Attacking Analysis on Wireless Communications of Autonomous Systems

Research Fellow: Dr. Zhuangkun Wei

Investigator: Prof. Weisi Guo

School of Aerospace, Transport and Manufacturing (SATM), Cranfield University, UK

1. Introduction

Communications of autonomous systems are vulnerable to attacks and eavesdropping, due to broadcasting communication nature.

4 Types of Attacks

Co-Eves:
Deployment of Eve devices to hold main propagation paths of legitimate users

Eve-IRS:
Eve controlled RIS to generate deceiving channels between Alice and Bob

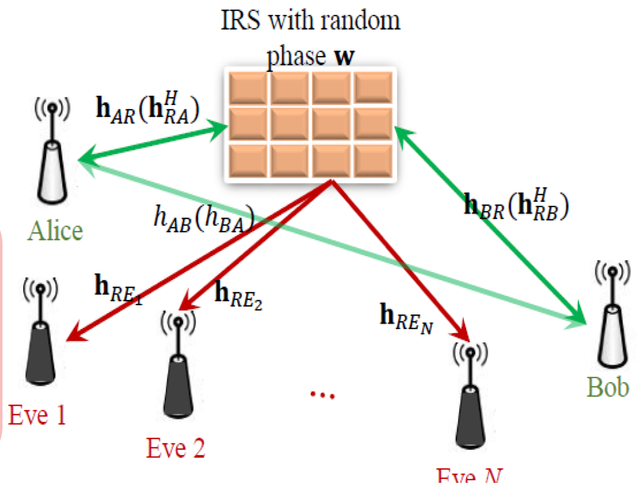
Spoofing Eve:
Eve pretends to be legitimate users by sending channel probing signals to legitimate users

All-jamming attacks:
Attackers send powerful jamming signals through all frequencies to destroy communication channels

2. Cooperative Passive Eves Design

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

However, the IRS-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 *N* Eves, each Eve's received signals are:

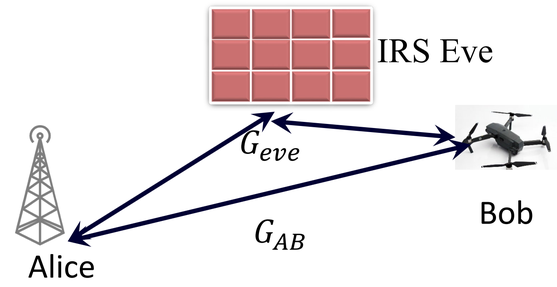
$$\mathbf{z}_n^{(odd)} = (h_{AE_n} + \mathbf{h}_{RE_n} \cdot diag(\mathbf{w}) \cdot \mathbf{h}_{AR}) \cdot \mathbf{u}_A + \varepsilon_n^{(odd)}$$
$$\mathbf{z}_n^{(even)} = (h_{BE_n} + \mathbf{h}_{RE_n} \cdot diag(\mathbf{w}^*) \cdot \mathbf{h}_{BR}) \cdot \mathbf{u}_B + \varepsilon_n^{(even)}$$

The deployment of *N* Eves is to ensure the mutual information between *N* Eves' received signals and the legitimate channel equal the information entropy of the latter, which suggests a successful estimation of the legitimate channel from Eves.

$$I\left(\hat{h}_A; \mathbf{z}_1^{(odd)}, \mathbf{z}_1^{(even)}, \cdots, \mathbf{z}_N^{(odd)}, \mathbf{z}_N^{(even)}\right)$$
$$\overset{(a)}{\lesssim} I\left(\mathbf{h}_{RA} diag(\mathbf{h}_{BR}) \cdot \mathbf{w}; \begin{bmatrix} \mathbf{H}_{RE} \cdot diag(\mathbf{h}_{AR}) \\ \mathbf{H}_{RE}^* \cdot diag(\mathbf{h}_{BR}^*) \end{bmatrix} \cdot \mathbf{w}\right) \overset{(b)}{=} H(h)$$

3. When Eve is IRS

Another type of passive Eve is when Eve acts as part of the legitimate channel between Alice and Bob, e.g., using an intelligent reflecting surface (IRS) to generate a random channel between Alice and Bob.



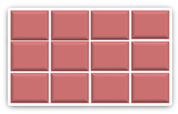
Theory of Eve created Channel Randomness

Alice

$G_{AB} + G_{eve}$
$Cov(G_{AB}, G_{eve}) = 0$

Bob

$G_{BA} + G_{eve}$



IRS Eve

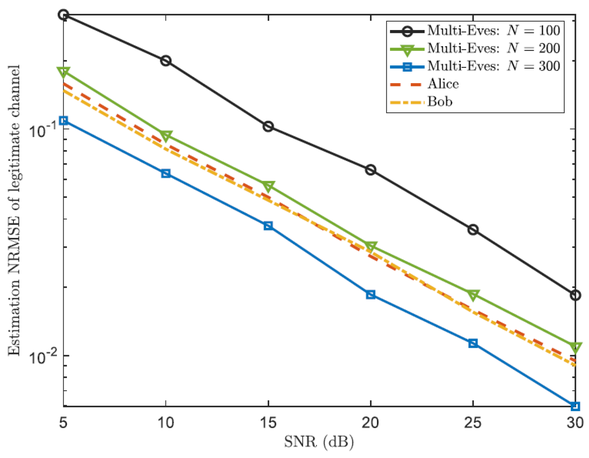
G_{eve}

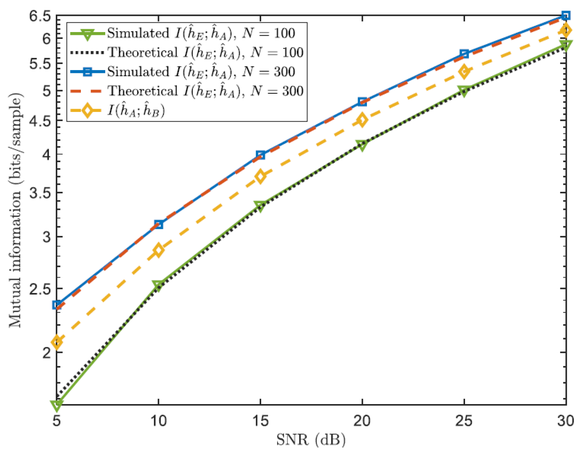
$$SKR = I(G_{AB} + G_{eve}; G_{BA} + G_{eve}) - I(G_{eve}; G_{AB} + G_{eve}) = H(G_{AB}) = I(G_{AB}; G_{BA})$$

Indicates if eve IRS generate an unrelated channel G_{eve}, the secret key rate (SKR) of Alice-Bob will not be decreased.

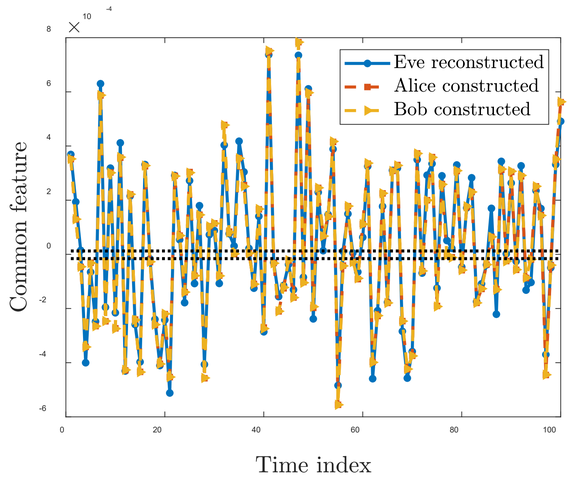
However, Alice and Bob do not know the statistic of Eve's adding channel. So, they will use $G_{BA} + G_{eve}$ for key generation. This will make the key related to Eve.

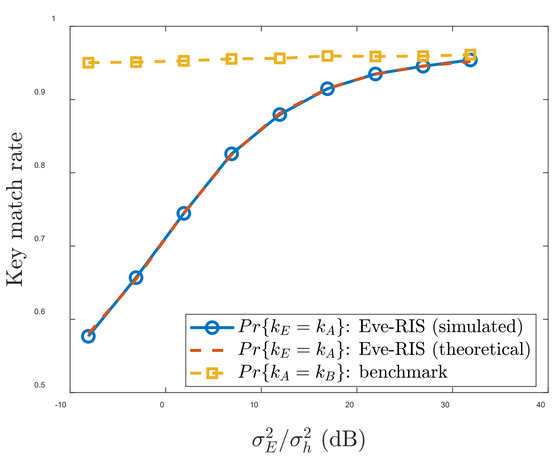
Results of Multi-Eve Design





Results of Eve-IRS





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