Xu *et al.*
EURASIP Journal on Advances in Signal Processing (2024) 2024:56
https://doi.org/10.1186/s13634-024-01124-4

EURASIP Journal on Advances in Signal Processing

RESEARCH Open Access

Event-Triggered confidentiality fusion estimation against eavesdroppers in cyber-physical systems

Daxing Xu[1,2], Zhiqiang Chen[1] and Hailun Wang[1*]

*Correspondence:
wanghl@qzc.edu.cn

[1] College of Electrical and Information Engineering, Quzhou University, Quzhou 324000, China
[2] Kerun Intelligent Control Co., Ltd, Quzhou, China

Abstract

System state plays an important role in cyber-physical systems (CPSs). Ensuring the security of the CPSs is a key issue that can be widely applied. The confidentiality of system state is a fundamental feature of the CPSs security. This paper studies the distributed fusion estimation problem in the presence of eavesdropper, where local sensors send their estimates to a remote fusion center (FC). To prevent eavesdropping, the event triggered scheduling strategy was adopted on each sensor. Some sufficient conditions on the triggers' threshold were derived to make the eavesdropping expected covariance unbounded while the expected error covariance for the user remains bounded. Moreover, the distributed confidentiality fusion estimation algorithm is provided to achieve perfect expected secrecy. Finally, simulations of different trigger levels for two local systems are employed to show the effectiveness of the proposed methods.

Keywords: Fusion estimation, Eavesdropping, Privacy protection, Event triggering, Cyber-physical systems

1 Introduction

Cyber-physical systems (CPSs) have been widely integrated in many application fields, such as intelligent transportation, power system, and medical device systems [1, 2, 3–5]. Multi-sensor fusion estimation is an information processing process that uses the observations from multiple sensors to complete the system state estimation under certain criteria. It is widely used in CPSs because of the high reliability and strong robustness [6, 7, 8–10]. However, due to its open connectivity, CPSs have become the target of malicious attackers. Eavesdropping attack is one of the typical network attacks [11, 12]. The security of CPSs has received a lot of attention, among which confidentiality is a basic security issue [13]. The data transmitted in channel is easily intercepted by eavesdropper over another channel. It can launch the complex attacks after analyzing a large amount of intercepted data, such as false data injection attacks [14]. Therefore, studying secure fusion estimation in presence of eavesdropper has great important theoretical and practical significance.

Encrypting messages to prevent eavesdropping has been studied from the perspective of information theory [15, 16]. The energy of sensors often comes from batteries, which limits their energy. Thus, it is difficult to exploit conventional strong encryption scheme due to the large energy demand. In recent years, secure communication problem has been studied by using physical layer information and artificial noise (AN). From the perspective of control theory, the concept of perfect encryption has been proposed. In [17], which required that the user's state estimation error is bounded, while the eavesdropper's estimation error tends to be unbounded over time. Then, an optimal confidentiality strategy against eavesdropper without feedback was given to obtain the perfect secrecy. Meanwhile, with feedback, similar results were derived in [18]. An event triggered sensor data scheduling strategy was designed to prevent eavesdropping by recurrent Markov chain in [19]. Moreover, considering the dynamic characteristics and physical layer information of the CPSs, state-secrecy codes was introduced to achieve the goal of perfect encryption for stable, unstable, and arbitrary systems in [20–22]. Consider the operation cost, an optimal encryption schedule was proposed to improve system state confidentiality in [23]. Under the distributed framework, the problem of secure fusion estimation with state privacy protection was studied in [24], where perfect secrecy was achieved by injecting AN. In the framework of state component transmission, an AN design strategy based on the system parameters was developed, which makes the eavesdroppers' fusion error covariance became worse in [25]. Then, the strategies for actively polluting local estimation components were presented to enhance the privacy level of local estimates in [26]. The finite-horizon energy-to-peak state estimation issue was considered for time-varying systems in [27], where the desired time-varying estimator parameter was designed for online computation. For a networked system with multi-rate measurements, a novel encryption-decryption scheme was proposed to protect the privacy of the system state in [28]. Under the constraint of sensor energy, the confidentiality fusion estimation against eavesdroppers algorithm was proposed in [29] by combining event triggers and artificial noise. Recently, the AN based on the channel gain matrix was introduced to maintain confidentiality for distributed fusion estimation in [30]. However, the injected AN consumed more sensor energy, which added the challenge of anti-eavesdropping strategy design.

Based on the above-analysis, we shall study the event-based confidentiality fusion estimation problem with limited sensor energy for CPSs. To save the sensor power, we do not encrypt signals, but schedule the transmission based on event triggers. In our scenario, the sensors transmitting their outputs to a user, where all transmission channels may be tapped by the eavesdroppers. Under this case, the eavesdroppers can obtain an accurate state estimation result through the fusion estimation method. From the user's perspective, in order to protect state privacy, each local sensor needs to design rules for transmitting local estimates to prevent the eavesdropper from getting the real system state through fusion estimation. This is the most important goal of this article, and the main contributions include: (1) We provide some sufficient conditions about the threshold of event triggering to achieve perfect expected secrecy. (2) The event-based distributed confidentiality fusion estimation algorithm is proposed to ensure the effective of the transmission scheduling strategy.

2 Problem formulation

2.1 System model

The system structure is shown in Fig. 1, which is described by the following physical model:

$$\begin{aligned} x(t+1) &= Ax(t) + w(t) \\ y_i(t) &= C_i x(t) + v_i(t) \quad (i = 1, 2, ..., L) \end{aligned} \tag{1}$$

where $x(t) \in R^n$ is state vector with dimension n, and $y_i(t) \in R^{q_i}$ is sensor observation value of the i-th sensor with dimension q_i. $w(t)$ and $v_i(t)$ are Gaussian white noise with zero mean value, and the variances are Q and R_i respectively. L means there are L sensors to observe the system state. Assume that the matrix pair (C_i, A) is detectable and $(A, Q^{1/2})$ is controllable.

In our scenario, all sensors are smart sensors with computing capability [31]. At time t, the i-th sensor observes the physical process to obtain the observation $y_i(t)$. After collecting the observations until time t, the information set of the ith local estimator is given as $\mathrm{Y}_i(t) = y_i(1), \ldots, y_i(t)$ with $\mathrm{Y}_i(-1) = \emptyset$. Further, define

$$\begin{cases} \hat{x}_i^-(t) \triangleq \mathrm{E}[x(t)|\mathrm{Y}_i(t-1)], \hat{y}_i^-(t) \triangleq \mathrm{E}[y_i(t)|\mathrm{Y}_i(t-1)] \\ e_i^-(t) \triangleq x(t) - \hat{x}_i^-(t), P_i^-(t) \triangleq \mathrm{E}[e_i^-(t) e_i^{-T}(t)|\mathrm{Y}_i(t-1)] \\ \hat{x}_i(t) \triangleq \mathrm{E}[x(t)|\mathrm{Y}_i(t)], e_i(t) \triangleq x(t) - \hat{x}_i(t), \\ P_i(t) \triangleq \mathrm{E}[e_i(t) e_i^T(t)|\mathrm{Y}_i(t)] \end{cases} \tag{2}$$

where $\hat{x}_i^-(t)$and $\hat{x}_i(t)$ are a priori and a posteriori MMSE estimates,$P_i^-(t)$ and $P_i(t)$ are estimation error covariance, and $\mathrm{E}[\cdot]$ represents the mathematical expectation. Recall from the standard Kalman filter [32], $\hat{x}_i(t)$ and $P_i(t)$ can be obtained according to the local estimator (LE) of the i-th sensor:

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

According to literature [33], it usually takes only a few iterations for $P_i(t)$ to converge exponentially to the steady-state value. Therefore, for simplicity, let $P_i(0)$ be the initial

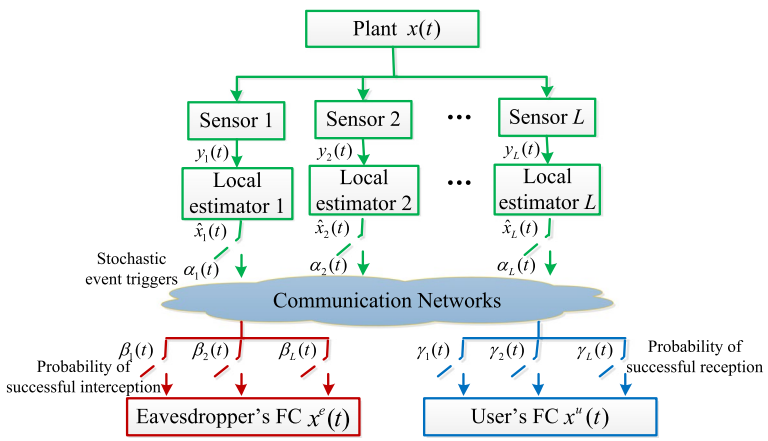

Fig. 1 Block diagram of the system model

error covariance of the i-th sensor, and it is equal to $\overline{P}_{ii}$. Further, we know that $P_i(t) = \overline{P}_{ii}$ for all times t.

After obtaining the LE $\hat{x}_i(t)$, the i-th sensor decides whether to transmit it to the fusion center (FC). We introduce the binary variable $\alpha_i(t)$ to model the decision process. $\alpha_i(t) = 1$ indicates that the LE $\hat{x}_i(t)$ is sent by the i-th sensor, otherwise it will not send. The channels between the sensors and the FC are not reliable, which may lead to data packet loss. In addition, the packets transmitted on the channel can be intercepted on another channel by eavesdroppers. Let the binary variable $\beta_i(t) = 1$ and 0 denote whether the i-th LE is intercepted by the eavesdropper or not. Let the binary variable $\gamma_i(t) = 1$ and 0 denote whether the i-th LE is successfully received by the user or not.

In the FC, in order to obtain accurate state estimation, user and eavesdropper use the weighted matrix fusion method to obtain the final state estimation based on the received LE. To avoid symbol misuse, the fusion estimation of the user's FC is taken as an example to illustrate how to implement the weighted matrix fusion algorithm. Let h and h^k be functions. In specific, $h(X) \triangleq AXA^T + Q$ and $h^k(X) \triangleq \underbrace{h \circ h \circ \cdots \circ h}_{k \text{ times}}(X)$. According to [34, 35], if $k_1 \leq k_2, k_1, k_2 \in Z^+$, then $\overline{P}_{ii} < h^{k_1}(\overline{P}_{ii}) \leq h^{k_2}(\overline{P}_{ii})$.

In the user's FC, the LE of the i-th sensor cannot be successfully received in two cases by. One is that the i-th sensor does not send LE to the FC, in which case $\alpha_i(t) = 0$. The second is that the i-th LE is sent, but packet loss occurs in the channel with $\gamma_i(t) = 0$. In this case, it needs to perform a one-step prediction compensation on the local estimate. Therefore, the final LE $\hat{x}_i^u(t)$ and covariance $P_{ii}^u(t)$ is computed as

$$(\hat{x}_i^u(t), P_{ii}^u(t)) = \begin{cases} (\hat{x}_i(t), \overline{P}_{ii}), & \text{if } \alpha_i(t)\gamma_i(t) = 1 \\ (A\hat{x}_i^u(t-1), h(P_{ii}^u(t-1))), & \text{otherwise} \end{cases} \tag{4}$$

Further, the distributed matrix-weighted fusion filter $\hat{x}^u(t)$ can be obtained by4

$$\hat{x}^u(t) = \sum_{i=1}^{L} W_i(t)\hat{x}_i^u(t) \tag{5}$$

where,

$$\sum_{i=1}^{L} W_i(t) = I_n \tag{6}$$

Then, define $\Xi(t) \triangleq \begin{bmatrix} P_{11}^u(t) \ldots P_{1L}^u(t) \\ \vdots \quad \vdots \\ P_{L1}^u(t) \ldots P_{LL}^u(t) \end{bmatrix}$, where $P_{ij}^u(t)$ $(i \neq j)$ is cross-covariance matrix between any two LEs, which is calculated by:

$$P_{ij}^u(t) = [I_n - K_i(t)C_i][AP_{ij}^u(t-1)A^T + Q][I_n - K_j(t)C_j]^T \tag{7}$$

It usually takes only a few iterations for $P_{ij}^u(t)$ to converge exponentially to the steady-state value [36]. For simplicity, we represent the initial error cross-covariance

matrix as $P_{ij}(0)$ for the i-th sensor, and it is equal to $\overline{P}_{ij}$. Then, it can be concluded that $P^u_{ij}(t) = \overline{P}_{ij}$ for all times t, and the initial of $\Xi(0)$ is $\begin{bmatrix} \overline{P}_{11} \dots \overline{P}_{1L} \\ \vdots \quad \vdots \\ \overline{P}_{L1} \dots \overline{P}_{LL} \end{bmatrix}$.

Under the linear minimum variance criterion, in terms of the result in [37], the optimal W_1(t), W_2(t),...,W_L(t) in (6) can be given by:

$$[W_1(t), \dots, W_L(t)] = ((\Upsilon^s)^T \Xi^{-1}(t)\Upsilon^s)^{-1}(\Upsilon^s)^T \Xi^{-1}(t) \tag{8}$$

where $\Upsilon^s = [I_n, I_n, \dots, I_n]^T$. Further, the fusion error covariance $P^u(t) \triangleq \mathrm{E}\{(x(t) - \hat{x}^u(t))(x(k) - \hat{x}^u(t))^T\}$. can be computed by:

$$P^u(t) = ((\Upsilon^s)^T \Xi^{-1}(t)\Upsilon^s)^{-1} \tag{9}$$

Remark 1 For the eavesdropper, if he is strong enough to eavesdrop on the transmission data of multiple sensors at the same time, he can use the intercepted LEs to obtain more accurate state estimation through fusion estimation method. This brings challenges to the distributed secure fusion estimation.

2.2 Problem of interest

First, we denote by p_i the probability that the i-th sensor decides to send the LE to the FC. To prevent eavesdropping, the stochastic event triggering strategy is adopted for all sensors. In detail, the processor of the i-th sensor can generate a random variable ζ_i at each time t. These variables obey a uniform distribution on (0, 1), i.e.,$\zeta_i \sim U(0, 1)$. The stochastic event triggers are given by

$$\alpha_i(t) = \begin{cases} 1, \ 0 < \zeta_i \leq \eta_i, \\ 0, \ \eta_i < \zeta_i < 1. \end{cases} \tag{10}$$

Further, assume that each sensor always decides to send LE to the FC, i.e., $\alpha_i(t) = 1$ for all time t. We model the packet drops and packet interceptions as i.i.d. over time, which are commonly used assumptions by researchers. In particular, we let ρ_i represent the probability that the i-th local estimate is intercepted by the eavesdropper. Similarly, λ_i denotes the probability that the i-th local estimate is received by the user. Thus, the channel model can be given as follows:

$$\begin{cases} \beta_i(t) = \begin{cases} 1, \text{ with probability } \rho_i, \\ 0, \text{ with probability } 1 - \rho_i. \end{cases}' \\ \gamma_i(t) = \begin{cases} 1, \text{ with probability } \lambda_i, \\ 0, \text{ with probability } 1 - \lambda_i. \end{cases} \end{cases} \tag{11}$$

Remark 2 In the description of physical layer security problems, knowing exactly the channel model of the eavesdropper for the user is a common assumption[38]. The channel gain can be obtained by using blind estimation, pilot-based estimation, etc. Under this case, knowing the probability ρ_i is less restrictive than knowing the exact

eavesdropper's channel model. In fact, ρ_i can be considered as the confidence level of the system designer on the ability of the eavesdropper to successfully eavesdrop data packs.

Next, the concept of perfect encryption is introduced in the following definition.

Definition 1 (*Perfect Expected Secrecy*) [17]. For any initial condition $P(0)$, a secrecy mechanism achieve perfect expected secrecy if and only if both of the following condition hold:

$$\lim_{t\to\infty} \mathrm{Sup}\ \mathrm{Tr}\{\mathrm{E}\{P^u(t)\}\} < \infty \tag{12}$$

$$\lim_{t\to\infty} \mathrm{Tr}\{\mathrm{E}\{P^e(t)\}\} = \infty \tag{13}$$

where the covariance of the state estimation error for the eavesdropper is denoted by $P^e(t)$, Sup represents upper bound, and Tr denotes trace operator.

Remark 3 For any initial system estimation error covariance, when the data transmitted is encrypted according to a scheduling mechanism, the trace of the user's covariance tends to be bounded in the expected sense over time, while the trace of the eavesdroppers' tends to be unbounded. In this case, the eavesdropper's state estimation error is infinite, and the accurate information of the system state cannot be obtained. Therefore, it can be said that perfect expected encryption is achieved under this encryption mechanism.

Further, the problems we need to solve is described as follows:

(1) For the distributed fusion estimation, the first aim of this paper is to answer "how to design event-triggered data scheduler for the sensors so that the user's estimation error is convergent, but the estimation error for the eavesdropper will be unbounded".
(2) From the perspective of the defender, another goal is to design the event-triggered confidentiality fusion estimation algorithm, which guarantee the effectiveness of our data scheduling method.

3 Main results

For a stable system, as long as the eavesdropper has the system model parameters, the system state can be predicted in real time without eavesdropping, and the prediction error is always bounded. Therefore, we studies the problem of confidentiality fusion estimation for unstable systems. As pointed out in the literature [17], fusion estimation to against eavesdroppers for unstable systems is more interesting than that for stable systems. Let the spectral radius of A in the unstable system (1) satisfy $\rho(A) > 1$. We will explore some sufficient conditions under which we can obtain the distributed security fusion estimation algorithm to protect state privacy.

Theorem 1 *For the unstable system* (1) *with channel model* (11), *under the encryption mechanism* (10), *if the trigger thresholds of all sensors satisfy*:

(i) *There is an positive integer i such that*

$$\eta_i > \frac{1}{\lambda_i}\left(1 - \frac{1}{\rho(A)^2}\right) \tag{14}$$

(ii) *For any positive integer i, the following inequality holds*

$$\eta_i < \min\left\{\frac{1}{\rho_i}(1 - \rho(A)^{-\frac{2}{L}}), 1\right\} \tag{15}$$

Then the Perfect Expected Secrecy can be obtained.

Proof According to the Definition 1, we need to prove that Eqs. (12) and (13) holds simultaneously under condition (14) and (15). We first prove that the Perfect Expected Secrecy condition (12) is satisfied under the condition (14). Suppose that the event trigger threshold η_i of the s_0th sensor satisfies $\eta_i > \frac{1}{\lambda_i}(1 - \frac{1}{\rho(A)^2})$, then we have

$$\eta_i \lambda_i > 1 - \frac{1}{\rho(A)^2} \tag{16}$$

In this case, the probability that the user's FC can successfully receive the LE of the s_0th sensor always satisfies $p(\alpha_i(t)\gamma_i(t) = 1) > 1 - \frac{1}{\rho(A)^2}$. Then, according to [37], the estimation error covariance of the s_0 th sensor is bounded, i.e. $P^u_{ii}(t) < \infty$. Denote $\Upsilon^s_i = [\mathbf{0}, \ldots, I_n, \ldots, \mathbf{0}]^T \in R^{nL\times n}$, where, the i-th block place is an identity matrix I_n.$\mathbf{0}$ represents zero matrix with dimension n. Then, we have

$$\begin{aligned}
P^u(t) &= ((\Upsilon^s)^T \Xi^{-1}(t)\Upsilon^s)^{-1} \\
&= ((\Upsilon^s)^T \Upsilon^s_i)^T ((\Upsilon^s)^T \Xi^{-1}(t)\Upsilon^s)^{-1}((\Upsilon^s)^T \Upsilon^s_i) \\
&= [(\Xi^{-1/2}(t)\Upsilon^s)^T (\Xi^{1/2}(t)\Upsilon^s_i)]^T \\
&\quad \times [(\Xi^{-1/2}(t)\Upsilon^s)^T \times (\Xi^{-1/2}(t)\Upsilon^s)]^{-1} \\
&\quad \times [(\Xi^{-1/2}(t)\Upsilon^s)^T (\Xi^{1/2}(t)\Upsilon^s_i)] \\
&\leq (\Xi^{1/2}(t)\Upsilon^s_i)^T (\Xi^{1/2}(t)\Upsilon^s_i) = P^u_{ii}(t) < \infty
\end{aligned} \tag{17}$$

This means that as long as the LE error covariance of one sensor is bounded, the state error covariance obtained after the FC fuses all local estimates must be bounded. Therefore, the conditions (12) is satisfied.

Further, we prove that the Perfect Expected Secrecy condition (13) is satisfied under the condition (15). Let Ω denote the event that the event triggers of all sensors are not triggered and all LEs are not successfully intercepted when the LEs are transmitted. $\Omega^{\perp}$ represents its complement. Further, we consider the probability of the event Ω over the finite time N, one has

$$\begin{aligned} p_e(\Omega) &= p_e(\alpha_i(t)=0,\beta_i(t)=0|\alpha_i(t)=1) \\ &= \prod_{i=1}^{L}\prod_{t=1}^{N}(1-p_e(\alpha_i(t)=1)\times p_e(\beta_i(t)=1|\alpha_i(t)=1)) \\ &= \prod_{i=1}^{L}\prod_{t=1}^{N}(1-\eta_i\rho_i) \end{aligned} \tag{18}$$

where $t=1,2,\ldots,N, i=1,2,\ldots,L$.

Similar to (9), for all times N in event Ω, we have the terminal estimation error covariance for the eavesdropper $P^e(N)=((I^a)^T(\sum^e(N))^{-1}I^a)^{-1}$. Then, according to the definition of Ω, we know that the eavesdropper cannot successfully intercept the LEs of all sensors at all times N. In this case, the eavesdropper can only perform one-step prediction instead of LE. According to (4), we have

$$\sum^e(N)=\begin{bmatrix} h^N(\overline{P}_{11})\ldots h^N(\overline{P}_{1L}) \\ \vdots \quad\quad \vdots \\ h^N(\overline{P}_{L1})\ldots h^N(\overline{P}_{LL}) \end{bmatrix} \triangleq h^N(\sum(0)) \tag{19}$$

where, $h^N(\overline{P}_{ij})=A^N\overline{P}_{ij}(A^T)^N+\sum_{s=0}^{N-1}A^sQ(A^T)^s$。

Taking the trace of terminal estimation error covariance $P^e(N)$, one can get:

$$\begin{aligned} \mathrm{Tr}\{\mathrm{E}\{P^e(N)\}\} &= \mathrm{Tr}\{\mathrm{E}\{P^e(N)|\Omega\}\}p^e(\Omega) \\ &\quad + \mathrm{Tr}\{\mathrm{E}\{P^e(N)|\Omega^\perp\}\}p^e(\Omega^\perp) \\ &> \mathrm{Tr}(I_a^T(\sum^e(N))^{-1}I_a)^{-1}p^e(\Omega) \end{aligned} \tag{20}$$

Then, there is an positive integer i, which makes the following equation hold:

$$\mathrm{Tr}\{\mathrm{E}\{P^e(N)\}\} > \frac{1}{L}\mathrm{Tr}(A^N\overline{P}_{ii}(A^T)^N)p^e(\Omega) \tag{21}$$

Furthermore, according to the condition (15), we can get $\eta_i\rho_i<1-\rho(A)^{-\frac{2}{L}}$. Combing (21), the following inequality can be obtained:

$$\begin{aligned} \mathrm{Tr}\{\mathrm{E}\{P^e(N)\}\} &> \frac{1}{L}\mathrm{Tr}(\overline{P}_i(A^T)^NA^N)\prod_{i=1}^{L}\prod_{k=1}^{N}(1-\eta_i\rho_i) \\ &> \frac{1}{L\rho(A)^{2N}}\mathrm{Tr}(\overline{P}_{ii}(A^T)^NA^N) \end{aligned} \tag{22}$$

Therefore, it can be concluded that $\mathrm{Tr}\{\mathrm{E}\{P^e(N)\}\}\to\infty$ when N goes to infinity, i.e. $\lim_{t\to\infty}\mathrm{Tr}\{\mathrm{E}\{P^e(t)\}\}=\infty$.

Remark 4 The above theorem shows that as long as the event trigger threshold of one sensor is greater than $\frac{1}{\lambda_i}(1-\frac{1}{\rho(A)^2})$, the user's fusion estimation error can be guaranteed to be bounded. On this basis, if the event trigger thresholds of all sensors are controlled to satisfy the condition (15), the state estimation error for eavesdropper will tend to be unbounded. For the perspective of user, to protect the privacy of state data from leakage,

Table 1 Event-triggered confidentiality fusion estimation against eavesdroppers algorithm

1: Input parameter: P^{δ}, $\overline{\sigma}$, $\underline{\sigma}$ $\overline{P}$. Input system parameter A, C_i, Q, R_i, $P_i(0)$, $P_{ij}(0)$, λ_i, ρ_i ($i = 1, 2, 1, \ldots, L$);

2: **for** $i := 1$ **to** L **do**

3: Step 1: Calculate the stable error covariance $\overline{P}_{ii}$ of each local estimation system;

4: Step 2: Compute $\frac{1}{\lambda_i}\left(1 - \frac{1}{\rho(A)^2}\right)$, $\frac{1}{\rho_i}\left(1 - \rho(A)^{-\frac{2}{L}}\right)$;

5: Step 3: Select event trigger thresholds η_i according to conditions (14)–(15), and feed back to each local sensor;

6: **end for**

7: Step 4: The user's FC processes the received signal according to (4), and performs state fusion estimation according to formulas (5)–(9);

8: Step 5: Go to step (4) and continue to calculate the fusion estimate value at the next time

the event trigger thresholds should be reduced as much as possible when the condition (14) is satisfied. In this case, the probability that the eavesdropper successfully intercepts each local estimation is small, which makes the fusion estimation performance worse. In addition, the larger the number of sensors L is, the more local estimates the eavesdropper may intercept. Then, the user needs to reduce the event trigger threshold to a greater extent to ensure confidentiality. In the special case of only a single sensor with $L = 1$, the result $1 - \rho(A)^{-\frac{2}{L}}$ degenerate into $1 - \frac{1}{\rho^2(A)}$, which is consistent with the result in literature [39].

Remark 5 The proposed stochastic event triggering strategy ensures that eavesdroppers cannot obtain the true system state information by fusing data from the local sensors intercepted on unreliable channels. At the same time, the energy of local sensors is saved under the event triggering mechanisms. It is worth noting that the fusion estimation performance of the user will also decrease. This is a compromise on the fusion estimation performance for the sake of confidentiality.

We provide two sufficient conditions for event triggered security fusion estimation above. Next, we present a distributed confidentiality fusion estimation algorithm to achieve the Perfect Expected Secrecy. The specific steps are as follows (Table 1):

4 Result and discussion

Consider a scene where two sensors observe a dynamic system. The model parameters are given as follows

$$A = \begin{bmatrix} 1.2 & 1 \\ 0.3 & 1.1 \end{bmatrix},\ C_1 = [1 \quad 0],\ C_2 = [1 \quad 1],\ Q = \begin{bmatrix} 1 & 0.5 \\ 0.5 & 2 \end{bmatrix},\ R_1 = 1,\ R_1 = 2.$$

Through several iterations, the steady-state covariance matrices can be obtained as:

$$\overline{P}_{11} = \begin{bmatrix} 0.8656 & 0.6412 \\ 0.6412 & 2.6544 \end{bmatrix},\ \overline{P}_{22} = \begin{bmatrix} 1.1354 & -0.3315 \\ -0.3315 & 1.1855 \end{bmatrix},\ \overline{P}_{12} = \begin{bmatrix} 0.0080 & 0.0602 \\ -0.9288 & 1.2829 \end{bmatrix}.$$

Suppose that the probability λ_i ($i = 1, 2$) of successful data reception between the user's FC and the two local sensors are 0.7 and 0.9, respectively. Both channels are

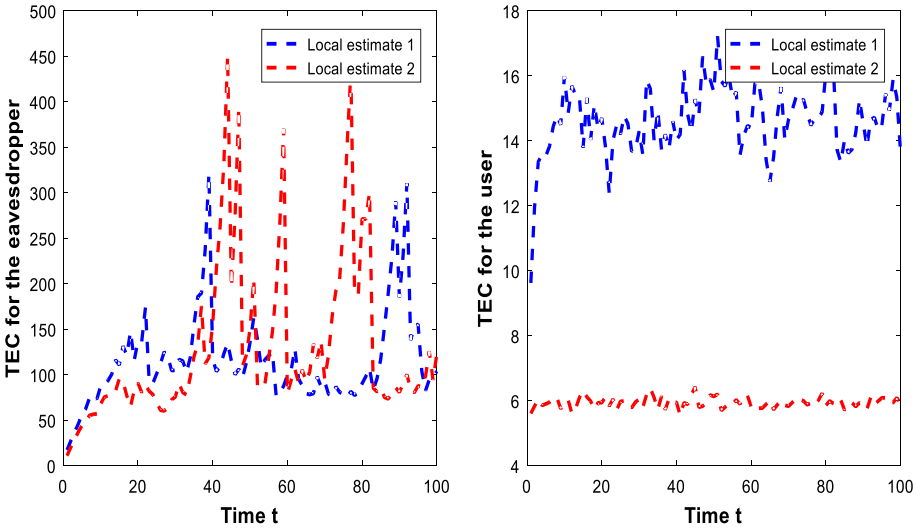

Fig. 2 The TEC of final local estimates without event triggers

eavesdropped, and the data interception probability ρ_i $(i = 1, 2)$ are both 0.4. We can calculate the values of $\frac{1}{\lambda_i}(1 - \frac{1}{\rho(A)^2})$ $(i = 1, 2)$ as 0.5080 and 0.3951 respectively, and the values $\frac{1}{\rho_i}(1 - \rho(A)^{-\frac{2}{L}})$ $(i = 1, 2)$ are both 0.4932. All results are 1000 Monte Carlo simulations. To better interpret the simulation results, we define the following abbreviations: trace of error covariance (TEC), and trace of fusion error covariance (TFEC).

First, we do not set event triggers for all local sensors, and observe the fusion estimation performance for the eavesdropper and the user. In fact, this is equivalent to making the event trigger thresholds η_i $(i = 1, 2)$ of both sensors. The specific simulation results are shown in Figs. 2 and 3.

Figure 2 shows the final LE error covariance curve of the eavesdropper and user's FC, and Fig. 3 shows the trace curve of their fusion estimation error covariance. It is seen that the final LE error of the eavesdropper is much larger than that of the user. This is because the successful reception rate of the user's FC is higher than that of the eavesdropper. Notice that both the eavesdropper and the user can obtain much smaller estimation error than the final local estimation through the fusion estimation method. Therefore, the fusion estimation can greatly reduce the user's state estimation error, but at the same time, it may lead to more state privacy disclosure. Next, the anti-eavesdropping strategy based on event triggering is verified.

The stochastic event triggers are designed for two local sensors according to (10). Let the trigger thresholds combinations for two local sensors be (0.4, 0.4), (0.45, 0.9), (0.9, 0.9). The specific simulation results are shown in Figs. 4 and 5.

Figure 4 shows the final local estimation curve of the eavesdropper's FC, and Fig. 5 reflects the fusion estimation performance under different event trigger threshold combinations of two sensors. It is seen from Fig. 4 that the eavesdropper's TEC grows unbounded when the communication rate between the sensors and the FC is low. From Fig. 5, when the trigger thresholds is selected as (0.4, 0.4), the eavesdropper's estimation performance is poor. Its TFEC grows unbounded over time. This is because the sufficiency condition (15) is satisfied under this communication rate combination, so that the

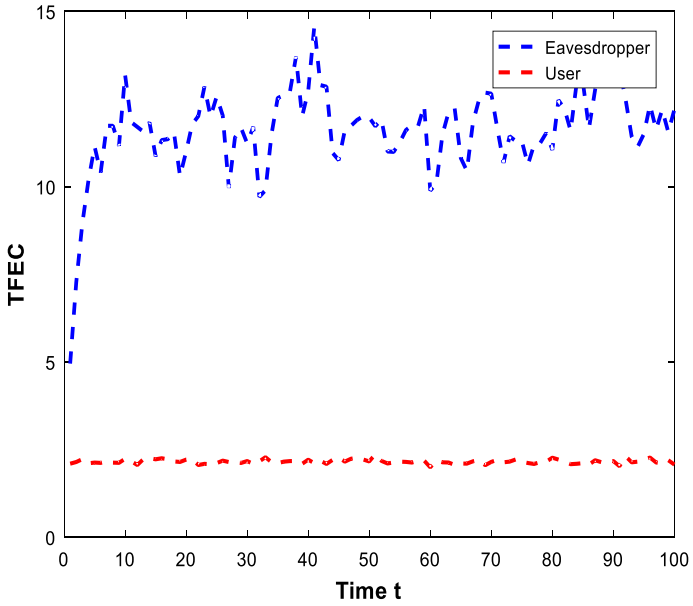

Fig. 3 The TFEC without event triggers

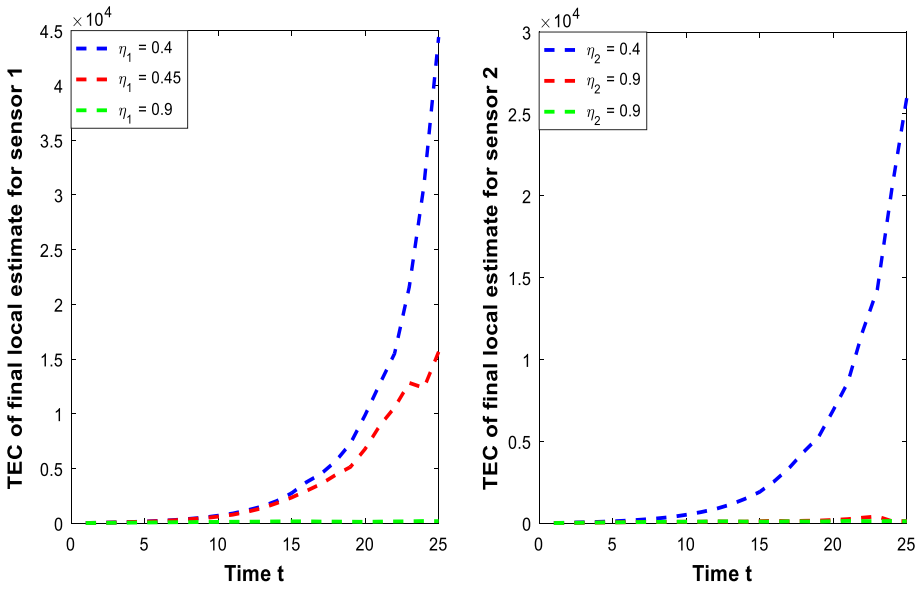

Fig. 4 The TEC of final local estimate for the eavesdropper

eavesdropper cannot obtain the real state information. In this case, the user's TFEC is bounded. This is because the user's FC has a high successful rate of receiving data from the local sensors, which makes the sufficiency condition (14) satisfied. For other combinations, the conditions (14) and (15) are not satisfied at the same time. The eavesdropper can always obtain a bounded estimation error, which makes the event trigger invalid. Therefore, in order to prevent the disclosure of state privacy, the user must design smaller trigger thresholds so that the sufficiency conditions of Theorem 1 are satisfied.

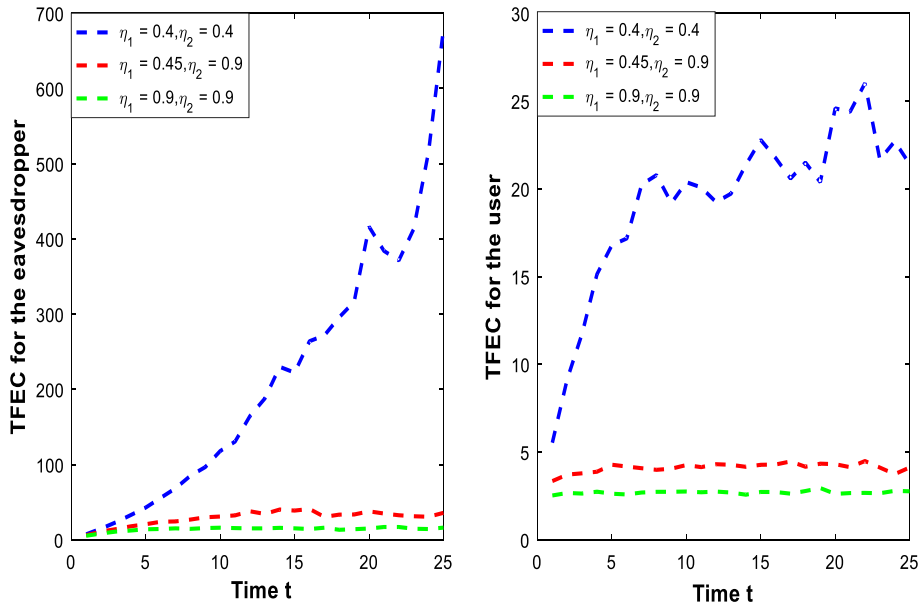

Fig. 5 TFEC with different trigger thresholds

5 Conclusions

This paper studied the state privacy protection of distributed fusion estimation for CPSs. The goal was to make the TFEC matrix of the eavesdropper become unbounded over time while the expected error covariance for the user remained bounded. The random event triggering strategy was adopted to maintain confidentiality. The relationship between event triggering thresholds and estimation performance in FC was established. Some sufficient conditions of trigger thresholds were derived to guarantee the Perfect Expected Secrecy. Finally, a simulation example was employed to verify the effectiveness of the proposed method. Future research topics include (1) the privacy protection for stable systems; (2) the perfect encryption strategies based on encryption and decryption, and (3) the encryption strategy design and security fusion estimation for nonlinear systems.

Abbreviations

CPSs	Cyber-physical systems
FC	Fusion center
AN	Artificial noise
LE	Local estimator
TEC	Trace of error covariance
TFEC	Trace of fusion error covariance

Acknowledgements
The authors thank the editor and anonymous reviewers for their helpful comments and valuable suggestions.

Author contributions
Methodology, D.X.; software, Z.C.; formal analysis, D.X., Z.C. and H.W.; investigation, D.X.; resources, Z.C. and H.W.; data curation, Z.C.; writing—D.X. and Z.C.; writing—review and editing, H.W.; project administration, Z.C.; funding acquisition, D.X. and H.W. All authors have read and agreed to the published version of the manuscript.

Funding
This research was funded by Natural Science Foundation of Zhejiang Province, Grant No. LZY23F030001, LZY22E050003, LZY22E050005, and the Quzhou Science and Technology Plan Project under Grant 2023K223, 2022K100, 2021F013.

Availability of data and materials
Please contact authors for data requests.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare that they have no competing interests.

Received: 9 October 2023 Accepted: 20 February 2024
Published online: 25 April 2024

References

1. G. Cisotto, M. Capuzzo, A.V. Guglielmi et al., Feature stability and setup minimization for EEG-EMG-enabled monitoring systems. EURASIP J. Adv. Signal Process. **2022**(1), 1–22 (2022)
2. A.S.S. Thuluva, M.S. Somanathan, R. Somula et al., Secure and efficient transmission of data based on Caesar Cipher Algorithm for Sybil attack in IoT. EURASIP J. Adv. Signal Process. **2021**, 1–23 (2021)
3. Q. Yang, S. Jagannathan, Reinforcement learning controller design for affine nonlinear discrete-time systems using online approximators. IEEE Trans. Syst. Man Cybern. Part B Cybern. **42**(2), 377–390 (2011)
4. Q. Yang, W. Cao, W. Meng, J. Si, Reinforcement-learning-based tracking control of waste water treatment process under realistic system conditions and control performance requirements. IEEE Trans. Syst. Man Cybern. Syst. **52**(8), 5284–5294 (2022)
5. A. Arunan, Y. Qin, X. Li, C. Yuen, A federated learning-based industrial health prognostics for heterogeneous edge devices using matched feature extraction. IEEE Trans. Autom. Sci. Eng. (2023). https://doi.org/10.1109/TASE.2023.3274648
6. S.Y. Lai, B. Chen, T. Li, L. Yu, Packet-based feedback control under Dos attacks in cyber-physical systems. IEEE Trans. Circuits Syst. II Express Briefs **66**(8), 1421–1425 (2019)
7. B. Chen, D. Ho, G.Q. Hu, L. Yu, Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks. IEEE Trans. Cybern. **48**(6), 1862–1876 (2018)
8. Z. Ruan, Q. Yang, S.S. Ge, Y. Sun, Adaptive fuzzy fault tolerant control of uncertain MIMO nonlinear systems with output constraints and unknown control directions. IEEE Trans. Fuzzy Syst. **30**(5), 1224–1238 (2022)
9. K. Q. Zhou, Y. Qin, C. Yuen, Lithium-ion battery online knee onset detection by matrix profile. arXiv preprint arXiv:2304.00691 (2023)
10. Y. Qin, A. Auran, C. Yuen, Digital twin for real-time Li-ion battery state of health estimation with partially discharged cycling data. IEEE Trans. Ind. Inf. **19**(5), 7247–7257 (2023)
11. B. Chen, G.Q. Hu, D. Ho, L. Yu, Distributed covariance intersection fusion estimation for cyber-physical systems with communication constraints. IEEE Trans. Autom. Control **61**(12), 4020–4026 (2018)
12. K. Koo, D. Moo, J.H. Huh et al., Attack graph generation with machine learning for network security. Electron. **11**(9), 1332 (2022)
13. Q.N. Wang, H.B. Mu, Privacy-preserving and lightweight selective aggregation with fault-tolerance for edge computing-enhanced IoT. Sens. **21**(16), 5369 (2021)
14. B. Chen, D. Ho, W. Zhang, L. Yu, Distributed dimensionality reduction fusion estimation for cyber-physical systems under DoS attacks. IEEE Trans. Syst. Man Cybern. **49**(2), 455–468 (2019)
15. C. Shannon, Communication theory of secrecy systems. Bell Syst. Tech. J. **28**(4), 656–715 (1949)
16. S. William, *Cryptography and network security: principles and practices* (Pearson Education India, Noida, 2006)
17. A. Tsiamis, K. Gatsis, G.J. Pappas, State estimation with secrecy against eavesdroppers. In *Proceedings of IFAC world congress*, Toulouse, France, pp. 8715–22 (2017)
18. A.S. Leong, D.E. Quevedo, D. Dolz, Transmission scheduling for remote state estimation over packet dropping links in the presence of an eavesdropper. IEEE Trans. Autom. Control. **64**(9), 3732–3739 (2019)
19. J. Lu, A.S. Leong, D.E. Quevedo, Optimal event-triggered transmission scheduling for privacy-preserving wireless state estimation. Int. J. Robust Nonlinear Control **30**(11), 4205–4224 (2020)
20. A. Tsiamis, K. Gatsis, G. Pappas, State-secrecy codes for networked linear systems. IEEE Trans. Autom. Control **65**(5), 2001–2015 (2019)
21. A. Tsiamis, K. Gatsis, G. Pappas, An information matrix approach for state secrecy. In *Proceedings of the Conference on Decision and Control*, Fontainebleau Miami Beach, United States, 17–19 December 2018; pp. 2062–2067(2018)
22. A. Tsiamis, K. Gatsis, G. Pappas, State-Secrecy Codes for Stable Systems. In *Proceedings of the Annual American Control Conference* , Milwaukee WI, USA, 27–29, 2018; pp. 171–17(2018)
23. L.Y. Huang, A.S. Leong, D.E. Quevedo, L. Shi, Finite time encryption schedule in the presence of an eavesdropper with operation cost. arXiv preprint arXiv:1903.11763 (2019).
24. D. X. Xu, B. Chen, L. Yu, Secure fusion estimation against eavesdroppers. In *Proceedings of the 37th Chinese control conference*, Wuhan, China, 25–27 July 2018; pp. 4310–4315 (2018)
25. D.X. Xu, B. Chen, L. Yu, W.A. Zhang, Secure dimensionality reduction fusion estimation against eavesdroppers in cyber–physical systems. ISA Trans. **104**, 154–161 (2020)
26. X.H. Yan, Y.C. Zhang, D.X. Xu, B. Chen, Distributed confidentiality fusion estimation against eavesdroppers. IEEE Trans. Aerosp. Electron. Syst. **58**(4), 3633–3642 (2021)

27. L. Zou, Z.D. Wang, B. Shen, H.L. Dong, G.P. Lu, Encrypted finite-horizon energy-to-peak state estimation for time-varying systems under eavesdropping attacks: tackling secrecy capacity. IEEE/CAA J Autom Sin **10**(4), 985–996 (2023)
28. L. Zou, Z.D. Wang, B. Shen, H.L. Dong, Encryption-decryption-based state estimation with multi-rate measurements against eavesdroppers: a recursive minimum-variance approach. IEEE Trans. Autom. Control (2023). https://doi.org/10.1109/TAC.2023.3288624
29. D.X. Xu, B. Chen, Y.C. Zhang, L. Yu, Energy-constrained confidentiality fusion estimation against eavesdroppers. IEEE Trans. Circuits Syst. II Express Briefs **69**(2), 624–628 (2021)
30. D.X. Xu, B. Wang, L. Zhang, A new adaptive high-degree unscented Kalman filter with unknown process noise. Electron. **11**(12), 1863 (2020)
31. A. Jazwinski, *Stochastic processes and filtering theory* (Academic, New York, 1970)
32. B. Li, Y. Lu, H.R. Karimi, Adaptive fading extended Kalman filtering for mobile robot localization using a doppler–azimuth radar. Electron. **10**(20), 2544 (2021)
33. L. Shi, P. Cheng, J.M. Chen, Sensor data scheduling for optimal state estimation with communication energy constraint. Autom. **47**(8), 1693–1698 (2011)
34. H. Zhang, Y.F. Qi, J.F. Wu, L. Fu, L.D. He, DoS attack energy management against remote state estimation. IEEE Trans. Control Network Syst. **5**(1), 383–394 (2016)
35. Y. Gao, Z. Deng, Robust integrated covariance intersection fusion Kalman estimators for networked mixed uncertain time-varying systems. IMA J. Math. Control. Inf. **38**(1), 232–266 (2021)
36. M. Sun, M.E. Davies, I.K. Proudler, Adaptive kernel Kalman filter. IEEE Trans on Signal Process. **71**, 713–726 (2023)
37. P. A. Regalia, A. Khisti, Y. Liang, S. Tomasin, Secure communications via physical-layer and information-theoretic techniques. In *Proceeding of the IEEE* 2015, 103, pp. 1698–1701 (2015)
38. T. Rhouma, J.Y. Keller, M.N. Abdelkrim, A Kalman filter with intermittent observations and reconstruction of data losses. Int. J. Appl. Math. Comput. Sci. **32**(2), 241–253 (2022)
39. J. Qin, J. Wang, L. Shi et al., Randomized consensus-based distributed Kalman filtering over wireless sensor networks. IEEE Trans. Autom. Control **66**(8), 3794–3801 (2020)

Publisher's Note