(Slide 5 - Experiment & Implementation)

Now we’re going to explain a bit more of the simulation using Bluetooth signals behave under different conditions. To do this, we created a parametrized simulation environment. This allowed us to test various scenarios and fine-tune our Physical Layer Authentication, or 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. This approach gave us a unique “fingerprint” for each transmission. To make our simulation as realistic as possible, we varied two critical parameters; distances, ranging between realistic values (1-50) and the tolerated SNR ratios, able to reflect in depth the analysis and refine overtime the selected simulation conditions. The basic idea is to have a sender and receiver sending a signal consisting of a key (authentication) and a data message, mixed with known power parameters.

Speaking of noise, we didn't forget about the inherent messiness of real-world wireless channels. We applied white noise to our signals, specifically what's known as Additive White Gaussian Noise, or AWGN, which adds noise to the same level of frequency, which simulation the effects interference and distortion you'd expect in a real Bluetooth transmission.

About the experiment,

(Slide 6 - FA (False Alarm) Study)

(Slide 7 - FA (False Alarm) Study – Results)

(Slide 8 - MD (Miss Detection) Study)

(Slide 9 - MD (Miss Detection) Study – Results)

(Slide 10 - Conclusions & Future Work)