**SLIDE 6 - FA (False Alarm) Study**

Now, let's focus on our False Alarm study, which is crucial for evaluating the effectiveness of our authentication scheme, using binary signals and realistic noise conditions

In this part of our simulation, we exclusively sent authentic messages. These messages were created by combining the actual signal with the correct authentication key. The primary goal here was to assess the reliability of our transmission system by measuring how often these genuine messages were incorrectly flagged as non-authentic - what we call “false alarms” or “false negatives”.

We conducted this study using the already defined simulation parameters, which are the different distances/SNR ratios. To determine whether a message was authentic, we established an error tolerance for the key bits. If the number of incorrect bits in the decoded key exceeded this tolerance when compared to the original key, we classified it as a false alarm.

**SLIDE 7 - FA (False Alarm) Study – Results**

Interestingly, after multiple simulation runs, we observed a False Alarm rate of 0% across all distance-SNR pairs. While this might seem surprisingly good, it's actually a testament to the effectiveness of our variable threshold decoding algorithm. This method significantly reduced the number of errors in the key bits compared to the fixed-threshold approach, consistently keeping the error count below our set threshold.

Secondly, our variable decoding algorithm proved to be highly effective. It consistently managed to keep the number of key bit errors below the set threshold. This is crucial because it demonstrates the robustness of our decoding method across various transmission conditions.

Lastly, these results strongly validated the effectiveness of both our chosen tolerance level and the decoding algorithm itself. The fact that we achieved a 0% false alarm rate indicates that our approach to authentication is both accurate and reliable.

It's important to note that while these results are extremely positive, they also prompted us to critically examine our methodology. A 0% false alarm rate, while ideal, is uncommon in real-world scenarios. This led us to consider whether our thresholds might be too lenient or if our simulation conditions might not fully capture all real-world complexities. These results are infact motivated by the choice of the variable decoding method used inside of this specific simulation, which allowed the choice of the possible thresholds and analysis on the wrong bits, particularly by the variable decoding.

**SLIDE 8 - MD (Miss Detection) Study**

Now, let's move on to our Miss Detection study, which is crucial for understanding how our system handles non-authentic messages.

In this part of our simulation, we focused exclusively on sending non-authentic messages. Our goal was to see how many of these illegitimate transmissions our system would mistakenly interpret as authentic - what we call “miss detections” or “false positives”, since they were already sent as non-authentic upfront. Here, we assume for the sake of correct threat modeling, the attacker has knowledge of all the channel parameters and the structure of the message, simulating correctly a MITM attack.

The attacker attempts to decode the signal based on peaks, similar to how a legitimate receiver would, based on the same principle of dynamic thresholding as found before. What changes is the evident guess on the part of the possible attacker, so as to combine the signal once the decoding of the dynamic thresholds thus composed of power and authentication. The legitimate receiver, with decoding depending on the dynamic thresholds using same logic seen above.

The attacker attempts to decode the signal based on peaks, similar to how a legitimate receiver would. They try to emulate our decoding process, including the use of dynamic thresholds and bit discordance logic.

**SLIDE 9 - MD (Miss Detection) Study – Results**

Here, in fact, the miss detection values reveal fluctuating values, averaging between 20 and 30-35% after a series of detections, confirming the effectiveness of the approach highlighted. In this way, it is possible to note that an attacker can insert himself inside the decoding mechanism, thus not being detected. Since the attacker partially knows the transmission powers, the attacker was unable to perfectly reconstruct messages.

This is due to his partial knowledge of transmission powers. While he could derive maximum and minimum power levels, he couldn't accurately separate the power components of the key and data signals. However, even with this knowledge, they can't perfectly reconstruct the original signal. They have to make educated guesses about how to split the observed power between the key and data components. These results confirm the robustness of our decoding methods. We were able to detect a good portion of invalid messages, even under these realistic attack conditions.

The results confirm the effectiveness of our decoding methods. Even when the attacker had significant information about transmission powers, our system could still detect a substantial portion of invalid messages.

**SLIDE 10 - Conclusions & Future Work**

The parametrized simulation study yielded several observations:

* the solidity of a single simulation, modeled as a wireless communication system with combined data and authentication signals enabled analysis of different simulation parameters, so to constrain the simulation as much as possible to get the best possible performance out of those. Both fixed-threshold and variable-threshold decoding methods were tested. The variable threshold approach provided more effective decoding, particularly for determination of wrong bits and calculation of BER values
* both only authentic and non-authentic messages were sent, so to simulate the retention of the tested decoding methods, using only non-authenticate messages for a model as realistic as possible, so to mimic the legitimate receiving process
* despite the successes, the miss detection rates observed, which vary between 20% and 35%, indicate that there is substantial room for improvement. Also, the false alarm rates, while good, are strictly dependent on the soundness of the system defined, so it may represent a start for a PLA scheme based on variable thresholding but there is still a good way to go

To address the issues raised by the current miss detection rates, we propose the implementation of noise-based simulations in future studies. Introducing additive noise to the signal before transmission could potentially complicate the attacker’s ability to decode and reconstruct the messages accurately. This method would enhance the robustness of the system against sophisticated attacks.

Also, the exploring of advanced filtering systems that can work in conjunction with existing authentication techniques. These systems would be designed to 'clean' the signal of additive noise, but only for authorized receivers who share a secret key or parameter