*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**

…

**SLIDE 5 – EXPERIMENT AND IMPLEMENTATION**

…