**Conclusion**

In this paper, a new scheme is introduced in order to establish a secure communication at the physical layer between a base station, Alice, and a legitimate user, Bob, in the presence of a passive eavesdropper, Eve. Alice uses a time reversal precoder, implemented in the frequency domain with OFDM, to add to the transmitted data an artificial noise that lies in the null-space of Bob but degrade Eve’s channel. The proposed technique only requires a single transmit antenna and is therefore well suited for devices with limited capabilities, such as in IoT for instance.

The ergodic secrecy rate performance is analytically derived, assuming Rayleigh channels, for three different optimal decoding structures at Eve, whose implementation depends on the amount of CSI she can estimate, which in turn depends on the handshake procedure of the considered protocol. The obtained analytical formulations allow Alice to determine the optimal amount of artificial noise energy to inject in order to maximize the secrecy rate. The performance depends on the communication parameters but can be tuned thanks to the back-off rate factor (i.e., sampling rate to symbol rate ratio), used while implementing the time reversal precoder.

Under the assumptions of fast-fading and uncorrelated channels, it is shown that a positive secrecy rate can be guaranteed even when Eve’s SNR is infinite, for moderate values of Bob’s SNR. For instance, with an upsampling of 8, a secrecy rate of 0.75 and 2.2 bits/channel use is obtained with a Bob’s SNR of 5 dB and 10 dB, respectively, with Eve’s SNR is infinite. Furthermore, Alice can be aware of this guaranteed secrecy rate if she knows Bob’s SNR. She can thus communicate while not exceeding this secrecy rate and therefore ensures the secrecy of the communication. Finally, an enhancement of this scheme is proposed via an optimal power allocation strategy over the subcarriers depending on the instantaneous CSI.

This paper shows, consequently, with analytic and simulation results, that a scheme exploiting only frequency degrees of freedom can achieve a positive ergodic secrecy rate to considerably jeopardize any attempt of an eavesdropper to retrieve the data. This approach can be easily integrated into existing standards based on OFDM and does not necessitate extra hardware. However, a perspective of this work is to extend it to multiple antenna systems to assess the benefit of the extra spatial degree of freedom.