Physical Layer Authentication using SDRs

Gencsek Ewan, PhD Student
Electrical Engineer, focusing on AI and Smart Communications

Supervisor: Mégret Patrice
Co-supervisor: Moeyaert Véronique

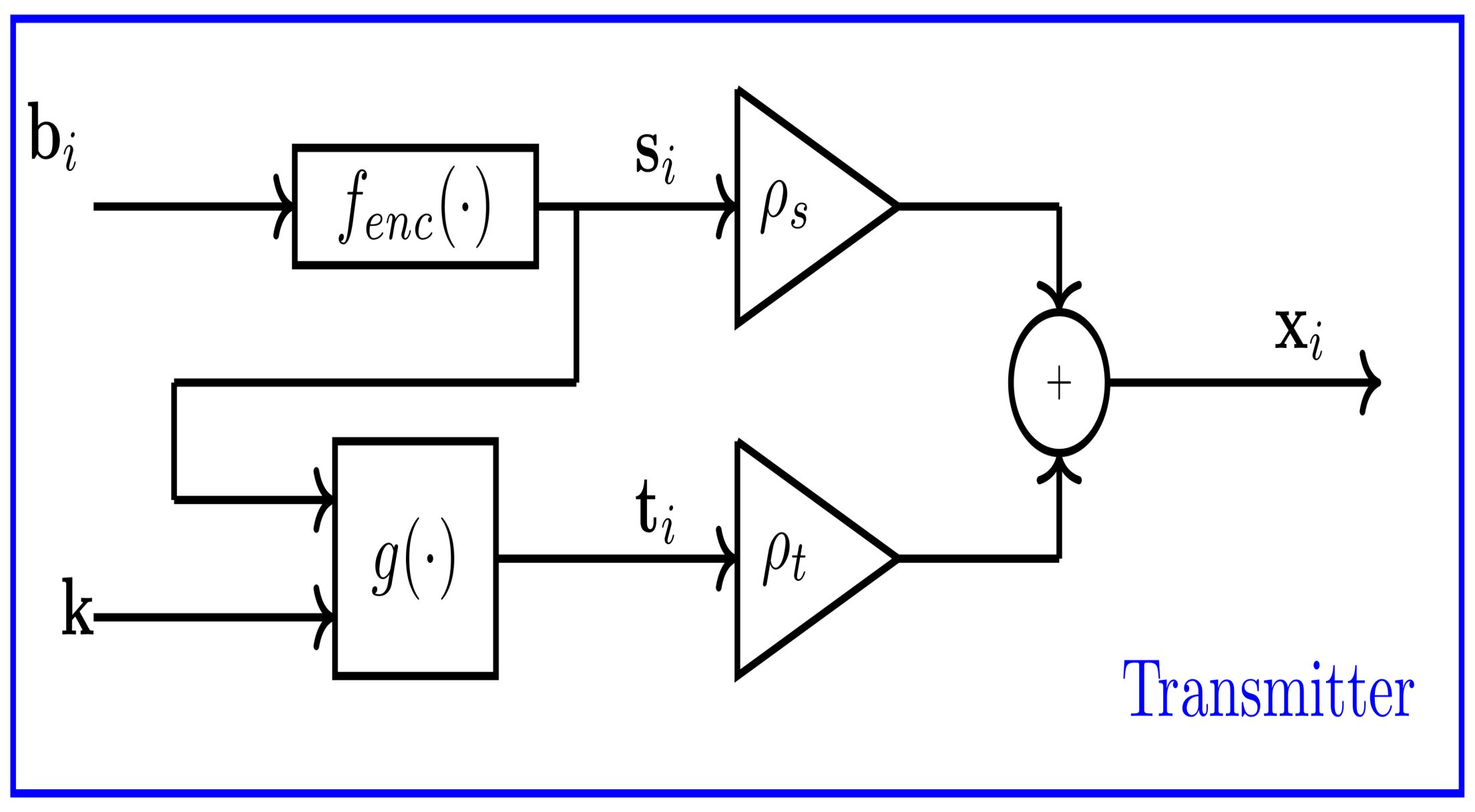
Context

Physical layer authentication (PLA) is an authentication technique occuring at the physical layer of the OSI digital communication model [1]. This secures communication by adding another step of authentication directly after receiving a signal. The active superimposed (SUP) scheme consists of sending an authentication tag signal $\mathbf{t}_i$ superimposed to the data signal $\mathbf{s}_i$ [2]. $\mathbf{t}_i = g(\mathbf{s}_i, \mathbf{k})$, with $g(\cdot)$ a cryptographic function and $\mathbf{k}$ a key. Both are known from the transmitter and the receiver. The transmitted tagged signal $\mathbf{x}_i$ is:

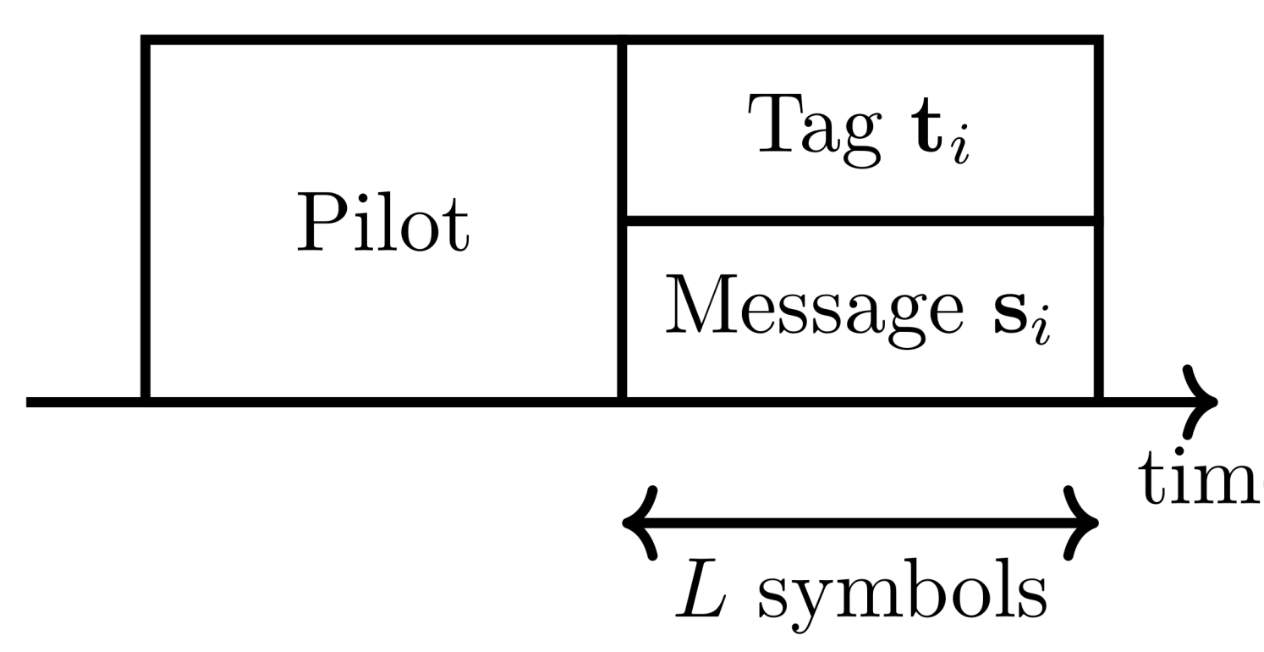
$$\mathbf{x}_i = \rho_s \mathbf{s}_i + \rho_t \mathbf{t}_i$$

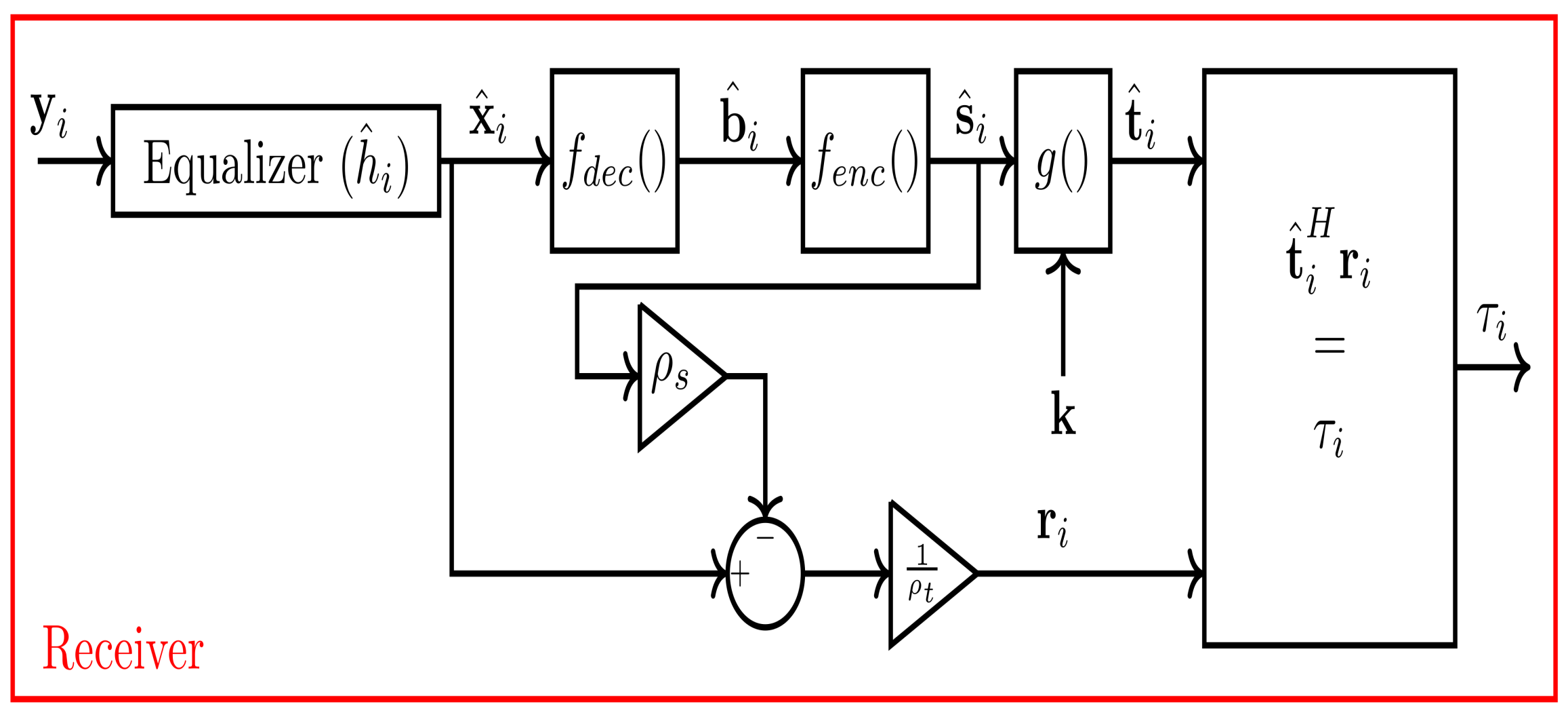
with ρ_t and ρ_s corresponding to the energy allocated to the tag signal or the data signal, respectively, and with $\rho_t^2 + \rho_s^2 = 1$. The transmitter is authenticated if $\tau_i = \hat{\mathbf{t}}_i^H \mathbf{r}_i$ is above a threshold θ. $\hat{\mathbf{t}}_i^H$ is the Hermitian transpose of the tag generated at the receiver side with the decoded data and $\mathbf{r}_i = \frac{1}{\rho_t}\left(\hat{x}_i - \rho_s \hat{\mathbf{s}}_i\right)$ a residual signal which should be the transmitted tag signal. The threshold depends on the communication channel (fading and noise effects), the tag energy allocation, the modulation used for transmission and the probability of false alarm ϵ_{FA}, i.e. the probability of considering an unauthentic signal authentic, fixed by users. The flow diagrams of the transmitter (blue frame) and the receiver (red frame) are shown below with the tagged signal frame structure in the middle.

[1] N. Xie, Z. Li et H. Tan. « A Survey of Physical-Layer Authentication in Wireless Communications ». In: *IEEE Communications Surveys Tutorials 23.1* (2021), p.282-310.
[2] P. L. Yu, J. S. Baras and B. M. Sadler, "Physical-Layer Authentication," in *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 38-51, March 2008.



Tagged signal frame structure:

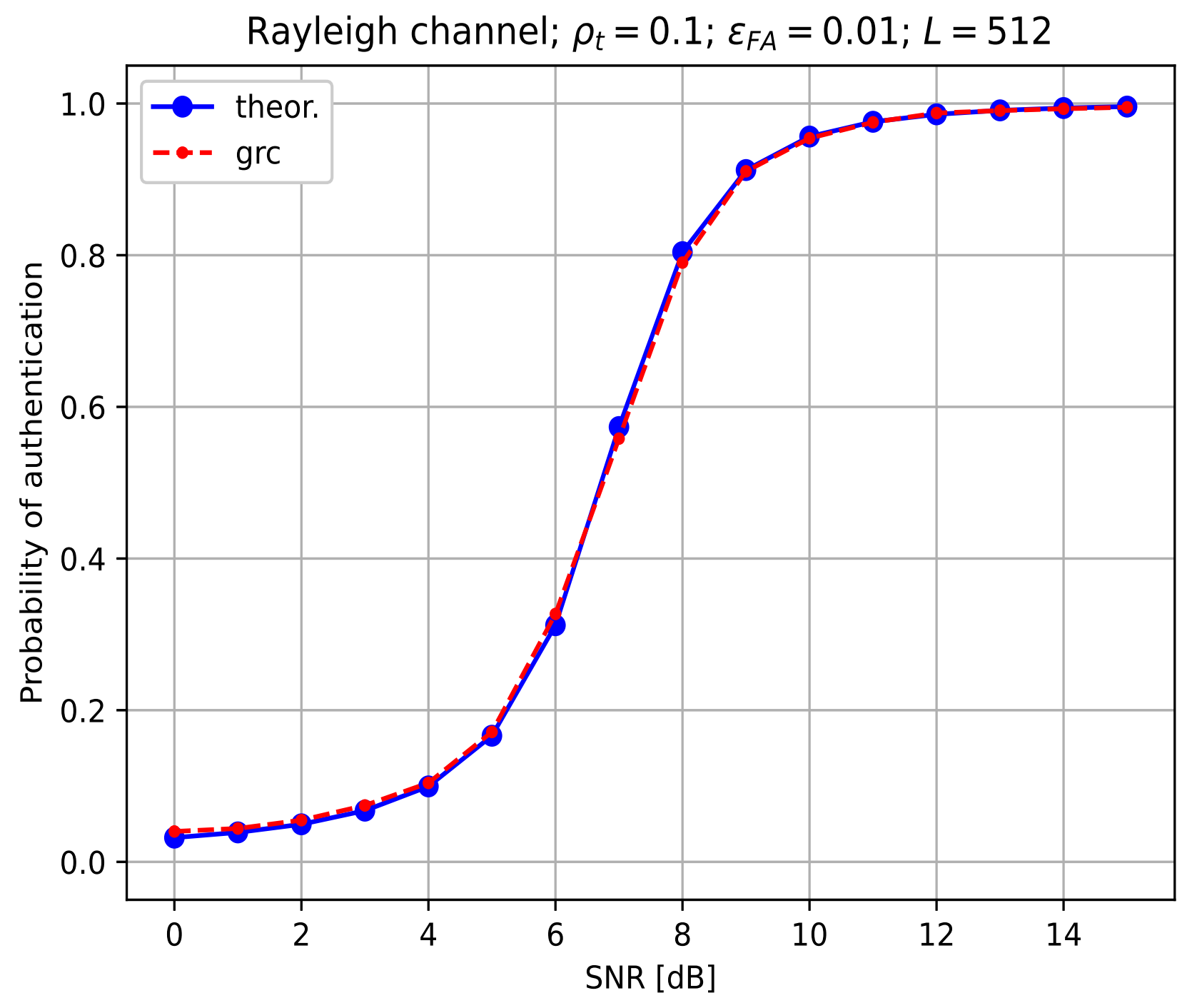


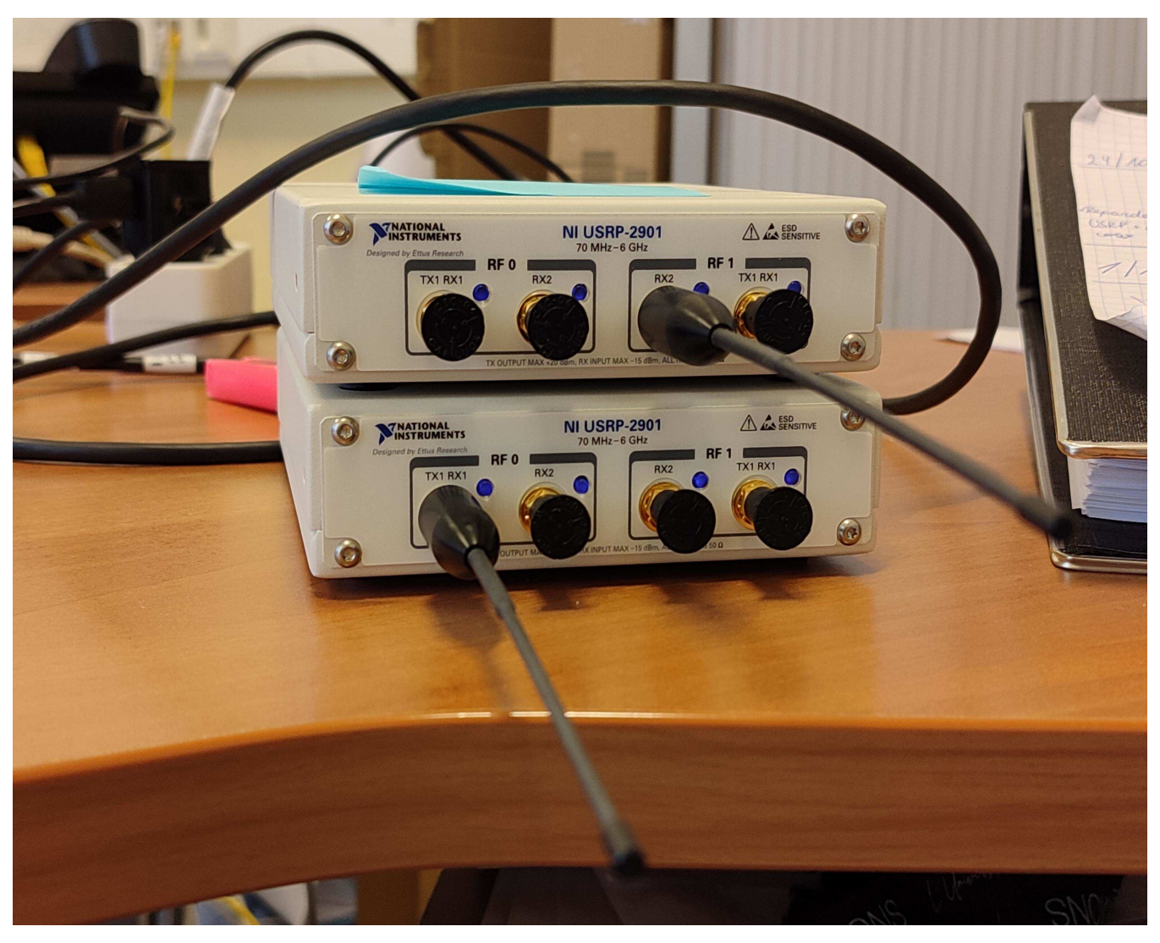


$f_{enc}(\cdot)$ is the encoding function encapsulating the modulation, the channel coding and the pulse shaping.
$f_{dec}(\cdot)$ is its inverse function.

Theory and simulation

Real-time authentication was first imlplemented in simulated environment using GNU Radio. Probabilities of authentication of simulated transmission and theoretical ones concur toegether. 10000 packets were simulated for each SNR value. A Rayleigh block-fading channel is considered.



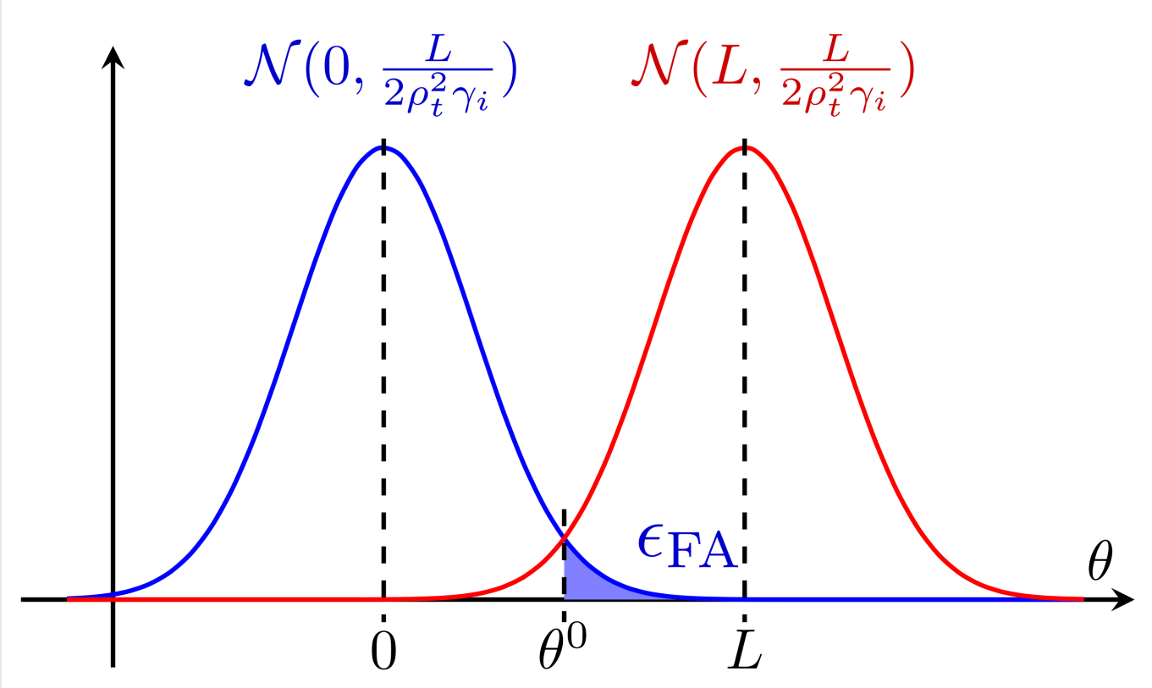


Experimental set-up

The experimental setup, shown on the right, consists of two NI USRP-2901. GNU Radio software is used to implement the SUP scheme on the software-defined radios, one for transmission and the other for reception and authentication. Steps were tested with BPSK modulation, 4 samples-per-symbols and RRC filter at a carrier frequency of 2 GHz. Absolute tranmission and reception gains were set to achieve error-less reception of the transmitted data bits (TX gain of 62 dB, RX gain of 60 dB).

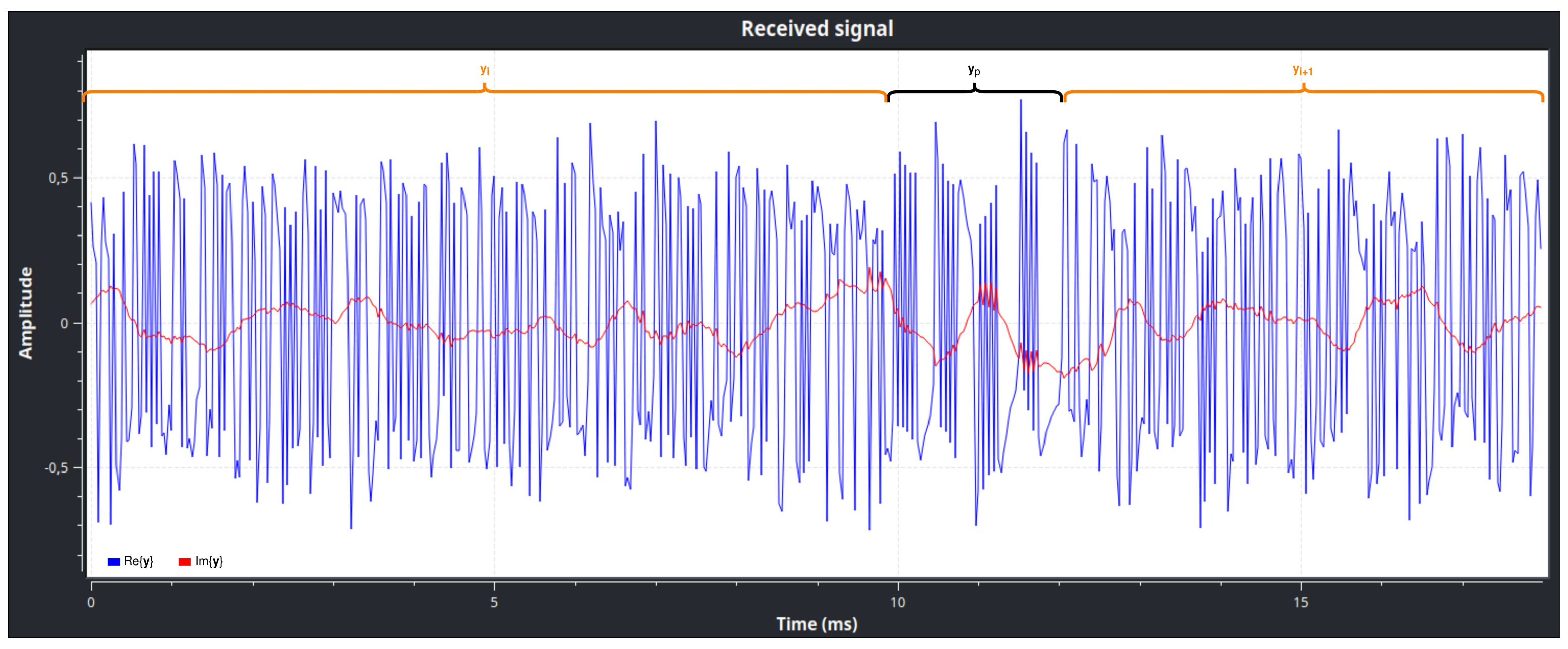
Threshold

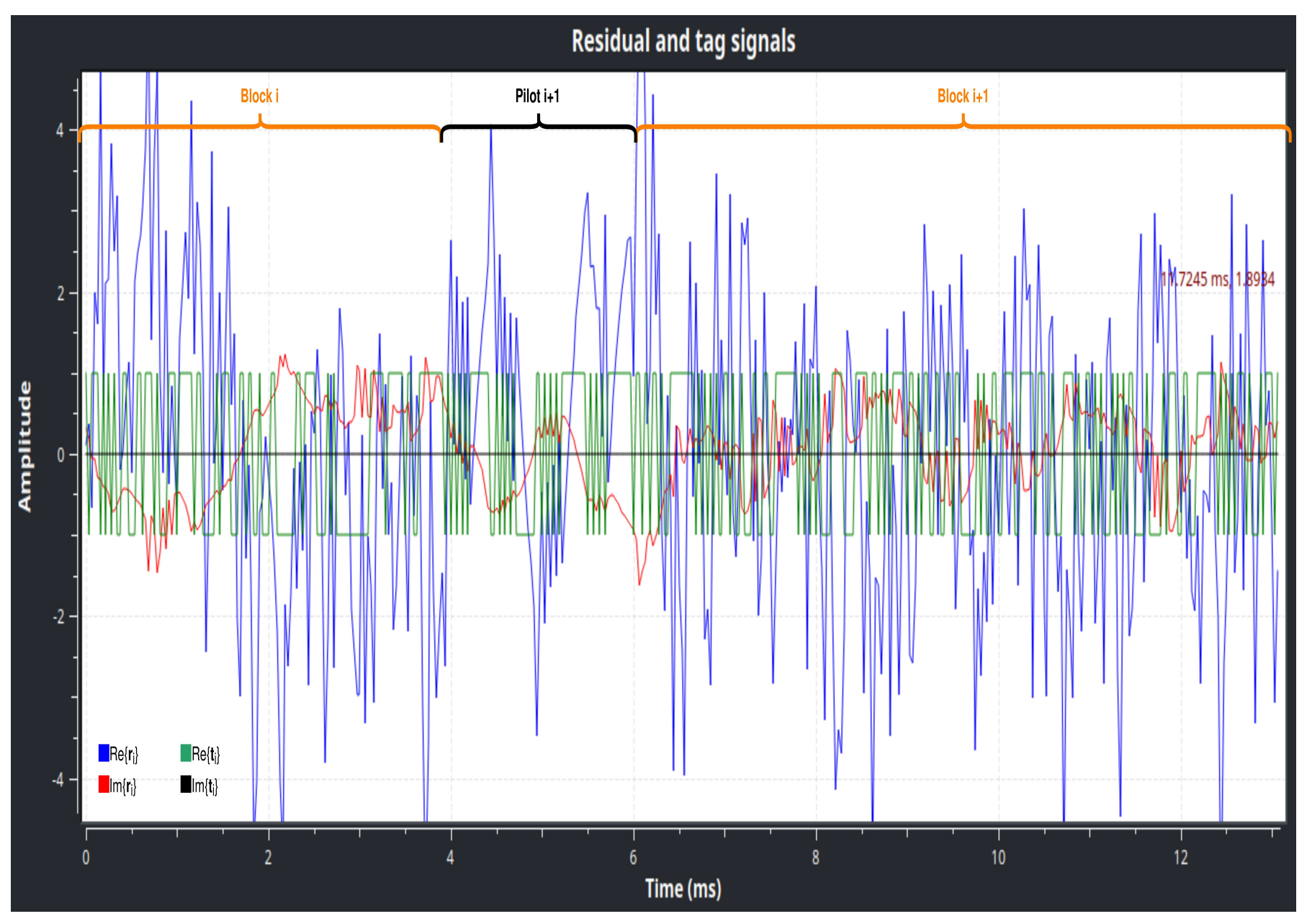
For a BPSK modulation and in a Rayleigh fading channel, τ_i is a normal random variable [3]. Figure below shows distributions of τ_i in the case of a tagged signal (red) and in a non-tagged signal (blue). Finding optimal threshold is finding θ^0 when blue area, representing the probability of false alarm, is equal to ϵ_{FA}, fixed by users.

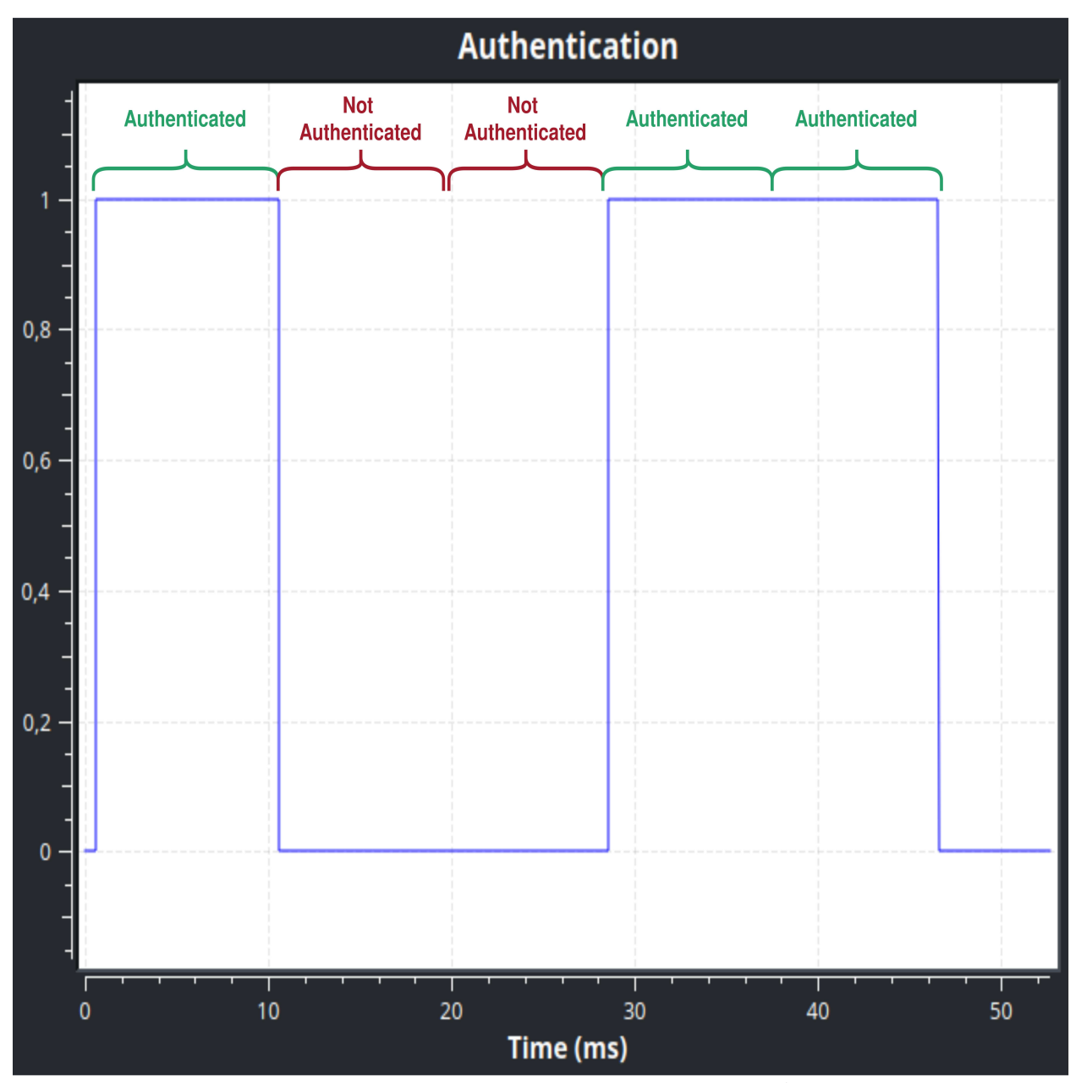


[3] N. Xie, C. Chen and Z. Ming, "Security Model of Authentication at the Physical Layer and Performance Analysis over Fading Channels," in *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 1, pp. 253-268, 1 Jan.-Feb. 2021

Here, the threshold is set up arbitrarely because the channel is not yet determined.







GNU Radio screenshots of the received signal (above), recovered data $\hat{\mathbf{s}}$ and transmitted $\hat{\mathbf{x}}_i$ signals (left bottom) and authentication decision (right bottom).
Parameters: - $L = 512$ bits, $\rho_t = 0.2$ and $\theta = 5$
- $g(\cdot)$ is HMAC with SHA3-256

Results

SDRs were configured to use the SUP scheme for communications, with each of the following steps being essential for implementation in a real-world environment, such as a factory:

- Transmission of a tagged signal without error on data at the receiver side
- Authentication operations (regeneration of $\hat{\mathbf{t}}_i$, $\mathbf{r}_i$ computation, threshold comparison) achieved on the received packets
- Channel equalization with pilot signal
- Channel model determination for threshold computation
- Real-time SNR estimation for automatic threshold adaptation

Green means that the operation can be done in real-time.
Red means that the operation is not yet implemented.

Next steps of the research

The SUP scheme was implemented on SDRs for real communication. It is now possible to authenticate real wireless BPSK signals at the reception of them. To implement the scheme into a real environment steps were presented above. The next steps of the research are:

- Parameter (L, ρ_t and ϵ_{FA}) effect study
- Channel effect study

One final objective is to add this authentication scheme to an already existing IIoT communication protocol, e.g. IEEE 802.15.4.

University of Mons

December 2024

Cyberwal in Galaxia