Physical Layer Authentication for Bluetooth Wireless Communications: A Parametrized Simulation Study

Gabriel Rovesti
Department of Mathematics
Università degli Studi di Padova
Padua, Italy - 2103389
gabriel.rovesti@studenti.unipd.it

Michael Amista'
Department of Mathematics
Università degli Studi di Padova
Padua, Italy - 2122865
michael.amista@studenti.unipd.it

***Abstract*— Physical Layer Authentication (PLA) is a promising approach for ensuring secure wireless communications by leveraging the inherent characteristics of the communication channel itself. In this study, we present a case study focused on Bluetooth wireless communications over defined distances ranges, where we investigate the potential of PLA techniques to authenticate legitimate transmissions while distinguishing them from spoofing attacks or non-authentic messages.**

The proposed approach relies solely on channel state information, such as signal power levels, signal-to-noise ratio (SNR), and distance-dependent attenuation, without relying on traditional cryptographic methods. Through a parametrized simulation framework, we analyze the behavior of wireless signals transmitted over a Bluetooth channel under various configurations, including different distances, SNR values, and desired false alarm and miss detection rates to refine the simulation.

By examining the effects of noise and signal degradation on the received signal, we show an efficient encoding/decoding algorithm that adapts authentication thresholds dynamically based on the observed signal characteristics. This threshold adaptation mechanism aims to improve authentication performance across varying transmission ranges by mitigating the impact of signal attenuation and noise.

The study evaluates the trade-off between false alarm rates, representing incorrect classification of authentic transmissions as non legitimate, and miss detection rates, corresponding to the failure to detect non authentic transmissions. Through an iterative process of transmitting authentic and non-authentic signals, decoding them using the current threshold values, and adjusting the thresholds based on the observed rates, we determine suitable threshold values for reliable authentication.

Finally, we discuss the associated challenges and potential future research directions, including the study of artificial noise and man-in-the-middle attacks, incorporation of more complex channel models, integration with higher-layer security protocols, and performance evaluation in real-world scenarios.

***Index terms*—Physical layer authentication, Wireless channel, Bluetooth, Channel state information, False alarm, Miss detection**

I. Introduction

Bluetooth is a wireless channel widely adopted because its simplicity and its low-energy consumption, reaching high data rate even at not so small distances. This has been chosen as a channel to consider a small-scale implementation over real problems which can easily happen when exchanging messages at this level: allow for them to be safe and secure, both considering authentication schemas and error rate over established methods of correction. Considering this kind of transmission is usually decentralized and done with a simple connection over a short range relying on pairing between two devices, authenticating each other and negotiating a secret key, to encrypt the communication channel and ensure the secure channel usage.

Consider for instance the *Man in the Middle*: an adversary can get the incoming message and simply retransmit it. In this way the message is no more authenticated since it has been retransmitted by the adversary, even if the message has not been modified. The simulation overall wants to make the channel aware of its state, adjusting the parameters of communication in order to correct and refine its communication avoiding such kinds of attacks.

Inside our case study, this is a situation which considers an authentication method dependant on the channel state and recognition of legitimacy of transmission.

In particular, the proposed study aims to model the power of the signal based on theoretical considerations. This modeling entails various factors such as the position of the receiver, the transmission power of the transmitter, and the attenuation of the signal over distance. By examining the absolute values of the peaks detected by the receiver, we intend to gauge the signal's strength directly without the influence of additive noise.

To achieve this, we plan to implement and validate a channel model that accurately represents the wireless communication environment. This involves simulating the effects of fading, which refers to the attenuation or weakening of the signal as it propagates through the wireless medium. By conducting tests within Bluetooth's operational range (typically within 150 meters, fixed inside our simulation on 50 to get a realistic maximum range obtained in reality), we aim to assess whether relying solely on channel state.

A. *Related works*

In this field, in recent years, this topic has been more and more studied overtime. Some papers propose surveys and different challenges inside the PLA environment, but none of them discuss about some concrete implementation. Inside of Bluetooth we can quote [1], [2], [3], all discussing the general features and vulnerabilities of Bluetooth per se, specifically more focused over general implementations or Bluetooth Low Energy (BLE). Each one of these sources is more focused on discussing the problem rather than implementing a more concrete solution removing the abstraction of the schema they propose. This is the main reason why this work has been done, in particular to provide an effective mechanism to protect communication among individuals or devices which work in the Bluetooth environment (e.g. reliability in sensors communication).

Anyway, all the related works must be mentioned for the authors' effort in highlighting the different main problems in the Bluetooth communications, simulating the possible attacks and proposing effective countermeasures.

II. Design and Overview of PLA simulation scheme

The main experiment is based on studying the behavior of wireless signals transmitted in a channel with precise configurations for its transmissions (e.g., power, distance, SNR, desired thresholds). The goal is to find an ideal configuration that allows the desired percentage of parameters and configurations to be achieved to make the transmissions in the channel safe. The final result will be very close to the concept of PLA where the goal is to build a secure transmission scheme without using any cryptographic technique but only the properties of the transmission channel (channel state).

Physical Layer Authentication (PLA) methods serve as a promising addition to higher-level encryption authentication. These techniques leverage distinctive physical layer attributes within wireless communication systems, including carrier frequency offset, channel impulse response, radio frequency fingerprint, and received signal strength indicator, to ascertain the legitimacy of the transmitter. The efficacy of spoofing detection is evaluated through two key metrics: false alarm rate and miss detection rate. These metrics are influenced by the test threshold utilized in receiver hypothesis testing and the probabilities of attacks by spoofers. Such analysis can be found in similar works, like [4].

A. *Case study on a Bluetooth channel*

In this study, we consider a Bluetooth wireless communication channel operating within a typical range of 50 meters (here, class 1 Bluetooth specs were taken, considering an ideal power of 20 dB and expected distance of 100 m.; to obtain realistic values, an average range was established here). The primary objective is to leverage the channel state information to authenticate legitimate transmissions while distinguishing them from potential spoofing attacks or non-authentic messages. In the context of Bluetooth communications, which are widely used for short-range wireless data transfer, the implementation of robust authentication mechanisms is crucial to mitigate potential vulnerabilities, such as man-in-the-middle attacks or spoofing attempts.

III. Experiment and Implementation

The simulation setup involves the following key points, describing step by step at a high-level the overall work setting:

- Signal Power: The signal power is characterized by two distinct values for bit '1' and bit '0' considering the square wave signal, denoted diffently for the data signal and the authentication signal, respectively. These values represent the peak amplitudes of the square wave signals used for encoding the data and authentication bits, reflecting the real data over the considered signals.
- Signal-to-Noise Ratio (SNR): The SNR values can range from 0 dB (poor) to 30 dB (excellent), with typical values between 10 dB and 30 dB for wireless systems. The SNR is expected to decrease as the distance between the transmitter and receiver increases due to signal attenuation and propagation losses.
- Distance: A range of distances is considered to analyze the impact of signal attenuation over varying transmission ranges.

- Target False Alarm (FA) and Miss Detection (MD) Rates: Desired intervals for the FA and MD rates, respectively, are specified to evaluate the authentication performance. Such are used to establish communication of only authenticate or non-authenticate messages, then refining the simulation parameters accordingly.
  - The false alarm rate represents the probability of incorrectly classifying a non-authentic transmission as legitimate (false positives), while the miss detection rate corresponds to the probability of failing to detect an authentic transmission (false negatives).
  - Achieving low FA and MD rates is crucial for reliable authentication and preventing unauthorized access or spoofing attacks (hence, retrieving a final plot describing for each simulation parameter a comparison between the two statistics), defining for that a ROC (Receiver Operating Characteristic curve).
  - The values of the FA and MD acceptable rates were studied thoroughly to give realistic ranges of values. Conventionally, they are considered as percentages, so to have an higher MD rate is important to actually evaluate how "bad" the transmission can get; an higher rate of this kind means the channel is behaving worse, giving it's accepting more false messages than authentic ones.

The simulation process consists of repeating the process a defined number of times, setting the simulation with fixed settings. The same signal gets crafted in order to be sent a specified number of times over defined distances and predefined false alarm/miss detection thresholds. More in detail, we can look at the following steps:

- Signal Generation: A data signal and an authentication signal are generated as bit sequences. These signals are then encoded based on their respective power levels to obtain the transmitted signals s1 and s2 and to consider an inital threshold for the signal; this will become useful in deciding if the thresholds will be static or dynamic. The combined signal S (the sum between the two) is transmitted over the wireless channel.
- Channel Simulation and Reception: For each combination of distance and SNR, the transmitted signal is subjected to additive white Gaussian noise (AWGN) to simulate the channel effects. The receiver then decodes the received signal using fixed thresholds to estimate the transmitted bits for both data and authentication signals.
  - In this case, the simulation studies which decoding strategy to use from the receiver point of view when, fixed a specified number of distances, SNR ratios and over the ranges.
  - The threshold initially present are found statically within the same signal which is being sent to destination; the BER analysis will actually help, when retrieving the number of wrong bits, in deciding which kinds of thresholds to use.
- Bit Error Rate (BER) Analysis: The BER is calculated by comparing the estimated bits with the originally transmitted bits. This analysis helps determine the optimal decoding strategy and dynamic threshold adaptation based on the observed BER performance
  - Specifically, the signal should stay "inside" the fixed thresholds and if BER is too high, the fixed thresholds encoding is not optimal, one should switch to the dynamic threshold approach.
  - More in detail, the dynamic threshold adaptation would work as follows: to account for signal attenuation and noise effects, dynamic thresholds (positive/negative) are computed based on the average power levels observed for different bit combinations. These dynamic thresholds are expected to provide a more robust decoding mechanism, potentially improving the BER performance across various distances.
  - Increasing the distances, BER grows, since fading is increasing and the signal moves.
- False Alarm and Miss Detection Analysis: Using the dynamic thresholds, the false alarm rate (FA) and miss detection rate (MD) are evaluated by transmitting authentic and non-authentic signals, respectively. The thresholds are iteratively adjusted until the desired FA and MD intervals are achieved, enabling the determination of suitable threshold values for reliable authentication. This iterative process involves transmitting a large number of authentic and non-authentic signals, decoding them using the current threshold values, and adjusting the thresholds based on the observed FA and MD rates.
  - Specifically, the schema follows the sending of only authenticate signals for the FA analysis, basically considering all the simulation parameters like distance, SNR, target FA intervals desired, creating an already authenticate signals, trasmitting said signal over the channel and checking if the obtained FA interval is within the defined fixed original range. In this case, if the obtained

FA is greater than the original one, the threshold gets increased (very few true messages), otherwise if less thet are too many true messages. This can be found within an interval of false alarm values, to find an ideal average on which to pivot the overall parameters of the simulation.

- The same exact reasoning gets duplicated specularly for the miss detection analysis, crafting a completely wrong signal and doing the exact same thing as before, refining accurately the desired thresholds. Such classification is done iteratively in order to get a desired range on which, even considered the noise effect, the signal can be considered authenticate or not. This strictly depends on the channel parameters, specified each time. The miss detection computation reduces the threshold if it is outside of the range (too many false messages), otherwise increments it (too few).
- It's important to not that when false alarm percentage increases, miss detection decreases. This behavior is expected since the decision thresholds used for authentication directly impact both metrics. While maintaining a low false alarm rate is essential to prevent unauthorized access, it is important to note that the miss detection rate holds slightly more significance in the context of this study. The miss detection rate represents the probability of failing to detect authentic transmissions, which could lead to legitimate messages being discarded or denied access.

IV. Results and Critical Analysis

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut.

V. Conclusions and future work

This study presented a comprehensive analysis of physical layer authentication in Bluetooth wireless communications using a parametrized simulation approach. By leveraging channel state information, such as signal power levels, SNR, and distance-dependent attenuation, we developed an authentication scheme that does not rely on traditional cryptographic methods, demonstrating how the dynamic threshold adaptation in mitigating the effects of noise and signal degradation, leading to improved authentication performance across varying transmission ranges.

A. *Noise-based simulation*

References

[1] J. C. B. J. M. Angela M. Lonzetta Peter Cope and T. Hayajneh, "Security Vulnerabilities in Bluetooth Technology as Used in IoT," *Journal of Sensor and Actuator Networks*, 2018.

[2] C. T. S. D. S. C. Saud Khan Student Member, "Access-based Lightweight Physical Layer Authentication for the Internet of Things Devices," *IEEE Internet of Things Journal*, 2023.

[3] R. D. Y. J. Z. L. Yue Zhang Jian Weng and X. Fu, "Breaking Secure Pairing of Bluetooth Low Energy Using Downgrade Attacks," *Proceedings of the 29th USENIX Security Symposium*, 2020.

[4] Q. G. Y. W. Y. H. Yue Wu Tao Jing, "Game-theoretic physical layer authentication for spoofing detection in internet of things," *Chongqing University of Posts and Telecommunications*, 2021.