Threat Analysis of current Physical Layer Security on Communication Surfaces of Autonomous Systems

Cranfield University

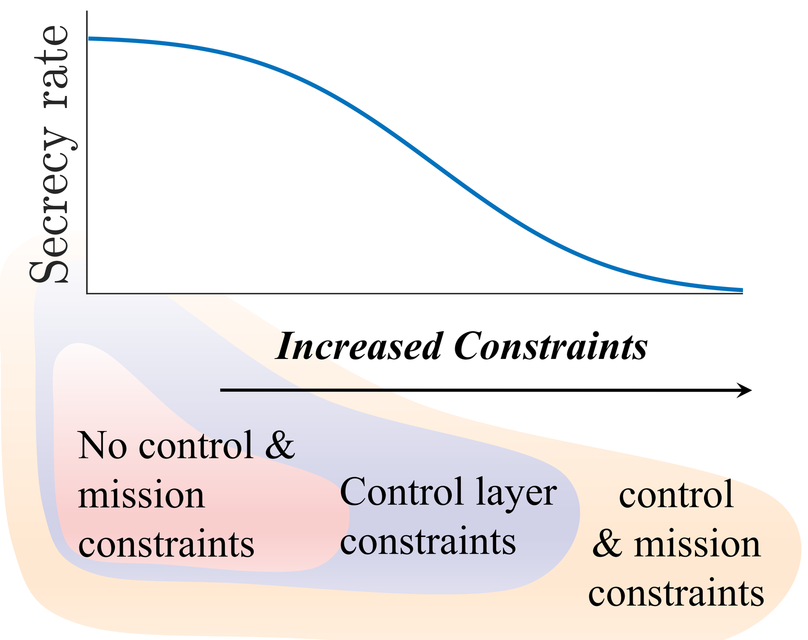
Researcher: Dr. Zhuangkun Wei

Investigator: Prof. Weisi Guo

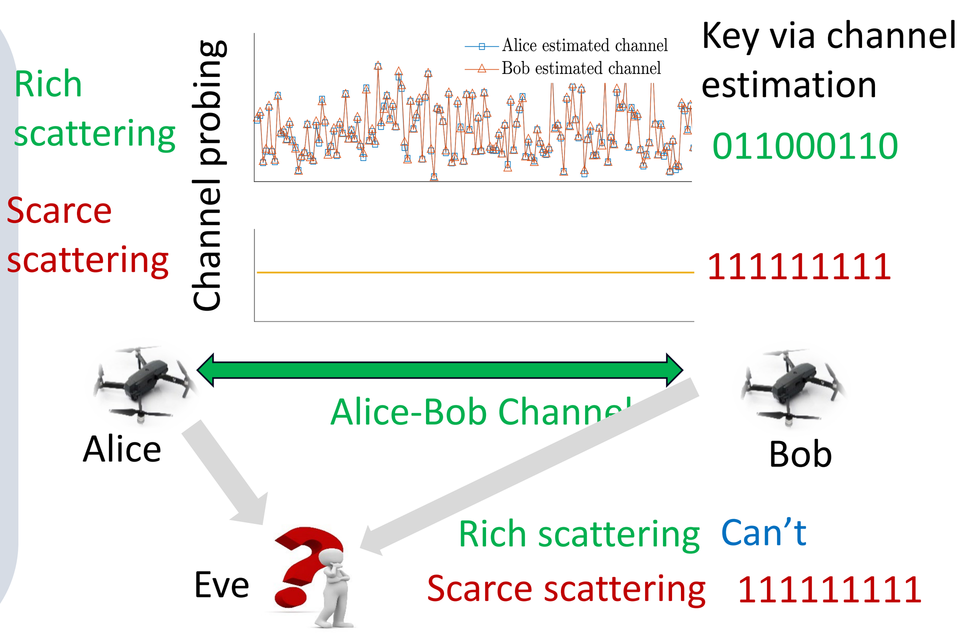
Introduction

Communications of autonomous systems are vulnerable to attacks and eavesdropping, due to broadcasting communication nature and the lack of randomness of communication channels

Key-Less Physical Layer Security (key-less PLS): maximize secrecy rate or signal-to-interference-noise-ratio (SINR), by optimizing trajectory, beamforming, IRS phase.
Advantage: key-less, easy deployment
Disadvantage: no solution guarantee when combined with mission & control layers objectives & constraints



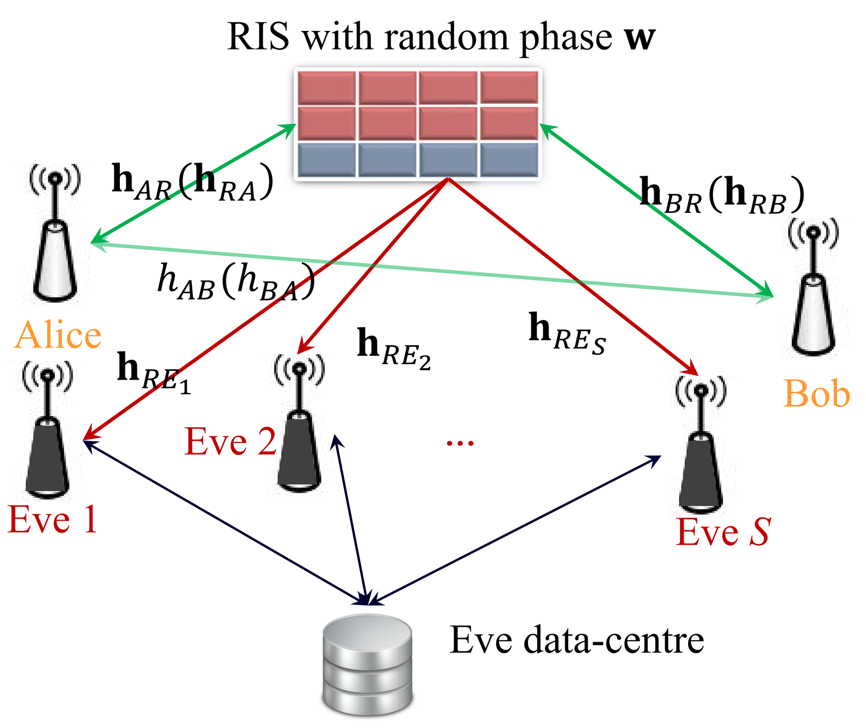
Physical Layer Secret Key Generation (PL-SKG): Generate shared secret sky via the reciprocal small-scale channel randomness.
Advantages: detached from mission & control layer optimization
Disadvantages: requires sufficient small-scale scattering & randomness



1. Cooperative Passive Eavesdropping Threat

Reconfigurable intelligent surface (RIS) is a promising technology to secure the LoS dominated low-entropy channels, by inducing randomness via IRS phases

However, the RIS-induced randomness is also contained in the Eves' received signals, which enables the estimation of the legitimate channel by multiple & cooperative Eves.



Theory of Multi-Eve Design

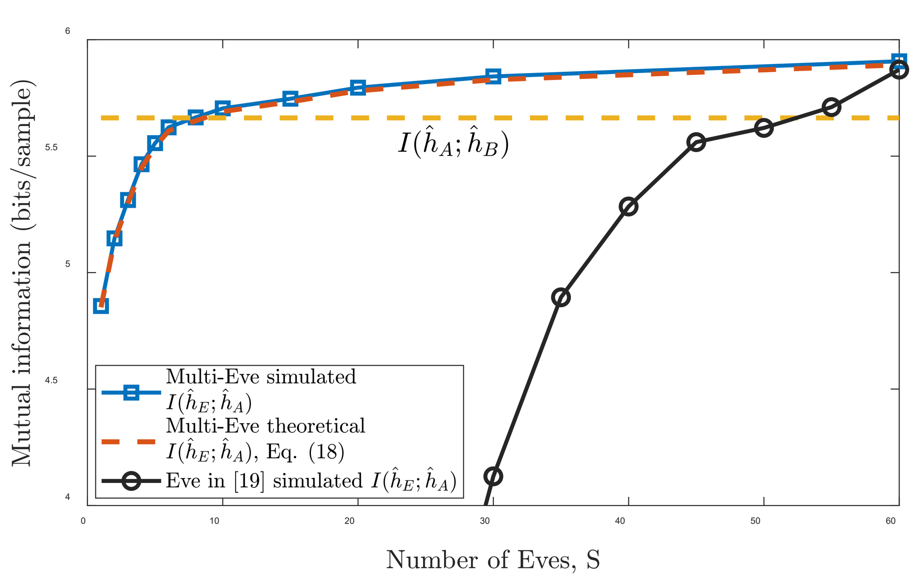
Consider S Eves, each Eve's received signals are:

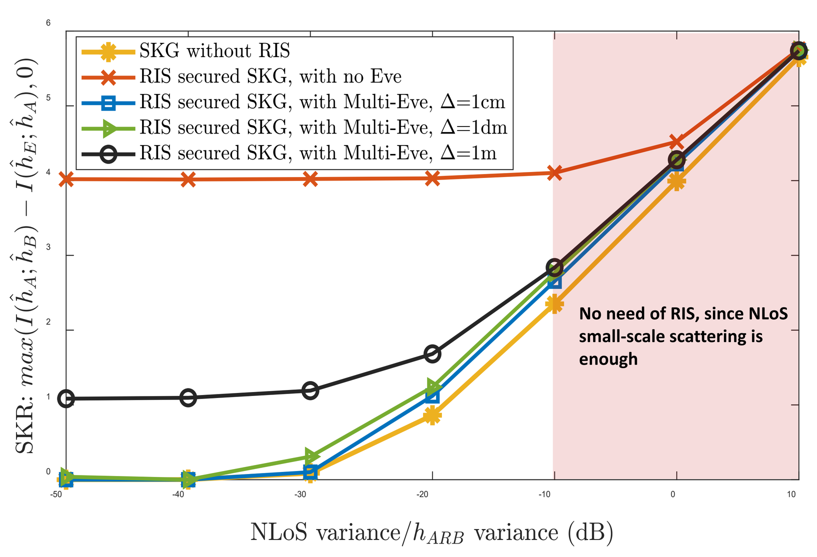
$$\mathbf{z}_s^{(odd)} = (h_{AE_s} + \mathbf{h}_{RE_s} \cdot diag(\mathbf{w}) \cdot \mathbf{h}_{AR}) \cdot \mathbf{u}_A + \varepsilon_s^{(odd)}$$
$$\mathbf{z}_s^{(even)} = (h_{BE_s} + \mathbf{h}_{RE_s} \cdot diag(\mathbf{w}) \cdot \mathbf{h}_{BR}) \cdot \mathbf{u}_B + \varepsilon_s^{(even)}$$

The deployment of S Eves is to ensure the conditional entropy of legitimate channel on S Eves' received equals 0, which suggests a successful estimation of the legitimate channel from Eves.

$$H\left(h_{BA}+h_{ARB}|\mathbf{z}_1^{(odd)}, \mathbf{z}_1^{(even)}, \cdots, \mathbf{z}_S^{(odd)}, \mathbf{z}_S^{(even)}\right) \overset{(a)}{\approx} H\left(\mathbf{h}_{RA} diag(\mathbf{h}_{BR}) \cdot \mathbf{w}; \begin{bmatrix} \mathbf{H}_{RE} \cdot diag(\mathbf{h}_{AR}) \\ \mathbf{H}_{RE} \cdot diag(\mathbf{h}_{BR}) \end{bmatrix} \cdot \mathbf{w}\right) \overset{(b)}{=} 0$$

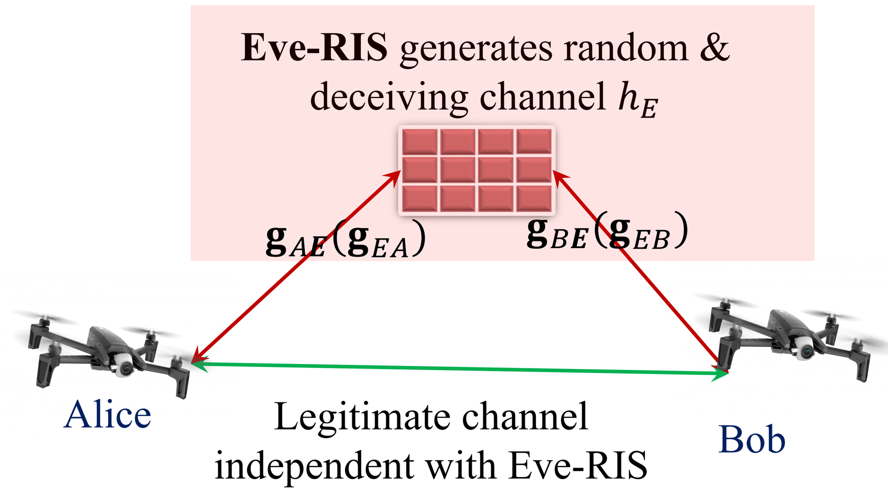
Results of Cooperative Eve Design



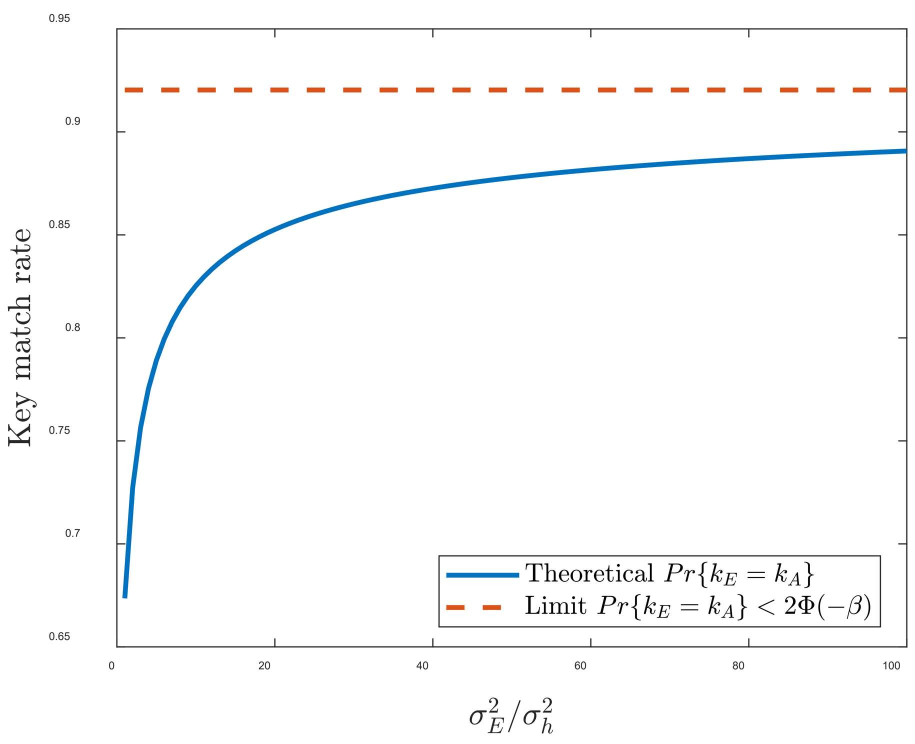


2. Eve-RIS: Concealed Man-in-the-middle Attack

With the advancement of RIS, an adversarial RIS can be used to generate and insert a deceiving channel to the legitimate channel, and then derive the legitimate secret keys. This is a more concealed way of man-in-the-middle attack, since RIS is naturally resistant to countermeasures for untrusted relay.



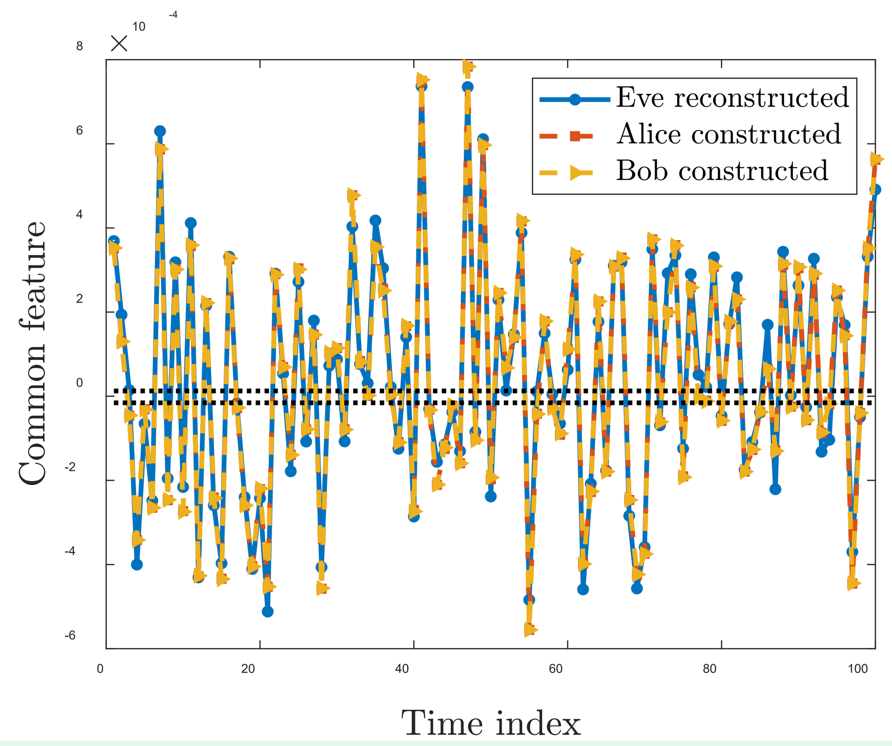
Theory of Eve created Channel Randomness

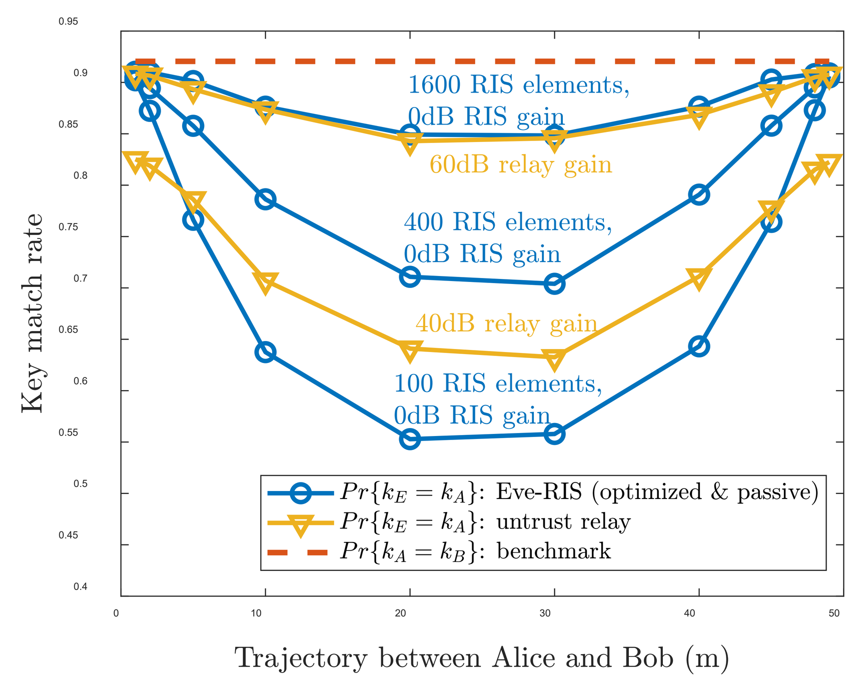


$$Pr\{k_A = k_E\} = \sqrt{\frac{2}{\pi}} \int_{\beta}^{+\infty} \Phi\left(-\beta\sqrt{\frac{\sigma_E^2}{\sigma_h^2}+1} + \frac{\sigma_E}{\sigma_h}\zeta\right) \exp\left(-\frac{\zeta^2}{2}\right) d\zeta$$

With the increase of the variance of Eve-RIS's inserted channel, σ_E^2, the theoretical key match rate between Eve-RIS and legitimate user increases drastically, indicating its potential of stealing the cipher keys

Results of Eve-RIS

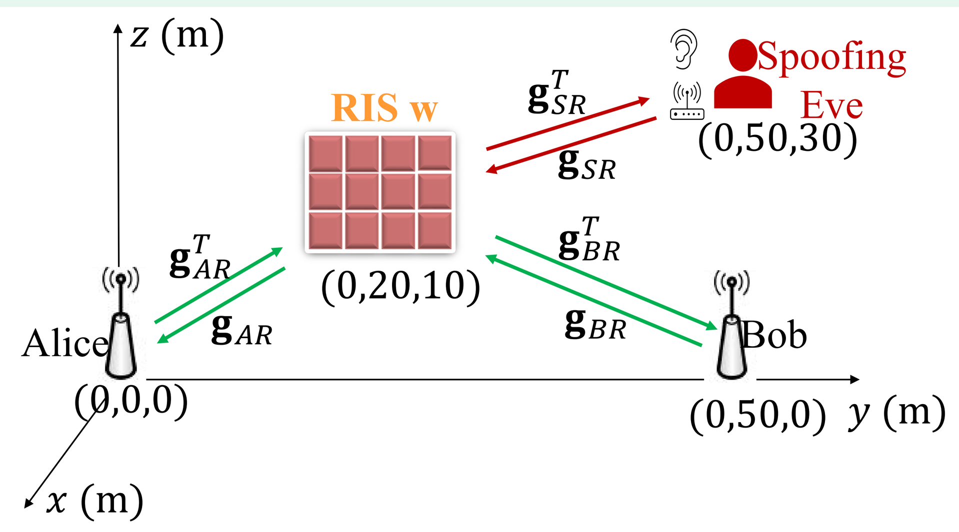




3. Spoofing: with friendly or adversarial RIS

Sketch of Pilot Spoofing

A spoofing Eve aims to pretend as Alice, by sending an amplified Alice's pilot sequence by ρ, simultaneously in the Alice's sending time-slot



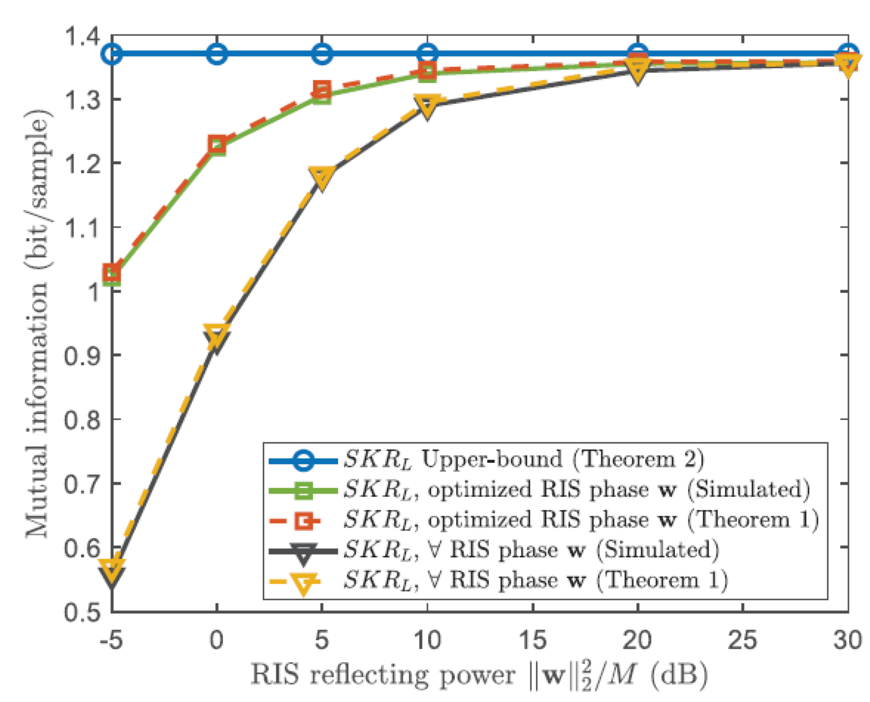
$$SKR_L \triangleq \max\left\{I\left(\hat{h}_A; \hat{h}_B\right) - I\left(\hat{h}_S; \hat{h}_B\right), 0\right\}$$
$$SKR_S \triangleq I\left(\hat{h}_S; \hat{h}_B\right)$$

Upper-bound of Legitimate SKR

Theorem 2: When $\sigma_\epsilon^2 \to 0$ (i.e., with high receiving signal-to-noise ratio, SNR), the legitimate SKR has an upper-bound as:

$$SKR_L < \max\left\{0.5\log_2 \frac{1}{\rho^2}\lambda_{max}\left((\mathbf{U}_{SB}^{-1})^H \mathbf{R}_{AB} \mathbf{U}_{SB}^{-1}\right), 0\right\},$$

where $\lambda_{max}(\cdot)$ represents the maximal eigenvalue of a matrix. $\mathbf{U}_{SB} \triangleq \mathbf{\Lambda}_{SB}^{0.5}\mathbf{\Gamma}_{SB}^H$, with the eigen-decomposition of $\mathbf{R}_{SB}$, i.e., $\mathbf{R}_{SB} = \mathbf{\Gamma}_{SB}\mathbf{\Lambda}_{SB}\mathbf{\Gamma}_{SB}^H$.



Upper-bound of Spoofing SKR

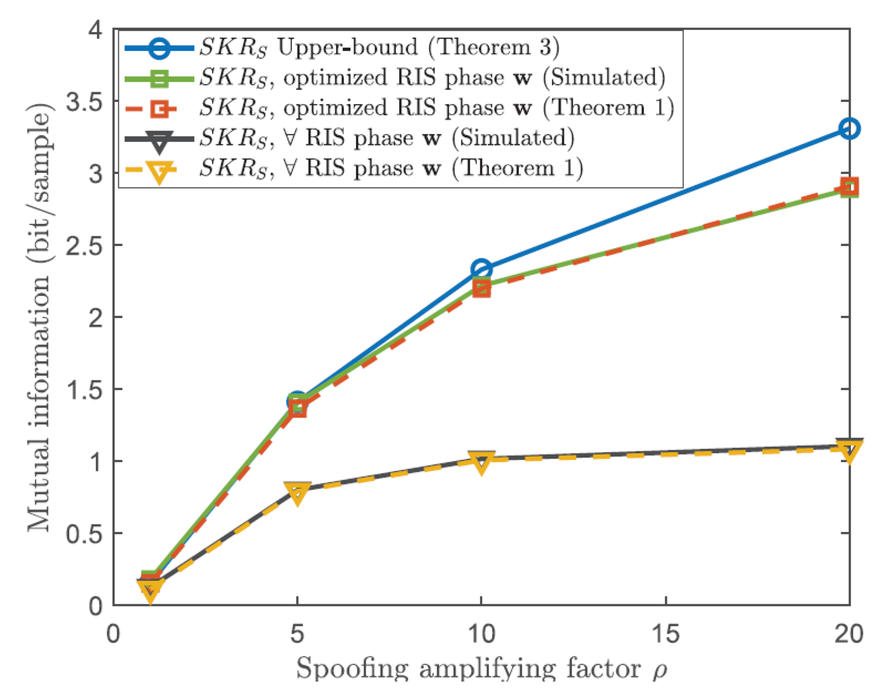
Theorem 3: The spoofing SKR is bounded by:

$$SKR_S < 0.5\log_2\left(1+\rho^2\lambda_{max}\left((\mathbf{U}_{AB}^{-1})^H \mathbf{R}_{SB} \mathbf{U}_{AB}^{-1}\right)\right), \quad (12)$$

where $\mathbf{U}_{AB} \triangleq \mathbf{\Lambda}_{AB}^{0.5}\mathbf{\Gamma}_{AB}^H$, with the eigen-decomposition of $\mathbf{R}_{AB}$, i.e., $\mathbf{R}_{AB} = \mathbf{\Gamma}_{AB}\mathbf{\Lambda}_{AB}\mathbf{\Gamma}_{AB}^H$.

One sub-optimal solution

$$(\mathbf{R}_{SB} - \lambda_{max}(\mathbf{R}_{SB}) \cdot \mathbf{I}_M) \cdot \mathbf{w}_{\text{s-opt}} = \mathbf{0}$$



Results show that RIS can help little against pilot spoofing in autonomous systems, but can be used to improve the spoofing if used by adversarial users

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]