Control Layer Security: Exploiting Unobservable Cooperative States of Autonomous Systems for Secret Key Generation

Zhuangkun Wei[1], Weisi Guo[1,2,*]

***Abstract*—The rapid growth of autonomous systems (ASs) with data sharing means new cybersecurity methods have to be developed for them. Existing computational complexity-based cryptography does not have information-theoretical bounds and poses threats to superior computational attackers. This post-quantum cryptography issue indeed motivated the rapid advances in using common physical layer properties to generate symmetrical cipher keys (known as PLS). However, PLS remains sensitive to attackers (e.g., jamming) that destroy its prerequisite wireless channel reciprocity. When ASs are in cooperative tasks (e.g., rescuing searching, and formation flight), they will behave cooperatively in the control layer. Inspired by this, we propose a new security mechanism called control layer security (CLS), which exploits the correlated but unobservable states of cooperative ASs to generate symmetrical cipher keys. This idea is then realized in the linearized UAV cooperative control scenario. The theoretical correlation coefficients between Alice's and Bob's states are computed, based on which common feature selection and key quantization steps are designed. The results from simulation and real UAV experiments show i) an approximately 90% key agreement rate is achieved, and ii) even an Eve with the known observable states and systems fails to estimate the unobservable states and the secret keys relied upon, due to the multiple-to-one mapping from unobservable states (pitch, roll and yaw angles) to the observable states (3D trajectory). This demonstrates CLS as a promising candidate to secure the communications of ASs, especially in the adversarial radio environment with attackers that destroys the prerequisite for current PLS.**

***Index Terms*—Cybersecurity, cooperative control, secret key generation, wireless communication, autonomous systems**

I. Introduction

Autonomous systems (AS) cover a broad range of platforms that have various degrees of autonomy, typically in control (stabilizing movement) and navigation (completing a mission objective). ASs that require control and navigation include but are not limited to autonomous vehicles, aerial drones, robots, and maritime vessels. Typically ASs cooperate to achieve a common purpose, or have to cooperate because they share a common space (e.g., a road or air corridor) [1]. Examples of cooperative ASs include platoon driving [2], swarm robotics [3], collision avoidance [4], [5], formation flying [6]. In all these cooperative cases, ASs observe each other via direct sensing or data exchange to achieve synchronized behaviour.

[1]School of Aerospace, Transport, and Manufacturing, Cranfield University, MK43 0AL, UK. [2]The Alan Turing Institute, UK. This work is funded by EPSRC TAS-S: Trustworthy Autonomous Systems: Security (EP/V026763/1). *Corresponding Author: weisi.guo@cranfield.ac.uk.

A. Review of Cybersecurity

Cybersecurity for wireless communications is important to secure the knowledge exchange between ASs and other stakeholders. Examples of wireless data transfer include the sensor data collected by ASs to map an environment, the position-navigation-timing signals to ensure safe navigation, and the federated gradient knowledge. Several wireless security approaches exist and we attempt to summarize them below in different categories. We then differentiate the proposed control layer security (CLS) from them.

1) Mathematical Complexity-based Cryptography: Cryptography relies on mathematical and computational complexity to pursue secret key generation, key management and key distribution [7]. The challenge lies in the lack of information-theoretically security [8], as most of the popular algorithms leverage the complexity of mathematical problems, e.g., the integer factorization problem, the discrete logarithm problem, and the elliptic-curve discrete logarithm problem. However, most of these security algorithms could be compromised by eavesdroppers (Eve) equipped with powerful quantum computers [9], [10].

2) Physical Mechanism-based Cipher Key: To achieve the information-theoretically security, an increasing effort has been spent on studying and exploiting the physics mechanism for symmetric cipher key generation. The most well-known example is the quantum key distribution (QKD), which leverages the quantum mechanisms (e.g., entanglement and indeterminacy) to create linked quantum states of two legitimate parties for symmetrical secret key generation [11], [12]. The main challenge is the extremely high cost of the devices for quantum entanglement and state measuring, and the prerequisite of existing authenticated channels.

3) Physical Layer to Graph Layer Security: Physical layer security (PLS) broadly covers a range of techniques in using physical attributes of the radio channel to secure data. At the very basic level, key-less PLS tries to maintain the superiority of legitimate channels by maximizing the secrecy rate in terms of the signal-to-interference-and-noise ratio (SINR). The corresponding works can be listed as the optimizations of beam steering/forming [13], AS's trajectory [13], anti-jamming artificial noise [14], or even leveraging the reconfigurable intelligent surface (RIS) to manipulate channels [15], [16]. The drawback of key-less PLS is the high dependency of Eve's channel statistics and the lack of guarantee of a feasible solution especially when combined with real-world constraints (e.g., from control and mission layers).

Another family of PLS leverages the wireless channel randomness that is reciprocal and unique at two legitimate parties to generate symmetrical secret keys (known as the physical layer secret key generation, PL-SKG) [17]–[21]. In this case, two legitimate parties (e.g., Alice and Bob) are required to send public pilot sequences to each other and pursue channel estimations to acquire this common channel state information (CSI) [22], [23], which will then be passed to the key quantization [24], [25], key reconciliation [26] and privacy amplification [27] modules for key generation. However, as PL-SKG derives its security from the very radio channel it is trying to protect, it remains sensitive to jamming [28], [29], secrecy leakage [30], high noise, poor channel entropy or reciprocity, and poor channel estimation quality.

Graph Layer Security (GLS) advances PLS to common sensed network states to encrypt digital data [31]. For example, two robots monitoring a sewage network can use commonalities in water flow to generate symmetrical cipher keys. This removes the prerequisite of channel reciprocity and the channel estimation dependency of PLS, pushing the burden to physical sensor accuracy. However, ASs do not usually share a common physical network (e.g., water or gas pipelines), and must seek other common states to exploit.

B. Motivation

As the aforementioned vulnerability of PLS to maintain channel reciprocity (under jamming) for ASs, this work aims to explore the common source from the cooperative control layer to generate symmetrical cipher keys. When ASs are in cooperative tasks (e.g., rescuing searching, platoon driving, and formation flight), they will behave cooperatively in the control layer. This yields the potential to exploit the mutual states of legitimate ASs to generate symmetric secret keys. In this work, we will study the existence of correlated states via cooperative control, and provide a secret key generation scheme relying on the cooperative control layer.

C. Novelty and Organisation

In this work, we show for the first time a new security mechanism called control layer security (CLS). In essence, CLS first creates state correlations between two legitimate ASs by cooperative but distributed control, and then exploits the unobservable & correlated states to generate symmetrical secret keys. The main contributions are listed in the following.

(1) We propose the basic idea of CLS, which aims to generate secured cipher keys at Alice and Bob. The commonality for cipher keys comes from the highly correlated states of two ASs by cooperative but distributed control. The security leverages Alice's (Bob's) secured states, which are unobservable and inestimable to Eves, due to the multiple-to-one mappings, e.g., UAV's different yaw, pitch, and roll angles (difficult to be measured by Eves) can reach the same trajectory (easily observed by Eves).

(2) We then realize this idea and provide a schematic flow to implement CLS in linearized UAV dynamics with cooperative and distributed controls. The theoretical expression of correlation coefficients is deduced in an iterative form, and further adds evidence to our CLS concept. Leveraging this, Alice and Bob can pursue selections of highly correlated and unobservable states, which then serve as the control layer common features for further key quantization, reconciliation and privacy amplification steps.

(3) We next propose and analyze three types of potential Eves, with the increasing knowledge of Alice's and Bob's observable states and dynamic & control model. Especially, a model-awareness Eve with the full knowledge of models and Alice's and Bob's 3D trajectories is considered. Neither of them can successfully estimate the unobservable states and the secret keys relied upon, due to the multiple-to-one mapping from unobservable states (e.g., pitch, roll, and yaw angles) to the observed trajectory states.

(4) We evaluate our proposed CLS via simulations. The results show high correlation coefficients (≈ 1) and promising secret key capacity (in terms of mutual information) of the selected Alice's and Bob's states, under cm to m levels of observing errors. As such, our proposed CLS provides a promising candidate to secure the data exchange of ASs, especially in the adversarial radio environment where the prerequisite of PL-SKG (channel reciprocity, rich entropy) does not hold.

The rest of this work is structured as follows. In Section II, we provide related works and background. In Section III, we describe the dynamic and cooperative control model of ASs, and how it would be used for cipher key designs. In Section IV, we elaborate on the idea and implementation of CLS, and analyze its capability on defending against potential Eves. In Section V, the simulation and real experimental results are illustrated. We finally conclude this work in Section VI.

II. Related Works & Background

To secure wireless communication between legitimate autonomous systems, recent studies focus on physical layer key generation methods, which avoid the computational complexity-based cryptography. In essence, PL-SKG exploits the reciprocal and random wireless channel properties (e.g., received signal strength RSS [18], [24] and CSI [22], [23], [32]) estimated at Alice and Bob for secret key generation, which are unique and different from those estimated at any Eve (that is half-wavelength from Alice and Bob) [33], [34]. In the context of AS communications, PL-SKG can be pursued by using either the time-varying distance, or the reciprocal small-scale scattering-based Rayleigh CSI between Alice and Bob.

Distance-based PL-SKG treats the time-varying distance-based RSS between Alice and Bob as the common features [24], and feeds them into the key quantization method for symmetrical secret key generation. The drawback lies in that the positions of Alice and Bob can be observed by Eve (e.g., equipped with camera [35] or thermal camera [36] technologies). Given the LoS channel property among UAVs, Eve can easily reconstruct the legitimate distance-based RSS feature via their positions, and then crack the secret keys relied upon.

CSI-based PL-SKG leverages the small-scale scattering-induced Rayleigh CSIs that are reciprocal at Alice and Bob as

the common features, and feeds them into the key quantization method to generate symmetrical secret keys. From the existing works, the channel estimation results at Alice and Bob, denoted as $\hat{h}^{(a)}$ and $\hat{h}^{(b)}$, are written as $\hat{h}^{(a)} = h_{ba} + \epsilon^{(a)}$, and $\hat{h}^{(b)} = h_{ab} + \epsilon^{(b)}$ [32], [37], where $\epsilon^{(a)}, \epsilon^{(b)}$ are the estimating noises at Alice and at Bob, respectively. h_{ab} and h_{ba} are the small-scale scattering components of Alice to Bob and Bob to Alice channels. The threats for CSI-based PL-SKG are categorized as the following two main aspects. First, the channel reciprocity (i.e., $h_{ab} = h_{ba}$) serves as the prerequisite for secret key generation, since it guarantees the commonality between Alice's and Bob's channel estimation results. This therefore suggests that the CSI-based PL-SKG is sensitive to attacks such as jamming [28], [29], [38], which destroys the channel reciprocity, i.e., making $h_{ab} \neq h_{ba}$. Second, even if the channel reciprocity holds, the channels between Alice and Bob (e.g., UAVs) are dominated mostly by LoS channel, which suggests the insufficient randomness of the NLoS small-scale channel scattering for key generation.

Given the aforementioned challenges of PLS to secure the legitimate AS channel, this work aims to explore the common source from the cooperative control layer to generate symmetrical cipher keys. To the best of our knowledge, this is the first paper to propose the concept of control layer security. Autonomous systems (e.g., UAV, UGV, and robotics) are generally modelled as the differential equations that describe the evolution of states [39], [40]. When ASs are in cooperative tasks (e.g., cooperative control exists for a wide range of tasks, e.g., rescuing searching, platoon driving, formation flight, swarm tasking ... etc), they will be cooperative in the control layer, which leads to the mutual states of legitimate ASs for symmetric cipher key generation. In the following of this work, we will show the existence of correlated states via cooperative control, and propose a CLS-based symmetrical cipher generation scheme.

III. System Model

In this work, we consider two legitimate ASs (Alice and Bob) which are cooperatively and distributed controlled by themselves for a given task. Alice and Bob here aim to generate symmetrical secret keys to protect their communication from eavesdropping by a potential Eve. In this work, rather than exploiting the wireless channel properties between Alice and Bob, we propose a novel symmetrical secret key generation scheme using their correlated and unobservable states that are cooperatively controlled. As such, the system modelling is composed of (i) the dynamic & control model for secret key generation, and (ii) the wireless communication model whose data is encrypted by the CLS-based secret key.

A. Dynamic & Control Model

1) Dynamic model: Two legitimate ASs, Alice and Bob, are modelled as two discrete identical ordinary differential equation (ODE) systems, i.e.,

$$\begin{aligned} \mathbf{x}_k^{(i)} &= \mathbf{A} \cdot \mathbf{x}_{k-1}^{(i)} + \mathbf{B} \cdot \mathbf{u}_{k-1}^{(i)}, \\ \mathbf{y}_k^{(i)} &= \mathbf{C} \cdot \mathbf{x}_k^{(i)} + \boldsymbol{\varepsilon}_k^{(i)}, \qquad i \in \{a(\text{Alice}), b(\text{Bob})\}. \end{aligned} \tag{1}$$

In Eq. (1), $\mathbf{x}_k^{(i)} \in \mathbb{R}^N$ is the N-stacked state of AS i at discrete time-step k, which is assumed to be obtained by AS i via embedding corresponding sensors on its own system. $\mathbf{A}$ of size $N \times N$ is the dynamic evolution matrix. $\mathbf{B}$ of size $N \times J$ is to transform the control signal $\mathbf{u}_{k-1}^{(i)} \in \mathbb{R}^J$ into state-space.

In Eq. (1), $\mathbf{y}_k^{(i)} \in \mathbb{R}^C$ is the observable states of AS i at k time-step. Here, we assume $\mathbf{y}_k^{(i)}$ is observable to other legitimate ASs and Eves (i.e., the observable states are shared information among all ASs). $\boldsymbol{\varepsilon}_k^{(i)} \sim \mathcal{N}(0, \boldsymbol{\Sigma})$ is the observing noise, with $\boldsymbol{\Sigma}$ the covariance matrix. $\mathbf{C}$ of size $C \times N$ is the observation matrix. Here, we assume $C < N$, e.g., the trajectory of a UAV can be easily observed by others, but its pitch, roll, and yaw angles are hard to be measured by others, e.g., due to the distance and geometric symmetry of a quadcopter. As such, we denote the remained states in $\mathbf{x}_k^{(i)}$ from $\mathbf{C}\mathbf{x}_k^{(i)}$ as the unobservable states. In Section IV. C, we will evaluate the security under three types of Eves, with the increase of the knowledge of Alice's and Bob's observable states and systems.

2) Control Signal Model: In cooperative and distributed control, we assign the control signals at two ASs by involving each other's observable states, i.e.,

$$\mathbf{u}_k^{(i)} = \mathbf{g}_{\boldsymbol{\phi}_1, \boldsymbol{\phi}_2, \boldsymbol{\phi}_3}\left(\mathbf{x}_k^{(i)}, \mathbf{y}_k^{(j)}, \mathbf{r}^{(i,ref)}\right), \; i \neq j \in \{a, b\}. \tag{2}$$

where $\mathbf{g}_{\boldsymbol{\phi}_1, \boldsymbol{\phi}_2, \boldsymbol{\phi}_3}(\cdot, \cdot, \cdot)$ is determined by specific control algorithms, and $\mathbf{r}^{(i,ref)}$ is the reference that is required to be achieved by the states. One implementation of Eq. (2) is provided in the experimental and simulation section.

From Eqs. (1)-(2), we emphasize three facts that will be used for further secret key generation. First, the AS's state has randomness, induced by (i) the distribution of initial states, (ii) the introduced observing noise from control signals, and (iii) the adjusted references given the random changes of the environment (e.g., an obstacle appears/disappears). Second, there exist correlations between the states of Alice and Bob, due to the involvement of other's observable states in their control signals (further deduced by Eq. (6) and illustrated by Fig. 1(b)). Third, the unobservable states create security to potential Eves, since Eve cannot estimate them via observable states, given the multiple-to-one mapping from unobservable to observable states (e.g., the UAV with forward trajectory can be pursued either by direct pitch angle controlling or by clockwise yawing $\pm 90^\circ$ and rolling). These three thereby render the potentials to exploit the cooperatively controlled ASs' state to generate random & symmetrical cipher keys.

B. Communication Model

After the secret key generated from the control layer, such cipher key will be used to secure the data transmitted between legitimate ASs. Here, different from PLS which requires the specification of communication models, control layer based secret keys do not involve any communication channel property, but can be used to encrypt the binary stream for further transmission.

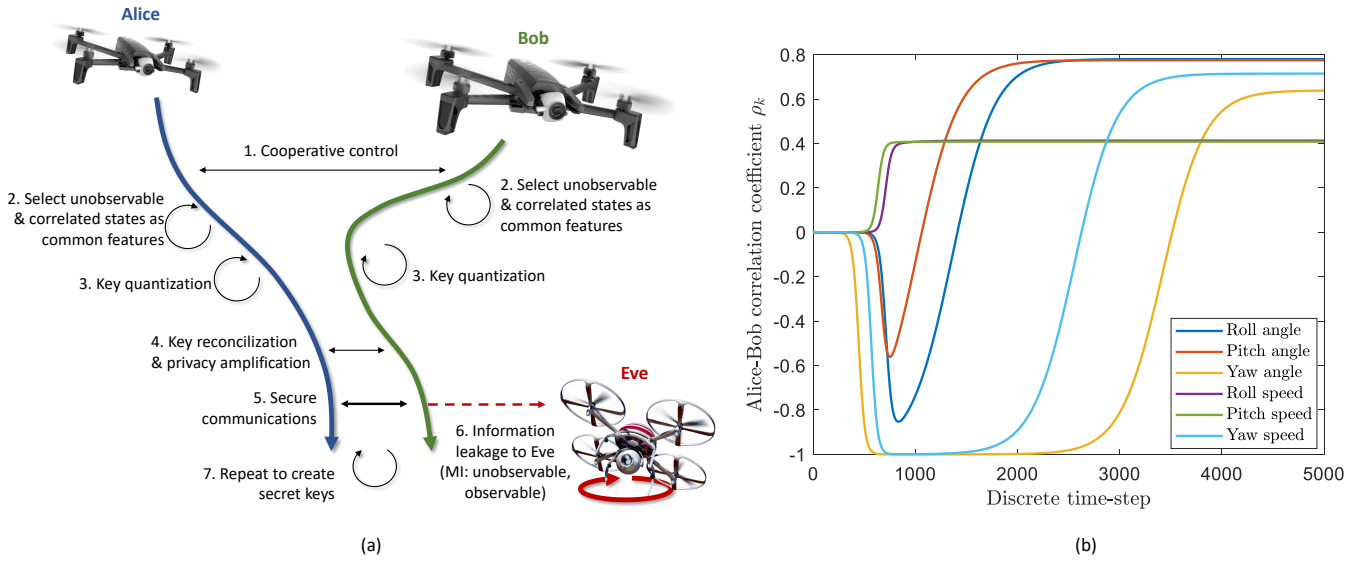


Fig. 1. Illustration of proposed CLS. (a) provides the schematic flow by (1) cooperative control to generate correlated states, (2) feature construction at Alice and Bob via their unobservable and correlated states, (3) key quantization, (4) key reconciliation and privacy amplification, and (5) securing the wireless communication via the derived secret key. (b) shows the theoretical correlation coefficients of Alice's and Bob's unobservable states (e.g., roll, pitch, yaw angles and their angular speeds) in Eq. (6), by cooperative control.

IV. Theory & Implementation of Control Layer Security

In this section, we elaborate on our CLS-based symmetrical secret key generation, and analyze its potential to defend against Eves. The schematic flow of CLS is provided in Fig. 1(a), whereby Alice's and Bob's correlated and unobservable states are created by cooperative control, and selected as common features, to feed into the further key quantization, reconciliation, and privacy amplification steps for final cipher keys generations.

A. Theory of Correlated States by Cooperative Control

We firstly compute the element-wise theoretical correlation coefficient of $\mathbf{x}_k^{(a)}$ and $\mathbf{x}_k^{(b)}$, which is defined as:

$$\boldsymbol{\rho}_k \triangleq diag(\mathbf{R}_k) \oslash \sqrt{diag\left(\mathbf{D}_k^{(a)}\right) \odot diag\left(\mathbf{D}_k^{(b)}\right)} \tag{3}$$

where $diag(\cdot)$ is to make a vector using the diagonal elements of a matrix, $\oslash$ is the element-wise division, and $\odot$ is the element-wise multiplication. The definitions of $\mathbf{R}_k$ and $\mathbf{D}_k^{(i)}$ are provided as follows:

$$\begin{aligned}\mathbf{R}_k \triangleq& \mathbb{E}\left(\mathbf{x}_k^{(a)} \cdot \left(\mathbf{x}_k^{(b)}\right)^T\right) - \mathbb{E}\left(\mathbf{x}_k^{(a)}\right) \cdot \mathbb{E}\left(\mathbf{x}_k^{(b)}\right)^T,\\ \mathbf{D}_k^{(i)} \triangleq& \mathbb{E}\left(\mathbf{x}_k^{(i)} \cdot \left(\mathbf{x}_k^{(i)}\right)^T\right) - \mathbb{E}\left(\mathbf{x}_k^{(i)}\right) \cdot \mathbb{E}\left(\mathbf{x}_k^{(i)}\right)^T\end{aligned} \tag{4}$$

where $\mathbb{E}(\cdot)$ represents the expectation.

To facilitate the computation of $\boldsymbol{\rho}_k$, we approximate the control signal using the first-order Taylor expansion, i.e.,

$$\begin{aligned}\mathbf{u}_k^{(i)} \approx& \boldsymbol{\Theta}_1 \cdot \mathbf{x}_k^{(i)} + \boldsymbol{\Theta}_2 \cdot \mathbf{y}_k^{(j)} + \boldsymbol{\Theta}_3 \cdot \mathbf{r}^{(i,ref)},\\ =& \boldsymbol{\Theta}_1 \cdot \mathbf{x}_k^{(i)} + \boldsymbol{\Theta}_2 \cdot \mathbf{C}\mathbf{x}_k^{(j)} + \boldsymbol{\Theta}_3 \cdot \mathbf{r}^{(i,ref)} + \mathbf{n}_k^{(i)},\end{aligned} \tag{5}$$

where $\boldsymbol{\Theta}_n \triangleq \partial \mathbf{g} / \partial (\boldsymbol{\phi}_n^T)$, $n \in \{1,2,3\}$, and $\mathbf{n}_k^{(i)} \triangleq \boldsymbol{\Theta}_2 \boldsymbol{\varepsilon}_k^{(j)}$. Here, the reason to choose the first-order Taylor expansion is to show that the linear part of cooperative control signals can generate correlated states of legitimate ASs, which corresponds to examples of linear controllers such as linear quadratic regulator (LQR). Further studies will focus on designing and analyzing nonlinear cooperative controllers (e.g., from reinforcement learning), and the Runge-Kutta method will be used for analyzing.

Then, $\mathbf{R}_k$ and $\mathbf{D}_k^{(i)}$ can be iteratively computed as:

$$\begin{aligned}\mathbf{R}_{k+1} =& \bar{\mathbf{A}}\mathbf{R}_k\bar{\mathbf{A}}^T + \bar{\mathbf{B}}\mathbf{R}_k^T\bar{\mathbf{B}}^T + \bar{\mathbf{A}}\mathbf{D}_k^{(a)}\bar{\mathbf{B}}^T + \bar{\mathbf{B}}\mathbf{D}_k^{(b)}\bar{\mathbf{A}}^T\\ \mathbf{D}_{k+1}^{(a)} =& \bar{\mathbf{A}}\mathbf{D}_k^{(a)}\bar{\mathbf{A}}^T + \bar{\mathbf{A}}\mathbf{R}_k\bar{\mathbf{B}}^T + \bar{\mathbf{B}}\mathbf{R}_k^T\bar{\mathbf{A}}^T + \bar{\mathbf{B}}\mathbf{D}_k^{(b)}\bar{\mathbf{B}}^T + \boldsymbol{\Upsilon}\\ \mathbf{D}_{k+1}^{(b)} =& \bar{\mathbf{A}}\mathbf{D}_k^{(b)}\bar{\mathbf{A}}^T + \bar{\mathbf{A}}\mathbf{R}_k^T\bar{\mathbf{B}}^T + \bar{\mathbf{B}}\mathbf{R}_k\bar{\mathbf{A}}^T + \bar{\mathbf{B}}\mathbf{D}_k^{(a)}\bar{\mathbf{B}}^T + \boldsymbol{\Upsilon}\end{aligned} \tag{6}$$

where $\bar{\mathbf{A}} \triangleq \mathbf{A} + \mathbf{B}\boldsymbol{\Theta}_1$, $\bar{\mathbf{B}} \triangleq \mathbf{B}\boldsymbol{\Theta}_2\mathbf{C}$, and $\boldsymbol{\Upsilon} \triangleq \mathbf{B}\boldsymbol{\Theta}_2\boldsymbol{\Sigma}\boldsymbol{\Theta}_2^T\mathbf{B}^T$, with initial value $\mathbf{R}_1 = \mathbf{O}$ and $\mathbf{D}_1^{(i)}$ the covariance matrix of AS i's initial state. The detailed deduction is provided in Supplementary.

The proof of concept of CLS is provided in the following, where the control signal in Eq. (5) is implemented by the cooperative LQR. The quadratic objective functions for Alice and Bob are assigned as:

$$\begin{aligned}\min_{\mathbf{u}_k^{(i)}} \mathcal{L}^{(i)} =& \sum_{k=1}^{K-1}\left(\mathbf{x}_k^{(i)} - \mathbf{r}^{(i,ref)}\right)^T\mathbf{Q}\left(\mathbf{x}_k^{(i)} - \mathbf{r}^{(i,ref)}\right) + \left(\mathbf{u}_k^{(i)}\right)^T\mathbf{u}_k^{(i)}\\ &+ \lambda \cdot \left(\mathbf{C}\mathbf{x}_{k+1}^{(i)} - \mathbf{y}_k^{(j)}\right)^T\left(\mathbf{C}\mathbf{x}_{k+1}^{(i)} - \mathbf{y}_k^{(j)}\right)\\ \text{s.t., } \mathbf{x}_{k+1}^{(i)} =& \mathbf{A}\mathbf{x}_k^{(i)} + \mathbf{B}\mathbf{u}_k^{(i)},\ i \neq j \in \{a,b\}\end{aligned} \tag{7}$$

where $\mathbf{Q}$ is a predefined semi-positive matrix, and λ serves as the cooperation parameter (configured in Supplementary). Here, the cooperative term in Eq. (7) does not serve any specific mission purpose, but an illustrative form of Alice and Bob cooperation. Other realistic and sophisticated forms can be designed and added into Eq. (7). In Eq. (7), it is noticed that

the controllers of Alice and Bob are distributed at each side, and dependent only on the observations of each other, i.e., $\mathbf{y}_k^{(j)}$. By solving Eq. (7), the control signals can be specified as:

$$\mathbf{u}_k^{(i)} = \mathbf{\Theta}_1 \mathbf{x}_k^{(i)} + \mathbf{\Theta}_2 \mathbf{y}_k^{(j)} + \mathbf{\Theta}_3 \mathbf{r}^{(i,ref)},\ i \neq j \in \{a, b\} \quad (8)$$

with

$$\begin{aligned}
\mathbf{\Theta}_1 &= -\left(\mathbf{I}_J + \mathbf{B}^T\mathbf{P}\mathbf{B} + \lambda \mathbf{B}^T\mathbf{C}^T\mathbf{C}\mathbf{B}\right)^{-1}\left(\mathbf{B}^T\mathbf{P}\mathbf{A} + \lambda \mathbf{B}^T\mathbf{C}^T\mathbf{C}\mathbf{A}\right), \\
\mathbf{\Theta}_2 &= \lambda \cdot \left(\mathbf{I}_J + \mathbf{B}^T\mathbf{P}\mathbf{B} + \lambda \mathbf{B}^T\mathbf{C}^T\mathbf{C}\mathbf{B}\right)^{-1}\mathbf{B}^T\mathbf{C}^T, \\
\mathbf{\Theta}_3 &= \left(\mathbf{I}_J + \mathbf{B}^T\mathbf{P}\mathbf{B} + \lambda \mathbf{B}^T\mathbf{C}^T\mathbf{C}\mathbf{B}\right)^{-1}\mathbf{B}^T\mathbf{P},
\end{aligned} \quad (9)$$

where $\mathbf{P}$ is the solution of Riccati function, i.e., $\mathbf{P} = \mathbf{Q} + \mathbf{A}^T\mathbf{P}\mathbf{A} - \mathbf{A}^T\mathbf{P}\mathbf{B}(\mathbf{I}_J + \mathbf{B}^T\mathbf{P}\mathbf{B})^{-1}\mathbf{B}^T\mathbf{P}\mathbf{A}$. The detailed deduction are displayed in Supplementary.

Under the control signal designed in Eqs. (8)-(9), the theoretical correlation coefficients of Alice's and Bob's states are plotted in Fig. 1(b). It is seen that in the process of the cooperative controlling of Alice and Bob, the correlation coefficients of their states (the absolute value) reach 1. This suggests that we can select a set of correlated states, whose correlation coefficients approach 1. Then, such selected states can be used as the common feature to generate the symmetrical cipher keys.

B. Common Feature Selection & Secret Key Generation

Leveraging the theoretical computation of the correlation coefficients $\boldsymbol{\rho}_k$ between Alice's and Bob's states, the secret key generation process can be provided. We first assign $M \in \mathbb{N}^+$ referenced destinations (i.e., 3D positions) for Alice and Bob, i.e., $\mathbf{r}_1^{(i,ref)}, \cdots, \mathbf{r}_M^{(i,ref)},\ i \in \{a, b\}$, whereby Alice and Bob are required to be cooperatively controlled to these destinations one-by-one. Then, we define m-th key generation round as the K controlling time-steps from last destination $\mathbf{r}_m^{(i,ref)}$ to current $\mathbf{r}_{m+1}^{(i,ref)}$. The detailed secret key generation relies on how to select common features, and how to generate keys from the common features.

1) Common Feature Index Set: After the computations of the theoretical correlation coefficients of Alice's and Bob's states, i.e., $\boldsymbol{\rho}_1, \cdots, \boldsymbol{\rho}_K$ from Eq. (3) and Eq. (6), a set of indices where Alice's and Bob's states that are theoretically proved to have high correlations can be constructed as:

$$\mathcal{G} = \{(s, k) |\ |\rho_{s,k}| > \varrho, s \neq \mathbf{C} \cdot \boldsymbol{\iota}\}. \quad (10)$$

where $\rho_{s,k}$ is the sth element of $\boldsymbol{\rho}_k$, and $\boldsymbol{\iota} \triangleq [1, \cdots, N]^T$. In Eq. (10), ϱ is a threshold to guarantee the large correlation coefficients of selected Alice's and Bob's states. $s \neq \mathbf{C} \cdot \boldsymbol{\iota}$ is to ensure the selected states cannot be observed by potential Eve (Further details will be provided in Section IV-C). Then, common features can be selected separately at Alice and Bob as the states whose indices belong to this common feature index set.

2) Common Feature Selection: For each mth key generation round, Alice and Bob construct common features at both sides as:

$$\begin{aligned}
\mathbf{f}^{(a)} &= \left[x_{g_1}^{(a)}, \cdots, x_{g_L}^{(a)}\right]^T, \\
\mathbf{f}^{(b)} &= \left[sgn(\rho_{g_1}) \cdot x_{g_1}^{(b)}, \cdots, sgn(\rho_{g_L}) \cdot x_{g_L}^{(b)}\right]^T,
\end{aligned} \quad (11)$$

where g_l is the lth element of set $\mathcal{G}$. With $g_l = (s, k)$, $x_{g_l}^{(a)}$ ($x_{g_l}^{(b)}$) is the sth element of $\mathbf{x}_k^{(a)}$ ($\mathbf{x}_k^{(b)}$), and $sgn(\rho_{g_l})$ is the sign of $\rho_{s,k}$, in order to make the same signs of Alice's and Bob's features.

3) Secret Keys from Common Feature: Given the constructed features, the secret key, denoted as $\boldsymbol{\psi}^{(i)} = [\psi_1^{(i)}, \cdots, \psi_L^{(i)}]^T$, can be generated via the key quantization method, i.e.,

$$\psi_l^{(i)} = \begin{cases} 1 & f_l^{(i)} > \gamma_{l,+}^{(i)} \\ 0 & f_l^{(i)} < \gamma_{l,-}^{(i)} \end{cases},\ i \in \{a, b\}, \quad (12)$$

where $f_l^{(i)}$ is the lth element of vector $\mathbf{f}^{(i)}$. $\gamma_{l,\pm}^{(i)}$ are the upper and lower quantization thresholds, which are assigned as [25]:

$$\gamma_{l,\pm}^{(i)} \triangleq \mathbb{E}\left(f_l^{(i)}\right) \pm \beta \cdot D_k^{(i)}(s, s),\ \beta \in [0, 0.5). \quad (13)$$

In Eq. (13), β is the quantization parameter. $D_k^{(i)}(s, s)$ is the variance of $f_l^{(i)} = x_{g_l}^{(i)}$ given $g_l = (s, k)$, which is actually the (s, s)th element of $\mathbf{D}_k^{(i)}$ computed in Eq. (6). $\mathbb{E}(f_l^{(i)}) = \mathbb{E}(x_{g_l}^i)$ is the mean of $f_l^{(i)}$, the sth element of $\mathbb{E}(\mathbf{x}_k^{(a)})$, which can be computed as follows:

$$\begin{aligned}
\mathbb{E}\left(\mathbf{x}_k^{(a)}\right) &= \bar{\mathbf{A}} \cdot \mathbb{E}\left(\mathbf{x}_{k-1}^{(a)}\right) + \bar{\mathbf{B}} \cdot \mathbb{E}\left(\mathbf{x}_{k-1}^{b)}\right) + \mathbf{B}\mathbf{\Theta}_3 \cdot \mathbf{r}_m^{(a,ref)}, \\
\mathbb{E}\left(\mathbf{x}_k^{(b)}\right) &= \bar{\mathbf{A}} \cdot \mathbb{E}\left(\mathbf{x}_{k-1}^{(b)}\right) + \bar{\mathbf{B}} \cdot \mathbb{E}\left(\mathbf{x}_{k-1}^{a)}\right) + \mathbf{B}\mathbf{\Theta}_3 \cdot \mathbf{r}_m^{(b,ref)}.
\end{aligned} \quad (14)$$

After the key generation at Alice and Bob, key reconciliation [26] and privacy amplification [27] can be done to derive the final secret key. In brief, key reconciliation can be pursued by one legitimate node sending the redundant part of its error-correction coded keys to the other to achieve high probability key agreement. Then, privacy amplification can be adopted to further remove the revealed information and enhance the key lengths. For example, one privacy amplification method is based on the digital chaotic system [41], i.e., $\varphi_{t+1} = \alpha \cdot \varphi_t(1 - \varphi_t)$, where $t \in \mathbb{N}^+$ represents the tth iteration, and $\alpha \in [3.574, 4]$ denotes the bifurcation parameter. By being equipped with the same chaotic system, Alice and Bob can feed their reconciled keys as the initial input (i.e., φ_1), and the output chaotic results can be used as the final key with compatible lengths to communication streaming. In this work, we mainly focus on the control layer feature construction and key quantization steps, since the feature space serves as the only source of common randomness for further key generation steps, and the key quantization by which features are transformed into binary keys enables the evaluation of our CLS design.

Algorithm 1: CLS-based Secret Key Generation (take Alice as an example)

Input: System model $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{C}$, and M referenced destinations for Alice to achieve one-by-one $\mathbf{r}_1^{(a,ref)}, \cdots, \mathbf{r}_M^{(a,ref)}$

1 Compute $\mathbf{\Theta}_1$, $\mathbf{\Theta}_2$, $\mathbf{\Theta}_3$ for control signals via Eq. (9);
2 Compute the theoretical correlation coefficients of Alice's and Bob's states, i.e., $\boldsymbol{\rho}_1, \cdots, \boldsymbol{\rho}_K$ via Eq. (3) and Eq. (6);
3 Construct the common feature index set $\mathcal{G}$ via theoretical correlation coefficients, i.e., Eq. (10);
4 Given M referenced destinations $\mathbf{r}_1^{(a,ref)}, \cdots, \mathbf{r}_M^{(a,ref)}$,
for *each* $m = 1, \cdots, M$ *key generation round* **do**
5 **for** *each* $k = 1, \cdots, K$ *controlling time* **do**
6 Obtain state $\mathbf{x}_k^{(a)}$ via Alice's sensor reading;
7 Obtain $\mathbf{y}_k^{(b)}$ by observing Bob's 3D positions;
8 Compute control signal $\mathbf{u}_k^{(a)}$ via Eq. (8);
9 Use $\mathbf{u}_k^{(a)}$ to control its system (i.e., taking $\mathbf{u}_k^{(a)}$ into Eq. (1) in simulation);
10 **end**
11 Select feature $\mathbf{f}^{(a)}$ via common feature index set $\mathcal{G}$ and the state $\mathbf{x}_1^{(a)}, \cdots, \mathbf{x}_K^{(a)}$ using Eq. (11);
12 Generate binary secret keys using Eq. (12);
13 Using key reconciliation [26] and privacy amplification [27] to derive final secret keys.
14 **end**

Output: Alice's secret keys.

4) Overall Algorithm Flow: The overall algorithm flow for CLS-based secret key generation is provided in Algorithm 1. Here, we take Alice as an example. The inputs are the system and control signal models, i.e., $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{\Theta}_1$, $\mathbf{\Theta}_2$, and $\mathbf{\Theta}_3$ in Eq (1), and Eqs. (8)-(9), and the M referenced destination points for Alice UAV to achieve. Steps 1-3 are initialization to compute the theoretical correlation coefficients of Alice's and Bob's states, and the common feature index set $\mathcal{G}$ for further feature selection.

The number of reference destinations determines the number of key generation rounds. In each mth key generation round, we have K discretized controlling time-steps to control the state to achieve the mth reference destination $\mathbf{r}_m^{(a)}$. In each controlling time step, step 6 is to obtain Alice's own states via sensor reading, step 7 is to observe Bob's observable states, step 8 is to create distributed control signals via Alice's state and Bob's observable state, and step 9 is to control Alice UAV via the computed control signal. Next, step 11 is to select the common feature via the common feature index set, and step 12 is to generate secret keys via the common features.

C. Defending Potential Eves

After the elaboration of the CLS-based secret key generation, we study how secure the proposed key is against different types of Eves. Here, the Eves we considered only contain those aiming to use the observable states of Alice and Bob to reconstruct their unobservable states, from which they can regenerate the legitimate cipher keys. Other types of attackers (e.g., spoofing one of the legitimate users) are out of the scope of this work, as they do not attack the theory of CLS directly. To evaluate the security performance of our proposed CLS-based secret key, we consider three types of Eves, with the increase of the knowledge of Alice's and Bob's observable states and systems.

1) Type-1 Eve with Brute-Force: The brute-force Eve is assumed to be the simplest Eve without any knowledge of the Alice's and Bob's systems, i.e., Eq. (1), nor their observable states (3D positions and speeds), i.e., $\mathbf{y}_1^{(i)}, \cdots, \mathbf{y}_K^{(i)}$, $i \in \{a, b\}$. In this case, the control-layer common features of Alice and Bob, i.e., $\mathbf{f}^{(a)}$ and $\mathbf{f}^{(b)}$, cannot be estimated by Eve, so do the generated secret keys relied upon.

2) Type-2 Eve with Alice's and Bob's Observable States: We then consider if the Eve can obtain the observable of Alice and Bob, i.e., the 3D positions and the speeds shown in $\mathbf{y}_1^{(i)}, \cdots, \mathbf{y}_K^{(i)}$, $i \in \{a, b\}$. In this case, Eve will use the observed states as Alice's and Bob's selected states for key generation. So, to evaluate the security of the CLS-based secret key, we test the correlation coefficients between the observable and the selected states of Alice and Bob. For a given $g_l = (s, k) \in \mathcal{G}$, such correlation can be computed as:

$$\begin{aligned}
&\mathbb{E}\left(\mathbf{y}_k^{(i)} \cdot x_{g_l}^{(i)}\right) - \mathbb{E}\left(\mathbf{y}_k^{(i)}\right)\mathbb{E}\left(x_{g_l}^{(i)}\right) \\
=&\mathbb{E}\left(\mathbf{y}_k^{(i)} \cdot \left(\mathbf{c}_s^T \cdot \mathbf{x}_k^{(i)}\right)^T\right) - \mathbb{E}\left(\mathbf{y}_k^{(i)}\right)\mathbb{E}\left(\mathbf{c}_s^T \cdot \mathbf{x}_k^{(i)}\right)^T \\
=&\mathbf{C} \cdot \left(\mathbb{E}\left(\mathbf{x}_k^{(i)} \cdot \left(\cdot \mathbf{x}_k^{(i)}\right)^T\right) - \mathbb{E}\left(\mathbf{x}_k^{(i)}\right)\mathbb{E}\left(\mathbf{x}_k^{(i)}\right)^T\right) \cdot \mathbf{c}_s \\
=&\mathbf{C}\mathbf{D}_k^{(i)}\mathbf{c}_s,\ i \in \{a, b\},
\end{aligned} \tag{15}$$

where $\mathbf{c}_s$ is the $N \times 1$ vector where only sth element is 1 and others are 0. Then, the correlation coefficients can be computed as:

$$\left(\mathbf{C}\mathbf{D}_k^{(i)}\mathbf{c}_s\right) \oslash \sqrt{\mathbf{D}_k^{(i)}(s,s) \cdot diag\left(\mathbf{C}\mathbf{D}_k^{(i)}\mathbf{C}^T + \mathbf{\Sigma}\right)} \tag{16}$$

where $\mathbf{D}_k^{(i)}(s,s)$ is the (s,s)th element of $\mathbf{D}_k^{(i)}$, and $\mathbf{\Sigma}$ is the covariance matrix of observing errors, i.e., $\boldsymbol{\varepsilon}_k^{(i)}$ in Eq. (1).

The security of our proposed CLS when defending Type-2 Eve comes from three points. First, from Eq. (1), the correlation between observable and unobservable states is weakened by the observing noise, which contains the position measuring error and the enhanced speed estimation error from noisy positioning observations. Second, Type-2 Eve does not know which states are selected, as she does not know the dynamic & control model. Third, even if she can know which states are selected, in UAV control, there exists a multiple-to-one mapping from the unobservable pitch, roll and yaw angles to the observable trajectories (e.g., going forward can be pursued either by direct pitch angle controlling or by clock wisely yawing $\pm 90^\circ$ and rolling). This means the existence of information entropy loss (in terms of the low correlation coefficients) from observable to unobservable states. We further evaluate the correlation coefficients between the observable and unobservable states and the mentioned entropy loss in Figs. 4-5 in simulation section.

3) Type-3 Eve with dynamic models & observable states: We next consider a strong Eve with (i) the knowledge of AS's dynamic & control model, i.e., $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{\Theta}_1$, $\mathbf{\Theta}_2$ and $\mathbf{\Theta}_3$ in Eq. (1) and Eq. (5), (ii) the observations of Alice and Bob, i.e., $\mathbf{y}_k$ which represents the ASs' 3D positions and their corresponding velocities, and (iii) the required destinations of all M key generation rounds, i.e., $\mathbf{r}_1^{(i,ref)}, \cdots, \mathbf{r}_M^{(i,ref)}$. It is noteworthy that these assumptions are extremely strong (even if guessing the modelling and intention is a separate research flow), but we will show that even so, Eve still cannot estimate the CLS-based secret key generated at Alice and Bob.

From Eve's perspective, the derivation of the secret key can be converted to estimate Alice's and Bob's states, i.e., $\mathbf{x}_k^{(a)}, \mathbf{x}_k^{(b)}$ via the observed states $\mathbf{y}_k^{(a)}, \mathbf{y}_k^{(b)}, k = \{1, \cdots, K\}$. This is done by (i) estimating the initial state $\mathbf{x}_1^{(a)}$ and $\mathbf{x}_1^{(b)}$, and (ii) taking the estimated initial states into the sequential state estimation algorithms (e.g., Kalman filter [42], [43] or Bayesian filter [44], [45]) for further state estimation.

Next, we show that the estimation of the initial state from observed states cannot be successful. An intuitive reason is that there are multiple combinations of yaw, pitch, and roll angles that can map to the same UAV trajectory, which renders the difficulty for Eve to estimate them via the observed trajectory. From mathematical perspectives, we take Alice as an example. The relation between Eve's observation of Alice and Alice's initial state $\mathbf{x}_1^{(a)}$ is expressed by the following linear equation, i.e.,

$$\mathbf{z}^{(a)} = \tilde{\mathbf{A}} \cdot \mathbf{x}_1^{(a)} + \tilde{\mathbf{B}} \cdot \mathbf{n}^{(a)}. \tag{17}$$

In Eq. (17), $\mathbf{z}^{(a)} \triangleq \mathbf{y}^{(a)} - \tilde{\mathbf{B}}\mathbf{v}^{(a)}$ is constructed by Eve's observations of Alice, i.e., $\mathbf{y}^{(a)} = [(\mathbf{y}_1^{(a)})^T, \cdots, (\mathbf{y}_K^{(a)})^T]^T$, and Eve's observations of Bob, i.e., $\mathbf{v}^{(a)} = [(\mathbf{v}_1^{(a)})^T, \cdots, (\mathbf{v}_{K-1}^{(a)})^T]^T$ where $\mathbf{v}_k^{(a)} \triangleq \mathbf{\Theta}_2\mathbf{y}_k^{(b)} + \mathbf{\Theta}_3\mathbf{r}^{(a)}$. $\mathbf{n}^{(a)} \triangleq [(\mathbf{n}_1^{(a)})^T, \cdots, (\mathbf{n}_{K-1}^{(a)})^T]^T$ is the stacked control noise which cannot be known by Eve. $\tilde{\mathbf{A}}$ and $\tilde{\mathbf{B}}$ are defined as:

$$\tilde{\mathbf{A}} = \begin{bmatrix} \mathbf{C} \\ \mathbf{C}\bar{\mathbf{A}} \\ \vdots \\ \mathbf{C}\bar{\mathbf{A}}^{K-1} \end{bmatrix}, \ \tilde{\mathbf{B}} = \begin{bmatrix} \mathbf{O} & & \\ \mathbf{CB} & & \\ \vdots & \ddots & \\ \mathbf{C}\bar{\mathbf{A}}^{K-2}\mathbf{B} & \cdots & \mathbf{CB} \end{bmatrix}.$$

The detailed deduction of Eq. (17) is provided in Supplementary.

Then, leveraging Eq. (17), the estimation of Alice's initial state can be pursued by the least-square (LS) method, i.e.,

$$\begin{aligned} \hat{\mathbf{x}}_1^{(a)} =& \tilde{\mathbf{A}}^\dagger \cdot \mathbf{z}^{(a)} = \tilde{\mathbf{A}}^\dagger \cdot \left(\tilde{\mathbf{A}} \cdot \mathbf{x}_1^{(a)} + \tilde{\mathbf{B}} \cdot \mathbf{n}^{(a)}\right) \\ =& \mathbf{x}_1^{(a)} + \tilde{\mathbf{A}}^\dagger \tilde{\mathbf{B}} \mathbf{n}^{(a)}, \end{aligned} \tag{18}$$

where $(\cdot)^\dagger$ represents the pseudo-inverse operator. From Eq. (18), the estimation error can be further expressed as $\|\hat{\mathbf{x}}_1^{(a)} - \mathbf{x}_1^{(a)}\|_2^2 = \|\tilde{\mathbf{A}}^\dagger \tilde{\mathbf{B}} \mathbf{n}^{(a)}\|_2^2$, whose magnitude is dependent on the condition number of $\tilde{\mathbf{A}}$. This therefore provides an insight to defend Type-3 Eve, i.e., the design of control signals should make $cond(\tilde{\mathbf{A}})$ large. In this work, our CLS will not go into that further, but provide a proper control signal design which gives a 10^7 level of $cond(\tilde{\mathbf{A}})$. The detailed evaluation is provided in the following simulation section.

TABLE I
SIMULATION PARAMETERS

Model & Parameters	Configurations
UAV states ($N = 12$ stacked vector)	$\mathbf{x}_k^{(i)} = \begin{bmatrix} x, y, z\text{-axes positions (m)} \\ x, y, z \text{ velocities (m/s)} \\ \text{roll, pitch, yaw (rad),} \\ \text{roll, pitch ,yaw speeds (rad/s)} \end{bmatrix}$
UAV linearised model	[39] $\mathbf{A}$, $\mathbf{B}$ in Eqs. (19)-(20).
System discretized time	$\Delta_t = 0.02$s
Gravitational acceleration	$g_v = 9.8\text{m/s}^2$
UAV x inertia moment	$I_x = 7.5 \times 10^{-3}\text{kg}\cdot\text{m}^2$
UAV y inertia moment	$I_y = 7.5 \times 10^{-3}\text{kg}\cdot\text{m}^2$
UAV z inertia moment	$I_z = 1.3 \times 10^{-2}\text{kg}\cdot\text{m}^2$
Mass of UAV	$m_U = 0.65kg$
Observing matrix	$\mathbf{C}$ in Eq. (21), x, y, z positions, velocities can be obtained (by each other and Eve)
Observing error	$\sigma \in [0.01m, 10m]$

V. SIMULATION & EXPERIMENTAL RESULTS

In this section, we evaluate the security performance of our proposed CLS on the distributed cooperative control of two quad-copters (Alice and Bob). Here, both simulation and real UAV experiments are performed.

A. Simulation Results

1) Environmental Setting: In the simulation part, the model and the CLS scheme are coded and tested via MATLAB. The simulation setting is summarized in Table I. The stacked state in Eq. (1), i.e., $\mathbf{x}_k^{(i)}$, has $N = 12$ states, which are the 3D positions of x, y and z axes (unit m), the corresponding velocities (unit m/s), the roll, pitch and yaw angles (unit rad), and the corresponding roll, pitch and yaw speed (unit rad/s). Given the linearized model in [39], we configure the dynamic model in Eq. (1) as:

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 0 & \Delta_t & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \Delta_t & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & \Delta_t & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -g_v\Delta_t & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & g_v\Delta_t & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \Delta_t & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \Delta_t & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \Delta_t \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \tag{19}$$

$$\mathbf{B} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{I_z} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{I_y} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{I_x} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{m_U} & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^T, \tag{20}$$

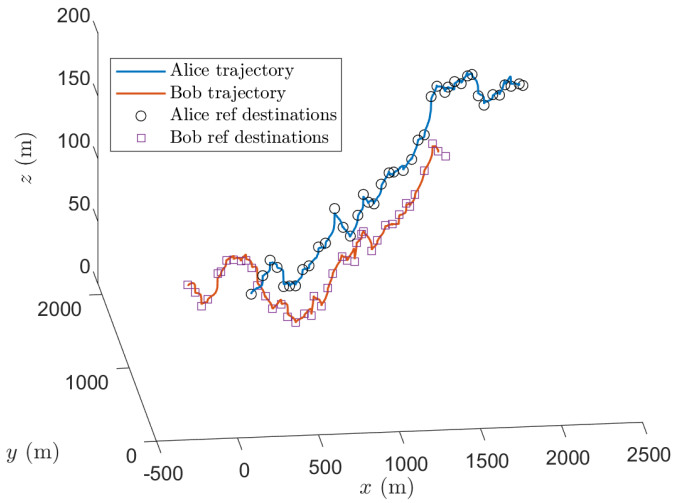


Fig. 2. Illustration of one Alice's and Bob's trajectories by cooperatively controlling to pre-assigned destinations.

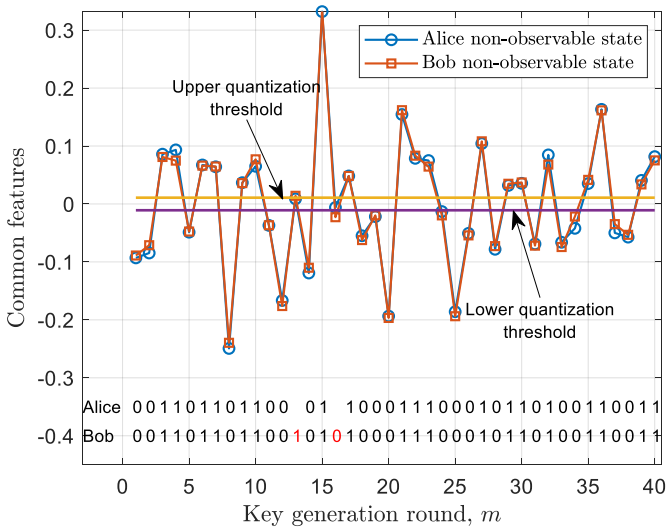


Fig. 3. Illustration of Alice's and Bob's control layer unobservable common states and their binary secret keys relied upon.

where the parameters are described and assigned in Table I. The observing matrix $\mathbf{C}$ is assigned as:

$$\mathbf{C} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{21}$$

where the 3D positions (first 3 variables of UAV states) can be observed by legitimate UAVs and Eve, with observing error ranging from $\sigma \in [0.01m, 10m]$. The corresponding velocities (the second 3 variables of UAV states) are then computed via the differences divided by the discretized time Δ_t.

For the secret key generation, we randomly assign $M = 1000$ 3D destination points for Alice and Bob, respectively. For any $m \in \{0, \cdots, M\}$, $\mathbf{r}_{m+1}^{(i,ref)} \sim \mathcal{N}(\mathbf{r}_m^{(i,ref)} + \mathbf{d}, \sigma_p^2)$, where $\mathbf{d} = [50, 50, 0]^T$ with unit m, and $\sigma_p = 10$m. $\mathbf{r}_0^{(i,ref)} \sim \mathcal{N}([10, 10, 100]^T, \sigma_p^2)$ represents the initial positions of Alice and Bob. As such, $M = 1000$ key generation rounds are considered in our simulation, and we assign $K = 800$ discrete time steps in each round.

2) Illustration of CLS performance: One illustration of our proposed CLS is presented via Figs. 2-3, where the observing error is assigned as $\sigma = 0.1$m. It is shown from Fig. 2 that our designed cooperative control in Eqs. (8)-(9) can achieve the referenced destination points. Then, from Fig. 3, it is seen that under our designed control signal, Alice and Bob can have highly correlated unobservable states in yaw angles, which then can be exploited to generate the symmetrical binary secret keys with very low mismatch rate.

3) Performance of CLS against Eves: In this part, we evaluate the performance of our proposed CLS when defending potential Eves. Here, we select the Type-2 and Type-3 Eves described in Section IV-C2 and Section IV-C3, where Type-2 Eve refers to as the Eve with Alice's and Bob's observed states, i.e., $\mathbf{y}_k^{(a)}, \mathbf{y}_k^{(b)}, k \in \{1, \cdots, K\}$, and Type-3 Eve refers to as the Eve with the knowledge of dynamic and control model, i.e., $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{\Theta}_1$, $\mathbf{\Theta}_2$ and $\mathbf{\Theta}_3$, the reference destinations, i.e.,$\mathbf{r}_m^{(a,ref)}, \mathbf{r}_m^{(b,ref)}, m \in \{0, \cdots, M\}$, and Alice's and Bob's observed states.

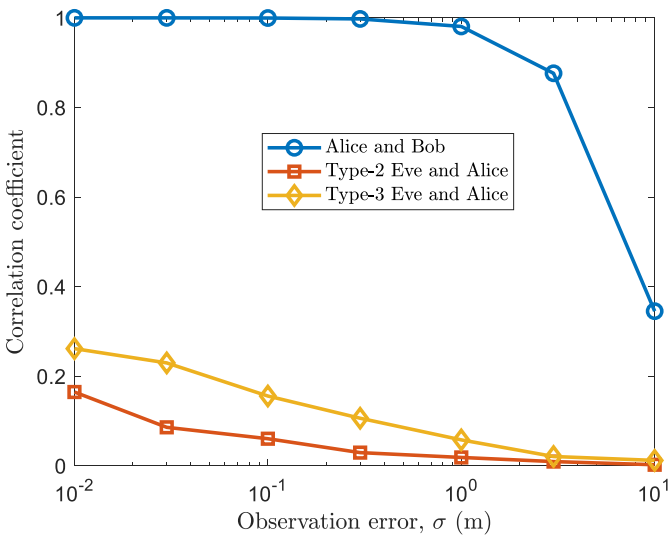


Fig. 4. Performance of CLS against two types Eves, where x-coordinate is the different levels of observing noises and y-coordinate is the correlation coefficients.

Fig. 4 provides the comparison of correlations between Alice and Bob (blue curve), Type-2 Eve and Alice (red curve), Type-3 Eve and Alice (yellow curve), where the x-coordinate is the observing error σ (with unit m), and y-coordinate is the correlation coefficient. It is firstly observed that with the observing error increases (e.g., from 0.01m to 10m), the correlation coefficients between Alice-Bob and Alice-Eve are all decreased (e.g., from 1 to 0.4 for Alice-Bob). This is because when involving Bob's observed states in Alice's control signal, the observing noise does not provide extra correlation between Alice's and Bob's states but extra variance, thereby rendering the reduction of the correlation coefficients.

Then, it is seen that the correlation coefficient between Alice

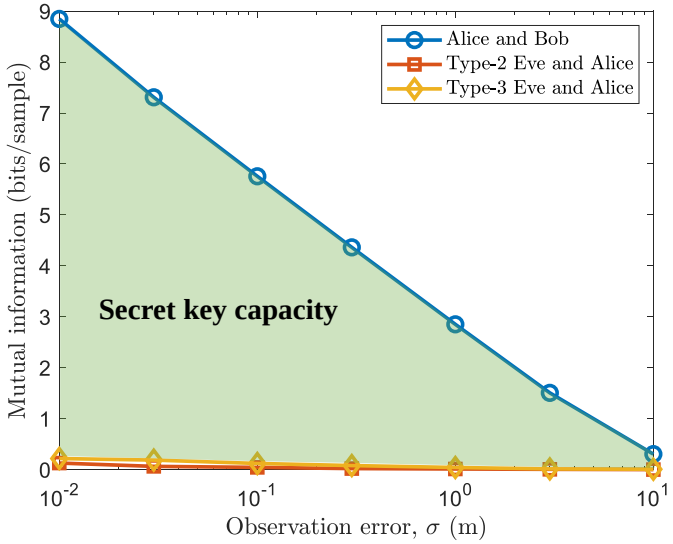


Fig. 5. Performance of CLS against two types Eves, where x-coordinate is the different levels of observing noises and y-coordinate is the mutual information.

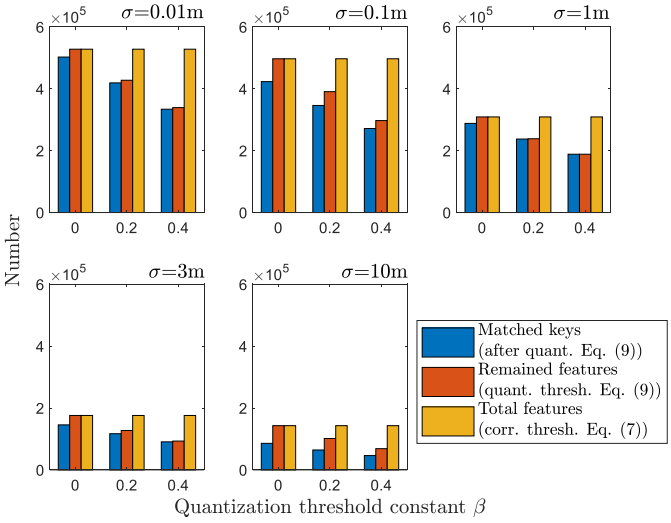


Fig. 6. Results of proposed CLS after key quantization. The numbers of match keys, of remained features (not discard by two quantization thresholds), and of total selected features are provided, under different quantization thresholds determined by quantization parameter β in Eq. (13) and different observing error σ.

and Bob is greatly larger than that between Eve and Alice. The gap is approximately $1-0.1=0.9$ for Type-2 Eve, and $1-0.2=0.8$ for Type-3 Eve. The reason is categorized into three aspects. First, the large correlation coefficient between Alice and Bob is attributed to the cooperative control. The control signals of Alice and Bob involve each other's observed states, which evolved by the dynamic model, leads to highly correlated states for common features and further secret key generation (as is theoretically deduced in Eq. (6) and depicted by Fig. 1(b)). Second, for Type-2 Eve that tries to steal the legitimate common features by Alice's and Bob's observed states, the selected correlated states of Alice and Bob for feature construction are unobservable and less correlated from the observable states, thereby giving rise to low correlation coefficients between the features of Type-2 Eve and Alice. Third, for Type-3 Eve with knowledge of the dynamic & control model and Alice's and Bob's observable states, the difficulty lies in that it is intractable to estimate the initial state from the observable states, since amounts of initial states can map to the same observable states. For example, one can imagine that there are multiple combinations of yaw, pitch, and roll angles that can lead to the same UAV trajectory (e.g., the UAV with forward trajectory can be pursued either by direct pitch angle controlling or by clockwise yawing $\pm 90^\circ$ and rolling). This can be also reflected by the condition number of $\tilde{\mathbf{A}}$ in Eq. (17), which is too large (e.g., $cond(\tilde{\mathbf{A}}) = 9.12\times 10^7$) to give an accurate estimation of the initial state, i.e., $\mathbf{x}_1^{(a)}$.

We next evaluate mutual information between features of Alice and Bob (blue curve), Type-2 Eve and Alice (red curve), Type-3 Eve and Alice (yellow curve) in Fig. 5, where x-coordinate is the observing error σ and y-coordinate is the mutual information (with unit bits/feature). It is noteworthy that in the theoretical point, if the feature is Gaussian distributed, the mutual information can be computed by the correlation coefficients as $MI = -0.5\log_2(1-\rho^2)$. Here, we simulate the mutual information via the ITE toolbox [46]. It is seen from

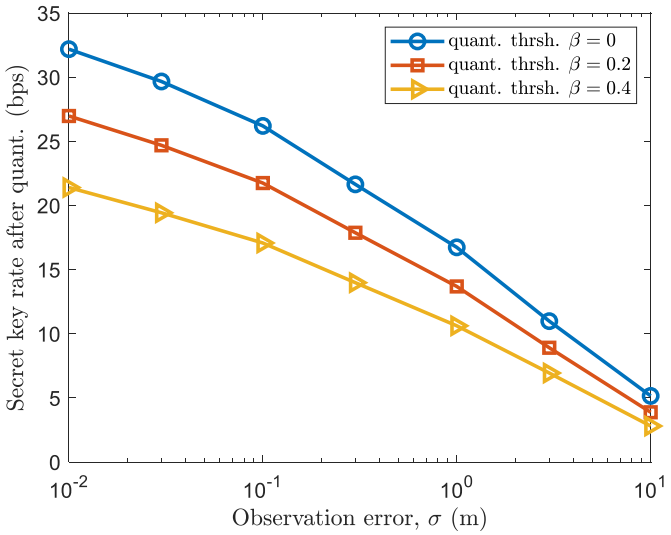
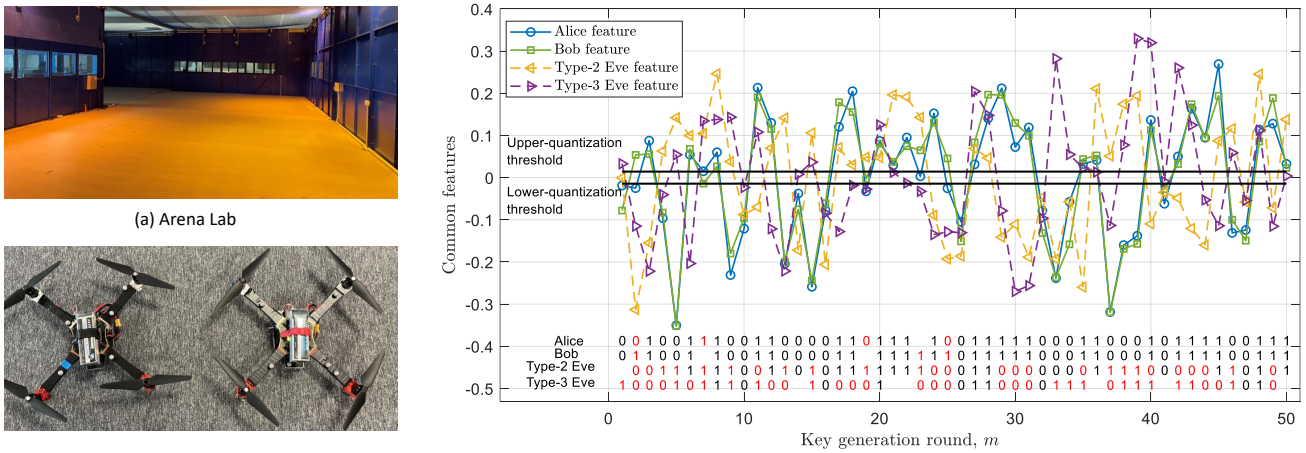


Fig. 7. Secret key rate after key quantization of our proposed CLS.

Fig. 5 that the mutual information has the same trends with correlation coefficient in Fig 4, due to the same monotonicity as the latter in terms of observing error.

Then, we calculate and depict the secret key capacity via the gap of mutual information between Alice and Bob and between Alice and Eves. It is seen from Fig. 5 that the secret key capacity of our proposed CLS is promising with the level of observing errors ranging from cm to m. This is attributed to the cooperative but distributed control of Alice and Bob, whereby the control signals involve each other's states and lead to high correlations of their unobserved states after dynamic evolution.

4) Secret key rate after Quantization: After the analysis of the secret key capacity of the proposed CLS in Fig. 5, we give one realization of the binary secret key generation via the two-thresholds based key quantization in Eq. (13). It is noteworthy



(a) Arena Lab

(b) Alice, Bob UAVs

(c) CLS-based cipher key performance

Fig. 8. Real UAV experiment on CLS-based cipher key generation. (a) shows the Area Indoor Flight Lab; (b) is the UAVs of Alice and Bob; (c) is the features and cipher keys generated by our proposed CLS. By counting the ratio of matched and the total number of the generated binary keys, an approximately 90% key agreement rate is achieved between Alice and Bob.

that other more sophisticated key quantization techniques also can be adopted based on the common features provided by the proposed CLS.

Fig. 6 shows the numbers of matched keys, of remaining features, and of total features, under different quantization parameters $beta$ in Eq. (13) and observing errors σ. As is provided in Eq. (13) and in Fig. 2, one matched key refers to as the feature of Alice and Bob are larger (lesser) than the upper (lower) threshold, and one remaining feature is when it is outside the area covered by upper and lower thresholds. The total features are selected by the set $\mathcal{G}$ in Eq. (10), with the correlation coefficient threshold set as $\varrho = 0.8$.

It is firstly observed from Fig. 6 that with the increase of observing error σ (from 0.01m to 10m), the total number of selected features decreases (from 5.2×10^5 to 1.4×10^5). This is because the correlation coefficients between Alice's and Bob's states decrease with extra observation noises added into their control signals, which thereby leads to the reduction of the number of selected states whose correlation coefficients are larger than threshold ϱ. Such a decrease of the selected features further makes the reduction of the number of match keys (e.g., from an average of 4×10^5 to 1×10^5), with the growth of the observing noises.

Second, it is seen from Fig. 6 that with the increase of the quantization parameter β, both numbers of the remained features and the matched keys decrease. This is because a larger quantization parameter β results in a larger gap between the upper and lower thresholds. As a consequence, the number of features that fall into this gap and are discarded increases, rendering the smaller numbers of the remained features and the matched keys. It seems that the large threshold gap can decrease the number of matched keys, however, it helps reduce the burden of the further key reconciliation step. To be specific, when the correlations of Alice's and Bob's common features are low, a large upper/lower threshold gap can effectively discard the uncorrelated features, leaving the number of remained keys equals (approximately) that of matched keys. This further makes the further key reconciliation easier to design forward error correction (FEC) code to achieve the same keys at Alice and Bob.

We finally provide the secret key rate after the key quantization step in Eq. (12), which is defined as the number of matched keys in one second. In Fig. 7, secret key rates under three quantization parameters $\beta = 0, 0.2, 0.4$ are provided with different observing error σ. It is observed that the secret key rates reduce (averagely from 25bps to 5bps) as the observing noises increase from cm level to m level. This seems less attractive as opposed to the existing CSI-based PL-SKG (about 10^3bps key rate) with reciprocal channel randomness and reliable channel estimation. However, it is noteworthy that the secrecy performance of the proposed CLS does not rely on the strict requirement of wireless channels (e.g., randomness, reciprocity and precise CSI estimator), which therefore makes the proposed CLS a promising candidate in the radio adversarial (e.g., jamming and LoS) scenarios to generate distributed and symmetrical secret keys between legitimate parties.

B. Real UAV Experiment

In this part, real UAV experiments are performed in the Indoor Flight Arena Lab of Cranfield University, which is an L-shape area equipped with VICON system to determine the 3D positions of UAVs, seen by Fig. 8(a). The UAVs for Alice and Bob are hand-made constructed via T-1045 frame, and motors with type AIR 2216/KV920, seen by Fig. 8(b). The CPU is chosen as Beagle-Bone-Blue with Debian system, and the controller in Eqs. (8)-(9) are coded with C++. Similar to the simulation, for key generation, two referenced paths are set for Alice and Bob to achieve. Eve is considered as someone who hacks the VICON system, and obtains all the observable states (i.e., x, y, z positions, and the corresponding velocities) of Alice and Bob.

The result is provided in Fig. 8(c). The measurement metrics are key agreement/disagreement rates, which are counted as the ratio of the matched/mismatched keys to the total generated

keys. The models and parameters of the quadcopters are the same as the simulation setting. It is illustrated that the features and cipher keys generated by Alice and Bob have large commonalities and randomness, which makes them difficult for a brute-force Eve to guess/estimate. Then, we can see that the key disagreement rates from Type-2 and Type-3 Eves are very high (approximated 0.5), indicating that neither of them could successfully reconstruct the cipher keys, although Type-3 Eve is aware of the knowledge of all observable states and systems. The real-experimental results match the simulation results and analysis in the previous subsection. The full video is attached by the media resource (or online), which shows the potential of our proposed CLS to secure the wireless communications among cooperative ASs.

C. Discussion

In this part, we make a pros-and-cons analysis of choosing our proposed CLS or existing PLS for securing AS communications. As is listed in Table II, the prerequisite of PLS is the existence of channel reciprocity and randomness, otherwise, the key disagreement rate and randomness cannot be guaranteed. This suggests that PLS is more suitable for the dense urban area with strong small-scale scattering-induced channel randomness, and for the scenarios where channel reciprocity destruction attacks are absent.

Then in the aerospace scenarios where LoS channels between legitimate ASs are dominated, or in scenarios with channel jamming attacks, PLS is unable to extract reciprocal channel randomness for cipher key generation. In these cases, when ASs are in cooperative tasks, CLS in this work is proposed to uncover and exploit the common control layer features, and has been demonstrated by experiments to show potential to generate cipher keys.

One limitation of CLS lies in the secret key leakage from the estimation of the unobservable states by Eve. For currently, the CLS is implemented on the cooperative control of the geometric symmetry quadcopters, whose yaw angles are hard to be estimated by GNSS or imaging-based Eves, and thereby serve as the unobservable states for secret key generation. Indeed, if Eve is very close to one legitimate quadcopter, it may be possible to estimate the changes in the yaw angle by image processing techniques, which then leads to secret key leakage issue. This should be further studied especially via real experiments, by taking into account the system design, image resolution, the sampling time-interval, and the physical safe distance (for now we are using the air-gear 450 quadcopter, which does not allow any object to be close at 1m or there will be a destroy of the propellers).

TABLE II
COMPARISON BETWEEN PLS, AND PROPOSED CLS APPROACHES

	PLS	CLS
Security idea	Use reciprocal wireless features to generate symmetric keys	Use mutual cooperative AS states to generate symmetric keys
Feature source	Wireless channel	Dynamic states of ASs
Key reciprocity	Strong for most EM materials and channels	Strong for cooperative ASs
Key dynamics & uniqueness	Strong for NLoS urban areas, Weak for LoS aerospace	Strong for multi-task autonomy
Limitations & attack vectors	Destroy channel reciprocity (e.g., jamming)	Unobservable state estimation determines leakage

VI. CONCLUSION

The concerns of cybersecurity in ASs have been increasing, due to the disparity between the computation capability of an AS platform v.s. a powerful premeditated external attacker (e.g., quantum computer). This post-quantum cryptography issue indeed motivated the rapid advances in PLS in recent years. However, PLS remains sensitive to attackers (e.g., jamming) that destroy its prerequisite channel properties (e.g., reciprocity).

In this work, we proposed a new security mechanism called control layer security. The idea of CLS is to exploit the correlated and unobservable states between cooperative ASs to generate cipher keys. We then realized this idea in the linearized UAV cooperative control scenario. The theoretical correlation coefficients between Alice's and Bob's states were computed, based on which common feature selection and key quantization steps were designed. We evaluated the security of our proposed CLS, and showed that even if the Eve with full knowledge of observable states and systems cannot estimate the unobservable states and the secret key relied upon, due to the multiple-to-one mapping from unobservable states (pitch, roll and yaw angles) to the observable states (3D trajectory). Simulation results showed the promising secret key capacity of our proposed CLS. This demonstrates a promising candidate to secure the communications of ASs, especially in the adversarial radio environment with attackers that destroys the prerequisite for current PLS.

REFERENCES

[1] C. Shen, T.-H. Chang, J. Gong, Y. Zeng, and R. Zhang, "Multi-uav interference coordination via joint trajectory and power control," *IEEE Transactions on Signal Processing*, vol. 68, pp. 843–858, 2020.

[2] A. Liu, L. Lian, V. Lau, G. Liu, and M.-J. Zhao, "Cloud-assisted cooperative localization for vehicle platoons: A turbo approach," *IEEE Transactions on Signal Processing*, vol. 68, pp. 605–620, 2020.

[3] T.-K. Hu, F. Gama, T. Chen, W. Zheng, Z. Wang, A. Ribeiro, and B. M. Sadler, "Scalable perception-action-communication loops with convolutional and graph neural networks," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 8, pp. 12–24, 2022.

[4] X. Zhang, A. Liniger, and F. Borrelli, "Optimization-based collision avoidance," *IEEE Transactions on Control Systems Technology*, vol. 29, no. 3, pp. 972–983, 2020.

[5] X. Wang, V. Yadav, and S. Balakrishnan, "Cooperative uav formation flying with obstacle/collision avoidance," *IEEE Transactions on control systems technology*, vol. 15, no. 4, pp. 672–679, 2007.

[6] X. Dong, Y. Zhou, Z. Ren, and Y. Zhong, "Time-varying formation tracking for second-order multi-agent systems subjected to switching topologies with application to quadrotor formation flying," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 6, pp. 5014–5024, 2017.

[7] J. Katz and Y. Lindell, *Introduction to modern cryptography*. CRC press, 2020.

[8] W. Diffie and M. E. Hellman, "New directions in cryptography," in *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*, 2022, pp. 365–390.

[9] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[10] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[11] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of modern physics*, vol. 74, no. 1, p. 145, 2002.

[12] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang *et al.*, "Continuous-variable qkd over 50 km commercial fiber," *Quantum Science and Technology*, vol. 4, no. 3, p. 035006, 2019.

[13] X. Pang, N. Zhao, J. Tang, C. Wu, D. Niyato, and K.-K. Wong, "Irs-assisted secure uav transmission via joint trajectory and beamforming design," *IEEE Transactions on Communications*, vol. 70, no. 2, pp. 1140–1152, 2022.

[14] Y. Zhou, P. L. Yeoh, H. Chen, Y. Li, R. Schober, L. Zhuo, and B. Vucetic, "Improving physical layer security via a uav friendly jammer for unknown eavesdropper location," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11 280–11 284, 2018.

[15] W. Jiang, B. Chen, J. Zhao, Z. Xiong, and Z. Ding, "Joint active and passive beamforming design for the irs-assisted mimome-ofdm secure communications," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 10, pp. 10 369–10 381, 2021.

[16] S. Hong, C. Pan, H. Ren, K. Wang, and A. Nallanathan, "Artificial-noise-aided secure mimo wireless communications via intelligent reflecting surface," *IEEE Transactions on Communications*, vol. 68, no. 12, pp. 7851–7866, 2020.

[17] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[18] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[19] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly gaussian random variables," in *2006 IEEE International Symposium on Information Theory*, 2006, pp. 2593–2597.

[20] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.

[21] X. Wu, Y. Song, C. Zhao, and X. You, "Secrecy extraction from correlated fading channels: An upper bound," in *2009 International Conference on Wireless Communications Signal Processing*, 2009, pp. 1–3.

[22] Y. Peng, P. Wang, W. Xiang, and Y. Li, "Secret key generation based on estimated channel state information for tdd-ofdm systems over fading channels," *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 5176–5186, 2017.

[23] K. Moara-Nkwe, Q. Shi, G. M. Lee, and M. H. Eiza, "A novel physical layer secure key generation and refreshment scheme for wireless sensor networks," *IEEE Access*, vol. 6, pp. 11 374–11 387, 2018.

[24] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 917–930, 2013.

[25] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, 2008, pp. 128–139.

[26] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptology — EUROCRYPT '93*, T. Helleseth, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 410–423.

[27] R. Impagliazzo, L. A. Levin, and M. Luby, "Pseudo-random generation from one-way functions," in *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, 1989, pp. 12–24.

[28] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Transactions on Wireless Communications*, vol. 11, no. 3, pp. 903–907, 2012.

[29] Y. Tao, X. Wang, B. Li, and C. Zhao, "Pilot spoofing attack detection and localization with mobile eavesdropper," *IEEE Transactions on Mobile Computing*, pp. 1–1, 2021.

[30] Z. Wei, B. Li, and W. Guo, "Adversarial reconfigurable intelligent surface against physical layer key generation," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2368–2381, 2023.

[31] Z. Wei, L. Wang, S. C. Sun, B. Li, and W. Guo, "Graph layer security: Encrypting information via common networked physics," *Sensors*, vol. 10, no. 3951, 2022.

[32] G. Li, C. Sun, W. Xu, M. Di Renzo, and A. Hu, "On maximizing the sum secret key rate for reconfigurable intelligent surface-assisted multiuser systems," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 211–225, 2021.

[33] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[34] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *Ieee access*, vol. 4, pp. 614–626, 2016.

[35] Z. Mahboubi, Z. Kolter, T. Wang, and G. Bower, "Camera based localization for autonomous uav formation flight," in *Infotech@ Aerospace 2011*, 2011, p. 1658.

[36] A. Thomas, V. Leboucher, A. Cotinat, P. Finet, and M. Gilbert, "Uav localization using panoramic thermal cameras," in *Computer Vision Systems: 12th International Conference, ICVS 2019, Thessaloniki, Greece, September 23–25, 2019, Proceedings 12*. Springer, 2019, pp. 754–767.

[37] Z. Wei, W. Guo, and B. Li, "A multi-eavesdropper scheme against ris secured los-dominated channel," *IEEE Communications Letters*, vol. 26, no. 6, pp. 1221–1225, 2022.

[38] Z. Wei, L. Wang, and W. Guo, "Secret key rate upper-bound for reconfigurable intelligent surface-combined system under spoofing," in *2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall)*, 2022, pp. 1–6.

[39] Z. Tahir, W. Tahir, and S. A. Liaqat, "State space system modelling of a quad copter uav," *arXiv preprint arXiv:1908.07401*, 2019.

[40] T. Luukkonen, "Modelling and control of quadcopter," *Independent research project in applied mathematics, Espoo*, vol. 22, no. 22, 2011.

[41] Y. Wu, Y. Yu, Y. Hu, Y. Sun, T. Wang, and Q. Zhang, "Channel-based dynamic key generation for physical layer security in ofdm-pon systems," *IEEE Photonics Journal*, vol. 13, no. 2, pp. 1–9, 2021.

[42] G. Bishop, G. Welch *et al.*, "An introduction to the kalman filter," *Proc of SIGGRAPH, Course*, vol. 8, no. 27599-23175, p. 41, 2001.

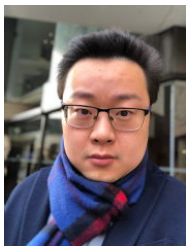
[43] J.-J. Xiong and E.-H. Zheng, "Optimal kalman filter for state estimation of a quadrotor uav," *Optik*, vol. 126, no. 21, pp. 2862–2868, 2015.

[44] P. M. Djuric, J. H. Kotecha, J. Zhang, Y. Huang, T. Ghirmai, M. F. Bugallo, and J. Miguez, "Particle filtering," *IEEE signal processing magazine*, vol. 20, no. 5, pp. 19–38, 2003.

[45] Z. Wei, B. Li, W. Guo, W. Hu, and C. Zhao, "On the accuracy and efficiency of sensing and localization for robotic," *IEEE Transactions on Mobile Computing*, 2020.

[46] Z. Szabó, "Information theoretical estimators toolbox," *The Journal of Machine Learning Research*, vol. 15, no. 1, pp. 283–287, 2014.

Zhuangkun Wei received his Ph.D from School of Engineering, University of Warwick, UK in 2021, and master's and bachelor's degree in Electronic Engineering from Beijing University of Posts and Telecommunications (BUPT), Beijing, China in 2014 and 2018 respectively. He is currently a research fellow in trustworthy autonomous systems node security (TAS-S) at School of Aerospace, Transport, Manufacturing (SATM) of Cranfield University, UK. His research interests cover physical layer security, reconfigurable intelligent surface, molecular communications, and graph signal processing.



Weisi Guo (S07, M11, SM17) received his MEng, MA, and Ph.D. degrees from the University of Cambridge. He is currently the Chair Professor of Human Machine Intelligence at Cranfield University, and was an Associate Professor at the University of Warwick. He has published over 130 papers and is PI on over £3.5m of research grants from EPSRC, H2020, Royal Society, InnovateUK, and DSTL. His research has won him several international awards (IET Innovation 15, Bell Labs Prize Finalist 14 and Semi-Finalist 16 and 19). He is a Turing Fellow at the Alan Turing Institute.