A Parametrized Simulation Study for Bluetooth Wireless Channels for Future Implementation in PLA Applications

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 channels 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 interference and signal degradation on the received signal, we show an efficient 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.

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.

This allows for the analysis of a study based purely on channel state information; this ensures the study of the potential of an decoding scheme aiming to refine and study ideal parameters on which to base deterministically the creation of a PLA scheme based on those (then, considering the "randomness" effect given by additive noise only from a theoretical point of view). On this base, many future applications can be based considering the channel state flaws and refining its properties.

Finally, we discuss how many messages are interpreted as legitimate when sent as non-authenticate or how many true messages are found to be wrong, respectively measuring the miss detection and false alarm rate, able to refine dynamically the presented simulation.

***Index terms*—Physical layer authentication, Bluetooth, Channel state information, False alarm, Miss detection, Parametrized simulation, Dynamic thresholding**

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.

In this context, the implementation of a Physical Authentication Layer (PLA) scheme was thought to be useful. The goal of the present simulation is, infact, to be able to parametrize a channel with fixed settings and, relying solely on

channel state information, understand how to pose a future implementation of this kind of scheme, which does not require any kind of cryptography in the middle but, like TCP, is able to understand, looking at how the transmission is going, how many errors are present.

Consider for instance the *Man in the Middle (MITM)*: an adversary can "sniff" the incoming message and simply retransmit it or exploit it for malicious purposes. In this way, the information of the channel has been successfully compromised, so to understand the channel parameters via guessing of its communication, possibly retransmitting the message via replay attacks, disturbing the channel successfully. 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. The MITM effect is analyzed within the context of the present simulation, so to understand the validity of encoding/decoding of the implemented scheme and so to see how much it can be considered valid, determining how many parameters he can have.

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, merely simulating the effect of the signal sending while adding gaussian white noise (AWGN).

Furthermore, we evaluate the trade-off between false alarm rates, which represent the incorrect classification of authentic transmissions as non-legitimate, and miss detection rates, which correspond to the failure to detect non-authentic transmissions. By conducting 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 aim to determine suitable threshold values that strike a balance between security and usability.

The source code of our system is freely available on GitHub here.

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. In this work, a parametrized simulation is implemented based on the theoretical background present in the field to push this kind of research and application even further.

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. Recent advancements highlight a significant reliance of integrity and security of transmitted data. Bluetooth, despite its mechanisms, remains mainly vulnerable from attacks like the MITM scenario. PLA mechanisms offer a promising alternative by integrating security directly into the transmission process, making it resistant to different types of cyber threats. By analyzing the channel's physical characteristics —such as signal strength, noise levels, and propagation delays—PLA can detect discrepancies that indicate tampering or unauthorized access attempts.

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]. The effectiveness of PLA is primarily assessed through two critical metrics: the false alarm rate and the miss detection rate.

These metrics reflect the performance of the authentication system in recognizing legitimate transmissions and identifying spoofing attempts, respectively. The thresholds set for these metrics are crucial, as they determine the sensitivity and specificity of the authentication process.

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.

Through this detailed exploration of PLA in a controlled Bluetooth environment, we aim to demonstrate the feasibility of enhancing traditional security mechanisms with physical layer attributes starting from a schema like this, providing a more robust defense against evolving cybersecurity threats. We hope this findings can possibly encourage the exploration of hybrid security models combining traditional encryption methods with PLA to provide a comprehensive security framework.

III. Experiment and Implementation

The simulation allows to study the behaviour of sending and receiving wireless signals in the Bluetooth domain by means of parametrised transmissions, in order to build a simulative environment for the study of future implementations of PLA schemes with the addition of artificial noise to make the authentication process more effective.

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 within the channel and sent at a series of observed distances each in the range of acceptable interference per distance (SNR - Signal-to-Noise Ratio).

What has actually been implemented is a simple PLA scheme that exploits the physical properties (power, distance and interference) of the transmission channel used to authenticate transmitted messages. The state of the channel itself only influences the conditioning of the simulation parameters, while it is the signal strength that is the most influential parameter, in particular given the chosen signal strength and the waveform that represents a recognizable "fingerprint" between receiver and sender, exploiting the shared knowledge of thresholds and decoding scheme. Within the receiver, the signal is decoded on the basis of fixed and variable power thresholds (thresholds), which allow for a more in-depth analysis at the channel performance level and to understand how to refine the simulation parameters themselves in order to obtain a message as close as possible to the one originally sent. Messages are defined as authentic if, from the decoding result used on the receiver side, an wrong number of bits (compared to the original generated key sequence) are obtained on the key within a certain predetermined limit.

To better explain how the simulation works, this section structure will be composed of different paragraphs, giving the reader a comprehensive overview of the whole experiment.

A. Single Simulation

The single simulation models a wireless communication system using combined data and authentication signals, with the aim of analyzing system performance in terms of *Bit Error Rate (BER)* (the number of bit errors divided by the total number of transferred bits during a studied time interval) for data and authentication signals, as the distance and *signal-to-noise ratio (SNR)* (ratio of signal power to noise power) vary.

Specifically, considering the realistic simulation of Bluetooth distances, messages are sent within a range of 50 meters, create acceptable ranges of SNR ratios over distances (considered on average between 30 and 10), representing a realistic decay of signal of the signal in terms of effective distance. This means that the signal strength decreases as the distance between the transmitter and receiver increases, due to different factors, for example dispersion and losses along the path.

Next, the creation of the two data and authentication signals was set up as a binary waveform, and then a predetermined power value was assigned for each, in order to exactly detect the power "peaks"; specifically, the authentication signal takes on lower power peaks within the signal, so that the two can be analyzed more accurately. This is important during the decoding phase; in fact, a method based on the concordance/discordance of the bits is set in order to correctly vary the given signal and the received authentication.

Based on variable distances and SNR, signal sending and receiving is simulated, to which white noise (AWGN) is applied to simulate the channel effect. In this context, two decoding methods are tested; *fixed-threshold* and *variable-threshold*. The presence of white noise is of interest in adding

realism to the simulation, given the presence of background noise in the channel, potentially carrying additional sources of noise.

Specifically, variable thresholds are set considering four peaks on the signal: *high-high* (maximum value), *low-low* (minimum value) and *intermediate values* (medium-low/ medium-high). These measurements are variable given the waveform of the signal when a *center* parameter is set to allow these peak values to be precisely defined and thus updated (as default, this is set to 0). This measurement refines the intermediate values in particular, considering previous value and current value (from theoretical/predefined values to calculated values). Then comes the *fixed threshold decoding*, given on the basis of the center parameter. At this point, the discordance of the data and authentication bits is defined, so that the received signals consistently reflect two received waveforms when mixed as originally.

If the received signal is greater than/equal to the center parameter, the received signal in its true form is rounded to the maximum threshold of the authentication signal (and the given bit takes on a discordant value); this allows for refinement of signal capture within the thresholds, considering possible theoretical distance ranges. Conversely, if the received signal is less than the center parameter, the real-form received signal is rounded to the minimum threshold of the authentication signal (and the given bit takes on a discordant value).

Once the signals have been received, by means of Hamming distance with the original signals, it is possible to determine the number of wrong bits; this is particularly important when calculating BER thresholds, which are calculated on the entire signal and are useful for calculating false alarms and missed detections. In order to determine the authenticity or otherwise of a certain decoded message, it was deemed necessary to set a maximum number of permitted error bits on the key/authentication signal.

The choice of the number of wrong bits comes from the Hamming distance control; since the single analyzed signal is sent mixed, the presence of a control on the number of bits makes it possible, after repeated simulations, to activate a certain type of decoding rather than another (e.g. if the wrong bits calculated on the statically decoded key exceeds a pre-established threshold then the decoding of the message takes place dynamically; it has been observed that dynamic decoding always lowers the value of the wrong bits on the key, bringing them below the chosen threshold, in this case as an example $3b$). We are within a simulative environment, so the tolerance threshold has been included as a control parameter in order to refine, after a few executions, this threshold to verify the correctness or otherwise of the transmission performed; this is done according to the desired security performance in the first place.

In this case, the authentication signal is part of the high-medium-high or low-medium-low peak, taking the given signal as a reference, thus realizing the discordance in terms of bits. The signal will take on one value when it is in the high-high and medium-low range and another value in the low-medium-high range, ensuring correct decoding of the signal. Also for this decoding, the number of incorrect bits with Hamming distance is checked. BER values are then used in order to calculate the average BER rate, which is useful for the subsequent detections in the other simulation files, thus correctly calculating the FA and MD rates.

B. False Alarm (FA) Study

Inside the false alarm simulation, only *authenticate* messages are sent; this happens mixing the effective signal with the correct key.

The simulation makes it possible to determine and study the level of reliability of the transmission system by identifying the rate of false alarms on authentic messages alone. The study is carried out under different configurations of the transmission system, varying the transmitter-receiver distance ($1 - 50$ meters) and the SNR ratio ($10 - 30$ dB). Binary signals of a predetermined length mixed again with a data packet and a key packet transmitted at different powers, with the power of the key being lower than the transmission power of the data, are considered equally with the rest of the simulation. The methods for generating, merging and sending these signals are the same as those described for the single simulation in Section III.A.

To authenticate a message, an error tolerance is set on the bits of the key to be respected for authentication. Ideally, if the number of wrong bits on the key, calculated between the decoding output and the original key packet, exceeds this tolerance, the message cannot be declared authentic and, for this reason, is counted as a false alarm since, in this context, we are assuming we are only sending authentic messages.

False alarm has been studied over diverse pairs $(\text{distance}, \text{SNR})$, generating for each one N different message transmissions. The FA is calculated as the following ratio:

$$\frac{\text{Apparently non-authentic messages}}{N}$$

The final result observed on the basis of several runs is a FA rate of 0% for all pairs $(\text{distance}, \text{SNR})$. However, this result is not so surprising as the variable decoding algorithm considerably lowers the number of errors on the key bits, obtained by the fixed-threshold algorithm, by always manag-

ing to stay below the set threshold for errors in the key's bits. This result has consolidated the chosen implementation for the dynamic threshold decoding algorithm.

C. Miss Detection (MD) Study

Inside the miss detection simulation, only *non-authentic* messages are sent. To define a message as non-authentic, an error tolerance is set on the bits of the key to be respected for authentication. Ideally, if the number of wrong bits on the key, calculated between the decryption output and the original key packet, exceeds this tolerance, the message cannot be declared authentic.

Binary signals of a predetermined length mixed again with a data packet and a key packet transmitted at different powers, with the power of the key being lower than the transmission power of the data, are considered in the same way as the rest of the simulation. The methods for generating, merging and sending these signals are the same as those described for the single simulation in Section III.A.

In the simulation, we assume for the sake of correct threat modeling, the attacker has knowledge of all the channel parameters and the structure of the message, composed by a key signal and original signal.

Once again, the attacker attempts to decode the signal given the high/low peaks and average levels on the signals, determining the authentication signal to be smaller in amplitude than the data, thus emulating the operation of the decoding in a similar manner to the legitimate one; 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, keeping the logic of bit discordance similar and guaranteeing a square waveform signal very similar to the legitimate one.

In this context, we then have the legitimate receiver, capable of decoding the signal in the same manner as in the first miss detection approach; decoding at fixed thresholds given the setting of the center parameter and activating decoding at variable thresholds once the number of wrong bits allowed on the key has been exceeded, following the logic defined above. In this case, the main interest is in the result of the aforementioned miss detection final rate. 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 (but, being a simulative domain, one is able to 'notice' the misinterpretation of messages, giving useful data to correct the starting parameters of the simulation).

The reason why the attacker cannot reconstruct the message correctly is that he "partially" knows the transmission powers. Specifically, the attacker derives the maximum and minimum power by observing the transmission peaks and two average values (*medium-high*, *medium-low*). The powers he derives, however, are the sum of the transmission power of the key and the data. A major knowledge we assume he possesses is the fact that the superimposed signal consists of a data component and a key component and that it is therefore necessary to derive a power for the data and one for the key. Another constraint we assume is that the key is transmitted at a lower power than the data. The attacker at this point attempts to calculate these powers (with the constraint that their sum cannot exceed the maximum peak value and that the key power must be less than the data).

This way, this shows how the simulation remains solidly capable of detecting wrong messages interpreted as legitimate, ultimately confirming the validity of the detection performed and described in its various approaches.

IV. Results and Critical Analysis

The parametrized simulation study of the proposed PLA scheme for Bluetooth wireless channels yielded several key findings:

- within the *single simulation*, discussed in Section III.A, the channel is modeled as a wireless communication system with combined data and authentication signals enabled analysis of BER. Both fixed-threshold and variable-threshold decoding methods were tested. The variable threshold approach provided more effective decoding and comparing the decoded signals to the original using Hamming distance allowed determination of wrong bits and calculation of BER values. Setting a maximum allowed number of bit errors on the authentication key enabled a starting point for classification of messages as authentic or non-authentic.
- with the *false alarm* study, discussed in Section III.B, only authentic messages were sent over different SNR/distances as parameters. Across multiple simulation runs, a 0% false alarm rate was observed for all tested configurations. This validates the effectiveness of the variable threshold decoding algorithm in keeping key bit errors below the set threshold.
- lastly, with the *miss detection* study, discussed in Section III.C, only non-authentic messages were sent over different SNR/distances as parameters. The attacker's decoding mimicked the legitimate process (relying similarly on estimation of power levels) and was assumed to have partial knowledge of the channel parameters. Constraints were imposed based on observing

transmission peaks and assuming the key signal used lower power than the data signal. Miss detection rates varied between $20 - 35\%$ across simulations. This confirms the approach can detect a significant portion of invalid messages and shows the attacker's inability to reconstruct the message perfectly under realistic constraints.

V. Conclusions and future work

Critically analyzing what was produced inside the single simulation, the proposed parametrized simulation demonstrates adequate promise to be leveraged inside real PLA schemas, detecting spoofing attempts quite well. The use of combined data and authentication signals with differing power levels proves effective in establishing a fingerprint for legitimate transmissions.

The variable threshold decoding strong performance, particularly in minimizing false alarms, highlights its value. However, the miss detection rates indicate room for improvement in reliably identifying all non-authentic messages. Further refinement of the threshold selection and decoding process may help reduce miss detections (indicating sophisticated attackers can partially evade detection, showing how much the knowledge of the channel from the point of view of an attacker may effectively change the results). Future work should expand the simulation to incorporate more diverse channel conditions and explore integration with existing security protocols. Investigating techniques to further reduce miss detections while maintaining low false alarm rates is another priority.

A. Noise-based simulation

Since the implementation of the missed-detection study, discussed in Section III.C, introduced the possibility for an attacker to correctly send messages interpreted by the receiver as authentic ones, it is fundamental to consider further implementation to increase the strength of the above described scheme.

A way to improve the performances of MD rate, making so more challenging for an attacker to compromise the communication reliability, is to introduce an *additive noise* before sending the original message. The aim of the additive noise is to change the shape of the signal making it difficult for an attacker to decode the signal as described above. Obviously this implementation is effective only if there is some secret shared knowledge between the authorized transmitter-receiver. In particular, a receiver can "clean" the signal with the additive noise using a filtering system configurated with shared secret parameters in a way only authorized receivers can obtain the original message, decreasing so the missed-detection rates obtained with the basic implementation.

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.