Control Layer Secret Key Generations for Autonomous Systems

Cranfield University

Researchers: Dr. Zhuangkun Wei, Dr. Oscar J. Gonzalez V.

Investigators: Prof. Weisi Guo, Prof. Antonio Tsourdos

Engineering and Physical Sciences Research Council

TAS-S

Introduction

Current strategies to secure the communication surfaces of autonomous systems include cryptography and physical layer security (PLS). However, both have some severe security issues (shown in the following), which motivates the design of control layer security (CLS) that is specific for autonomous systems.

Cryptography

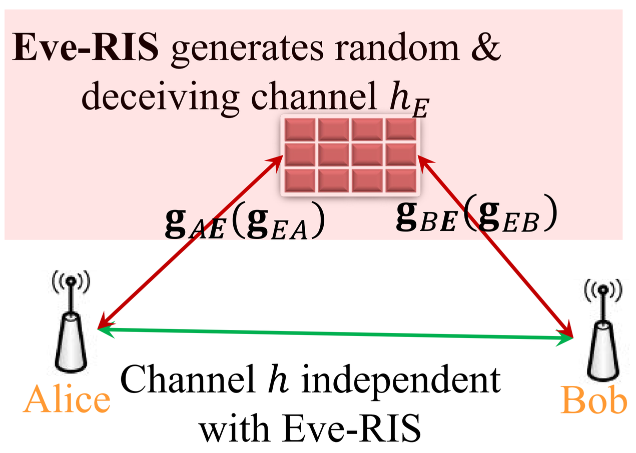
uses common key pool for cipher key generation, but has following issues:

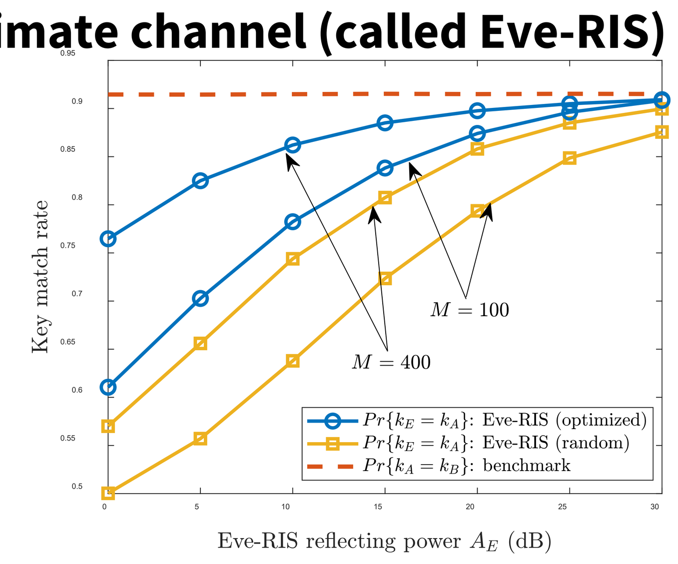
- ➢Complex key generation & management & distribution
- ➢No secrecy guaranteed against post-quantum computing
- ➢High computational complexity & latency

Physical Layer Security

generates shared secret keys via the reciprocal small-scale channel randomness of Alice and Bob, however, has following attack threats:

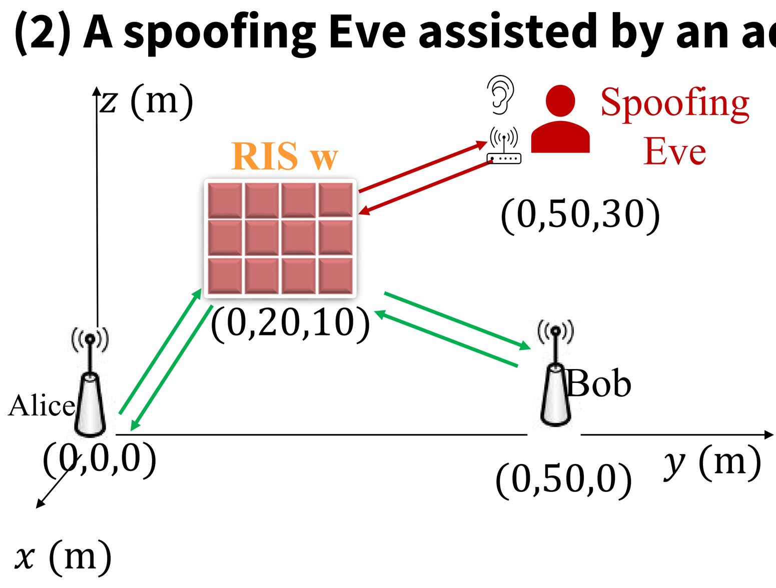
(1) When an adversarial reconfigurable intelligent surfaces (RIS) inserts a deceiving channel into the legitimate channel (called Eve-RIS)

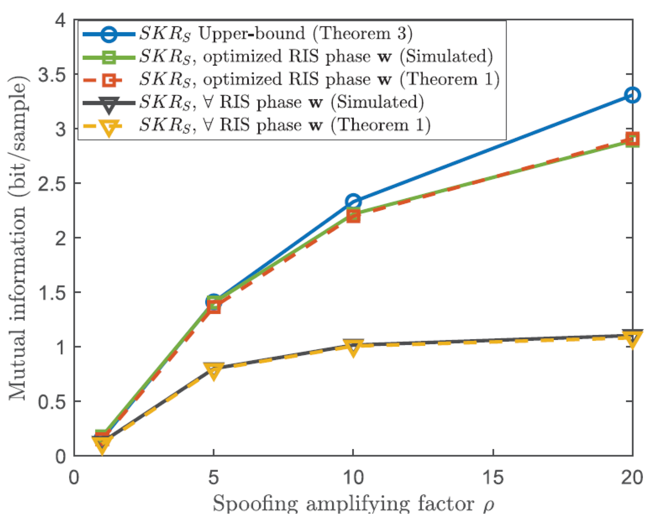




Results show that Eve-RIS can have high key match rate with legitimate users, therefore able to derive the cipher keys

(2) A spoofing Eve assisted by an adversarial RIS



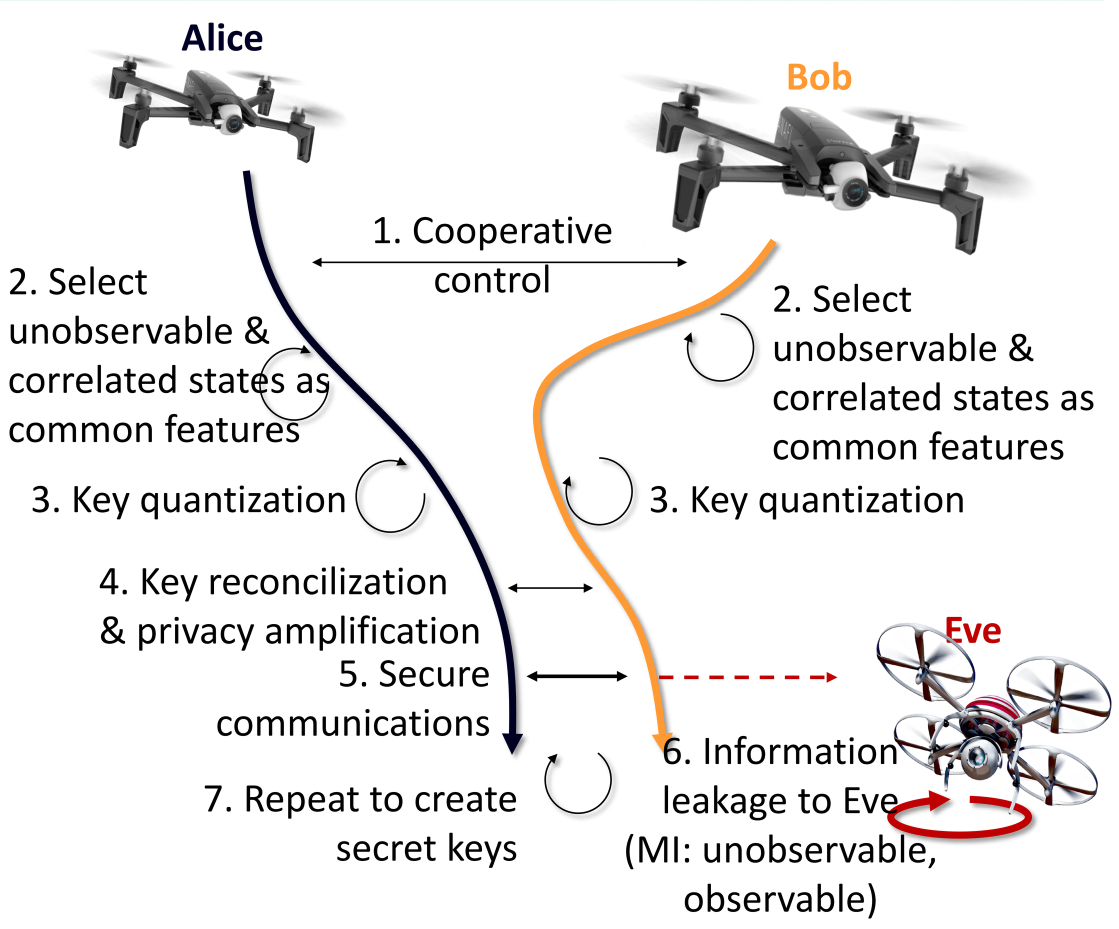


Results show that adversarial RIS can be used to improve the spoofing if used by adversarial users

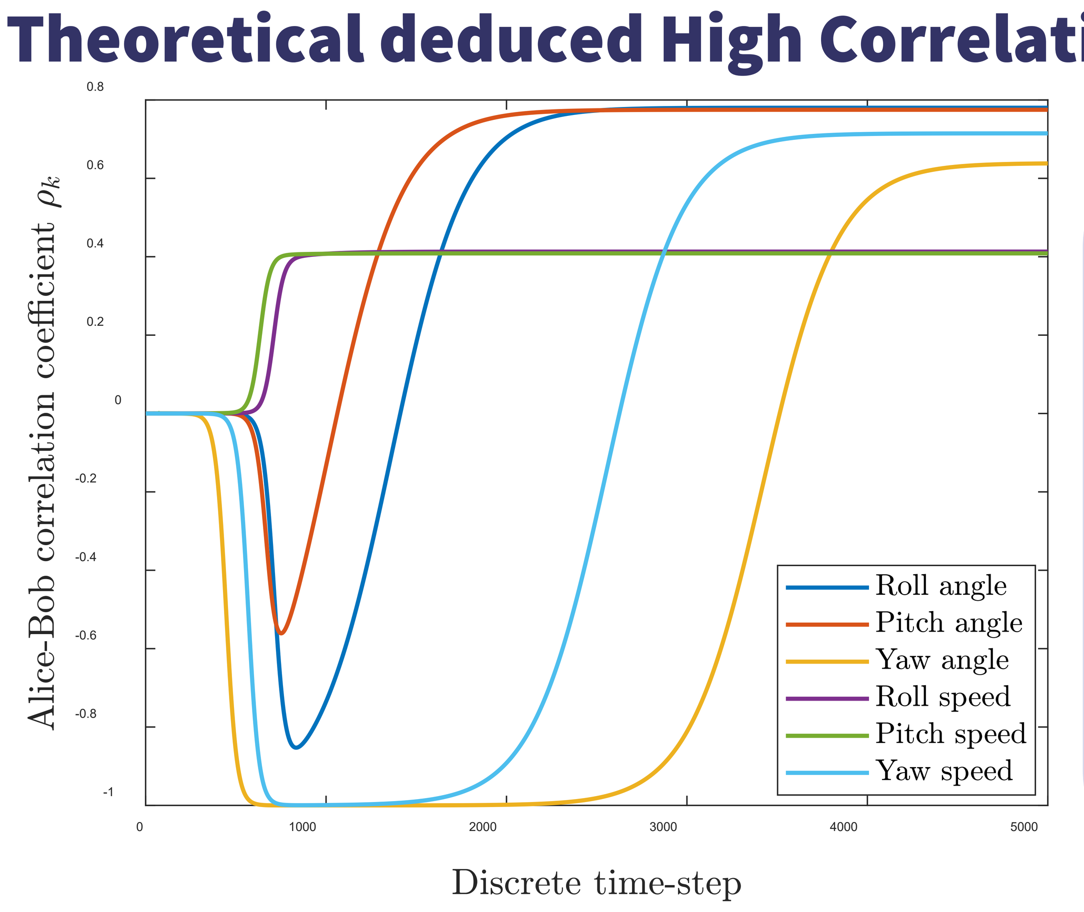
1. Concept & Theory of Control Layer Security

Legitimate Alice and Bob (two UAVs) create correlated but unobservable states (e.g., yaw angles), via cooperative control, and use these correlated states for cipher key generation.

$$\mathbf{x}_k^{(i)} = \mathbf{A}\cdot\mathbf{x}_{k-1}^{(i)} + \mathbf{B}\cdot\mathbf{u}_{k-1}^{(i)}$$
$$\mathbf{y}_k^{(i)} = \mathbf{C}\cdot\mathbf{x}_k^{(i)} + \boldsymbol{\varepsilon}_k^{(i)}$$
$$i \in \{Alice, Bob\}$$



Theoretical deduced High Correlation



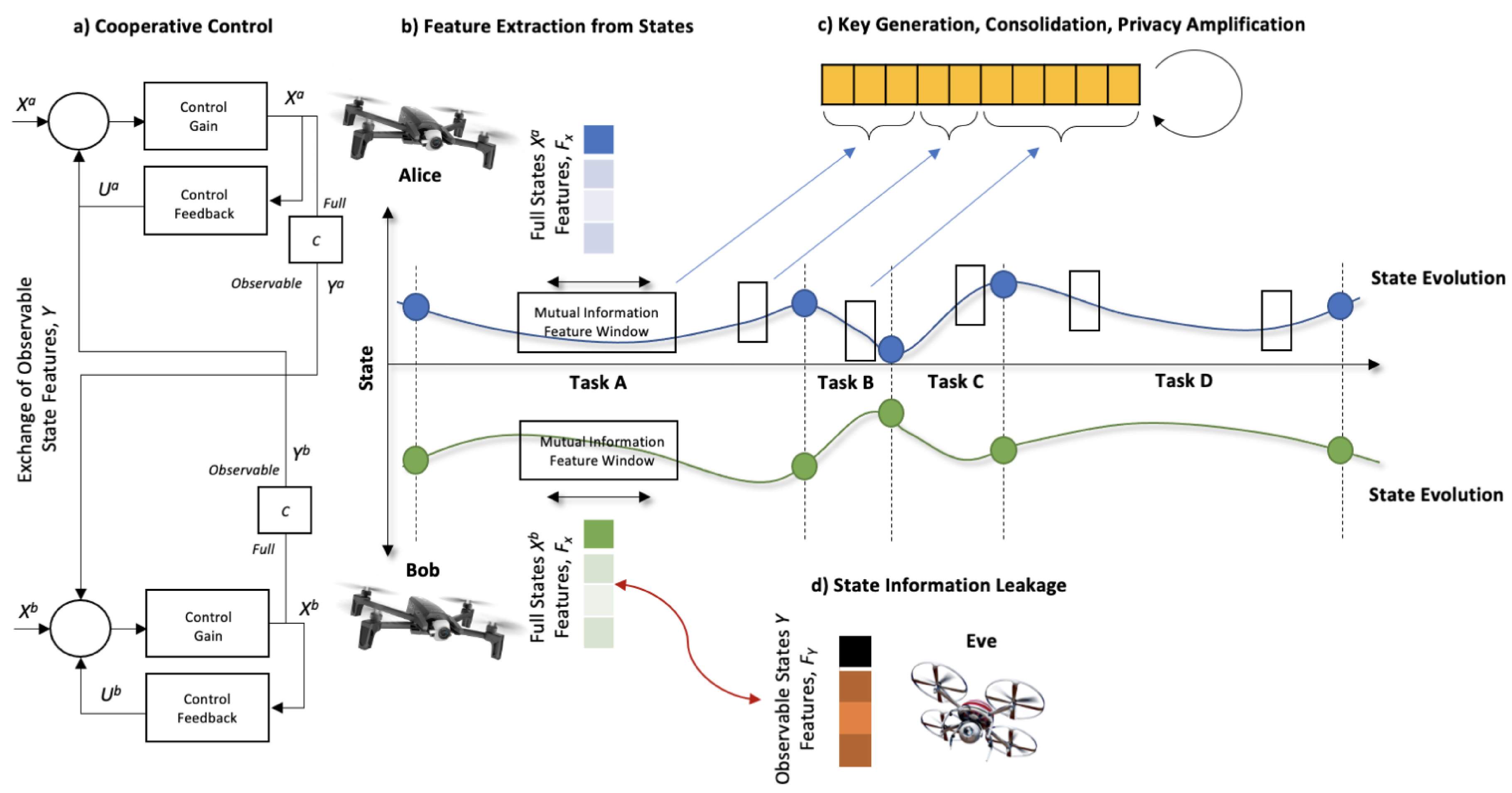
An appropriate cooperative control design can make the correlation between the states of two UAVs approach to ±1, rendering the potential to use these highly correlated states for cipher key generation, which avoids suffering from the aforementioned threats of cryptography and PLS

2. Difference from Physical Layer Security

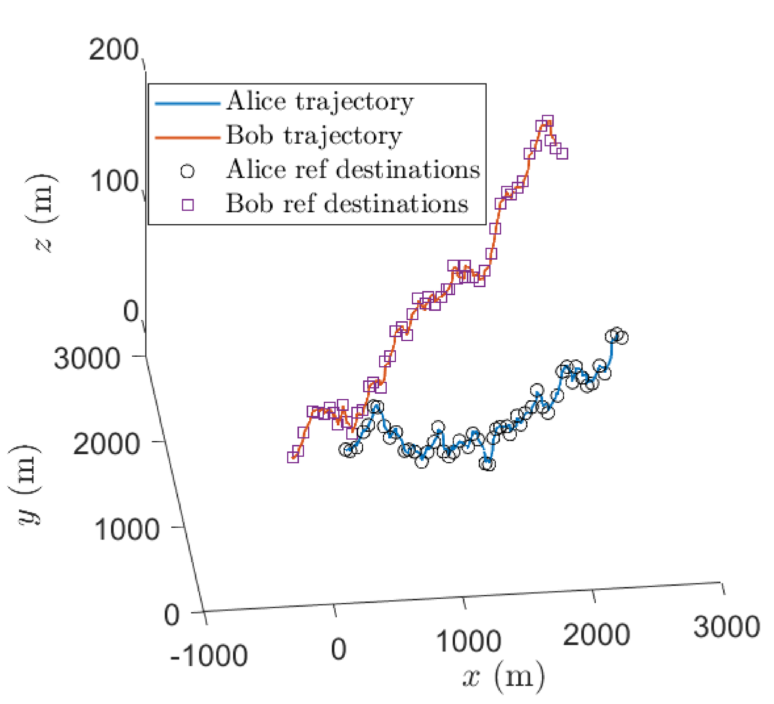
	Prerequisites	Available channel noise by jamming, pilot spoofing	Available positioning error
CLS (proposed)	Cooperative control, multiple to one map from unobservable to observable states	Not affected by channel attacks	cm-m level, to ensure selected states with correlation >0.8
PLS	Channel reciprocity, randomness	<-10dB s.t. correlation coefficient >0.8	Not affected by position observation error

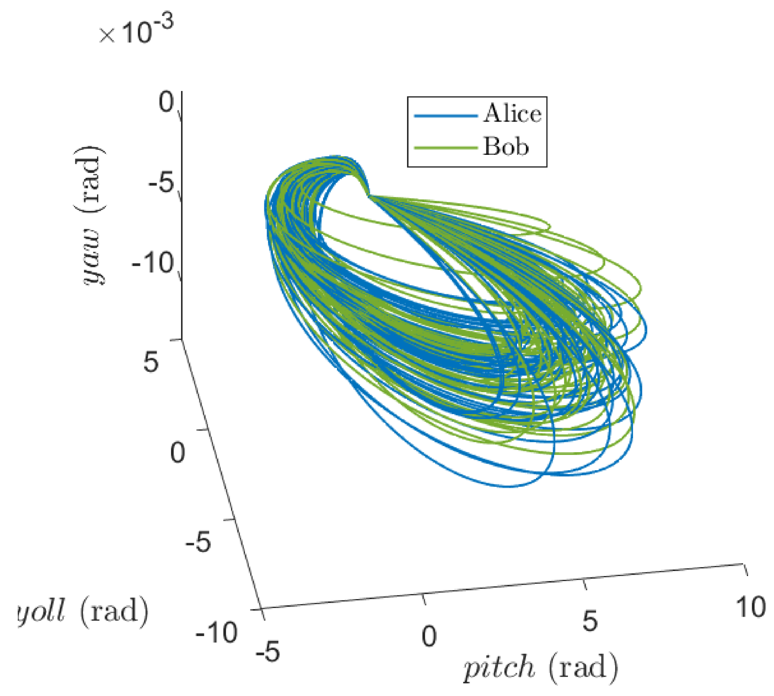
3. Implementation of Control Layer Security

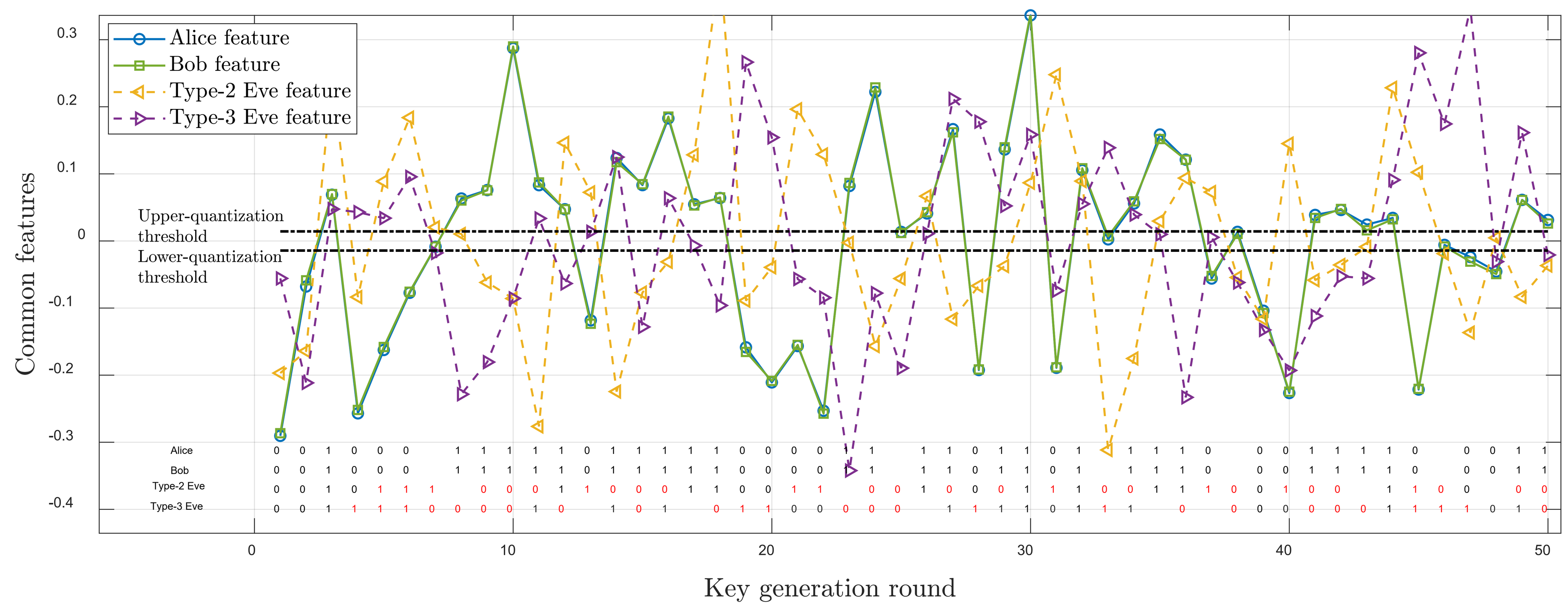
Schematic Sketch

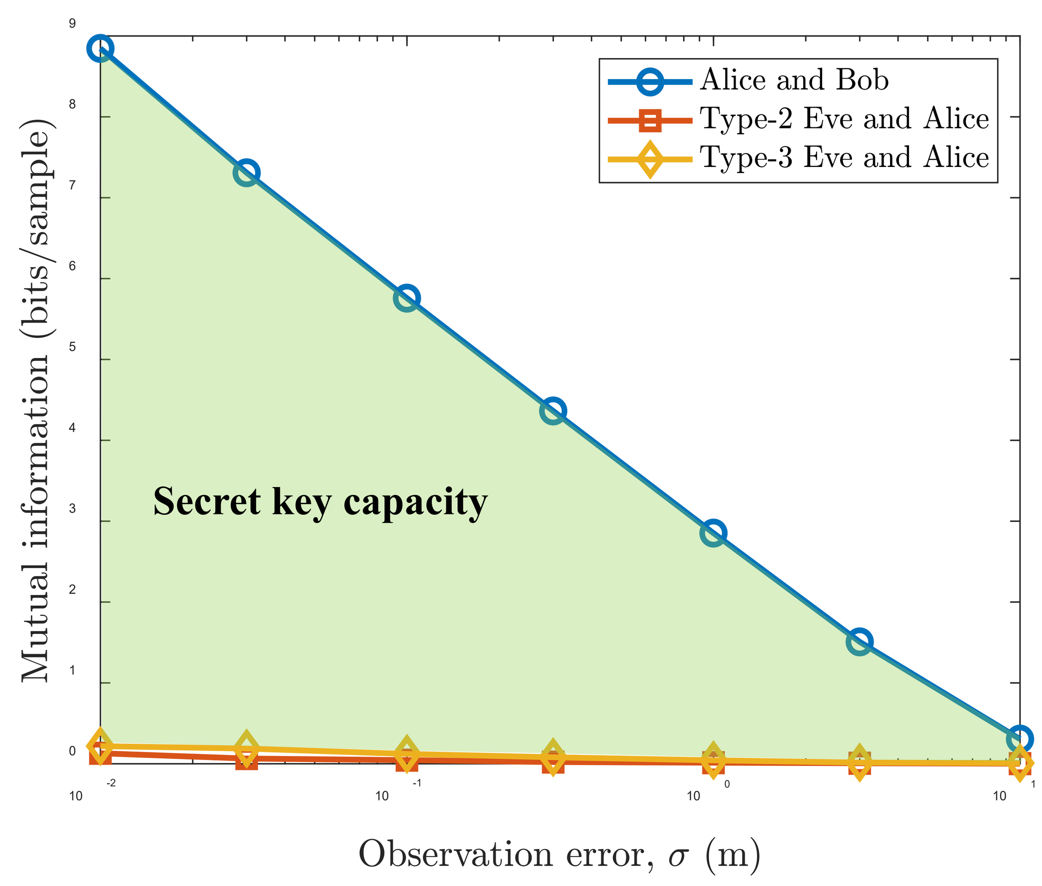


Simulation Results









Results show that by properly designing the cooperative control algorithm, UAV Alice and UAV Bob can (i) follow the referenced trajectory, (ii) have random but highly correlated states for cipher key generation, which prevent attackers from eavesdropping.

Lancaster University

Cranfield University

UKRI Trustworthy Autonomous Systems Hub

This work is supported by the Engineering and Physical Sciences Research Council [grant number: EP/V026763/1]