. According to (10) and (11), since the received signal for the FC of user does not contain any noise, the SNR of the received data is infinite. Then combined with (12), we have the successful decoding probability with 1 at all moments, which means that we can successfully decode the received signal to obtain $z_i(t)$. Furthermore, according to the known mapping $\mathcal{F}_i(\hat{x}_i(t))$, it is concluded that the local estimates can be successfully decoded with probability 1 for the user at each time, thus the fusion estimation performance has no loss under the injected AN.

However, for the FC of eavesdropper, the successful decoding probability of the local estimates depends on the energy of the injected AN. It should be noted that if the FC fails to decode the local estimate signal, it needs to perform a prediction compensation on the local estimate. In this case, the final local estimate $\hat{x}_i^e(t)$ and the corresponding error covariance $P_{ii}^e(t)$ can be computed as

$$(\hat{x}_i^e(t), P_{ii}^e(t)) = \begin{cases} (\hat{x}_i(t), \bar{P}_{ii}), & \text{if } \theta_i(t) = 1 \\ (A\hat{x}_i^e(t-1), h(P_{ii}^e(t-1))), & \text{Otherwise} \end{cases} \tag{13}$$

Then, the final fusion estimate $\hat{x}^e(t)$ and error covariance $P^e(t)$ of the eavesdropper can be similarly calculated by (6)-(8).

To protect state privacy, we need to impair the eavesdropper's fusion estimation performance to the greatest extent. Therefore, we design encryption strategies for local sensors to maximize the trace of the eavesdropper's fusion estimation error covariance. Notice that the AN can decrease the decoding success probability of adversary, the sensors under energy constraints should decide when to encrypt the transmitted sensor data and how much power should be injected on AN at each encryption instant. In this case, we introduce the following binary variable to model the encryption decision process: $\eta_i(t) = \begin{cases} 1 & \text{The } i\text{th sensor encrypts data } z_i(t) \\ 0 & \text{Otherwise} \end{cases}$.

Furthermore, it has been pointed out in [26], [27] that the encrypted transmission needs more storage, computation and energy resource, and thus the influence of the encryption cost is also considered in this paper. Let c_i be the normalized total encryption process cost of the ith sensor, and let σ_i be the energy required for one encryption. Denote the energy budget of the ith sensor as P_i^{δ}. Then, considering finite-time horizon N, the aim is to maximize the integrated cost J_N, which is a linear combination of the terminal error covariance $P^e(N)$ at the eavesdropper and the operation cost of the encryption process. Thus, the problem of interest can be formulated as the following finite horizon maximization problem:

$$\begin{cases} \max\limits_{\eta_i(t),\sigma_i} \begin{cases} \mathrm{J}_N \triangleq \mathrm{Tr}\{\alpha \mathrm{E}\{P^{\mathrm{e}}(N)\}\} \\ \quad -(1-\alpha)\sum_{i=1}^{L}\sum_{t=1}^{N}\eta_i(t)c_i \end{cases} \\ \text{s.t.} \begin{cases} \sum_{t=1}^{N}\eta_i(t)\sigma_i \leq P_i^{\delta} \\ \underline{\sigma}_i \leq \sigma_i \leq \bar{\sigma}_i \ (i = 1, 2, ..., L) \end{cases} \end{cases} \tag{14}$$

where $\alpha \in (0, 1)$ is the weighting factor to depict the importance between the eavesdroppers' terminal error covariance and the cost of encryption, a larger α means that minimizing the information leakage is more important than the cost of encryption. Here, $\underline{\sigma}_i$ and $\bar{\sigma}_i$ are the lower bound and upper bound of AN power.

Remark 2. Given the limited local sensors power budget P_i^{δ}, the user should solve the problem (14) to determine

at which time (i.e., $\eta_i(t)$) the encryption operation needs to be implemented and how much encryption power about AN energy σ_i to use. Under this encryption strategy, the eavesdropper's fusion performance will be the worst. Notice that the user focuses on the terminal estimation performance of the eavesdroppers, which is an important index to measure the quality of the state estimation [2], [5], [43].

IV. Main Results

Notice that the fusion estimation error covariance in (14) is coupled with each local estimation error covariance. The solution of the problem (14) needs to use system global information. Then, it requires the method of multiple exhaustion search to numerically solve the problem (14), which is unrealistic for real-time state estimation. In this case, we will transform the problem (14) into a sub-optimization problem, which can be decomposed into L sub-problems in Subsection *A*, and then an optimal encryption strategy is proposed for the L local sensors under a sufficient condition in Subsection *B*. We have the following two necessary lemmas before giving the main results.

Lemma 1 [1]. For a given matrix $\Xi(\in R^{n\times n}) > 0$, the following inequality holds:

$$\frac{1}{n}\mathrm{Tr}\{\Xi\} \le \|\Xi\|_2 \le \mathrm{Tr}\{\Xi\} \tag{15}$$

Lemma 2. Assume the data packet without encryption is delivered to the eavesdropper's FC successfully at time t_0 for the ith sensor, and the data encryption is performed from time t_0+1 to t_0+M. Then the distribution of the terminal error covariance matrix $P^e_{ii}(N)$ can be computed as

$$p\{P^e_{ii}(N) = h^j(\bar{P}_{ii})\} = \begin{cases} (\gamma_i)^j(1-\gamma_i), & j = 0, ..., M-1; \\ (\gamma_i)^M, & j = M. \end{cases} \tag{16}$$

where, γ_i is decoding failure probability when AN energy σ_i is injected.

Proof: The matrix space of the error covariance matrix $P^e_{ii}(t)$ in time $[t_0+1, t_0+M]$ is $\{\bar{P}_{ii}, h(\bar{P}_{ii}), \ldots, h^M(\bar{P}_{ii})\}$. Then it could be found that the process of the error covariance matrix $P^e_{ii}(t)$ during the consecutive encryption period is a stationary Markov chain, and the transition probability matrix is given by

$$\begin{aligned} &p\{P^e_{ii}(t) = h^j(\bar{P}_{ii}) | P^e_{ii}(t-1) = h^i(\bar{P}_{ii})\} \\ &= \begin{cases} \gamma_i, & j = i+1, \\ 1-\gamma_i, & j = 0, \\ 0, & \text{Others} \end{cases} \qquad i, j = 0, 1, 2, \ldots, M. \end{aligned} \tag{17}$$

Combining (17), we can get the result of (16). This completes the proof.

A. Sub-optimization problem

Let us define

$$\Gamma(\Sigma^e(N)) \triangleq (I_a^{\mathrm{T}}(\Sigma^e(N))^{-1}I_a) \tag{18}$$

Taking the partial derivative operation on $\Gamma(\Sigma^e(N))$ to $\mathrm{Tr}\{\Gamma^{-1}(\Sigma^e(N))\}$, we can get

$$\frac{\partial \mathrm{Tr}\{\Gamma^{-1}(\Sigma^e(N))\}}{\partial \Gamma(\Sigma^e(N))} = -\Gamma^{-2}(\Sigma^e(N)) < 0 \tag{19}$$

Therefore, $\mathrm{Tr}\{\Gamma^{-1}(\Sigma^e(N))\}$ is monotonically decreasing with $\Gamma(\Sigma^e(N))$. Then we have the following equivalence relation:

$$\begin{aligned} \max \mathrm{Tr}\{P^e(N)\} &= \max \mathrm{Tr}\{\Gamma^{-1}(\Sigma^e(N))\} \\ &\Leftrightarrow \min \|\Gamma(\Sigma^e(N))\|_2 \end{aligned} \tag{20}$$

By taking the partial derivative operation on $\Sigma^e(N)$ to $\mathrm{Tr}\{\Gamma(\Sigma^e(N))\}$, one has

$$\frac{\partial \mathrm{Tr}\{\Gamma(\Sigma^e(N))\}}{\partial \Sigma^e(N)} = -((\Sigma^e(N)^{-1}I_a))((\Sigma^e(N))^{-1}I_a)^{\mathrm{T}} \le 0 \tag{21}$$

Then, it is concluded from (21) that $\mathrm{Tr}\{\Gamma(\Sigma^e(N))\}$ is monotonically decreasing with $\Sigma^e(N)$. Thus we have another equivalence relation as follows:

$$\min \mathrm{Tr}\{\Gamma(\Sigma^e(N))\} \Leftrightarrow \max \|\Sigma^e(N)\|_2 \tag{22}$$

Under the relaxation condition (15) in Lemma 1 and the definition of $\Sigma^e(N)$, combing the results of (20) and (22), the optimization objective function of problem (14) can be reduced to the following form:

$$\begin{aligned} \max_{\eta_i(t),\sigma_i} \mathrm{J_S} &\triangleq \mathrm{Tr}\{\alpha \mathrm{E}\{\Sigma^e(N)\}\} - (1-\alpha) \\ &\quad \times \textstyle\sum_{i=1}^{L}\sum_{t=1}^{N}\eta_i(t)c_i \\ &\triangleq \textstyle\sum_{i=1}^{L}\mathrm{Tr}\{\alpha \mathrm{E}\{P^e_{ii}(N)\}\} - (1-\alpha) \\ &\quad \times \textstyle\sum_{i=1}^{L}\sum_{t=1}^{N}\eta_i(t)c_i \end{aligned} \tag{23}$$

Moreover, the maximization problem (23) can be transformed into the following sub-optimization problem:

$$\begin{cases} \max\limits_{\eta_i(t),\sigma_i} \begin{cases} \mathrm{J_S} \triangleq \sum_{i=1}^{L}\mathrm{Tr}\{\alpha \mathrm{E}\{P^e_{ii}(N)\}\} \\ \qquad -(1-\alpha)\sum_{i=1}^{L}\sum_{t=1}^{N}\eta_i(t)c_i \end{cases} \\ \text{s.t.} \begin{cases} \sum_{t=1}^{N}\eta_i(t)\sigma_i \le P_i^{\delta}, \\ \underline{\sigma}_i \le \sigma_i \le \bar{\sigma}_i, \ i = 1, 2, \ldots, L \end{cases} \end{cases} \tag{24}$$

Notice that the solution of optimization problem (24) is not the optimal solution of the optimization problem (14), but a set of suboptimal solutions. Denote $\mathrm{J}^i_{\mathrm{S}} \triangleq \mathrm{Tr}\{\alpha \mathrm{E}\{P^e_{ii}(N)\}\} - (1-\alpha)\sum_{t=1}^{N}\eta_i(t)c_i$, it is concluded from (24) that $\mathrm{J}^i_{\mathrm{S}}(i = 1, 2, \ldots, L)$ are mutually independent under the above constraint conditions. Thus, the sub-optimization problem (24) can be decomposed into the following L sub-problems:

$$\begin{aligned} &\max_{\eta_i(t),\sigma_i} \mathrm{J}^i_{\mathrm{S}} \\ &\text{s.t.} \begin{cases} \sum_{t=1}^{N}\eta_i(t)\sigma_i \le P_i^{\delta}, \\ \underline{\sigma}_i \le \sigma_i \le \bar{\sigma}_i, i \in \{1, 2, \ldots, L\}. \end{cases} \end{aligned} \tag{25}$$

Remark 3. Notice that the suboptimal solution of the maximization problem (14) in fusion estimation can be obtained by solving the sub-optimization problems (25) at each local sensor separately. That is to say, the solution to anti-eavesdropping problem of distributed fusion systems can be a suboptimal encryption scheme by solving L local subsystem problems independently. During this process, there is no matrix inversion operation in solving the sub-optimization problems (25), and thus the complexity of solving the optimization problem is greatly reduced.

B. Optimal Encryption Strategy on AN

It is concluded from the maximization problem (14) and sub-problems (25) that the multiple exhaustion search has been reduced to a single exhaustion search to find the solution. To further ensure the real-time performance of the addressed systems, an optimal solution to sub-problems (25) will be presented under a sufficient condition in this subsection.

According to the relationship between the decoding failure probability and SNR as shown in (11)-(12), different levels of AN energy σ_i can lead to different decoding failure probability γ_i with the same number of encryptions on finite-time horizon N. Therefore, there may exist multiple

This article has been accepted for publication in IEEE Transactions on Automatic Control. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAC.2023.3250094

decoding failure probabilities for guaranteeing n_i times encryption. To clearly describe the above relationship, we introduce the set of the decoding failure probability as $\Omega_{n_i} = \{\gamma_i \,|\, \lfloor P_i^\delta/\sigma_i(\gamma_i)\rfloor = n_i\}$ which is corresponding to n_i times encryption, where $\sigma_i(\gamma_i)$ is the AN energy based on decoding failure probability γ_i. Let $n_i^{\max}$ and $n_i^{\min}$ be the upper and lower bounds of the encryption times, respectively. σ_i^d denotes the desired optimal encryption energy, that is computed by $\sigma_i^d = \arg\max\{\sigma_i \,|\, \lfloor P_i^\delta/\sigma_i\rfloor = n_i^{\max}\}$. Then, we have the following theorem.

Theorem 1. For the systems (1)-(2), there is an optimal encryption strategy for the ith local subsystem of (25), if all the eigenvalues λ of matrix AA^T are not less than 1, and the variables related to the initial system parameters satisfy:

$$\alpha(\sum_{j=1}^{n_i^{\max}}((\bar{\gamma}_i)^j-(\underline{\gamma}_i)^j)\bar{\omega}_i-\underline{\gamma}_i^{n_i^{\max}+1}\underline{\omega}_i)+(1-\alpha)c_i\leqslant 0 \tag{26}$$

where $\bar{\gamma}_i$ and $\underline{\gamma}_i$ are the upper bound and lower bound of the decoding failure probabilities that are corresponding to the lower bound and upper bound of AN energy, respectively, while $\bar{\omega}_i = \mathrm{H}^{n_i^{\max}}(\bar{P}_{ii})$ and $\underline{\omega}_i = \mathrm{H}^{n_i^{\min}+1}(\bar{P}_{ii})$ can be determined by known local system parameters. Furthermore, the optimal encryption level is

$$\sigma_i^* = \min\{\sigma_i^d, \bar{\sigma}_i\} \tag{27}$$

and the optimal encryption sequence for the ith sensor is to continuously encrypt the transmitted data at the last $n_i^{\max}$ moments, i.e.,

$$\eta_i^* = (0,0,\ldots,\underbrace{1,1,\ldots,1}_{n_i^{\max}\text{ times}}) \tag{28}$$

where 1 and 0 represent whether the local estimate is encrypted or not.

Proof: We firstly consider that the number of encryption times n_i is fixed for each sensor on finite-time horizon N. And the encryption sequence of the ith sensor is represented by $\eta_i = (\eta_i(1), \eta_i(2), \ldots, \eta_i(N))$. In this case, the objective function of the ith local subsystem is rewritten as:

$$\mathrm{J}_{\mathrm{S}}^i \triangleq \mathrm{Tr}\{\alpha\mathrm{E}\{P_{ii}^e(N)\}\} - (1-\alpha)n_ic_i \tag{29}$$

where $n_i = \sum_{t=1}^N \eta_i(t)$. Since c_i is a specified constant, maximizing $\mathrm{J}_{\mathrm{S}}^i$ is equivalent to maximizing $\mathrm{Tr}\{\mathrm{E}\{P_{ii}^e(N)\}\}$ for the fixed n_i, which can be divided into the following consecutive encryption sequences:

$$\eta_i = (\underbrace{1,1,\ldots,1}_{n_i^1\text{ times}},0\ldots0,\underbrace{1,1,\ldots,1}_{n_i^j\text{ times}},0\ldots0,\underbrace{1,1,\ldots,1}_{n_i^\tau\text{ times}}) \tag{30}$$

where $\sum_{j=1}^\tau n_i^j = n_i$. According to (30), the local estimate is not encrypted at the time $N-n_i^\tau$, and the data encryption is performed at the last n_i^τ moments. Then, it is concluded from (13) that the eavesdropper can obtain the data $\hat{x}_i^e(N-n_i^\tau)$ with error covariance $\bar{P}_{ii}$, which is the initial value. Therefore, the terminal error covariance is only related to last n_i^τ consecutive encryptions. It means that the previous continuous encryption sequences $n_i^1, n_i^2, \ldots, n_i^{\tau-1}$ have no effect on the eavesdropper's terminal estimation performance. Under this case, grouping the encryptions together leads to maximal degrading effect. Thus, the optimal encryption sequence with fixed encryption times can be given as:

$$\eta_{n_i}^* = (0,0,\ldots,\underbrace{1,1,\ldots,1}_{n_i\text{ times}}) \tag{31}$$

Under the encryption sequence (31), the matrix space of the error covariance matrix $P_{ii}^e(t)$ from time $N-n_i+1$ to N is $\{\bar{P}_{ii}, h(\bar{P}_{ii}), \ldots, h^{n_i}(\bar{P}_{ii})\}$. Then, combining the Lemma 2, we can compute the expected terminal estimation error covariance as

$$\begin{aligned}\mathrm{E}\{P_{ii}^e(N)\} = &\textstyle\sum_{j=0}^{n_i-1}((\gamma_i)^j-(\gamma_i)^{j+1})h^j(\bar{P}_{ii})\\ &+(\gamma_i)^{n_i}h^{n_i}(\bar{P}_{ii})\end{aligned} \tag{32}$$

Then, it follows from (29)-(32) that the maximum value of the objective function $\mathrm{J}_{\mathrm{S}}^i$ is taken as:

$$\begin{aligned}(\mathrm{J}_{\mathrm{S}}^i)_{\max} = \alpha\mathrm{Tr}\{&\textstyle\sum_{j=0}^{n_i-1}((\gamma_i)^j-(\gamma_i)^{j+1})h^j(\bar{P}_{ii})\\ &+(\gamma_i)^{n_i}h^{n_i}(\bar{P}_{ii})\}-(1-\alpha)n_ic_i\end{aligned} \tag{33}$$

From the definition of $\mathrm{H}^k(X)$, the first term of maximum objective function value $(\mathrm{J}_{\mathrm{S}}^i)_{\max}$ in (33) is rewritten as:

$$\begin{aligned}&\alpha\mathrm{Tr}\{\textstyle\sum_{j=0}^{n_i-1}((\gamma_i)^j-(\gamma_i)^{j+1})h^j(\bar{P}_{ii})+(\gamma_i)^{n_i}h^{n_i}(\bar{P}_{ii})\}\\ &=\alpha\mathrm{Tr}\{\textstyle\sum_{j=1}^{n_i-1}((\gamma_i)^j-(\gamma_i)^{j+1})h^j(\bar{P}_{ii})+(\gamma_i)^{n_i}h^{n_i}(\bar{P}_{ii})\\ &\quad+(1-\gamma_i)\bar{P}_{ii}\}\\ &=\alpha\mathrm{Tr}\{\sum_{j=1}^{n_i}(\gamma_i)^j(h^j(\bar{P}_{ii})-h^{j-1}(\bar{P}_{ii}))+\bar{P}_{ii}\}\\ &=\alpha\mathrm{Tr}\{\sum_{j=1}^{n_i}(\gamma_i)^j\mathrm{H}^j(\bar{P}_{ii})+\bar{P}_{ii}\}\end{aligned} \tag{34}$$

Let $\gamma_{i,1}$ and $\gamma_{i,2}$ be the two different decoding failure probabilities, which correspond to the same number of encryptions n_i, i.e., $\gamma_{i,1},\gamma_{i,2}\in\Omega_{n_i}$, and $\gamma_{i,2}>\gamma_{i,1}$, then one has by (34) that

$$(\mathrm{J}_{\mathrm{S}}^i)_{\max}^1(\gamma_{i,2}) > (\mathrm{J}_{\mathrm{S}}^i)_{\max}^1(\gamma_{i,1}) \tag{35}$$

Hence, it is concluded from (33) and (35) that for a given number of encryptions, the larger the eavesdropper's decoding failure probability is, the larger the objective function value of local subsystem is. In other words, to reduce the eavesdropper's estimation performance, the sensor should inject as much AN as possible into the transmitted signal.

On the other hand, assume $\gamma_{i,1}\in\Omega_{n_i+1}$ and $\gamma_{i,2}\in\Omega_{n_i}$. Since the total energy encrypted by the ith sensor is fixed, one has $\gamma_{i,1}<\gamma_{i,2}$. Then, it follows from (33)-(34) that

$$\begin{aligned}&(\mathrm{J}_{\mathrm{S}}^i)_{\max}(\gamma_{i,2})-(\mathrm{J}_{\mathrm{S}}^i)_{\max}(\gamma_{i,1})\\ &=\alpha\mathrm{Tr}\{\textstyle\sum_{j=1}^{n_i}((\gamma_{i,2})^j-(\gamma_{i,1})^j)\mathrm{H}^j(\bar{P}_{ii})\\ &\quad-(\gamma_{i,1})^{n_i+1}\mathrm{H}^{n_i+1}(\bar{P}_{ii})\}+(1-\alpha)c_i\end{aligned} \tag{36}$$

Next, we show that the trace of $\mathrm{H}^k(X)$ is non-decreasing with k if all the eigenvalues λ of matrix AA^T are not less than 1. Let t_1 and t_2 be any positive integers, and satisfy $t_2=t_1+1$. From the definition of $h(X)$ and $h^k(X)$, it is obtained that

$$h^{t_1+1}(\bar{P}_{ii})-h^{t_1}(\bar{P}_{ii}) = A(h^{t_1}(\bar{P}_{ii})-h^{t_1-1}(\bar{P}_{ii}))A^{\mathrm{T}} \tag{37}$$

Then, exploiting the properties of matrix trace, yields that

$$\begin{aligned}&\mathrm{Tr}\{\mathrm{H}^{t_2}(\bar{P}_{ii})\}-\mathrm{Tr}\{\mathrm{H}^{t_1}(\bar{P}_{ii})\}\\ &=\mathrm{Tr}\{A^{\mathrm{T}}A(h^{t_1}(\bar{P}_{ii})-h^{t_1-1}(\bar{P}_{ii}))\}-\mathrm{Tr}\{h^{t_1}(\bar{P}_{ii})-h^{t_1-1}(\bar{P}_{ii})\}\\ &=\mathrm{Tr}\{(A^{\mathrm{T}}A-I)(h^{t_1}(\bar{P}_{ii})-h^{t_1-1}(\bar{P}_{ii}))\}\end{aligned} \tag{38}$$

Since all the eigenvalues λ of matrix AA^T are not less than 1, one has

$$\mathrm{Tr}\{(A^{\mathrm{T}}A-I)(h^{t_1}(\bar{P}_{ii})-h^{t_1-1}(\bar{P}_{ii}))\}\geqslant 0 \tag{39}$$

We can readily obtain that $\mathrm{Tr}\{\mathrm{H}^{t_2}(\bar{P}_{ii})\}\geqslant\mathrm{Tr}\{\mathrm{H}^{t_1}(\bar{P}_{ii})\}$. Further, it is obtained from (36) that

$$\begin{aligned}&(\mathrm{J}_{\mathrm{S}}^i)_{\max}(\gamma_{i,2})-(\mathrm{J}_{\mathrm{S}}^i)_{\max}(\gamma_{i,1})\\ &=\alpha(\textstyle\sum_{j=1}^{n_i}((\gamma_{i,2})^j-(\gamma_{i,1})^j)\mathrm{Tr}\{\mathrm{H}^j(\bar{P}_{ii})\}\\ &\quad-(\gamma_{i,1})^{n_i+1}\mathrm{Tr}\{\mathrm{H}^{n_i+1}(\bar{P}_{ii})\})+(1-\alpha)c_i\\ &\leqslant\alpha(\sum_{j=1}^{n_i}((\gamma_{i,2})^j-(\gamma_{i,1})^j)\mathrm{Tr}\{\mathrm{H}^{n_i^{\max}}(\bar{P}_{ii})\}\\ &\quad-(\gamma_{i,1})^{n_i+1}\mathrm{Tr}\{\mathrm{H}^{n_i^{\min}+1}(\bar{P}_{ii})\})+(1-\alpha)c_i\end{aligned} \tag{40}$$

Combining (26) and the fact $\underline{\gamma}_i < \gamma_{i,1} < \gamma_{i,2} < \bar{\gamma}_i$, one has

$$\begin{aligned}&(\mathrm{J}_{\mathrm{S}}^i)_{\max}(\gamma_{i,2}) - (\mathrm{J}_{\mathrm{S}}^i)_{\max}(\gamma_{i,1})\\ &\leqslant \alpha(\sum_{j=1}^{n_i^{\max}}((\bar{\gamma}_i)^j - (\underline{\gamma}_i)^j)\bar{\omega}_i - \underline{\gamma}_i^{n_i^{\max}+1}\underline{\omega}_i) + (1-\alpha)c_i\\ &\leqslant 0\end{aligned} \tag{41}$$

This means that when the conditions in Theorem 1 hold, the maximum value of the objective function is related to the number of encryptions. In particular, the more encryption time is, the larger the objective function value can be obtained. Under this case, since the maximum number of encryptions $n_i^{\max}$ can be computed by $n_i^{\max} = \lfloor P_i^\delta / \underline{\sigma}_i \rfloor$, it is derived from (11), (12), (35) and the restrictions of sub-problems (25) that the desired optimal encryption energy is taken as:

$$\sigma_i^d = \arg\ \max\{\sigma_i \,\big|\, \lfloor P_i^\delta/\sigma_i \rfloor = n_i^{\max}\} \tag{42}$$

However if σ_i^d exceeds the upper bound of the AN energy constraint $\bar{\sigma}_i$, then the optimal encryption level should be chosen as

$$\sigma_i^* = \min\left\{\sigma_i^d, \bar{\sigma}_i\right\}$$

Under the optimal number of encryptions $n_i^{\max}$, combining (31), one can obtain the optimal encryption sequence (28). This completes the proof.

Remark 4. The weight factor α plays an important role for the condition (26) to be satisfied. It can be concluded that the larger α is, the easier the sufficient condition is to be established. When the sufficient condition (26) and the eigenvalues λ of matrix AA^T are satisfied in Theorem 1, the user should adopt the largest power level among the power level set in which any power level leads to most encryption times, and consecutively encrypt the local estimates in the end of the considered time horizon to maximize the eavesdropper's terminal fusion estimation error.

Based on the optimal encryption strategy, Algorithm 1 is given to design the distributed anti-eavesdropping fusion estimate method in the presence of energy constraints. Next, the maximum value of the objective function for problem (24) is presented by Theorem 2.

Algorithm 1 Distributed anti-eavesdropping fusion estimate $\hat{x}(t)$ under an optimal encryption criterion in the presence of energy constraints.

1: Initialization: Input parameters: P_i^δ, $\bar{\sigma}_i$, $\underline{\sigma}_i$, $\bar{P}_{ii}(i = 1, 2, \ldots, L)$.
2: **for** $i := 1$ **to** L **do**
3: Step 1: Calculate maximum number of encryptions $n_i^{\max}$ by $n_i^{\max} = \lfloor P_i^\delta / \underline{\sigma}_i \rfloor$;
4: Step 2: Calculate the desired optimal encryption energy σ_i^d by (42);
5: Step 3: Select the optimal encryption level σ_i^* by (27);
6: Step 4: Construct optimal encryption sequence η_i^* by (28).
7: Step 5: Inject the AN into the transmitted signal according to σ_i^*, η_i^*, and (9);
8: **end for**
9: Step 6: Decode the received signals and perform distributed fusion estimation according to (6)-(8) and (13);
10: Output: Optimal fusion estimate $\hat{x}(t)$.

Theorem 2. For the systems (1)-(2), if the condition (26) is satisfied, then the maximum value of the objective function for sub-optimization problem (24) can be computed by

$$\begin{aligned}(\mathrm{J}_{\mathrm{S}})_{\max} = \alpha\mathrm{Tr}\{\textstyle\sum_{i=1}^{L}(\sum_{j=0}^{n_i^{\max}-1}((\gamma_i^*)^j - (\gamma_i^*)^{j+1})h^j(\bar{P}_{ii})\\ + (\gamma_i^*)^{n_i^{\max}}h^{n_i^{\max}}(\bar{P}_{ii}))\} - \sum_{i=1}^{L}(1-\alpha)n_i^{\max}c_i\end{aligned} \tag{43}$$

where γ_i^* is the decoding failure probability with optimal encryption energy for the ith sensor, which can be calculated by $\gamma_i^* = 1 - f(\sigma_i^*)$.

Proof: In fact, we only need to calculate the maximum objective value of the L independent sub-problems for sub-optimization problem (24), and sum them to get the solution. According to Theorem 1, one has the optimal encryption level σ_i^* and the optimal number of encryptions η_i^*. Then, it follows from (11)-(12) that the corresponding decoding failure probability is determined by:

$$\gamma_i^* = 1 - f(\sigma_i^*) \tag{44}$$

Under this case, according to (33), the maximum objective value of the sub-problems can be computed by

$$\begin{aligned}(\mathrm{J}_{\mathrm{S}}^i)_{\max} = \alpha\mathrm{Tr}\{\textstyle\sum_{j=0}^{n_i^{\max}-1}((\gamma_i^*)^j - (\gamma_i^*)^{j+1})h^j(\bar{P}_{ii})\\ + (\gamma_i^*)^{n_i^{\max}}h^{n_i^{\max}}(\bar{P}_{ii})\} - (1-\alpha)n_i^{\max}c_i\end{aligned} \tag{45}$$

Since the sub-problems are mutually independent, we can obtain the maximum value of the objective function for sub-optimization problem (24) by summing $\mathrm{J}_{\mathrm{S}}^i(i = 1, 2, \ldots, L)$ as follows:

$$\begin{aligned}(\mathrm{J}_{\mathrm{S}})_{\max} = \alpha\mathrm{Tr}\{\textstyle\sum_{i=1}^{L}(\sum_{j=0}^{n_i^{\max}-1}((\gamma_i^*)^j - (\gamma_i^*)^{j+1})h^j(\bar{P}_{ii}))\\ + (\gamma_i^*)^{n_i^{\max}}h^{n_i^{\max}}(\bar{P}_{ii}))\} - (1-\alpha)\textstyle\sum_{i=1}^{L}n_i^{\max}c_i\end{aligned} \tag{46}$$

This completes the proof.

Remark 5. Notice that the calculation of optimal objective function value for sub-optimization problem (24) only depends on the L times irrelevant calculation of $(\mathrm{J}_{\mathrm{S}}^i)_{\max}$ with (45). Moreover, the optimization objective value in Theorem 2 can be used to evaluate the degree of data privacy protection, and it has guiding significance for the design of encryption strategy in this paper.

V. Simulation Examples

Consider a dynamic system monitored by two sensors, where system and measurement parameters are chosen by:

$$\begin{cases} A = \begin{bmatrix} 1.01 & 0.01 \\ 0 & 1.02 \end{bmatrix}, \begin{cases} C_1 = [1 \quad 0] \\ C_2 = [1 \quad 1] \end{cases} \\ Q = \begin{bmatrix} 1 & 0.2 \\ 0.2 & 0.5 \end{bmatrix}, \begin{cases} R_1 = 0.2 \\ R_2 = 1 \end{cases} \end{cases}$$

It is obvious that the addressed system is observable and controllable, and thus the steady-state covariance matrices can be obtained as follows:

$$\bar{P}_{11} = \begin{bmatrix} 0.1710 & 0.0777 \\ 0.0777 & 26.5854 \end{bmatrix}, \bar{P}_{22} = \begin{bmatrix} 11.7102 & -11.3350 \\ -11.3350 & 11.6865 \end{bmatrix}$$

In the simulation, we consider a finite-time horizon with $N = 10$, and choose the weighting factor $\alpha = 0.8$, which means that privacy is more important than the cost of encryption. Let the total energy budget of two sensors be $P_1^\delta = 16$ and $P_2^\delta = 30$, while the emission energy $\delta_i(t)$ of both sensors is taken as 2. Meanwhile, the AN powers for different sensors are $\sigma_1 \in [4,\ 12]$ and $\sigma_2 \in [5,\ 13]$, while the encryption process cost is taken as $c_1 = c_2 = 2$.

This article has been accepted for publication in IEEE Transactions on Automatic Control. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAC.2023.3250094

By calculation, the eigenvalues of the system matrix AA^{T} are 1.0159 and 1.0447 respectively. Further, one can compute the variables related to the initial system parameters, and it is not difficult to verify that the condition (26) is satisfied for the two subsystems. It is concluded from Theorem 1 that both subsystems have the optimal analytical solution with encryption level and encryption sequence. Particularly, according to the Theorem 1, the optimal encryption powers for both sensors are 4 and 5, and the optimal encryption times are the last 4 and 6 time instances respectively. To verify this conclusion, we compare the value $\mathrm{J}_{\mathrm{S}}^{i}(i=1,2)$ for different encryption levels under the encryption sequence (28). The simulation results are shown in Fig. 2-4, Tables 1 and 2. To better interpret the simulation results, we define the following abbreviations:

$$\begin{cases} \mathrm{RES}: \text{Random encryption sequence} \\ \mathrm{OES}: \text{Optimal encryption sequence} \\ \mathrm{OES}-\mathrm{REL}: \text{OES with random encryption level} \\ \mathrm{OES}-\mathrm{OEL}: \text{OES with optimal encryption level} \\ \mathrm{TFEC}: \text{Trace of fusion error covariance} \end{cases}$$

Table 1. Statistical results for sensor 1

σ_1	4	5	6	7	8	9	10	11
n_1	4	3	2	2	2	1	1	1
$(\mathrm{J}_{\mathrm{S}}^{1})_{\mathrm{RES}}$	27.83	26.28	26.26	26.47	26.29	26.56	26.51	26.58
$(\mathrm{J}_{\mathrm{S}}^{1})_{\eta_{n_1}^*}$	33.68	31.90	30.81	31.02	31.10	28.80	28.86	28.91

Table 2. Statistical results for sensor 2

σ_2	5	6	7	8	9	10	11	12
n_2	6	5	4	3	3	3	2	2
$(\mathrm{J}_{\mathrm{S}}^{2})_{\mathrm{RES}}$	24.47	22.91	22.95	22.89	22.81	23.03	22.96	23.04
$(\mathrm{J}_{\mathrm{S}}^{2})_{\eta_{n_1}^*}$	30.84	29.89	28.87	27.74	28.15	28.50	26.37	26.49

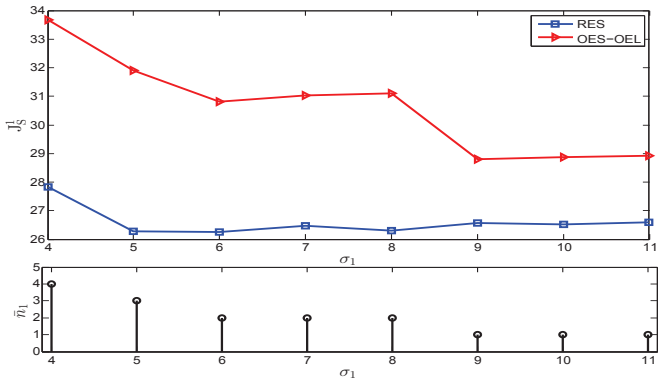

Fig. 2. $\mathrm{J}_{\mathrm{S}}^{1}$ with different encryption for sensor 1

Firstly, it is seen from Fig. 2-3 that, under different encryption energy levels, the $(\mathrm{J}_{\mathrm{S}}^{i})$ value curve based on the optimal encryption sequence decreases significantly as the number of encryptions decreases. When the number of encryptions is the same, the objective value curve is flat, but it still slightly increases with the increase of encryption energy. This is because the value of the probability of successful decoding is close under the condition of the same encryption times, which makes the $(\mathrm{J}_{\mathrm{S}}^{i})$ value increase slowly. Notice that under the random encryption sequence, the $(\mathrm{J}_{\mathrm{S}}^{i})$ value curve is flat. This is because the limited encryption times are evenly distributed in the time domain N.

Secondly, it is seen from the statistical results of Tables 1 and 2 that when the AN energy of the two sensors is 4 and 5 respectively, $(\mathrm{J}_{\mathrm{S}}^{1})_{\eta_{n_1}^*}=33.68$ and $(\mathrm{J}_{\mathrm{S}}^{2})_{\eta_{n_2}^*}=30.84$ are both the largest objective values. We can also find that for the same number of encryptions, the greater the encryption energy is, the larger the maximum value of $\mathrm{J}_{\mathrm{S}}^{i}(i=1,2)$ is. This is because the large AN energy reduces the successful decoding probability of the eavesdropper, resulting in poor fusion estimation performance. In addition, $(\mathrm{J}_{\mathrm{S}}^{i})$ increases as the encryption time increases. This implies that the user can achieve a bigger objective value by encrypting as much data as possible. It is concluded from the simulation results that the optimal encryption times of the local sensors are the last 4 and 6 time instances respectively, and the transmitted data is encrypted in the last few times on the finite-time horizon N. These results are completely consistent with the conclusion of Theorem 1. On the other hand, according to Theorem 2, the maximum value of the objective function $(\mathrm{J}_{\mathrm{S}})_{\max}$ can be computed as $\sum_{i=1}^{L}(\mathrm{J}_{\mathrm{S}}^{i})_{\max}=33.68+30.84=64.52$, which is the maximum value that can be achieved by using the suboptimal encryption strategy under energy constraints.

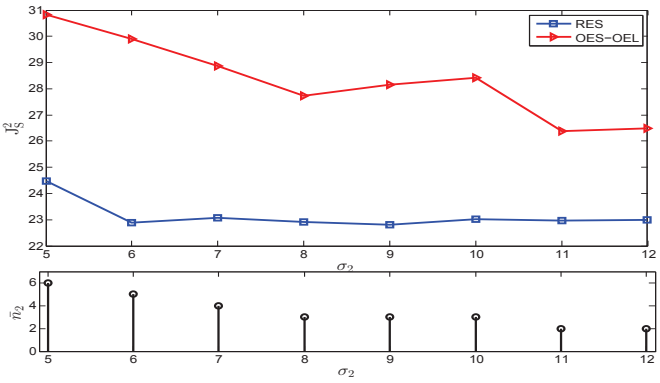

Fig. 3. $\mathrm{J}_{\mathrm{S}}^{2}$ with different encryption for sensor 2

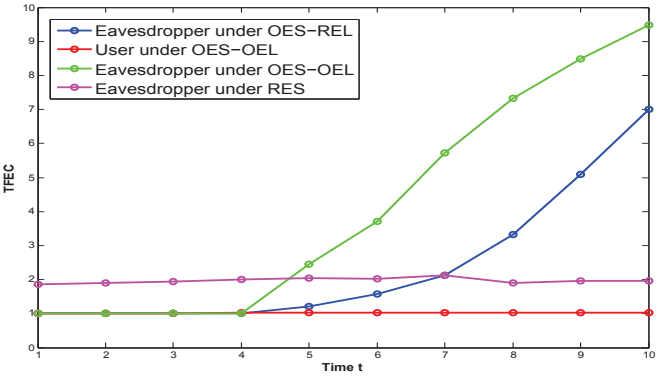

Fig. 4. Trace of fusion error covariance for different encryption strategies

Finally, the fusion performance with three encryption strategies are compared in Fig. 4. It is shown that the TFEC of user under OES-OEL is constant at 1.007. Because the designed encryption noise does not affect the successful decoding probability for the FC of user. Due to the key role of the OES, the TFEC of the eavesdropper increases rapidly under the OES-REL and OES-OEL. At the same time, compared with the OES-REL, the optimal encryption strategy proposed in this paper is more efficient to protect the state privacy of NMFSs.

VI. CONCLUSIONS

The distributed fusion estimation against eavesdroppers was studied in this paper for NMFSs under energy constraints. To resist eavesdropping, AN was injected into each transmitted local estimate, and the probability of the transmission being successfully encoded was dependent on the SNR of the received signal. Both the user and the eavesdroppers reconstructed a minimum mean square error estimate by fusing their received local messages. To model the privacy level of the system state, the optimization problem was established by determining encryption strategies in finite time domain. Moreover, the established optimization problem was decomposed into several independent sub-optimization problems, and a sufficient condition was derived such that the sub-optimization problems had optimal and simple solutions. Finally, simulation results verified the effectiveness of the proposed methods.

REFERENCES

[1] B. Chen, W.A. Zhang, L. Yu, G.Q. Hu, H.Y. Song. Distributed fusion estimation with communication bandwidth constraints, *IEEE Transactions on Automatic Control*, vol. 60, no. 5, 2015, pp. 1398-1403.

[2] H. Zhang, W. Zheng. Denial-of-service power dispatch against linear quadratic control via a fading channel, *IEEE Transactions on Automatic Control*, vol. 63, no. 9, 2018, pp. 3032-3039.

[3] S.Y. Lai, B. Chen, T. Li, L. Yu. Packet-based feedback control under Dos attacks in cyber-physical systems, *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 66, no. 8, 2019, pp. 1421-1425.

[4] S. Liu, Z.D Wang, G.L. Wei, M.Z. Li. Distributed set-membership filtering for multirate systems under the Round-Robin scheduling over sensor networks. *IEEE Transactions on Cybernetics*, vol. 50, no. 5, 2019, pp. 1910-1920.

[5] H. Zhang, Y.F. Qi, J.F. Wu, L. Fu, L.D. He. DoS attack energy management against remote state estimation, *IEEE Transactions on Control of Network Systems*, vol. 5, no. 1, 2016, pp. 383-394.

[6] B. Chen, D.W.C. Ho, W.A. Zhang, L. Yu. Distributed dimensionality reduction fusion estimation for cyber-physical systems under DoS attacks, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol 49, no. 2, 2019, pp. 455-468.

[7] H. Zhang, Y.F. Qi, J.F. Wu, L. Fu, L.D. He. False data injection attacks on networked control systems: A stackelberg game analysis, *IEEE Transactions on Automatic Control*, vol. 63, no. 10, 2018, pp. 3503-3509.

[8] B. Chen, D.W.C. Ho, G. Hu, L. Yu. Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks, *IEEE transactions on cybernetics*, vol. 48, no. 6, 2018, pp. 1862-1876.

[9] K. Wang, L. Yuan, T. Miyazaki, Y. Chen, Y. Zhang. Jamming and eavesdropping defense in green cyber-physical transportation systems using a stackelberg game, *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, 2018, pp. 4232-4242.

[10] L. Shi, P. Cheng, J.M. Chen. Optimal Periodic Sensor Scheduling With Limited Resources, *IEEE Transactions on Automatic Control*, vol. 56, no. 9, 2011, pp. 2190-2195.

[11] V.S. Varma, O. de, M. Andre, R. Postoyan. Energy-efficient time-rriggered communication policies for wireless networked control systems, *IEEE Transactions on Automatic Control*, vol. 65, no. 10, 2018, pp. 4324-4331.

[12] S.L. Sun, Z.L. Deng. Multi-sensor optimal information fusion Kalman filter, *Automatica*, vol. 40, no. 6, 2004, pp. 1017-1023.

[13] Y. Liu, G.H. Yang. Event-triggered distributed state estimation for cyber-physical systems under DoS attacks, *IEEE transactions on cybernetics*, 2020, pp.1-12.

[14] X.Q Ren, Y.L. Mo, J. Chen, K.H. Johansson. Secure state estimation with byzantine sensors: A probabilistic approach. *IEEE Transactions on Automatic Control*, vol. 65, no. 9, 2020, pp. 3742-3757.

[15] W.A. Zhang, L. Yu, D.F. He. Sequential fusion estimation for sensor networks with deceptive attacks. *IEEE Transactions on Aerospace and Electronic Systems*, vol. 56, no. 3, 2020, pp. 1829-1843.

[16] H.Y Song, P. Shi, C.C. Lim, W.A. Zhang, L. Yu. Attack and estimator design for multi-sensor systems with undetectable adversary. *Automatica*, vol. 109, 2019.

[17] J. Chen, C.X. Dou, L. Xiao, Z. Wang. Fusion state estimation for power systems under DoS attacks: A switched system approach. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, 2019, pp. 1679-1687.

[18] L. Yuan, K. Wang, T. Miyazaki, S. Guo, M. Wu. Optimal transmission strategy for sensors to defend against eavesdropping and jamming attacks, In *Proceedings of the international Conference on Communications*, 2017, pp. 1-6.

[19] A. Tsiamis, K. Gatsis, G. Pappas. State estimation with secrecy against eavesdroppers, In *Proceedings of IFAC world congress*, 2017, pp. 8715-8722.

[20] A.S. Leong, D. Quevedo, D. Dolz, D. Subhrakanti. Transmission scheduling for remote state estimation over packet dropping links in the presence of an eavesdropper, *IEEE Transactions on Automatic Control*, vol. 64, no. 9, 2019, pp. 3732-3739.

[21] J.Y. Lu, A.S. Leong, E. Danie. An event-triggered transmission scheduling strategy for remote state estimation in the presence of an eavesdropper, *arXiv preprint arXiv:1910.03759*, 2019.

[22] A.S. Leong, E. Danie, D. Daniel, S. Dey. On remote state estimation in the presence of an eavesdropper, In *Proceedings of International Federation of Automatic Control*, 2017, pp.7339-7344.

[23] A. Tsiamis, K. Gatsis, G. Pappas. State-secrecy codes for networked linear systems, *IEEE Transactions on Automatic Control*, vol 65, no. 5, 2020, pp. 2001-2015.

[24] A. Tsiamis, K. Gatsis, G. Pappas. An information matrix approach for state secrecy, In *Proceedings of the Conference on Decision and Control*, 2018, pp. 2062-2067.

[25] A. Tsiamis, K. Gatsis, G. Pappas. State-secrecy codes for stable systems, In *Proceedings of the Annual American Control Conference*, 2018, pp. 171-177.

[26] L. Huang, A.S. Leong, D. Quevedo, L. Shi. Finite time encryption schedule in the presence of an eavesdropper with operation cost, *arXiv preprint arXiv:1903.11763*, 2019.

[27] L. Wang, X.H. Cao, B.W. Sun, H. Zhang, C.Y. Sun. Optimal schedule of secure transmissions for remote state estimation against eavesdropping, *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, 2021, pp. 1987-1997.

[28] D.X. Xu, B. Chen, L. Yu. Secure fusion estimation against eavesdroppers, In *Proceedings of the 37th Chinese Control Conference*, 2018, pp. 4310-4315.

[29] D.X. Xu, B. Chen, L. Yu, W.A. Zhang. Secure dimensionality reduction fusion estimation against eavesdroppers in cyber-physical systems, *ISA Transactions*, vol 104, 2020, pp. 154-161.

[30] H. Zhang H, P. Cheng, L. Shi, J.M Chen. Optimal denial-of-service attack scheduling with energy constraint, *IEEE Transaction on Automatic Control*, vol. 60, no. 11, 2015, pp. 3023-3028.

[31] A. Jazwinski. Stochastic processes and filtering theory, New York: Academic, 1970.

[32] B. Anderson, J. Moore. Optimal filtering. Prentice-Hall Information and System Sciences Series, Englewood Cliffs: Prentice-Hall, 1979.

[33] Z. Deng, Y. Gao. New approach to information fusion steady state Kalman filtering, *Automatica*, vol. 41, 2005, pp. 1695-1707.

[34] H. Zhang, P. Cheng. Optimal denial-of-service attack scheduling with energy constraint, *IEEE Transactions on Automatic Control*, vol. 60, no. 11, 2015, pp. 3023-3028.

[35] L. Shi, P. Cheng, and J. Chen. Sensor data scheduling for optimal state estimation with communication energy constraint, *Automatica*, vol. 47, no. 8, 2011, pp. 1693-1698.

[36] L. Shi, P. Cheng, J.M. Chen. Optimal periodic sensor scheduling with limited resources. *IEEE Transactions on Automatic Control*, vol. 56, no. 9, 2011, pp. 2190-2195.

[37] R. Poisel. Modern communications jamming: principles and techniques. London, 2011.

[38] H. Luo, X.L. Yu, Z.F. Zhang, C.Q. Gan. Channel estimation for 5G mm wave communications systems: a survey. *Telecommunication Engineering*, vol. 61, no. 2, 2021, pp.254-262.

[39] A.S. Leong, A. Redder, E. Danie, S. Dey. On the use of artificial noise for secure state estimation in the presence of eavesdroppers, In *Proceedings of the European Control Conference*, 2018, pp.325-330.

[40] S. Goel, R. Negi. Guaranteeing secrecy using artificial noise, *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, 2008, pp. 2180-2189.

[41] Y.B. Liang, H.V. Poor, S. Sharnai. Secure communication over fading channels, *IEEE Transactions on Information Theory*, vol. 54, no. 6, 2008, pp. 2470-2492.

[42] F. Ramirez-Mireles. On the performance of ultra-wide-band signals in Gaussian noise and dense multipath, *IEEE Transactions on Vehicular Technology*, vol. 50, no. 1, 2001, pp. 244-249.

[43] Q. Jia, L. Shi, Y.L. Mo, B. Sinopoli. On optimal partial broadcasting of wireless sensor networks for kalman filtering, *IEEE Transactions on Automatic Control*, vol. 57, no. 3, 2011, pp. 715-721.