The following publication X. Yan, D. E. Quevedo, B. Chen and H. Huang, "Aggregation-Based Remote State Estimation Secrecy With Pseudo-Random Numbers for Networked Systems," in IEEE Transactions on Control Systems Technology, vol. 34, no. 2, pp. 657-670, March 2026 is available at https://doi.org/10.1109/TCST.2025.3628009.

Aggregation-Based Remote State Estimation Secrecy with Pseudo-Random Numbers for Networked Systems

Xinhao Yan, *Graduate Student Member, IEEE*, Daniel E. Quevedo, *Fellow, IEEE*, Bo Chen, *Senior Member, IEEE*, Hailong Huang, *Senior Member, IEEE*

***Abstract*—This paper is concerned with the remote state estimation secrecy problem for networked systems in the presence of eavesdroppers. The majority of current research centers on one kind of eavesdropper that is equipped with predefined estimation structures. To enhance the resistance against eavesdroppers, we simultaneously consider two distinct categories of logical eavesdroppers in this paper, namely: *smart eavesdroppers*, who possess the same level of knowledge as legitimate users, and *naive eavesdroppers*, who remain oblivious to the encoding process. Moreover, we propose an innovative aggregation-based secrecy code that employs pseudo-random numbers, incorporating both a pseudo-random real-number sequence and a pseudo-random binary scheduler. Also, an α-relative secrecy is proposed by introducing a relax variable, which offers higher flexibility than the traditional relative secrecy. Then, both the classical perfect secrecy and the newly proposed α-relative secrecy are proven under specific conditions. Furthermore, the estimation performance for users and eavesdroppers can be tuned by designing the aggregation structure and the probability distribution of the pseudo-random samples, rather than being solely determined by the communication channel characteristics as in previous work. Finally, the effectiveness of the proposed coding method is verified through numerical experiments conducted on two systems with differing stability characteristics.**

***Index Terms*—Remote state estimation, eavesdropping attacks, data aggregation, pseudo-random numbers, networked systems, packet dropping.**

I. Introduction

Cyber-physical systems (CPSs) represent highly intricate engineering integrations that coordinate, regulate, and incorporate perceptual and computational components [1]. They have been utilized in diverse fields, encompassing wireless sensor-actuator networks [2], multi-sensor fusion system [3], direct current microgrids [4], and unmanned systems [5]. Remote state estimation has gained significant attention as a crucial aspect of CPSs, because it offers real-time monitoring and supervision capabilities to these systems [6]. However, due to the increasing network openness and the remote interconnectivity among various parties of CPSs, the remote state estimators are vulnerable to a variety of cyberattacks [7], such as denial of service attacks [8]–[10], false data injection attacks [11], [12], and eavesdropping attacks [13]–[15]. It should be noted that the eavesdropping attacks can cause severe risks by intercepting communications, leading to the information leakage and the occurrences of other active cyberattacks. Hence, countering eavesdroppers has emerged as a vital and pressing research for remote state estimation.

Recently, a variety of privacy-preserving methods have gained significant attention to combat potential eavesdropping threats [13], such as cryptography [16]–[18], random perturbation [19]–[21], and transmission scheduling [15], [22]. Cryptographic approaches focus on encrypting the message with high-complexity secrete keys such that the attacker cannot easily decrypt it. Specifically, secure multi-party computation techniques, for example, homomorphic encryption [17], allow computation to be directly performed on ciphertexts. Perturbation methods aim to increase the uncertainty of transmitted data. Typically, this involves the injection of random noises with careful consideration from privacy metrics such as differential privacy [19] to design the probability distribution of the noises. Moreover, given the inherent unreliability of networks, which may occasionally result in packet dropping, plenty of scheduling or coding approaches have been proposed on the basis of this property. Secrecy codes represent a category that leverages packet dropping to prevent eavesdroppers from acquiring the complete real-time data and then create recursion to exacerbate the adverse impact of such losses [22].

Notice that secrecy codes possess superior estimation performance while consuming less computation resources when compared other encryption approaches, making them widely discussed in secure remote state estimation. The state-secrecy code stands as a cutting-edge method that operates by employing suitably defined noises and system matrices [22]. However, it poses a potential vulnerability to CPSs, since this method necessitates the reliable feedback of acknowledgments (ACKs) while the transmission of ACKs cannot be completely safeguarded and is also susceptible to cyberattacks. A dynamic switching strategy was developed to maintain resilience against flipped ACKs [23], including scenarios of sending both ciphertexts and plaintexts. Then, an enhanced coding scheme operating independently of ACKs was proposed in [24]. It relied on the random alternation between the transmission of system state values and of random noises, which possessed statistical property similar to that of the system state.

Injection of pseudo-random [25] or true-random [20] num-

This study was supported by Otto Poon Charitable Foundation Smart Cities Research Institute, The Hong Kong Polytechnic University.

Xinhao Yan is with the Department of Aeronautical and Aviation Engineering, The Hong Kong Polytechnic University, Hong Kong 999077, China (email: xin-hao-shawn.yan@connect.polyu.hk).

Daniel E. Quevedo is with the School of Electrical and Computer Engineering, The University of Sydney, NSW 2006, Australia (email: dquevedo@ieee.org).

Bo Chen is with the Department of Automation, Zhejiang University of Technology, Hangzhou 310023, China (email: bchen@aliyun.com).

Hailong Huang is with the Department of Aeronautical and Aviation Engineering and Otto Poon Charitable Foundation Smart Cities Research Institute, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong (email: hailong.huang@polyu.edu.hk).

Corresponding author: Hailong Huang.

bers is treated as a typical perturbation approach, since it can enhance the data uncertainty. Meanwhile, the pseudo-random scheduler can be synchronized for both sensor and legitimate user such that the sensor can realize the operation of user without feedback ACKs [24]. Further, a moving horizon summation method [21] was developed to diverge the estimation error of the eavesdropper by adding two-step sequential noises. It should be pointed out that there is only limited work discussing the presence of different kinds of eavesdroppers. Most existing findings only concern smart eavesdroppers [20], [21], which can create sophisticated estimation structures to decode packages. Although some studies do consider naive eavesdroppers that directly use the transmitted data [25], they cannot effectively destroy the performance of such eavesdroppers. Also, directly adding noises [20], [25] can only exaggerate the estimation error while not making its covariance diverge. Motivated by the above analysis, we propose an aggregation-based code in the presence of packet loss that can more effectively degrade the performance of multiple eavesdroppers. The main contributions of this paper can be summarized as follows.

1) Two distinct categories of eavesdroppers are rigorously defined and simultaneously taken into account, which are specifically named as the *smart eavesdropper* and the *naive eavesdropper*. For remote state estimation scenarios where packet dropping occurs, tailored estimators are meticulously designed for the legitimate user and each type of eavesdropper under corresponding definitions.
2) A novel aggregation-based coding approach with pseudo-random numbers is proposed for networked systems in the presence of packet dropping communications. Specifically, this technique involves a pseudo-random binary scheduler that alternates the transmission between the raw state estimate and the code encrypted with a pseudo-random real-number sequence.
3) The performance analyses for legitimate user and eavesdroppers under the proposed code are conducted, including estimation error covariances and their expectations. Following this, we provide conditions based on system stability and communication properties for achieving the secrecy metrics, encompassing the newly proposed low-level α-relative secrecy and the high-level perfect secrecy.

The rest of this paper is organized as follows. Section II provides the remote state estimation secrecy structure in the presence of eavesdroppers. Meanwhile, based on the channel modeling of networked system, the problem to be solved in this paper is discussed. In Section III, we propose the detailed design of aggregation-based coding scheme with pseudo-random numbers. Then, the minimum mean square error (MMSE) estimators for all the legitimate users and eavesdroppers are strictly analyzed. Next, the estimation error covariances for the above various MMSE estimators are discussed in Section IV. Furthermore, Section V discusses the expectations of the above covariances. Meanwhile, based on the calculated expectations, the secrecy targets including α-relative secrecy and perfect secrecy are proved to be achieved. Then, in Section VI, we provide the simulations on two systems with different stability characteristics to thoroughly demonstrate the effectiveness of the proposed methods. Finally, the conclusion of this work is given in Section VII. Besides, a brief summary of the notations that are commonly utilized throughout the entire paper is provided below.

Notations: The superscript "T" means the transpose of a matrix. $\lambda_i(A)$ stands for the i-th eigenvalue of a matrix A and $\rho(A)$ denotes the spectral radius that is calculated by $\rho(A) = \max_i |\lambda_i(A)|$. "$I_n$" represents the identity matrix with dimension n while "$0_{m\times n}$" denotes the zero matrix with dimension $m\times n$. $\operatorname{diag}\{a_1,\ldots,a_n\}$ is a block diagonal matrix and $\operatorname{col}\{a_1,\ldots,a_n\}$ is a column vector, whose corresponding elements are $a_1,\ldots,a_n$. Moreover, $\mathbb{Z}$, $\mathbb{Z}_+$, $\mathbb{R}$, $\mathbb{R}^n$, and $\mathbb{R}^{n\times m}$ respectively represent the sets of integers, positive integers, real numbers, n-dimensional real vectors, and $n\times m$ real matrices. $\mathbb{E}\{\cdot\}$ means the mathematical expectation and $\mathbb{P}\{\cdot\}$ represents the probability of an event. $\operatorname{tr}\{\cdot\}$ stands for the trace of a matrix. $X > (<)0$ represents a positive-definite (negative-definite) matrix, while $X \geq (\leq)0$ represents a non-negative definite (non-positive definite) matrix.

II. Remote State Estimation Secrecy

In this section, we begin with the state-space model and the basic remote state estimation structure of the CPS. Subsequently, we provide the transmission and channel models for both the user and the eavesdropper. Meanwhile, we construct general MMSE estimators for the above parties and summarize the problem to be solved in this paper.

A. Remote State Estimation

Consider the physical process of a CPS described by the following linear time-invariant state transition model:

$$x_{k+1} = Ax_k + w_k, \tag{1}$$

where $x_k \in \mathbb{R}^{n_x}$ represents the state, A is the state transition matrix, and w_k stands for the system process noise at discrete time $k \in \mathbb{Z}_+$. The covariance of the state is defined as $\Sigma_k \triangleq \mathbb{E}\left\{x_k x_k^{\mathrm{T}}\right\}$. Meanwhile, the spectral radius of the system matrix A is denoted by $\rho(A) = \max_i |\lambda_i(A)|$, where $\lambda_i(A)$ denotes the i-th eigenvalue. Then, a smart sensor is deployed to observe the above dynamic of the CPS. In this paper, we consider the linear measurement model that is expressed as

$$y_k = Cx_k + v_k, \tag{2}$$

where $y_k \in \mathbb{R}^{n_y}$ is the measurement, C means the measurement matrix, and v_k denotes the measurement noises that may come from sensing errors or environment disturbances.

Here, we assume that the initial state x_0, the system noise w_k, and the measurement noise v_k are zero-mean Gaussian distributed and mutually independent, satisfying

$$\begin{aligned}&\mathbb{E}\left\{[x_0^{\mathrm{T}}\ w_{k_1}^{\mathrm{T}}\ v_{k_1}^{\mathrm{T}}]^{\mathrm{T}}[x_0^{\mathrm{T}}\ w_{k_2}^{\mathrm{T}}\ v_{k_2}^{\mathrm{T}}]\right\}\\ &\quad= \operatorname{diag}\left\{\Sigma_0, \delta(k_1,k_2)Q, \delta(k_1,k_2)R\right\},\end{aligned} \tag{3}$$

where Σ_0, Q, and R are non-negative definite and represent the covariances of x_0, w_k, and v_k, respectively. Besides, $\delta(k_1,k_2)$ is an indicator function such that $\delta(k_1,k_2) = 1$ if $k_1 = k_2$; otherwise, $\delta(k_1,k_2) = 0$. Meanwhile, the

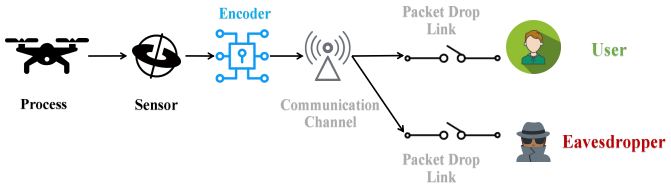

Fig. 1. The overall structure of the remote state estimation for networked systems in the presence of eavesdroppers.

above system is assumed to be controllable and observable, i.e., $\text{rank}\{[\sqrt{Q}\ \ A\sqrt{Q}\ \ \cdots\ \ A^{n_x-1}\sqrt{Q}]\} = n_x$ and $\text{rank}\{[C^{\mathrm{T}}\ \ (CA)^{\mathrm{T}}\ \ \cdots\ \ (CA^{n_x-1})^{\mathrm{T}}]^{\mathrm{T}}\} = n_x$.

In this paper, the smart sensor will compute the state estimates based on its measured data. Thanks to the controllability and observability of the considered system, the following steady-state Kalman filter is directly adopted to reduce computation resource [21]:

$$\hat{x}_k = (I_{n_x} - \bar{K}C)A\hat{x}_{k-1} + \bar{K}y_k. \tag{4}$$

The optimal steady-state Kalman gain $\bar{K}$ is calculated by

$$\bar{K} = \bar{P}^{-}C^{\mathrm{T}}(C\bar{P}^{-}C^{\mathrm{T}} + R)^{-1}, \tag{5}$$

where $\bar{P}^{-}$ is the steady-state prediction error covariance satisfying the following Riccati equation:

$$\begin{aligned}\bar{P}^{-} =& A\bar{P}^{-}A^{\mathrm{T}} + Q \\ &- A\bar{P}^{-}C^{\mathrm{T}}(C\bar{P}^{-}C^{\mathrm{T}} + R)^{-1}C\bar{P}^{-}A^{\mathrm{T}}.\end{aligned} \tag{6}$$

Meanwhile, the steady-state estimation error covariance becomes $\bar{P} = (I_{n_x} - \bar{K}C)\bar{P}^{-}$.

B. Transmission and Channel Models

Due to the existence of potential eavesdroppers, in this work, an encoder will be designed and utilized by the smart sensor to protect data privacy. The general form of the encoder can be described by the following form:

$$z_k \triangleq f_k(y_{1:k}, \hat{x}_{1:k}, \text{PRNs}). \tag{7}$$

Here, $y_{1:k} \triangleq \{y_1, \cdots, y_k\}$ means the whole set of the valid measurements and $\hat{x}_{1:k} \triangleq \{\hat{x}_1, \cdots, \hat{x}_k\}$ represents the corresponding state estimate set. $f_k(\cdot)$ is the encoder function that required to be designed for destroying the performance of eavesdroppers. Specifically, "PRNs" denotes the pseudo-random numbers used to aid in the coding process. After successfully encrypting the state estimates, the output z_k, or so called the ciphertext, will be modulated and sent to the communication network by the smart sensor.

In this paper, we consider the situation where the channels of the network in CPS are unreliable. Owing to a diverse array of unstable factors, network packet dropping arises when data packets from the sensor are unable to reach their designated recipients, generally the legitimate user. These factors span a wide range, encompassing network congestion and constrained bandwidth, as well as hardware malfunctions and environmental circumstances that impede the communication pathway. In this case, there exists a probability that the data packet originating from the remote sensor may be lost or discarded during the networked transmission, and similarly, networked eavesdropping will also introduce the risk of packet dropping.

Here, we define two binary indicators $\gamma_{u,k}$ and $\gamma_{e,k}$ to respectively stand for the successful reception for the legitimate user and the eavesdropper, i.e.,

$$\begin{aligned}\gamma_{u,k} &= \begin{cases}1, & \text{if user receives packet } z_k,\\ 0, & \text{if user does not receive packet } z_k,\end{cases}\\ \gamma_{e,k} &= \begin{cases}1, & \text{if eavesdropper receives packet } z_k,\\ 0, & \text{if eavesdropper does not receive packet } z_k.\end{cases}\end{aligned} \tag{8}$$

The corresponding probabilities of successful receptions are presented as follows:

$$\begin{aligned}\mathbb{P}\{\gamma_{u,k} = 1\} =& \mu_u, \quad (0 \le \mu_u \le 1),\\ \mathbb{P}\{\gamma_{e,k} = 1\} =& \mu_e, \quad (0 \le \mu_e \le 1).\end{aligned} \tag{9}$$

Obviously, the failure rates are $(1-\mu_u)$ and $(1-\mu_e)$. Besides, we assume that all the communication channels are independent with each other, i.e., $\gamma_{u,k}$ and $\gamma_{e,k}$ are independent random variables and $\mathbb{E}\{\gamma_{u,k}\gamma_{e,k}\} = 0$.

Furthermore, we delve into a more challenging scenario, in which the transmission is one-way. More concretely, the sensor is the only entity responsible for dispatching its data to the user, with no requirement for the user to transmit ACKs, feedback, or any other synchronous information in real time. Such an unidirectional structure can improve efficiency, reduce latency, and enhance the scalability of the CPS. However, it also poses the unique difficulty of ensuring data integrity and minimizing performance loss, as there is no immediate mechanism for the sensor to verify whether its packets have been successfully received. The overall structure of the remote state estimation for networked systems in the presence of eavesdroppers is shown in Fig. 1.

C. MMSE Estimation

Obviously, the legitimate user knows all the encoding information, because it is the intended recipient of the communication and typically has access to the most comprehensive and accurate information set. In this case, its valid data set for state estimation can be constructed as $\mathcal{I}_{u,k} \triangleq \{h_{u,1:k}, f_{1:k}, \text{PRNs}\}$, where $h_{u,1:k} \triangleq \{h_{u,1}, \cdots, h_{u,k}\} = \{\gamma_{u,1}z_1, \cdots, \gamma_{u,k}z_k\}$ represents all the received packages. Then, the minimum mean square error (MMSE) estimate for the legitimate user can be generally expressed by

$$\begin{aligned}\hat{x}_{u,k} &= \mathbb{E}\{x_k|\mathcal{I}_{u,k}\},\\ P_{u,k} &= \mathbb{E}\{(x_k - \hat{x}_{u,k})(x_k - \hat{x}_{u,k})^{\mathrm{T}}|\mathcal{I}_{u,k}\}.\end{aligned} \tag{10}$$

Notice that an eavesdropper's capability of wiretapping can be influenced by several factors, such as technical proficiency, access to advanced eavesdropping equipment, and the proximity to the target communication network. Therefore, the eavesdroppers possess distinct and generally unequal information sets due to their varying abilities. The segmentation of eavesdroppers is crucial as it allows for a more nuanced understanding of the different types of eavesdropping activities, enabling more effective countermeasures to be implemented.

Here, the eavesdropping data set is generally defined as $\mathcal{I}_{e,k}$ that contains $h_{e,1:k} = \gamma_{e,k} z_{1:k}$ and other possible information. Also, it is pivotal to point out that, despite the varying abilities of eavesdroppers and the resulting diversity in their information sets, none of these sets will surpass the completeness of the information possessed by the legitimate user, i.e., $\mathcal{I}_{e,k} \subseteq \mathcal{I}_{u,k}$. Then, the MMSE estimate for an eavesdropper will be described as

$$\begin{aligned} \hat{x}_{e,k} &= \mathbb{E}\{x_k | \mathcal{I}_{e,k}\}, \\ P_{e,k} &= \mathbb{E}\{(x_k - \hat{x}_{e,k})(x_k - \hat{x}_{e,k})^{\mathrm{T}} | \mathcal{I}_{e,k}\}. \end{aligned} \tag{11}$$

To summarize, the primary aim is to designed a secrecy code mechanism f_k, which can maintain the high performance of the legitimate estimator and maximize, better diverge, that of the eavesdroppers. Moreover, we will thoroughly discuss the estimators employed by each eavesdropper, and carefully analyze their respective performances and the impact that the secrecy code mechanism has on them.

Remark 2.1: It is worth noting that the proposed secrecy code operates independently of the local estimation structure of the sensor. This implies that smart sensors can also employ other types of estimators with varying performance metrics. This flexibility stems from the fact that the coding mechanism utilized by the sensor is designed for state estimates rather than raw measurements. Consequently, the coding process is indifferent to the specific estimation methodology adopted. Nonetheless, the privacy metric shall be re-evaluate due to the differing performances of alternative local estimates.

III. Aggregation-Based Code with Pseudo-Random Numbers

In this section, we aim to develop an encoding method that delivers a relatively optimal state estimate to the legitimate user while preventing eavesdroppers from accurately estimating the states. This design is of great significance, because providing the user a precise state estimate can greatly improve the performance of many applications. At the same time, destroying the performance of eavesdroppers can maintain trust and reliability in the communication system.

At the start, we introduce a pseudo-random real-number sequence denoted as $\beta_k (\neq 0)$, which can be generated by deterministic algorithms starting from an initial seed, such as linear congruential generator (LCG) [26]. It is designed to exhibit random-like characteristics while maintaining a degree of determinism, allowing it to serve as a foundation for our encoding method. The statistical properties of this sequence are assumed to possess a mean of μ_β and a covariance of Q_β. In parallel, we introduce another pseudo-random binary scheduler η_k. Besides, it is assumed that all the mentioned pseudo-random numbers are well synchronized. The probability of η_k taking the value of 1, or the mathematical expectation, is μ_η, i.e.,

$$\mathbb{P}\{\eta_k = 1\} = \mu_\eta \ (0 \leq \mu_\eta \leq 1). \tag{12}$$

Also, we assume that this indicator is independent of the above packet dropping indicators.

With the above pseudo-random sequence and scheduler, an aggregation-based encoder is proposed in this work to encrypt the remote state estimate as follows:

$$z_k = \begin{cases} \hat{x}_k, & \text{if } \eta_k = 0, \\ \beta_k(\hat{x}_{k-1} + \hat{x}_k), & \text{if } \eta_k = 1. \end{cases} \tag{13}$$

In other words, the plaintext, i.e., the raw state estimate, will be sent when $\eta_k = 0$, while the ciphertext, i.e., the aggregation results with pseudo-random number multiplication, will be transmitted when $\eta_k = 1$. Here, we treat β_k and η_k or their corresponding pseudo-random seeds as the synchronous key PRNs, and they can be acquired by the legitimate user.

Then, from the perspective of the legitimate user, it has access to the key PRNs and thus can successfully recover the complete pseudo-random sequence β_k and scheduler η_k. This implies that the user is aware of the aggregation-based encoding structure and it can apply the difference for decoding. Besides, due to the possible packet dropping, the user has to consider one-step prediction $A\hat{x}_{u,k-1}$ to minimize the mean square errors (MSEs). Then, the detailed estimator design for the legitimate user can be delineated as follows:

$$\hat{x}_{u,k} = \begin{cases} A\hat{x}_{u,k-1}, & \text{if } (\gamma_{u,k} = 0 \ \& \ \forall \ \eta_k), \\ z_k, & \text{if } (\gamma_{u,k} = 1 \ \& \ \eta_k = 0), \\ \dfrac{z_k}{\beta_k} - \hat{x}_{u,k-1}, & \text{if } (\gamma_{u,k} = 1 \ \& \ \eta_k = 1). \end{cases} \tag{14}$$

For eavesdroppers, their estimators should be categorized based on their respective capabilities as previously mentioned. In this work, we distinguish between two types of eavesdroppers, referred to as the *smart eavesdropper* and the *naive eavesdropper*. First, according to Kerckhoffs' principle [27], all the information except for secret keys can be known to the eavesdropper. In this case, the encoding structure should not be assumed to be protected and it could be acquired by the smart eavesdropper. Meanwhile, the pseudo-random numbers are not complicated enough to be treated as secret key. Therefore, the worst case is that the eavesdropper knows all the valid information of the proposed coding scheme, and we define such an adversary as a smart eavesdropper.

Definition 3.1: (Smart Eavesdropper) A smart eavesdropper has comprehensive access to all relevant system information, including the system dynamics, the structure of the encoder, and the real-time access to the transmitted data. It can effectively decode, analyze, and potentially manipulate the intercepted communications.

Specifically, according to the above definition, a smart eavesdropper knows the encoding function $f_{1:k}$ and the synchronous key PRNs. Hence, its estimator can be designed exactly the same way as that of the legitimate user:

$$\hat{x}^s_{e,k} = \begin{cases} A\hat{x}^s_{e,k-1}, & \text{if } (\gamma_{e,k} = 0 \ \& \ \forall \ \eta_k), \\ z_k, & \text{if } (\gamma_{e,k} = 1 \ \& \ \eta_k = 0), \\ \dfrac{z_k}{\beta_k} - \hat{x}^s_{e,k-1}, & \text{if } (\gamma_{e,k} = 1 \ \& \ \eta_k = 1). \end{cases} \tag{15}$$

Moreover, in this work, we recognize the existence of not only the smart eavesdroppers who possess advanced techniques and resources, but also the naive eavesdroppers. These eavesdroppers, unlike the smarter counterparts, may lack the

TABLE I
AN EXAMPLE OF THE COMPARISON FOR THE DATA UNDER VARIOUS CODING SCHEMES.

System Parameters	time step k	0	1	2	3
	indicator $\gamma_{u,k}$	0	1	1	1
	indicator $\gamma_{e,k}$	1	0	1	1
State-Secrecy Code in [22]	coding result z_k	$\hat{x}_0$	$\hat{x}_1$	$\hat{x}_2 - A\hat{x}_1$	$\hat{x}_3 - A\hat{x}_2$
	user $h_{u,k}$	0	$\hat{x}_1$	$\hat{x}_2 - A\hat{x}_1$	$\hat{x}_3 - A\hat{x}_2$
	eavesdropper $h_{e,k}$	$\hat{x}_0$	0	$\hat{x}_2 - A\hat{x}_1$	$\hat{x}_3 - A\hat{x}_2$
Scheduled State-Secrecy Code in [24]	scheduler v_k	0	1	0	1
	coding result z_k	$\hat{x}_0$	$\hat{x}_1 - A\hat{x}_0 + \chi_1$	$\hat{x}_2$	$\hat{x}_3 - A\hat{x}_2 + \chi_3$
	user $h_{u,k}$	0	$\hat{x}_1 - A\hat{x}_0 + \chi_1$	$\hat{x}_2$	$\hat{x}_3 - A\hat{x}_2 + \chi_3$
	eavesdropper $h^s_{e,k}$	$\hat{x}_0$	0	$\hat{x}_2$	$\hat{x}_3 - A\hat{x}_2 + \chi_3$
Aggregation-Based Code in This Paper	pseudo-random sequence β_k	0	1	2	3
	pseudo-random scheduler η_k	0	1	1	1
	coding result z_k	$\hat{x}_0$	$\hat{x}_1 + \hat{x}_0$	$2(\hat{x}_2 + \hat{x}_1)$	$3(\hat{x}_3 + \hat{x}_2)$
	user $h_{u,k}$	0	$\hat{x}_1 + \hat{x}_0$	$2(\hat{x}_2 + \hat{x}_1)$	$3(\hat{x}_3 + \hat{x}_2)$
	eavesdropper $h^s_{e,k}$	$\hat{x}_0$	0	$2(\hat{x}_2 + \hat{x}_1)$	$3(\hat{x}_3 + \hat{x}_2)$

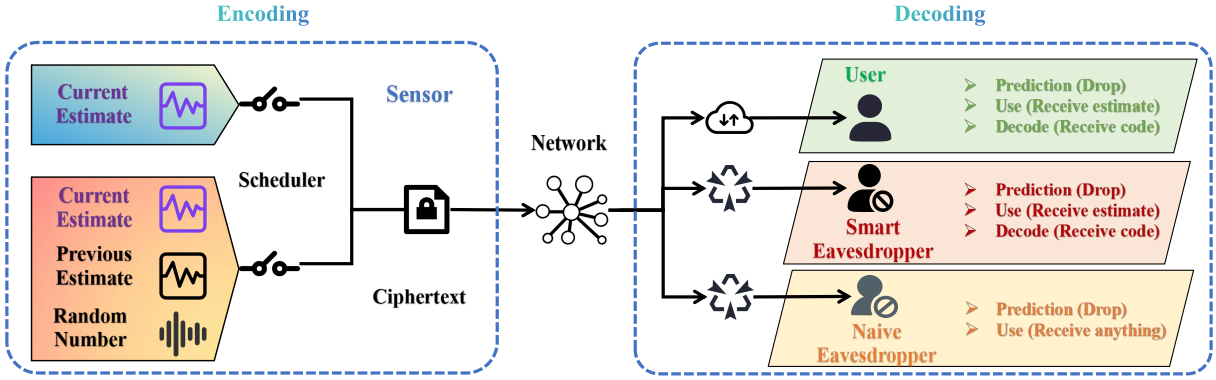

Fig. 2. The overall system structure with both encoding and decoding for the remote state estimation in the presence of the eavesdroppers.

technical expertise or knowledge to effectively understand or manipulate the decoding operations, and we propose the detailed definition as follows.

Definition 3.2: (Naive Eavesdropper) A naive eavesdropper has access to the data being transmitted in real time, while it lacks knowledge of the underlying coding mechanisms used to encode or encrypt the data. As a result, the naive eavesdropper treats the received signals as plain and unencoded information, devoid of any extra operations.

Based on this definition, the naive eavesdropper will directly treat the transmitted data as its original type, i.e., the real-time state estimates from the sensor. This leads to the following naive state estimator:

$$\hat{x}^n_{e,k} = \begin{cases} A\hat{x}^n_{e,k-1}, & \text{if } (\gamma_{e,k} = 0 \ \& \ \forall \ \eta_k), \\ z_k, & \text{if } (\gamma_{e,k} = 1 \ \& \ \forall \ \eta_k). \end{cases} \tag{16}$$

By considering all the encoding and decoding processes mentioned above, the overall system structure for the networked remote state estimation in the presence of the eavesdroppers is illustrated in Fig. 2. Meanwhile, we provide a detailed example to compare the data under various coding schemes in TABLE I, including original state-secrecy code in [22], scheduled secrecy code in [24], and the aggregation-based code proposed in this paper.

Moreover, we employ MMSE as a benchmark to evaluate the estimation performance of all the parties. Given the varying performance capabilities of eavesdroppers, we introduce two privacy metrics to provide a comprehensive assessment, which are both based on the expected MMSE. First, we introduce a concept of secrecy called α-relative secrecy.

Definition 3.3: (α-Relative Secrecy) The relative secrecy is achieved when the following conditions hold. First, the trace of the legitimate user's expected MMSE is bounded, i.e., there exists a constant Ω_u such that

$$\mathrm{tr}\{\mathbb{E}\{P_{u,k}\}\} < \Omega_u, \ \forall \ k. \tag{17}$$

Second, the trace of the eavesdropper's expected MMSE is bounded, i.e., there exists a constant Ω_e such that

$$\mathrm{tr}\{\mathbb{E}\{P_{e,k}\}\} < \Omega_e, \ \forall \ k. \tag{18}$$

Meanwhile, the trace of the legitimate user's expected MMSE, when multiplied by $\alpha \in \mathbb{Z}_+$, is less than that of the eavesdropper's, i.e.,

$$\alpha \cdot \mathrm{tr}\{\mathbb{E}\{P_{u,k}\}\} < \mathrm{tr}\{\mathbb{E}\{P_{e,k}\}\}, \ \forall \ k. \tag{19}$$

Compared with the traditional relative privacy [24], a relax variable α is introduced to further enhance the flexibility and provide the quantitative secrecy level. Nevertheless, it still represents a somewhat lenient condition, because the eavesdropper may possess relative high estimation performance as legitimate user. Therefore, we introduce a metric with high privacy level below, which is called perfect secrecy. It indicates that the user's performance is optimal and the eavesdroppers' covariance grows unbounded.

Definition 3.4: (Perfect Secrecy) The perfect secrecy is achieved when both the following two conditions hold. First, the trace of the legitimate user's MMSE performance is bounded, i.e., there exist a constant Ω such that

$$\mathrm{tr}\{\mathbb{E}\{P_{u,k}\}\} < \Omega, \ \forall \ k. \tag{20}$$

Second, the trace of the eavesdropper's MMSE performance grows unbounded, i.e.,

$$\lim_{k\to\infty} \mathrm{tr}\{\mathbb{E}\{P_{e,k}\}\} \to \infty. \tag{21}$$

Remark 3.1: It should be noted that the proposed smart eavesdropper differs significantly from that presented in [24]. That particular eavesdropper is not classified as the strongest due to its limitation of not knowing whether the data it intercepts is encrypted. In fact, according to Kerckhoff's principle, a fundamental concept in cryptography, the strongest eavesdropper should ideally possess all the knowledge about the system except for certain secrete keys. In this case, the smart eavesdropper emerges as a more potent threat, and its corresponding estimator proposed in this paper demonstrates superior performance when compared to that in [24].

Remark 3.2: The majority of existing research papers primarily focus on smart eavesdroppers possessing specific state estimation structures, while scant attention has been devoted to the scenarios involving naive eavesdroppers. In fact, numerous practical eavesdroppers are naive, because they always commence their interception halfway after system initialization. This means that they are unaware of certain initial conditions, encompassing the coding mechanism and other private information. Hence, a naive eavesdropper only tries to directly utilize the received data for estimation.

Remark 3.3: Note that the pseudo-random number is directly added in [24]. The straightforward addition of a pseudo-random number cannot effectively destroy the performance for the eavesdropper, and in most cases, it cannot produce significant divergence [25]. By contrast, in our approach, we apply the pseudo-random numbers to multiply certain data during the encryption process. Such a strategy can thwart some uninformed eavesdroppers, including the naive eavesdropper defined in this work, thanks to to the rapid divergence introduced by the multiplication process.

IV. Estimation Error Covariance Analysis

In this section, we analyze the estimation performance for all parties involved, including the legitimate user and the eavesdroppers. Specifically, we calculate their estimation error covariances based on the proposed encoder and the previously mentioned estimator designs.

A. User Estimation Error Covariance

Under the proposed coding scheme, we first analyze the estimation performance for the legitimate user, mainly related to the estimation error covariance of the estimator in (14). The segmented covariance corresponding to each possible case is derived in the following theorem.

Theorem 4.1: The estimation error covariance for the legitimate user's estimator (14) under the aggregation-based code (13) can be described by

$$P_{u,k} = \begin{cases} AP_{u,k-1}A^{\mathrm{T}} + Q, & \text{if } (\gamma_{u,k} = 0 \ \& \ \forall \ \eta_k), \\ \bar{P}, & \text{if } (\gamma_{u,k} = 1 \ \& \ \eta_k = 0), \\ P_{u,k-1} + \Gamma_{u,k-1}, & \text{if } (\gamma_{u,k} = 1 \ \& \ \eta_k = 1), \end{cases} \tag{22}$$

where

$$\begin{aligned} \Gamma_{u,k} =& (I_{n_x} + A - \bar{K}CA)\bar{P}(I_{n_x} + A - \bar{K}CA)^{\mathrm{T}} \\ & - (I_{n_x} + A - \bar{K}CA)\Phi_{u,k}^{\mathrm{T}} \\ & - \Phi_{u,k}(I_{n_x} + A - \bar{K}CA)^{\mathrm{T}} \\ & + (I_{n_x} - \bar{K}C)Q(I_{n_x} - \bar{K}C)^{\mathrm{T}} + \bar{K}R\bar{K}^{\mathrm{T}}, \\ \Phi_{u,k} =& -\Phi_{u,k-1}M + N, \\ M =& (A - \bar{K}CA)^{\mathrm{T}}, \\ N =& (I_{n_x} + A - \bar{K}CA)\bar{P}(A - \bar{K}CA)^{\mathrm{T}} \\ & + (I_{n_x} - \bar{K}C)Q(I_{n_x} - \bar{K}C)^{\mathrm{T}} + \bar{K}R\bar{K}^{\mathrm{T}}. \end{aligned} \tag{23}$$

Proof 1: For legitimate user, there exist three possible different usages of packages, each serving different purposes and requirements. These usages reflect functionality of the packages in various application scenarios, and we require to compute them respectively. In the first case, the package will be discarded and the user cannot receive anything from the communication network, i.e., $(\gamma_{u,k} = 0 \ \& \ \forall \ \eta_k)$. The one-step prediction, that is the MMSE estimation under the set $\mathcal{I}_{u,k-1}$ without current information, will be applied to minimize the error as much as possible. Given the system dynamics described in (1), the estimation error $\tilde{x}_{u,k} \triangleq x_k - \hat{x}_{u,k}$ can be expressed by the following form:

$$\tilde{x}_{u,k} = A\tilde{x}_{u,k-1} + w_{k-1} \ (\gamma_{u,k} = 0 \ \& \ \forall \ \eta_k). \tag{24}$$

Since w_{k-1} is an independent noise with covariance Q according to (3), the corresponding covariance of the above estimation error can be easily written by

$$P_{u,k} = AP_{u,k-1}A^{\mathrm{T}} + Q \ (\gamma_{u,k} = 0 \ \& \ \forall \ \eta_k). \tag{25}$$

For the second scenario, the indicators are determined as $(\gamma_{u,k} = 1 \ \& \ \eta_k = 0)$. This means that the legitimate user receives the raw state estimate without any encoding. In this case, it becomes evident that the legitimate estimator is equivalent to the steady-state Kalman filter (4), i.e., $\hat{x}_{u,k} \equiv \hat{x}_k$, and likewise, the covariance exhibits the same equivalence as

$$P_{u,k} \equiv \bar{P} \ (\gamma_{u,k} = 1 \ \& \ \eta_k = 0). \tag{26}$$

In the final case, only the encoding result can be acquired through the network, indicating that $(\gamma_{u,k} = 1 \ \& \ \eta_k = 1)$ is met. This implies that the data is successfully transmitted and encoded, but retrieving the original information through

decoding becomes challenging due to the incorporation of pseudo-random numbers. Fortunately, the legitimate user is well-informed about the type of package being used as well as the encryption key thanks to the synchronization of all the pseudo-random numbers. Despite this advantage, the complexity of the estimation error remains high, because it is still challenging to accurately reconstruct the original data in the presence of packet dropping communications.

Based on the valid information, the legitimate user will try to perform the opposite of the encoding process to decode the ciphertext as $\hat{x}_{u,k} = \frac{z_k}{\beta_k} - \hat{x}_{u,k-1}$. By substituting the encoding output (13), the estimation error can be expressed by

$$\tilde{x}_{u,k} = -\tilde{x}_{u,k-1} + \tilde{x}_k + \tilde{x}_{k-1} \ (\gamma_{u,k} = 1 \ \& \ \eta_k = 1). \quad (27)$$

According to the Kalman filter design in (4), the recursive form of raw estimation error $\tilde{x}_k$ can be described as $\tilde{x}_k = (A - \bar{K}CA)\tilde{x}_{k-1} + (I_{n_x} - \bar{K}C)w_{k-1} - \bar{K}v_k$, deriving the following relationship:

$$\begin{aligned} \tilde{x}_k + \tilde{x}_{k-1} =& (I_{n_x} + A - \bar{K}CA)\tilde{x}_{k-1} \\ &+ (I_{n_x} - \bar{K}C)w_{k-1} - \bar{K}v_k. \end{aligned} \quad (28)$$

After being integrated with the above formula, the estimation error (27) of the legitimate user becomes

$$\begin{aligned} \tilde{x}_{u,k} =& -\tilde{x}_{u,k-1} + (I_{n_x} + A - \bar{K}CA)\tilde{x}_{k-1} \\ &+ (I_{n_x} - \bar{K}C)w_{k-1} - \bar{K}v_k \ (\gamma_{u,k} = 1 \ \& \ \eta_k = 1). \end{aligned} \quad (29)$$

Obviously, before deducing the covariance, it is required to compute $\Phi_{u,k} \triangleq \tilde{x}_{u,k}\tilde{x}_k^{\mathrm{T}}$, serving as a fundamental component in the expression of the final covariance.

By combining (27)-(29), the intermediate variable $\Phi_{u,k}$ can be described by the following recursive form:

$$\begin{aligned} \Phi_{u,k} =& \mathbb{E}\big\{\big(-\tilde{x}_{u,k-1} + (I_{n_x} + A - \bar{K}CA)\tilde{x}_{k-1} \\ &+ (I_{n_x} - \bar{K}C)w_{k-1} - \bar{K}v_k\big) \\ &\times \big(\tilde{x}_{k-1}^{\mathrm{T}}(A - \bar{K}CA)^{\mathrm{T}} \\ &+ w_{k-1}^{\mathrm{T}}(I_{n_x} - \bar{K}C)^{\mathrm{T}} - v_k^{\mathrm{T}}\bar{K}^{\mathrm{T}}\big)\big\} \\ =& -\Phi_{u,k-1}(A - \bar{K}CA)^{\mathrm{T}} \\ &+ (I_{n_x} + A - \bar{K}CA)\bar{P}(A - \bar{K}CA)^{\mathrm{T}} \\ &+ (I_{n_x} - \bar{K}C)Q(I_{n_x} - \bar{K}C)^{\mathrm{T}} + \bar{K}R\bar{K}^{\mathrm{T}} \\ &(\gamma_{u,k} = 1 \ \& \ \eta_k = 1). \end{aligned} \quad (30)$$

By introducing M and N in (23), the recursion of $\Phi_{u,k}$ can be reformulated in the manner presented in (23).

Eventually, through utilizing the above result (30), the estimation error covariance $P_{u,k}$ can be derived:

$$\begin{aligned} P_{u,k} =& \mathbb{E}\big\{\big(-\tilde{x}_{u,k-1} + (I_{n_x} + A - \bar{K}CA)\tilde{x}_{k-1} \\ &+ (I_{n_x} - \bar{K}C)w_{k-1} - \bar{K}v_k\big) \\ &\times (-\tilde{x}_{u,k-1}^{\mathrm{T}} + \tilde{x}_{k-1}^{\mathrm{T}}(I_{n_x} + A - \bar{K}CA)^{\mathrm{T}} \\ &+ w_{k-1}^{\mathrm{T}}(I_{n_x} - \bar{K}C)^{\mathrm{T}} - v_k^{\mathrm{T}}\bar{K}^{\mathrm{T}})\big\} \\ =& P_{u,k-1} - \Phi_{k-1}(I_{n_x} + A - \bar{K}CA)^{\mathrm{T}} \\ &+ (I_{n_x} + A - \bar{K}CA)\bar{P}(I_{n_x} + A - \bar{K}CA)^{\mathrm{T}} \\ &- (I_{n_x} + A - \bar{K}CA)\Phi_{k-1}^{\mathrm{T}} \\ &+ (I_{n_x} - \bar{K}C)Q(I_{n_x} - \bar{K}C)^{\mathrm{T}} + \bar{K}R\bar{K}^{\mathrm{T}} \\ &(\gamma_{u,k} = 1 \ \& \ \eta_k = 1). \end{aligned} \quad (31)$$

The terms except for recursion are gathered as $\Gamma_{u,k}$ that is expressed in (23). Now, by integrating all the above cases, the estimation error covariance is obtained, shown by the segmented form (22) in the theorem. This completes the proof.

B. Eavesdropper Estimation Error Covariance

After analyzing the estimation performance of the legitimate user, that of the eavesdroppers shall be simultaneously analyzed, given their pivotal role in privacy concerns. Note that eavesdroppers are categorized into two classes in Definition 3.1 and Definition 3.2 according to their varying capabilities and competencies. In light of this classification, we proceed to respectively compute the estimation error covariance for each possible case. First, we focus on the smart eavesdropper defined in Definition 3.1. Based on the estimator form given in (15) for the smart eavesdropper, the corresponding covariance is presented in the following theorem.

Theorem 4.2: The estimation error covariance for the smart eavesdropper's estimator (15) under the aggregation-based code (13) can be expressed by

$$P_{e,k}^s = \begin{cases} AP_{e,k-1}^s A^{\mathrm{T}} + Q, & \text{if } (\gamma_{e,k} = 0 \ \& \ \forall \ \eta_k), \\ \bar{P}, & \text{if } (\gamma_{e,k} = 1 \ \& \ \eta_k = 0), \\ P_{e,k-1}^s + \Gamma_{e,k-1}, & \text{if } (\gamma_{e,k} = 1 \ \& \ \eta_k = 1), \end{cases} \quad (32)$$

where $\Gamma_{e,k}$ follows the same recursion as $\Gamma_{u,k}$ in (23).

Proof 2: It is obvious that the estimation structure in (15) for smart eavesdropper exhibits the similarity to that in (14) for the legitimate user. This suggests the parallelism in their underlying mathematical expressions. Consequently, we can describe the covariance for the smart eavesdropper as presented in (32), which follows the same recursive pattern as (22) for the user. This completes the proof.

Second, we turn our attention to discussing the performance of the naive eavesdropper. The covariance for its estimator, as presented in (16), is analyzed as follows.

Theorem 4.3: The estimation error covariance for the naive eavesdropper's estimator (16) under the aggregation-based code (13) can be expressed by

$$P_{e,k}^n = \begin{cases} AP_{e,k-1}^n A^{\mathrm{T}} + Q, & \text{if } (\gamma_{e,k} = 0 \ \& \ \forall \ \eta_k), \\ \bar{P}, & \text{if } (\gamma_{e,k} = 1 \ \& \ \eta_k = 0), \\ A_{\beta,k}\Sigma_{k-1}A_{\beta,k}^{\mathrm{T}} + H_k, & \text{if } (\gamma_{e,k} = 1 \ \& \ \eta_k = 1), \end{cases} \quad (33)$$

where

$$\begin{aligned} A_{\beta,k} &= (1 - \beta_k)A - \beta_k I_{n_x}, \\ H_k &= \beta_k^2(I_{n_x} + A - \bar{K}CA)\bar{P}(I_{n_x} + A - \bar{K}CA)^{\mathrm{T}} \\ &\quad + (I_{n_x} - \beta_k\bar{K}C)Q(I_{n_x} - \beta_k\bar{K}C)^{\mathrm{T}} + \beta_k^2\bar{K}R\bar{K}^{\mathrm{T}}. \end{aligned} \quad (34)$$

Proof 3: The naive eavesdropper is a special yet common type of adversary in remote state estimation systems. It operates in a straightforward manner by directly treating the received data packet as the real-time raw estimate without applying any sophisticated processing or decoding techniques. Despite the fact that the operation is limited to just two types, the covariance manifests itself in three distinct forms, which

is a variation stemming from the proposed coding mechanism. First, when ($\gamma_{e,k}=0$ & $\forall\ \eta_k$), all parties involved, including the naive eavesdropper, must engage in prediction. Hence, the prediction error and covariance are analogous to those previously calculated, i.e.,

$$\tilde{x}^n_{e,k} = A\tilde{x}^n_{e,k-1} + w_{k-1}\ (\gamma_{e,k}=0\ \&\ \forall\ \eta_k), \tag{35}$$

and

$$P^n_{e,k} = AP^n_{e,k-1}A^{\mathrm{T}} + Q\ (\gamma_{e,k}=0\ \&\ \forall\ \eta_k). \tag{36}$$

Next, the scenario ($\gamma_{e,k}=1$ & $\forall\ \eta_k$) necessitates a more detailed examination and shall be divided into the following two distinct cases: ($\gamma_{e,k}=1$ & $\eta_k=0$) and ($\gamma_{e,k}=1$ & $\eta_k=1$). This division is crucial because the received data vary significantly between these two cases, leading to different estimation outcomes. Consequently, the estimation process for the naive eavesdropper can be expressed as follows:

$$\hat{x}^n_{e,k} = \begin{cases} \hat{x}_k, & \text{if } (\gamma_{e,k}=1\ \&\ \eta_k=0), \\ \beta_k(\hat{x}_{k-1}+\hat{x}_k), & \text{if } (\gamma_{e,k}=1\ \&\ \eta_k=1). \end{cases} \tag{37}$$

For the plaintext transmission situation, i.e., when ($\gamma_{e,k}=1$ & $\eta_k=0$), it is evident that the covariance is equivalent to the steady-state one:

$$P^s_{e,k} \equiv \bar{P}\ (\gamma_{e,k}=1\ \&\ \eta_k=0). \tag{38}$$

On the other hand, we discuss the ciphertext communication situation when ($\gamma_{e,k}=1$ & $\eta_k=1$). Based on the relation $x_k=\hat{x}_k+\tilde{x}_k$, the estimation error can be written as

$$\tilde{x}^s_{e,k} = (1-\beta_k)x_k - \beta_k x_{k-1} + \beta_k\tilde{x}_k + \beta_k\tilde{x}_{k-1}. \tag{39}$$

Combining the transition relations of state and local Kalman filtering error, i.e., $x_k = Ax_{k-1}+w_{k-1}$ and $\tilde{x}_k = (A-\bar{K}CA)\tilde{x}_{k-1} + (I_{n_x}-\bar{K}C)w_{k-1} - \bar{K}v_k$, the final estimation error for the case ($\gamma_{e,k}=1$ & $\eta_k=1$) can be simplified as

$$\begin{aligned} \tilde{x}^s_{e,k} =& A_{\beta,k}x_{k-1} + \beta_k(I_{n_x}+A-\bar{K}CA)\tilde{x}_{k-1} \\ &+ (I_{n_x}-\beta_k\bar{K}C)w_{k-1} - \beta_k\bar{K}v_k, \end{aligned} \tag{40}$$

where $A_{\beta,k}$ is defined in (34). Note that $\hat{x}_k$ is orthogonal to $\tilde{x}_k$ under the Kalman filtering structure, one has $\mathbb{E}\{\hat{x}_k\tilde{x}_k^T\}=0$ and $\mathbb{E}\{x_k\tilde{x}_k^T\}=\mathbb{E}\{\tilde{x}_k\tilde{x}_k^T\}=\bar{P}$. Also, w_{k-1} and v_k are both independent noises. Therefore, the estimation error covariance can be obtained as shown in (33) and (34) in the theorem. This completes the proof.

V. Privacy Guarantees

Due to the still randomness of the estimation error covariances presented in the last section, our primary objective in this section is to systematically compute and analyze the expected values of these covariances. Subsequently, based on these expected performances, we propose the conditions necessary to achieve the previously defined privacy metrics.

A. User Expected Performance

After obtaining the covariance (22) given in Theorem 4.1 for the legitimate user, we will now proceed to compute its expectation as follows.

Theorem 5.1: The expectation of the estimation error covariance (22) for the legitimate user's estimator (14) under aggregation-based code (13) is

$$\begin{aligned} \mathbb{E}\{P_{u,k}\} =& (1-\mu_u)A\mathbb{E}\{P_{u,k-1}\}A^{\mathrm{T}} \\ &+ \mu_u\mu_\eta\mathbb{E}\{P_{u,k-1}\} + \Theta_{u,k}, \end{aligned} \tag{41}$$

where

$$\Theta_{u,k} = \mu_u(1-\mu_\eta)\bar{P} + (1-\mu_u)Q + \mu_u\mu_\eta\Gamma_{u,k-1}. \tag{42}$$

Proof 4: According to the result (22) in Theorem 4.1, there are three outcomes for the legitimate user's estimator, including:

1) Failed receipt of the package with probability $p_{u,1} = \mathbb{P}\{\gamma_{u,k}=0\} = (1-\mu_u)$.
2) Successful receipt of raw remote state estimate with probability $p_{u,2} = \mathbb{P}\{\gamma_{u,k}=1, \eta_k=0\} = \mu_u(1-\mu_\eta)$.
3) Successful receipt of the code with probability $p_{u,3} = \mathbb{P}\{\gamma_{u,k}=1, \eta_k=1\} = \mu_u\mu_\eta$.

Here, we introduce a temporary variable, denoted as $\phi_k = j\ (j\in\{1,2,3\})$, which is specifically designated to represent the above j-th scenario or case being considered. By applying the expectation, the expected covariance can be calculated by

$$\begin{aligned} \mathbb{E}\{P_{u,k}\} =& \sum_{j=1}^{3}\mathbb{E}\{P_{u,k}|\phi_k=j\}\mathbb{P}\{\phi_k=j\} \\ =& p_{u,1}(A\mathbb{E}\{P_{u,k-1}\}A^{\mathrm{T}}+Q) \\ &+ p_{u,2}\bar{P} + p_{u,3}(\mathbb{E}\{P_{u,k-1}\}+\Gamma_{k-1}). \end{aligned} \tag{43}$$

After substituting corresponding probabilities in Theorem 4.1 for all $p_{u,j}$, we can easily derive the result in the theorem. This completes the proof.

B. Eavesdropper Expected Performance

Next, we present the expected covariances for the eavesdroppers. Since the estimator of the smart eavesdropper is same as the user, we can directly acquire its expectation by imitating the derivation process in Theorem 5.1.

Theorem 5.2: The expectation of the estimation error covariance (32) for the smart eavesdropper is

$$\begin{aligned} \mathbb{E}\{P^s_{e,k}\} =& (1-\mu_e)A\mathbb{E}\{P^s_{e,k-1}\}A^{\mathrm{T}} \\ &+ \mu_e\mu_\eta\mathbb{E}\{P^s_{e,k-1}\} + \Theta_{e,k}, \end{aligned} \tag{44}$$

where

$$\Theta_{e,k} = \mu_e(1-\mu_\eta)\bar{P} + (1-\mu_e)Q + \mu_e\mu_\eta\Gamma_{e,k-1}. \tag{45}$$

Proof 5: Since the estimator employed by the smart eavesdropper closely resembles that used by the legitimate user, we will omit the detailed proof in this context and proceed to directly present the covariance as given in the theorem.

Unlike the legitimate user and the smart eavesdropper, who possess certain levels of knowledge and expertise, the estimator of the naive eavesdropper lacks most information. Therefore, the computation of its expected covariance requires a more intricate approach, which is detailed as follows.

Theorem 5.3: The expectation of the estimation error covariance (22) for the naive eavesdropper is

$$\mathbb{E}\{P^n_{e,k}\} =(1-\mu_e)A\mathbb{E}\{P^n_{e,k-1}\}A^{\mathrm{T}} + \mu_e\mu_\eta(\hat{\Sigma}_{\beta,k}+\hat{H}_{\beta,k}), \tag{46}$$

where

$$\begin{aligned}\hat{\Sigma}_{\beta,k} =&((\mu_\beta-1)^2+Q_\beta)A\Sigma_{k-1}A^{\mathrm{T}} + (\mu_\beta^2+Q_\beta)\Sigma_{k-1}\\ &+(\mu_\beta(1-\mu_\beta)+Q_\beta)(A\Sigma_{k-1}+\Sigma_{k-1}A^{\mathrm{T}}),\\ \hat{H}_{\beta,k} =&(\mu_\beta^2+Q_\beta)(\bar{K}CQC^{\mathrm{T}}K^{\mathrm{T}}+\bar{K}R\bar{K}^{\mathrm{T}}\\ &+(I_{n_x}+A-\bar{K}CA)P(I_{n_x}+A-\bar{K}CA))^{\mathrm{T}}\\ &+Q-\mu_\beta(\bar{K}CQ+QC^{\mathrm{T}}K^{\mathrm{T}}).\end{aligned} \tag{47}$$

Proof 6: For the naive eavesdropper, there also exist three kinds of cases, including:

1) Failed receipt of the package with probability $p_{e,1} = \mathbb{P}\{\gamma_{e,k}=0\} = (1-\mu_e)$.
2) Successful receipt of raw remote state estimate with probability $p_{e,2} = \mathbb{P}\{\gamma_{e,k}=1,\eta_k=0\} = \mu_e(1-\mu_\eta)$.
3) Successful receipt of the code with probability $p_{e,3} = \mathbb{P}\{\gamma_{e,k}=1,\eta_k=1\} = \mu_e\mu_\eta$.

Then, the expected covariance can be calculated by

$$\begin{aligned}\mathbb{E}\{P^n_{e,k}\} =&\sum_{j=1}^{3}\mathbb{E}\{P^n_{e,k}|\phi_k=j\}\mathbb{P}\{\phi_k=j\}\\ =&p_{e,1}(A\mathbb{E}\{P^n_{e,k-1}\}A^{\mathrm{T}}+Q)\\ &+p_{e,2}\bar{P}+p_{e,3}\mathbb{E}\{(A_{\beta,k}\Sigma_{k-1}A^{\mathrm{T}}_{\beta,k}+H_k)\}.\end{aligned} \tag{48}$$

Now, we start to analyze the part $\mathbb{E}\{(A_{\beta,k}\Sigma_{k-1}A^{\mathrm{T}}_{\beta,k}+H_k)\}$. According to the property of the mathematical expectation: $\mathbb{E}\{aA+bB\} = a\mathbb{E}\{A\}+b\mathbb{E}\{B\}$, the expectations for the items with respect to β_k can be computed as:

$$\begin{aligned}\hat{\Sigma}_{\beta,k} =&\mathbb{E}\{((1-\beta_k)A-\beta_kI_{n_x})\Sigma_{k-1}((1-\beta_k)A-\beta_kI_{n_x})^{\mathrm{T}}\}\\ =&((\mu_\beta-1)^2+Q_\beta)A\Sigma_{k-1}A^{\mathrm{T}}+(\mu_\beta^2+Q_\beta)\Sigma_{k-1}\\ &+(\mu_\beta(1-\mu_\beta)+Q_\beta)(A\Sigma_{k-1}+\Sigma_{k-1}A^{\mathrm{T}})\end{aligned} \tag{49}$$

and

$$\begin{aligned}\hat{H}_{\beta,k} =&\mathbb{E}\{\beta_k^2(I_{n_x}+A-\bar{K}CA)\bar{P}(I_{n_x}+A-\bar{K}CA)^{\mathrm{T}}\\ &+(I_{n_x}-\beta_k\bar{K}C)Q(I_{n_x}-\beta_k\bar{K}C)^{\mathrm{T}}+\beta_k^2\bar{K}R\bar{K}^{\mathrm{T}}\}.\end{aligned} \tag{50}$$

By resorting to the statistical information of β_k, the results in (46) and (47) are derived. This completes the proof.

C. Guarantees of α-Relative Secrecy

As previously discussed, we have proposed two different secrecy metrics tailored to accommodate the varying capabilities of eavesdroppers. Initially, we provide the condition for realizing α-relative secrecy that is defined in Definition 3.3. This objective is relatively lenient and straightforward to fulfill. The following theorem demonstrates how this target is met for the smart eavesdropper.

Theorem 5.4: (α-Relative Secrecy Under Smart Eavesdropper) With the coding scheme (13), for the legitimate user's estimator (14) and the smart eavesdropper's estimator (15), the relative secrecy in Definition 3.3 can be achieved when the following conditions hold:

$$(1-\mu_e)\rho(A)^2+\mu_e\mu_\eta<1, \tag{51}$$

$$\alpha\cdot\mathrm{tr}\{\bar{P}_u\}-\mathrm{tr}\{\bar{P}^s_e\}<0, \tag{52}$$

where $\bar{P}_u$ and $\bar{P}^s_e$ are the respective solutions to (41) and (44).

Proof 7: According to the requirement of realizing relative secrecy, the detailed comparison for the traces of the aforementioned expectations should be analyzed and examined. At first, the trace of the expectation (41) for the legitimate user can be easily obtained as:

$$\begin{aligned}\mathrm{tr}\{\mathbb{E}\{P_{u,k}\}\} =&\mathrm{tr}\left\{(1-\mu_u)A\mathbb{E}\{P_{u,k-1}\}A^{\mathrm{T}}\right.\\ &\left.+\mu_u\mu_\eta\mathbb{E}\{P_{u,k-1}\}+\Theta_{u,k}\right\}.\end{aligned} \tag{53}$$

Based on the properties $\mathrm{tr}\{AB\} = \mathrm{tr}\{BA\}$ and $\mathrm{tr}\{A+B\} = \mathrm{tr}\{B+A\}$, the above first part $\mathrm{tr}\left\{(1-\mu_u)A\mathbb{E}\{P_{u,k-1}\}A^{\mathrm{T}}\right\}$ can be written as $\mathrm{tr}\left\{(1-\mu_u)A^{\mathrm{T}}A\mathbb{E}\{P_{u,k-1}\}\right\}$. In this case, the trace (53) can be further expressed by the following form:

$$\begin{aligned}\mathrm{tr}\{\mathbb{E}\{P_{u,k}\}\} =&\mathrm{tr}\left\{\left((1-\mu_u)A^{\mathrm{T}}A\right.\right.\\ &\left.\left.+\mu_u\mu_\eta I_{n_x}\right)\mathbb{E}\{P_{u,k-1}\}+\Theta_{u,k}\right\}.\end{aligned} \tag{54}$$

The spectral radius of above user's trace system, denoted by ρ_u, can be obtained as

$$\rho_u =(1-\mu_u)\rho(A)^2+\mu_u\mu_\eta. \tag{55}$$

Hence, in accordance with the first condition (17) of relative secrecy, it is imperative to ensure the stability of the above system. This indicates that the spectral radius is required to be bounded by "1", which means that the inequality in (51) should be satisfied.

On the other hand, we can similarly describe the trace for the smart eavesdropper as

$$\begin{aligned}\mathrm{tr}\{\mathbb{E}\{P^s_{e,k}\}\} =&\mathrm{tr}\{((1-\mu_e)A^{\mathrm{T}}A\\ &+\mu_e\mu_\eta I_{n_x})\mathbb{E}\{P^s_{e,k-1}\}+\Theta_{e,k},\end{aligned} \tag{56}$$

with the spectral radius

$$\rho^s_e =(1-\mu_e)\rho(A)^2+\mu_e\mu_\eta. \tag{57}$$

In this case, to guarantee the requirement $\alpha\cdot\mathrm{tr}\{\mathbb{E}\{P_{u,k}\}\} < \mathrm{tr}\{\mathbb{E}\{P^s_{e,k}\}\}$, the spectral radius of the legitimate user must be smaller than that of the smart eavesdropper. In this case, we have $(1-\mu_u)\rho(A)^2+\mu_u\mu_\eta < (1-\mu_e)\rho(A)^2+\mu_e\mu_\eta$, thereby only the requirement (51) can simultaneously guarantee the conditions (17) and (18). Then, we assume that the solutions to (41) and (44) are $\bar{P}_u$ and $\bar{P}^s_e$. According to the requirement $\alpha\cdot\mathrm{tr}\{\mathbb{E}\{P_{u,k}\}\} < \mathrm{tr}\{\mathbb{E}\{P^s_{e,k}\}\}$ in (19), the result (52) is derived, and this completes the proof.

Then, we give the theorem of α-relative secrecy for the naive eavesdropper in the similar way.

Theorem 5.5: (α-Relative Secrecy Under Naive Eavesdropper) With the coding scheme (13), for the legitimate

user's estimator (14) and the naive eavesdropper's estimator (16), the relative secrecy in Definition 3.3 is achieved when the following condition holds:

$$(1-\mu_u)\rho(A)^2+\mu_u\mu_\eta<1, \tag{58}$$

$$\alpha\cdot\mathrm{tr}\{\bar{P}_u\}-\mathrm{tr}\{\bar{P}_e^n\}<0, \tag{59}$$

where $\bar{P}_u$ and $\bar{P}_e^n$ are the respective solutions to (41) and (46).

Proof 8: For the naive eavesdropper, the trace of its expected performance (46) can be expressed by

$$\mathrm{tr}\{\mathbb{E}\{P_{e,k}^n\}\}=\mathrm{tr}\{(1-\mu_e)A^{\mathrm{T}}A\mathbb{E}\{P_{e,k-1}^n\}+\hat{\Sigma}_{\beta,k}+\hat{H}_{\beta,k}\}, \tag{60}$$

and obviously, its spectral radius can be obtained as

$$\rho_e^n=(1-\mu_e)\rho(A)^2. \tag{61}$$

Since the term $\mu_u\mu_\eta$ is positive, one has $(1-\mu_u)\rho(A)^2+\mu_u\mu_\eta>(1-\mu_u)\rho(A)^2$, and thus the requirement (58) can simultaneously guarantee the conditions (17) and (18). After acquiring the solutions $\bar{P}_u$ and $\bar{P}_e^s$ for the equations (41) and (46), the result (59) can be obtained under the condition in (19). This completes the proof.

D. Guarantees of Perfect Secrecy

Now, we delve into presenting the condition for perfect secrecy, a benchmark that stands as one of the most stringent criteria. This notion of perfect secrecy is different from the concept of relative secrecy, especially for the requirements for the eavesdroppers. Under the relative secrecy, there is some tolerance for the eavesdropper's performance to deviate from the ideal. However, perfect secrecy demands an uncompromising standard, where the eavesdropper's performance must be entirely divergent. In accordance with the conditions proposed in Definition 3.4, we prove its achievements as follows.

Theorem 5.6: (Perfect Secrecy Under Smart Eavesdropper) With the coding scheme (13), for the legitimate user's estimator (14) and the smart eavesdropper's estimator (15), the perfect secrecy in Definition 3.4 can be achieved when the following condition holds:

$$(1-\mu_u)\rho(A)^2+\mu_u\mu_\eta<1, \tag{62}$$

$$(1-\mu_e)\rho(A)^2+\mu_e\mu_\eta\geq 1. \tag{63}$$

Proof 9: According to the specifications in Definition 3.4, we must ensure that two crucial conditions are met regarding the expected performances of both the legitimate user and the eavesdropper. On the one hand, the trace of the legitimate user's covariance should remain bounded, which means that the spectral radius should be less than "1". The expression of this condition, shown in (62), aligns with the conditions stated in (51) and (58). On the other hand, the trace of the smart eavesdropper's covariance should diverge, indicating that the spectral radius should be greater than "1". In this case, according to its radius computed in (57), the condition (63) can be easily obtained. By combining the above two results, this theorem is derived, and the proof is completed.

Then, the results for the naive eavesdropper is given below.

Theorem 5.7: (Perfect Secrecy Under Naive Eavesdropper) With the coding scheme (13), for the legitimate user's estimator (14) and the naive eavesdropper's estimator (16), the perfect secrecy in Definition 3.4 can be achieved when the following condition holds:

$$(1-\mu_u)\rho(A)^2+\mu_u\mu_\eta<1, \tag{64}$$

$$(1-\mu_e)\rho(A)^2\geq 1. \tag{65}$$

Proof 10: For brevity, we omit the detailed proof of this theorem. In a similar manner to Theorem 5.6, we can derive the results given in (64) and (65) by taking into account the spectral radius conditions outlined in Definition 3.4.

VI. Experiment Results

Since the results vary with the system stability, we thoroughly discuss two kinds of systems, including stable and unstable cases, to more comprehensively illustrate the effectiveness of the proposed method. Furthermore, we compare the performances of the proposed aggregation-based method (13) with that of the following recently advanced approaches:

1) Moving summation with two-step sequential true-random noise injection in [21], where summation length is set as $t_q=2$;
2) Scheduled state-secrecy code with no ACKs in [24], where the pseudo-random scheduler v_k is set as same to the scheduler η_k in this paper.
3) True random noise injection in [20];
4) Pseudo random noise injection in [25].

A. Numerical Simulation

First, let us consider a numerical CPS described by the following parameters in (1) and (2):

$$A=\begin{bmatrix}0.8 & 0.2\\ 0.0 & 0.5\end{bmatrix},\ C=\begin{bmatrix}1.0 & 0.0\\ 0.4 & 0.6\end{bmatrix}, \tag{66}$$

The covariances of noises are assumed to be $Q=\mathrm{diag}\{0.02,0.04\}$, $R=\mathrm{diag}\{0.01,0.02\}$. The spectral radius is $\rho(A)=0.8$. Then, the steady-state prediction error covariance is obtained as $\bar{P}^-=\begin{bmatrix}0.0248 & 0.0019\\ 0.0018 & 0.0464\end{bmatrix}$ by solving the Riccati equation in (6), and the corresponding steady-state estimation error covariance can be further computed as $\bar{P}=\begin{bmatrix}0.0069 & -0.0018\\ -0.0018 & 0.0257\end{bmatrix}$.

We presume that the packet dropping rates are respectively specified as $\mu_u=0,9,\mu_e=0.1$. Meanwhile, the pseudo-random sequence in this section is randomly selected from the set $\{-2,2\}$. The probability of choosing -1 is set at 0.5, which indicates $\mu_\beta=0$ and $Q_\beta=4$. The mathematical expectation of the binary pseudo-random scheduler is established with $\mu_\eta=0.2$. Then, the traces of various expected estimation error covariances are plotted in Fig. 3.

Moreover, the metrics outlined in the theorems for relative secrecy with respect to α are depicted in Fig. 4. The dotted lines denote the parameters of the metric, while the solid lines

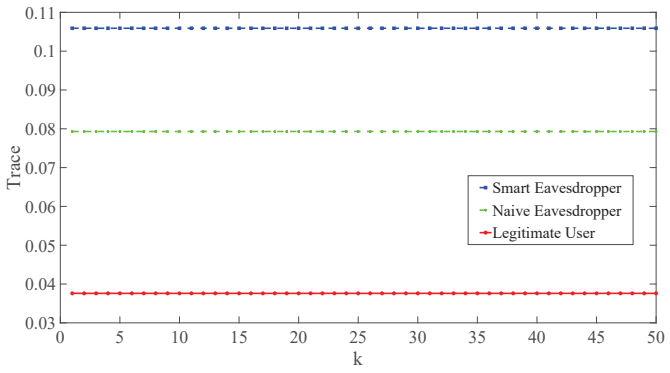

Fig. 3. The traces of various expected estimation error covariances.

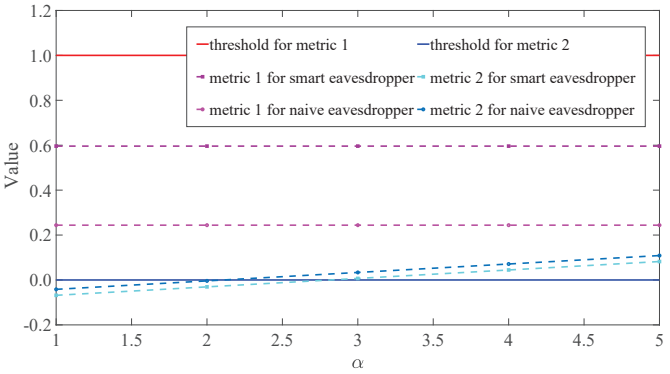

Fig. 4. The metrics of various conditions for relative secrecy with respect to α.

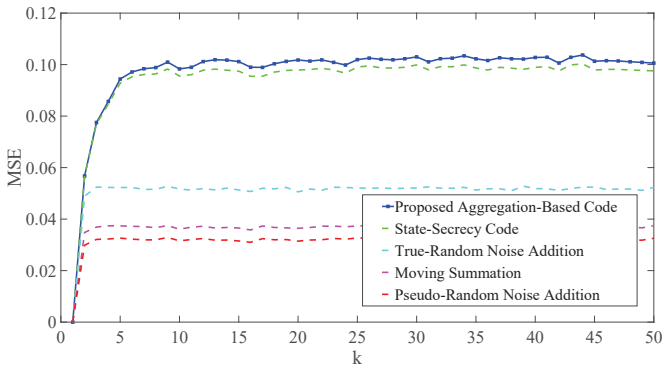

Fig. 5. The MSEs of the smart eavesdropper under various methods.

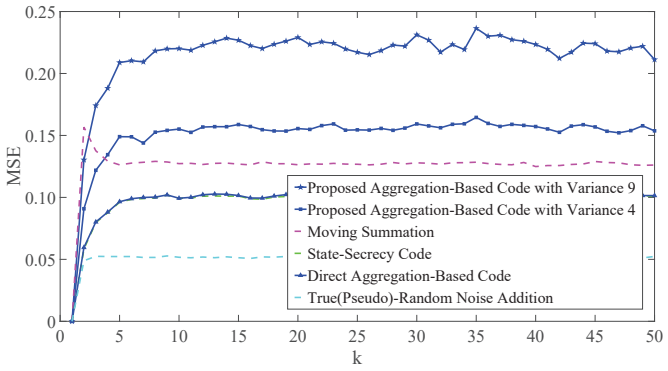

Fig. 6. The MSEs of the naive eavesdropper under various methods.

represent the corresponding thresholds. It is apparent from this figure that the first conditions in (51) and (58) remain below the threshold value of 1, whereas the second conditions in (52) and (59) are lower than the threshold value of 0 when $\alpha < 2$. Also, we proceed with a numerical analysis for the case where $\alpha = 2$, and the conditions specified in (51), (52), (58), and (59) are calculated as

$$(1-\mu_e)\rho(A)^2 + \mu_e\mu_\eta = 0.5960 < 1, \tag{67}$$
$$\alpha \cdot \mathrm{tr}\{\bar{P}_u\} - \mathrm{tr}\{\bar{P}_e^s\} = -0.0307 < 0, \tag{68}$$
$$(1-\mu_u)\rho(A)^2 + \mu_u\mu_\eta = 0.2440 < 1, \tag{69}$$
$$\alpha \cdot \mathrm{tr}\{\bar{P}_u\} - \mathrm{tr}\{\bar{P}_e^n\} = -0.0041 < 0. \tag{70}$$

Evidently, all the prerequisites in Theorem 5.4 and 5.5 are met, thus ensuring the attainment of α-relative secrecy for both the smart and naive eavesdroppers.

Furthermore, we apply MSEs to assess the practical performances of various estimators, where the theoretical MSEs are approximated by 100 runs of the Monte Carlo method. On the one hand, the MSEs of the smart eavesdropper under various privacy-preserving methods mentioned previously are plotted in Fig. 5. From this figure, one can observe that the MSE associated with the proposed aggregation-based code is higher when compared to all the other approaches. The direct incorporation of pseudo-random noise fails to degrade the performance, because the smart eavesdropper defined in this paper is aware of all the simple secret keys. On the other hand, the MSEs of naive eavesdroppers are plotted in Fig. 6, while the relations with respect to the variance Q_β is illustrated. Although the MSE of the direct aggregation-based method is higher than that of random noise addition, it is lower than that of moving summation. Moreover, by increasing the variance of the pseudo-random sequence, the MSE can be significantly elevated. This strongly highlights the benefits of incorporating pseudo-random numbers into the secrecy code.

B. Target Tracking

Note that performance is related to system stability. Here, we employ another system to present some supplementary results that enrich the findings with the proposed methods. This additional system allows us to gain a more comprehensive understanding of the privacy implications associated with our methods. Meanwhile, we do the real-world experiment in this section to demonstrate the effectiveness and practical usage of the proposed methods.

Here, we consider a target tracking system to observe the real-time trajectory of an unmanned aerial vehicle (UAV). A real-world UAV platform called Crazyflie is utilized for the experimental assessment of this work. Apart from the essential elements like the battery, rotors, and propellers, this mini drone is equipped a micro-controller as well as a reflective marker. We presume its flight path to be within a horizontal plane, subject to white-noise acceleration. The height is fixed at a

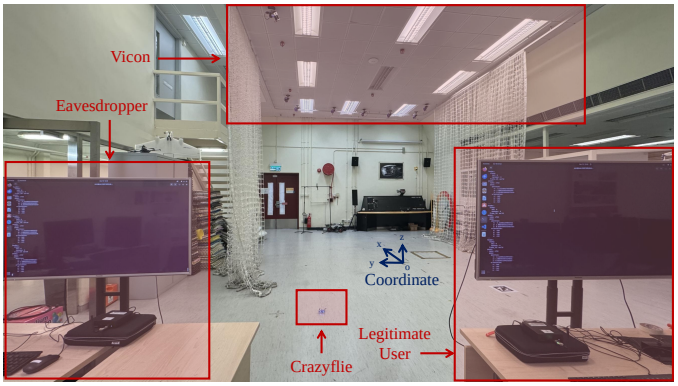

Fig. 7. The platform of a drone used for experiment.

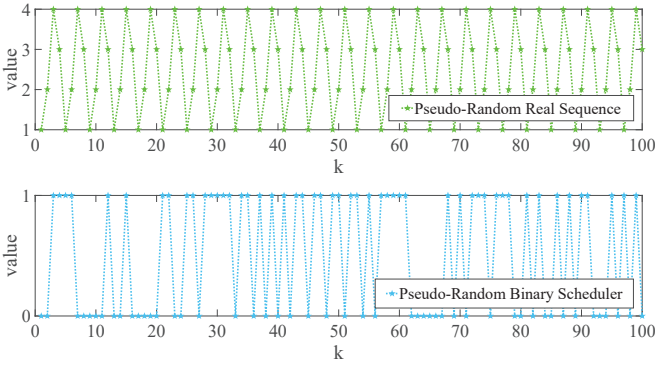

Fig. 8. The pseudo-random numbers used in code.

constant value of 0.5m, and the kinematic model in X-Y plane can be expressed by

$$\begin{aligned} pos_{x,k} =& pos_{x,k-1} + vel_{x,k-1}T + 0.5w_{x,k-1}T^2, \\ vel_{x,k} =& vel_{x,k-1} + w_{x,k-1}T, \\ pos_{y,k} =& pos_{y,k-1} + vel_{y,k-1}T + 0.5w_{y,k-1}T^2, \\ vel_{y,k} =& vel_{y,k-1} + w_{y,k-1}T. \end{aligned} \tag{71}$$

$(pos_{x,k}, pos_{y,k})$ represents the 2-dimensional coordinate of the Crazyflie in the X-Y plane and $(vel_{x,k}, vel_{y,k})$ denotes the corresponding velocity, where the initial state is $[pos_{x,0}, vel_{x,0}, pos_{y,0}, vel_{y,0}] = [0; -1; 0; 1]$. $[w_{x,k}; w_{y,k}]$ is the process noise and the sampling frequency $1/T$ is 50Hz.

Then, we deploy a motion capture system called Vicon to monitor various states of the Crazyflie drone in real time. The Vicon utilizes multiple high-precision cameras to capture the real-time information of the reflection marker, which is deployed on the target drone and represents the center Cartesian coordinates of the drone. In this scenario, the Vicon will provide the 2-dimensional position of the Crazyflie, and thus the measurement model can be described as

$$\begin{aligned} \overline{pos}_{x,k} =& pos_{x,k} + v_{x,k}, \\ \overline{pos}_{y,k} =& pos_{y,k} + v_{y,k}. \end{aligned} \tag{72}$$

$(\overline{pos}_{x,k}, \overline{pos}_{y,k})$ denotes the 2-dimensional coordinate observed by Vicon, and $[v_{x,k}; v_{y,k}]$ is the measurement noise.

In this paper, Vicon will initially compute state estimates grounded on its local measurements. A mini computer known as Next Unit of Computing (NUC) serves as the legitimate user, poised to receive the estimates from Vicon. The communication for the above drone system is based on Wifi, implying that Vicon will broadcast the estimates via the wireless network. In this case, the eavesdropper could potentially intercept the wireless transmission, leading to a breach of privacy. The complete system structure is demonstrated in Fig. 7.

To prevent the eavesdropper from obtaining accurate real-time estimates, the estimate will be encrypted by the proposed aggregation-based code in (13). In this scenario, the pseudo-random real numbers β_k are generated by resorting to LCG. The parameters of LCG are $a = 2$, $c = 0$, $m = 5$, and $\beta_0 = 1$. Then, the pseudo-random sequence will cycle through the fixed set $\{1, 2, 4, 3\}$. These pseudo-random numbers, including real and binary numbers, are depicted in Fig. 8.

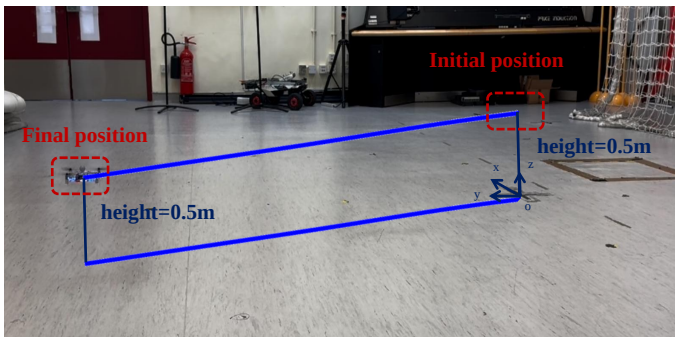

Fig. 9. The actual flight path of the Crazyflie.

The actual flight path of the Crazyflie is depicted in Fig. 9. Starting from the coordinates $(0, 0)$, the UAV intends to move toward approximately $(-2, 2)$ with a velocity of $(-0.2, 0.2)$. The tracking trajectories for all the parties are depicted in Fig. 10. From this illustration, it becomes evident that the error associated with the naive eavesdropper is extremely large, to the extent that we cannot even discern the rough outline of the trajectory. Furthermore, although both the legitimate user and the smart eavesdropper are capable of nearly accurate target tracking, the small inset figure shows that the smart eavesdropper appears to miss some key positions. Then, Figure 11 presents the real-time square errors (SEs) between the various compensated estimates and the originally optimal estimates. It demonstrates that the legitimate user's error generally remains below that of the eavesdroppers, further proving the practical realization of relative secrecy.

Moreover, the packet dropping rate of legitimate user and eavesdropper are respectively tested to be approximately $\gamma_u = 0.99$ and $\gamma_e = 0.9$. The real-time packet dropping indicators are displayed in Fig. 12, which are collected through networking protocols in the real world. Under the above scenario, considering the proposed aggregation-based code as shown in Fig. 2 and the packet dropping links in Fig. 12, the traces of various real-time estimation error covariances are presented in Fig. 13. It clearly illustrates the relations between the traces and the indicators, with the trends being consistent with the SEs in Fig. 11.

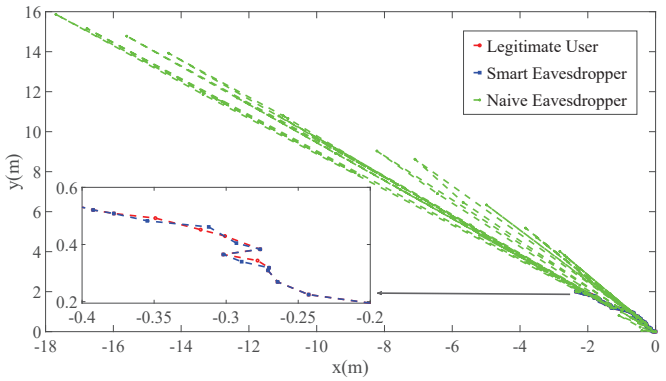

Fig. 10. The tracking trajectories for all the parties.

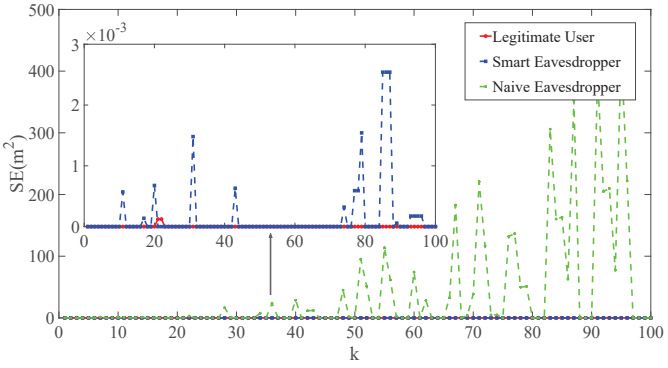

Fig. 11. The real-time SEs of various estimates.

VII. Conclusion

The issue of privacy preservation has been investigated in the context of remote state estimation in the presence of smart and naive eavesdroppers. An aggregation-based encryption approach was proposed, involving the seamless switching between the raw state estimate and a code derived from the product of local state estimates and pseudo-random numbers. Then, under specific and carefully defined conditions about the system stability and channel models, the relative secrecy and the perfect secrecy were rigorously proved to be feasible and achievable. Finally, analytical, numerical, and experimental results were comprehensively provided to demonstrate that the proposed encoding methods offer substantial privacy benefits.

Note that in this paper, we have only considered the simplest aggregation form, which involves gathering just two estimates. In the future, we may delve deeper into the complicated relationship between estimation performance and the length of aggregation. Furthermore, the form of aggregation itself can be modified and refined to better suit specific applications. By exploring different aggregation strategies, we may uncover new ways to improve the privacy and estimation performances. Also, it may be interesting and valuable to explore the effectiveness of the aggregation-based code within the frameworks of multi-sensor fusion estimation, multi-agent distributed estimation, and time-varying estimation. These scenarios present unique challenges and opportunities, and understanding how aggregation-based codes can be leveraged in these contexts may lead to significant advancements.

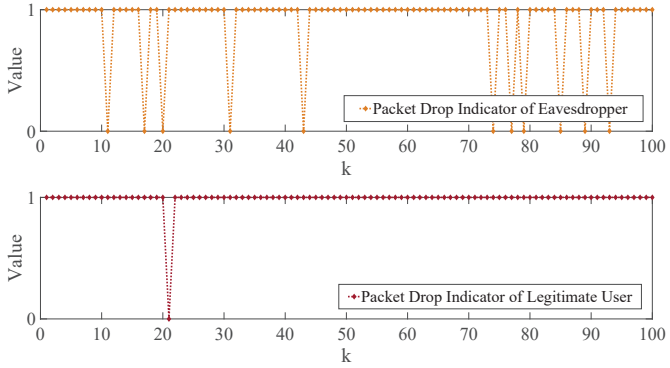

Fig. 12. The real-time packet dropping indicators.

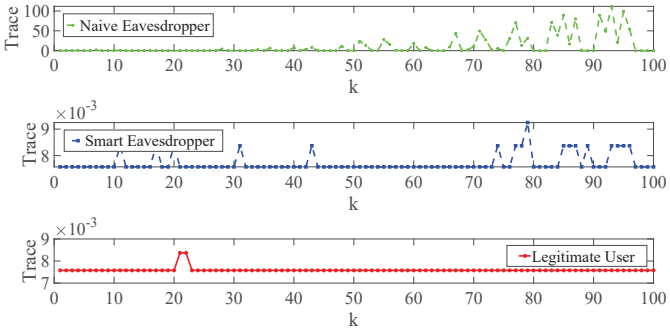

Fig. 13. The trace of the real-time estimation error covariance.

References

[1] A. Fu and J. A. McCann, "Dynamic decentralized periodic event-triggered control for wireless cyber–physical systems," *IEEE Transactions on Control Systems Technology,* vol. 29, no. 4, pp. 1783-1790, July 2021.

[2] C. Lu, A. Saifullah, B. Li, M. Sha, H. Gonzalez, D. Gunatilaka, C. Wu, L. Nie, and Y. Chen, "Real-time wireless sensor-actuator networks for industrial cyber-physical systems," *Proceedings of the IEEE,* vol. 104, no. 5, pp. 1013-1024, May 2016.

[3] M. Liu, Y. Shi, and H. Gao, "Aggregation and charging control of PHEVs in smart grid: A cyber–physical perspective," *Proceedings of the IEEE,* vol. 104, no. 5, pp. 1071-1085, May 2016.

[4] M. S. Sadabadi, "A resilient-by-design distributed control framework for cyber-physical DC microgrids," *IEEE Transactions on Control Systems Technology,* vol. 32, no. 2, pp. 625-636, March 2024.

[5] R. Shakeri, M. A. Al-Garadi, A. Badawy, A. Mohamed, T. Khattab, A. Khalid Al-Ali, K. A. Harras, and M. Guizani, "Design challenges of multi-UAV systems in cyber-physical applications: A comprehensive survey and future directions," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 4, pp. 3340-3385, Fourthquarter 2019.

[6] B. Chen and G. Hu, "Nonlinear state estimation under bounded noises," *Automatica,* vol. 98, pp. 159-168, 2018.

[7] D. Ding, Q. Han, Y. Xiang, X. Ge, and X. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing,* vol. 275, pp. 1674-1683, 2018.

[8] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS attack scheduling in wireless networked control system," *IEEE Transactions on Control Systems Technology,* vol. 24, no. 3, pp. 843-852, May 2016.

[9] X. Li, Z. Tian, and D. Lu, "Event-triggered protocol-based control for cyber–physical systems vulnerable to dual-channel DoS attacks," *IEEE Transactions on Control Systems Technology,* 2024, doi: 10.1109/TCST.2024.3477936.

[10] J. Lu and D. E. Quevedo, "A jointly optimal design of control and scheduling in networked systems under denial-of-service attacks," *Automatica,* vol. 148, 110774, 2023.

[11] Y. Dong, N. Gupta, and N. Chopra, "False data injection attacks in bilateral teleoperation systems," *IEEE Transactions on Control Systems Technology,* vol. 28, no. 3, pp. 1168-1176, May 2020.

[12] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Transactions on Control Systems Technology,* vol. 22, no. 4, pp. 1396-1407, July 2014.
[13] X. Yan, G. Zhou, D. E. Quevedo, C. Murguia, B. Chen, and H. Huang, "Privacy-preserving state estimation in the presence of eavesdroppers: A survey," *IEEE Transactions on Automation Science and Engineering,*, vol. 22, pp. 6190-6207, 2025.
[14] X. Yan, Y. Zhang, D. Xu, and B. Chen, "Distributed confidentiality fusion estimation against eavesdroppers," *IEEE Transactions on Aerospace and Electronic Systems,* vol. 58, no. 4, pp. 3633-3642, 2022
[15] A. S. Leong, D. E. Quevedo, D. Dolz, and S. Dey, "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, pp. 3732-3739, Sept. 2019.
[16] M. S. Darup, A. B. Alexandru, D. E. Quevedo, and G. J. Pappas, "Encrypted control for networked systems: An illustrative introduction and current challenges," *IEEE Control Systems Magazine,* vol. 41, no. 3, pp. 58-78, 2021.
[17] X. Yan, G. Zhou, Y. Huang, W. Meng, A.-T. Nguyen, H. Huang, "Secure estimation using partially homomorphic encryption for unmanned aerial systems in the presence of eavesdroppers," *IEEE Transactions on Intelligent Vehicles,* 2024, doi: 10.1109/TIV.2024.3378288.
[18] Z. Zhang, P. Cheng, J. Wu, and J. Chen, "Secure state estimation using hybrid homomorphic encryption scheme," *IEEE Transactions on Control Systems Technology,* vol. 29, no. 4, pp. 1704-1720, July 2021.
[19] J. Le Ny and G. J. Pappas, "Differentially private filtering," *IEEE Transactions on Automatic Control,* vol. 59, no. 2, pp. 341-354, 2014.
[20] X. Yan, B. Chen, Y. Zhang, and L. Yu. "Guaranteeing differential privacy in distributed fusion estimation," *IEEE Transactions on Aerospace and Electronic Systems,* vol. 59, no. 3, pp. 3416-3423, 2023.
[21] X. Yan, B. Chen, Y. Zhang, and L. Yu, "Distributed encryption fusion estimation against full eavesdropping," *Automatica,* vol. 153, 111025, 2023.
[22] A. Tsiamis, K. Gatsis, and G. J. Pappas, "State-secrecy codes for networked linear systems," *IEEE Transactions on Automatic Control,* vol. 65, no. 5, pp. 2001-2015, 2020.
[23] M. Lücke, J. Lu, and D. E. Quevedo, "Coding for secrecy in remote state estimation with an adversary," *IEEE Transactions on Automatic Control,* vol. 67, no. 9, pp. 4955-4962, Sept. 2022.
[24] J. M. Kennedy, J. J. Ford, D. E. Quevedo, and F. Dressler, "Innovation-based remote state estimation secrecy with no acknowledgments," *IEEE Transactions on Automatic Control,* vol. 69, no. 11, pp. 7433-7448, Nov. 2024.
[25] M. Ristic, B. Noack, and U. D. Hanebeck, "Cryptographically privileged state estimation with Gaussian keystreams," *IEEE Control Systems Letters,* vol. 6, pp. 602-607, 2022.
[26] A. K. Panda and K. C. Ray, "A coupled variable input LCG method and its VLSI architecture for pseudorandom bit generation," *IEEE Transactions on Instrumentation and Measurement,* vol. 69, no. 4, pp. 1011-1019, April 2020.
[27] A. Kerckhoffs, "La cryptographie militaire," *Journal des sciences militaires,* vol. IX, pp. 5-83, Jan. 1883.

Xinhao Yan (Graduate Student Member, IEEE) received the B.Eng. degree in communication engineering and the M.Eng. degree in control science and engineering from Zhejiang University of Technology, Hangzhou, China, in 2020 and 2023, respectively. He is currently pursuing the Ph.D. degree at the Department of Aeronautical and Aviation Engineering, The Hong Kong Polytechnic University, Hong Kong. In 2023, he was a recipient of the Outstanding Master's Thesis Award of Chinese Association of Automation. His current research interests include estimation and control, security and privacy, information fusion, cyber-physical systems, machine learning, and intelligent vehicles.

Daniel E. Quevedo (Fellow, IEEE) received Ingeniero Civil Electrónico and MSc degrees from Universidad Técnica Federico Santa María, Valparaíso, Chile, in 2000, and in 2005 the PhD degree from the University of Newcastle, Australia. Since 2024 he has been Professor of Electrical and Computer Engineering at The University of Sydney. Prior to his current appointment he served as a faculty at Queensland University of Technology in Brisbane and at Paderborn University, Germany. In 2003 he received the IEEE Conference on Decision and Control Best Student Paper Award and was also a finalist in 2002. He is co-recipient of the 2018 IEEE Transactions on Automatic Control George S. Axelby Outstanding Paper Award.

Prof. Quevedo currently serves as Associate Editor for *IEEE Control Systems*, for *IEEE Transactions on Control of Network Systems* and in the Editorial Board of the *International Journal of Robust and Nonlinear Control*. From 2015–2018 he was Chair of the IEEE Control Systems Society *Technical Committee on Networks & Communication Systems*. His research interests are in networked control systems, control of power converters and cyberphysical systems security.

Bo Chen (Senior Member, IEEE) received the B.S. degree in information and computing science from Jiangxi University of Science and Technology, Ganzhou, China, in 2008, and the Ph.D degree in Control Theory and Control Engineering from Zhejiang University of Technology, Hangzhou, China, in 2014. He jointed the Department of Automation, Zhejiang University of Technology in 2018, where he is currently a Professor. He was a Research Fellow with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from 2014 to 2015 and from 2017 to 2018. He was also a Postdoctoral Research Fellow with the Department of Mathematics, City University of Hong Kong, Hong Kong, from 2015 to 2017. His current research interests include information fusion, distributed estimation and control, networked fusion systems, and secure estimation of cyber-physical systems. Prof. Chen was a recipient of the Outstanding Thesis Award of Chinese Association of Automation in 2015 and also was a recipient of the First Prize of Natural Science of Ministry of Education in 2020. He serves as Associate Editor for IET Control Theory and Applications, Journal of the Franklin Institute and Frontiers in Control Engineering, and also serves as Guest Editor for IEEE Transactions on Industrial Cyber-Physical Systems.

Hailong Huang (Senior Member, IEEE) received his Ph.D degree in Systems and Control from the University of New South Wales, Sydney, Australia, in 2018. He was a post-doctoral research fellow at the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia. He is now an Assistant Professor at the Department of Aeronautical and Aviation Engineering, the Hong Kong Polytechnic University, Hong Kong. He is also the Program Leader of MSc for Low-Altitude Economy. His current research interests include guidance, navigation, and control of UAVs and mobile robots. He is an Associate Editor of IEEE Transactions on Automation Science and Engineering, Journal of Field Robotics, IEEE Transactions on Vehicular Technology, IEEE Transactions on Intelligent Vehicles, and Intelligent Service Robotics and International Journal of Advanced Robotic Systems, an editorial board member of the International Journal of Dynamics and Control, the registration chair of IEEE International Conference on Control & Automation.