*Short introduction (group and table of contents)…*

**SLIDE 3 – INTRODUCTION TO PLA**

The environment in which we have worked is the PLA (Physical Layer Authentication), which constitutes a cutting-edge approach to enhancing security in wireless communication systems.

PLA leverages the unique physical characteristics of the communication channel to authenticate transmitters. Unlike traditional methods that rely on cryptographic techniques, PLA focuses on properties such as the amplitude, phase, and frequency response of the signal.

There are several notable advantages to using PLA. First, it offers enhanced security because it’s extremely challenging for an attacker to mimic the physical properties of the legitimate transmitter’s signal. Second, it has a low overhead since it doesn’t require the computational resources needed for complex cryptographic algorithms. Lastly, PLA enables real-time authentication, allowing for a quick verification process that is crucial in many applications.

It is possible to count several related works in the PLA environment, a lot of them regarding communications between Bluetooth Low Energy devices. Other related works propose surveys that try to collect different works done in this field, useful to introduce people like us to the PLA environment. Even if there are several related works, none of them propose an effective PLA scheme to authenticate wireless communications, this led us to conduct the experiment we are presenting today.

**SLIDE 4 – OVERVIEW OF THE PROJECT**

Before entering in the details, we want to give you an overview of our project. The goal of the project was to study the behavior of Bluetooth wireless transmissions to develop a simulation environment to design and test PLA schemes.

The high-level reasoning that we applied is the following:

* We considered the transmission of binary signals between a transmitter and receiver, formed by an authentication key and data message.
* From the data that we have collected from the different transmissions, we developed a decoding algorithm able to reconstruct the received signal and split it into the two packets (key and data), recovering so the original message.
* We tested the strength of the decoding in classifying legitimate and not legitimate signals, considering the scenario of a man-in-the-middle that captures and retransmit the signal.

**SLIDE 5 – EXPERIMENT AND IMPLEMENTATION**

Now we're going to explain in depth our simulation of how Bluetooth signals behave under different conditions. We created a parametrized simulation environment that allowed us to test various scenarios and design our PLA scheme.

Our implementation involved several key steps. First, we combined data and authentication signals. We represented these as binary waveforms with different power levels, using the peaks to distinguish between them. Specifically, the authentication signal was designed with lower power peaks, allowing for more accurate analysis of both components. This approach gave us a unique 'fingerprint' for each transmission.

To make our simulation as realistic as possible, we varied two critical parameters. We tested distances transmitter-receiver ranging from 1 to 50 meters, covering the typical range of Bluetooth communications. We also adjusted the Signal-to-Noise Ratio, or SNR, from 10 to 30 decibels. This helped us model how signal quality degrades over distance and in different noise environments.

Under this configuration, we sent several signals to study how they arrive to the receiver. Initially, we tried to decode the received signal using a simple fixed-threshold decoding based on a center value of the signal and two fixed thresholds.

In several scenarios this method does not work, resulting in a signal much different than the original one. This depends on the extremely simplicity of this decoding. On the other hand, this method has been really useful to us to study the critical point of the decoding, leading to an effective decoding implementation based on variable-threshold, depending so on the signal itself.

To determine the authenticity of a decoded message, and so to test the effectiveness of the chosen decoding implementation, we set a maximum number of permitted error bits on the key signal. Using Hamming distance, we calculated the number of incorrect bits compared to the original signals. This is crucial for computing the Bit Error Rate (BER), which we use to calculate false alarm and missed detection rates. Since we are considering a parametrized simulation, it is fundamental to highlight that even the number of errors on the key is a parameter that can be changed depending on the performance that you want to reach in your system. Anyway we tried different low values for this parameter, for instance 3 allowed bits, and the results are promising, confirming the strength of the variable-threshold decoding algorithm.

Extra:

(The core of our simulation revolves around a sender transmitting a signal consisting of a key for authentication and a data message, mixed with known power parameters. Within the receiver, we implemented two decoding methods: fixed-threshold and variable-threshold.

For the variable threshold method, we considered four peaks on the signal: high-high (maximum value), low-low (minimum value), and two intermediate values (medium-low and medium-high). These measurements are adjusted based on a 'center' parameter, allowing us to precisely define and update these peak values. This approach helps refine the intermediate values by considering both previous and current measurements.

The fixed threshold decoding is based on the center parameter. We defined a method of bit concordance/discordance to ensure the received signals consistently reflect the originally mixed waveforms.

Our simulation environment allows for iterative refinement. After multiple executions, we can adjust the tolerance threshold to verify transmission correctness, tailoring it to desired security performance levels. By adjusting all these parameters, we created a flexible, realistic simulation environment. This setup allowed us to design, test, and refine our PLA schemes, giving us valuable insights into how they might perform in real-world Bluetooth communications.)