PLA Bluetooth Environment: A parametrized simulation

Michael Amista' - Gabriel Rovesti

July 2nd, 2024

Supervisor: Alessandro Lotto

Advanced Topics in Computer Network and Security

2023-2024

UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO MATEMATICA

Table of contents

Introduction to PLA

What is PLA?

- Utilizes unique physical characteristics of the communication channel
- Provides security by verifying the authenticity of the transmitter

Why this approach is promising:

- Enhanced Security: Difficult for attackers to mimic physical properties
- Low Overhead: No need for additional cryptographic algorithms
- Real-Time Authentication: Quick verification process

Related works:

- A lot of different studies overtime, mainly in Bluetooth Low Energy
- More focused on discussing of Bluetooth vulnerabilities rather than proposing an effective authentication system

Overview of the project

UNIVERSITÀ DEGLI STUDI DI PADOVA

Objective: Study the behavior of Bluetooth signals transmissions and receptions to develop a simulation environment to design and test Physical Layer Authentication (PLA) schemes.

Methodology:

- We considered the transmission of binary signals between a transmitter and receiver, formed by an authentication key and data message
- We developed a decoding algorithm able to reconstruct the received signal and split it into the two packets (key and data)
- We tested the strength of the decoding in classifying legitimate and not legitimate signals

Experiment & Implementation

Parametrized simulation to design an effective decoding:

1. Combined data and authentication signals with different power levels based on the peaks as binary waveforms

2. Varied distance (1-50 meters) and SNR (10-30 dB) to represent realistic signal decay over several transmissions

3. Tested decoding of received signals with a simple fixed-threshold based method

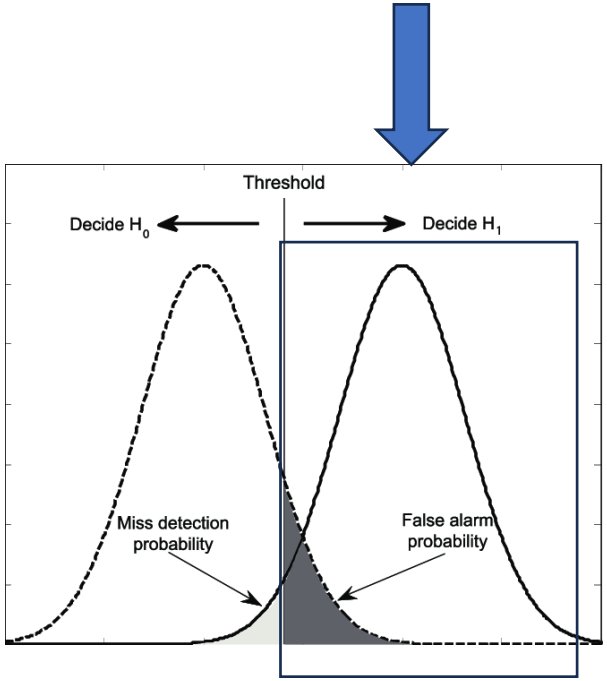
4. Design of an effective decoding based on variable-threshold by observing the collected results from the several transmissions

FA (False Alarm) Study

False Alarm: only *authenticate* messages are sent and check how many of those are interpreted as *wrong* (*false negatives*)

<u>Parametrized</u> simulation to test the transmissions:

1. Varied distance and SNR to test different configurations
2. Set error tolerance on key bits for authentication
3. Counted messages exceeding tolerance as false alarms



Source: https://www.researchgate.net/figure/PDF-of-test-statistics-Miss-detection-and-false-alarm-cannot-be-reduced-simultaneously_fig1_252063675

FA (False Alarm) Study - Results

This simulation reported the following **results**:

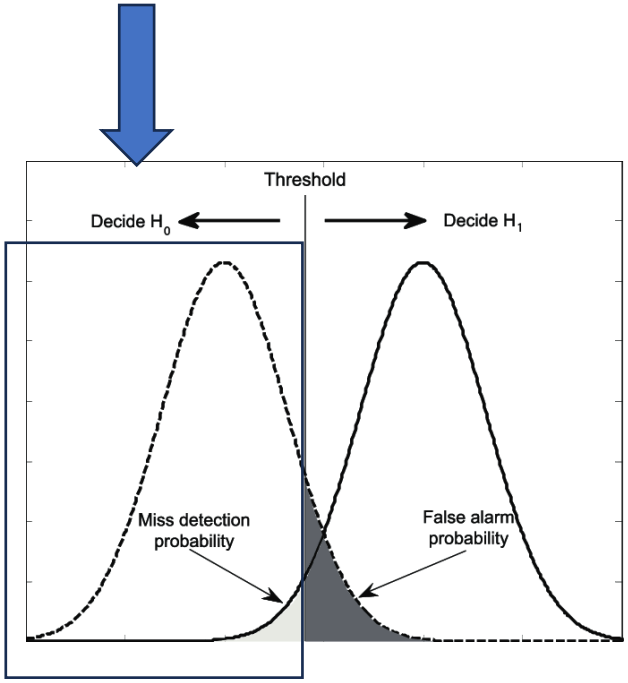
- Observed 0% false alarm rate across all distance-SNR pairs
- Variable decoding algorithm effectively kept key bit errors below the set threshold
- Results validated the effectiveness of the tolerance and the decoding algorithm chosen

MD (Miss Detection) Study

Miss Detection: only *non-authenticate* messages are sent and check how many of those are interpreted as *legitimate* (false positives)

Parametrized simulation to test the transmissions:

1. Varied parameters as previous configurations showed
2. Assumed realistic threat model: attacker having knowledge of channel parameters and structure (MITM scenario)
3. Attacker trying to decode signal based on peaks similarly to legitimate receiver



Source: https://www.researchgate.net/figure/PDF-of-test-statistics-Miss-detection-and-false-alarm-cannot-be-reduced-simultaneously_fig1_252063675

MD (Miss Detection) Study - Results

UNIVERSITÀ DEGLI STUDI DI PADOVA

This simulation reported the following **results**:

- Miss detection rates varies between 20% and 35% across simulations
- Attacker unable to reconstruct messages perfectly due to partial knowledge of transmission powers
- Results confirm the solidity of the decoding methods, able to detect good portions of invalid messages

Conclusions & Future Work

Final considerations:

- Parametrized simulation demonstrates promise for real PLA schemes
- Tested decoding methods proved more effectiveness in variable-threshold decoding methods, minimizing false alarms
- Miss detection rates indicate room for improvement, further refining thresholds and decoding methods

Future development:

- *Noise-based* simulation (additive noise) to improve MD performance
- *Filtering systems* and improved auth techniques