Impersonation Attack Identification For Secure Communication

Mustafa Harun Yılmaz, Hüseyin Arslan
Department of Electrical Engineering, University of South Florida, Tampa, Florida 33620
Email: myilmaz@mail.usf.edu, arslan@usf.edu

Abstract—Security possesses a significant role in wireless communication. While the studies about secure communication are performed through the upper layers, recent trends shift attention to security in physical layer. In this study, we propose a solution about how to identify the impersonation attacks. If illegitimate transmitter is further away from the receiver when compared to legitimate transmitter, we can detect the spoofing signal by utilizing the hypothesis test which can be carried out depending on the power delay profile of the channel. After setting the hypothesis test, we look at the probability of detection and probability of false alarm of the received signal. It is shown that if the impersonation attack is carried out from further distance, it can be identified with high probability of detection.

Index Terms—Impersonation attack, physical layer security, power delay profile, probability of false alarm, probability of detection.

I. INTRODUCTION

Wireless technology has an important place by providing a mobile connection in a wide range of coverage area at anytime and anywhere. Demand on wireless usage increases with the number of new users and the expectation on higher data rates of current users. Because of its many advantages such as less costly on reaching far places and the installation in terms of physical structure when compared to wire communication, it is preferred in health monitoring, military, public safety, government and service sector such as cellular providers. On the other hand, this increasing demand brings some problems. One of the most important problems is the security. After the signal comes out from the transmitter antenna, it propagates through the air. That signal can easily be captured by any receiver. If two transmitters send the message to the same receiver, both messages would be received and processed. The intention of the second transmitter possesses an importance. If it is to spoof the receiver, i.e. to act as a legitimate transmitter, this might cause a very serious problem in some cases. For instance, in health monitoring systems, this type of signals causes that the wrong report would reach the medical doctor about his patient and he would make a wrong decision unintentionally about that patient. This might result with a fatal error. Therefore, it is very critical to provide security.

In wireless communication, security is handled in upper layers such as in Media Access Control (MAC) or network layer in general. Encryption is the well-known and mostly used technique to provide security. In encryption, the data is encrypted with a key. This process makes the message, called as ciphertext, meaningless. Meaningful data can only be attained by having and using a decryption algorithm. Even though encryption/decryption provides security in wireless communication, it can still be decrypted by illegitimate receivers after an exhaustive process. Therefore, security became important topic for the researchers who work on other layers.

Studies about security on physical layer started with Wyner (1975) who identified the wiretap channel [1]. In his study, Wyner assumed that there is a wire-tapper(eavesdropper) in the environment. His aim is to make the signal meaningless for wire-tapper by doing the channel encoding addition to source encoding. So, when the wire-tapper captures the data, because it will be noisy version of the data received by legitimate receiver, it is not able to decode it.

In general, security on physical layer is investigated under three groups; eavesdropping, jamming and impersonation.

- **Eavesdropping**: When a transmitter sends a message to a receiver, if any other user(s) receives the message illegally, too, this behavior is called eavesdropping. Detecting eavesdroppers is almost impossible with today’s systems. Because of that, studies are carried out with the assumption of eavesdroppers’ existence. The proposed solutions focus on making the message meaningless. So, when an eavesdropper receives the message, he is not able to understand what the message is. In [2] and [3], authors propose a solution by adding an artificial noise to nulls of the transmitted signal. On the other hand, in [4] and [5], authors utilize relays for both to send message to the receiver and to jam the eavesdropper.

- **Jamming**: When a transmitter-receiver pair communicates with each other, a jammer can corrupt the message to make it unreadable at the receiver side. This attack is called jamming. Jamming causes the desired signal to be observed as noise at the receiver. To prevent jamming attacks, Ling et al. consider using frequency hopping spread spectrum (FHSS) technique in [6]. The goal is to change the frequency band continuously. So, the jammer won’t be able to jam the proper band. This provides the communication to be held clearly in between transceiver.

- **Impersonation**: In this case, there are two transmitters who send meaningful message to the receiver; one is legitimate and the other one is illegitimate. Illegitimate transmitter aims at spoofing the receiver by sending both meaningful and wrong information. This type of attack is called impersonation attack. Because the receiver does not know that there is a cheater in the environment,
he takes and processes that message as is. This is a very serious issue in especially military and public safety domain. To overcome this issue, secret key sharing is proposed as a potential solution as in [7] and [8]. Authors make use of the channel between legitimate transmitter and receiver. Because this channel belongs to only this pair, they share the fading channel coefficients to use them as a source of the secret keys. This solution is also used to prevent eavesdropping.

- Groups defined above are to defend the signal against the illegitimate users. Other group can also be considered as to be in attacker position instead of being in defending position, i.e. we will be an eavesdropper, a jammer and a cheater.

In this study, we focus on the impersonation attack. We identify if the signal comes from legitimate or illegitimate transmitter. To achieve this, the power delay profile (PDP) of the received signals is utilized. Whenever the delay profiles of those received signals are different, e.g. one’s maximum excess delay might be larger than the other one, this can be made use of differentiating the desired and undesired signals. Here, PDP is obtained by taking Inverse Fast Fourier Transform (IFFT) of the channel frequency response (CFR) of orthogonal frequency-division multiplexing (OFDM) signal in frequency domain. Also, the channel where the signal passes through is taken as the exponentially decaying which is attained by Erceg et al. in [9]. If those two transmitters are in different distances from the receiver as seen in Fig.1, their delay profiles would be different based on their channel and distance. The decision is given by looking at the probability of false alarm and probability of detection of the received signal.

Remaining of this paper is organized as follows: In Section II, the system model is introduced. Section III comprises numerical results of the proposed approach, and finally, conclusions are drawn in Section IV.

II. SYSTEM MODEL

A. Channel Model

In this study, we use a channel model which shows exponentially decaying characteristics as obtained experimentally in [9]. The exponential component \(^1\) of the delay profile, \(P_{exp}(\tau)\), can be achieved as

\[
P_{exp}(\tau) = (1 - e^{-\alpha}) \sum_{i=0}^{\infty} e^{-i\alpha}, \quad \alpha = \frac{\Delta \tau}{\tau_0}
\]

where \(\tau_0\) is a constant which is achieved from the data, and \(\Delta \tau\) shows the spacing the between discrete terms of the profile.

On the other hand, \(\tau_0\) is

\(^1\)Complete definition of the channel can be obtained from [9].
lag, and the mean of the other user’s PDP is in $c(\tau) + S$, or simply in $S$ lag. Binary hypothesis can be defined as

$$\begin{align*}
\mathcal{H}_0: c(\tau) &= \sigma^2. \\
\mathcal{H}_1: c(\tau) &= S + \sigma^2.
\end{align*}$$

(6)

Probability density function (PDF) of the PDP is

$$
\frac{1}{(2\pi\sigma^2)^{\frac{\tau}{2}}} e^{-\frac{1}{2\sigma^2} \sum_{t=0}^{\tau-1} (c(\tau) - S)^2} \quad > \xi
$$

(7)

where $\xi$ shows the threshold for $\mathcal{P}_{FA}$. After taking the logarithm of the both side, (8) can be obtained as

$$
-\frac{1}{2\sigma^2} \sum_{t=0}^{\tau-1} (2c(\tau)S + S^2) > ln \xi
$$

(8)

$$
\frac{1}{\tau} \sum_{t=0}^{\tau-1} c(\tau) > \frac{\sigma^2 ln \xi}{\tau S} + \frac{S}{2}
$$

(9)

$\frac{\sigma^2 ln \xi}{\tau S} + \frac{S}{2}$ can be assumed to be equal to $\xi'$. The left side of the inequality gives the sample mean. So, the estimate of $\xi'$ is compared to the sample mean. If $\xi'$ is positive and large, then it can be said that the signal is present. Under this condition, the variance would be achieved as $\sigma^2/\tau$. So, $\mathcal{P}_{FA}$ and $\mathcal{P}_{D}$ can be written as

$$\mathcal{P}_{FA} = Q \left( \frac{\xi'}{\sqrt{\sigma^2/\tau}} \right) : \mathcal{H}_0.$$  

(10)

$$\mathcal{P}_{D} = Q \left( \frac{\xi' - S}{\sqrt{\sigma^2/\tau}} \right) : \mathcal{H}_1.$$  

(11)

III. PERFORMANCE EVALUATION

In this section, we derive the performance results in terms of probability of false alarm and probability of detection from equations (10) and (11), respectively. These metrics are important in detection theory when dealing with hypothesis testing. As it is known, there are two hypotheses in binary hypothesis test as seen from Eq.10 and 11.

1) $\mathcal{H}_0$: Null hypothesis
2) $\mathcal{H}_1$: Alternative hypothesis

When an analysis is performed, two types of errors can be made.

1) Type I Error: This error occurs when $\mathcal{H}_1$ is decided, but $\mathcal{H}_0$ is true. It is also called as false alarm.
2) Type II Error: This error occurs when $\mathcal{H}_0$ is decided, but $\mathcal{H}_1$ is true. It is also called as miss detection.

False alarm and miss detection can be explained with another way, too. When a medical doctor tries to diagnose patient’s illness whether there is a tumor or not; if the result is positive, i.e. tumor is diagnosed, but, in fact, there is no tumor, this case (error) is named as false alarm. In contrast, if the result is negative, i.e. no tumor is diagnosed, but, there is a tumor, this error is named as miss detection.

In detection theory, $P(\mathcal{H}_1|\mathcal{H}_0)$ and $P(\mathcal{H}_0|\mathcal{H}_1)$ show the probability of false alarm which is denoted as $\mathcal{P}_{FA}$ and probability of miss detection which is denoted as $\mathcal{P}_{MD}$, respectively. The intention is to minimize $\mathcal{P}_{FA}$. Because, high $\mathcal{P}_{FA}$ can cause vital wrong decision-makings, e.g. a soldier who uses radar signal to determine enemies can assume there is an enemy while there is not, and may want to defend himself unnecessarily. Thus, he can unveil his place. Another intention is to maximize the probability of detection which is denoted as $\mathcal{P}_{D}$. Mathematically, $\mathcal{P}_{D}$ can be formulated as $1 - P(\mathcal{H}_0|\mathcal{H}_1)$.

Fig.2 shows the pictorial representation of $\mathcal{P}_{FA}$ and $\mathcal{P}_{MD}$. These two curves are obtained after taking the IFFT of the received signal for legitimate user who is in 10m and illegitimate user who is in 20m. $\mathcal{P}_{D}$ is the remaining part of the red curve from the area of $\mathcal{P}_{MD}$.

A. PDP of OFDM Signal

As we mentioned above, we consider OFDM signal in this study. After the signal passes through the channel described above, it reaches the receiver with noise. When cyclic prefix (CP) is removed, the received signal can be defined as

$$r_n(t) = \sum_{k=0}^{K-1} x_n(t-k)h_n(k) + w_n(t),$$  

(12)

where $K$ is the number of tap, $h_n(k)$ is the exponentially decaying channel, $w_n(t)$ is the Additive White Gaussian Noise (AWGN) with zero mean and variance of $\sigma^2_w$.

After taking the FFT of $r_n(t)$, the received signal can be obtained in frequency domain as

1277
\[ R_n(m) = \text{FFT}[r_n(t)] = X_n(m)H_n(m) + W_n(m), \]  
(13)
where \( X_n, H_n, W_n \) are the FFT of \( x_n, h_n, w_n \), respectively. When transmitted training symbols are subtracted from the received signal, the CFR can be attained as

\[ \hat{H}_n(m) = \frac{R_n(m)}{X_n(m)} = H_n(m) + W_n(m). \]  
(14)

Autocorrelation of the CFR \( \hat{H}_n(m) \) can be achieved as

\[ C(\Psi) = E_n\{\hat{H}_n(m)\hat{H}_n^*(m + \Psi)\}, \]  
(15)
where \( E_n \) shows the expectation based on \( n \). By taking the IFFT of (15), PDP can be obtained as

\[ c(\tau) = \text{IFFT}\{C(\Psi)\} \]  
(16)

B. Simulation

While distance between legitimate transmitter and receiver is 10m, it is 20m, 40m and 80m for illegitimate transmitter. Table 1 shows system parameters for this study.

<table>
<thead>
<tr>
<th>Simulation Parameters</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modulation Order</td>
<td>QPSK</td>
</tr>
<tr>
<td>Noise Figure</td>
<td>5dB</td>
</tr>
<tr>
<td>Subcarrier Bandwidth</td>
<td>15KHz</td>
</tr>
<tr>
<td>Distance for legitimate transmitter</td>
<td>10m</td>
</tr>
<tr>
<td>Distance for illegitimate transmitter</td>
<td>20m, 40m, 80m</td>
</tr>
<tr>
<td>FFT size</td>
<td>1024</td>
</tr>
</tbody>
</table>

In Fig.3, we obtained the probability of detection of the signal with respect to Signal to Noise Ratio (SNR). We took probability of false alarm constant, i.e. \( 10^{-3} \). This figure indicates that when the distance increases, to detect the signal with a certain \( P_D \) value can be achieved in low SNR values. If \( P_D \) is taken as 0.9, SNR value of the received signal coming from the illegitimate transmitter who is in 80m needs to be at least 3.5dB to be able to be detected by the receiver. On the other hand, it needs to be at least 23dB for the legitimate transmitter. This means that if the received signal which has low SNR value such as 5dB will be considered as the signal which is not transmitted by the legitimate transmitter since the base is the SNR value of the legitimate transmitter. For the same \( P_D \) value, if the illegitimate transmitter is in 40m and 20m, minimum SNR values providing detectability would be 12dB and 16dB, respectively. This shows that if the distance gets closer and closer, it would make more difficult to detect impersonation attacks for the receiver.

We also obtained \( P_D \) by keeping the illegitimate transmitter in 20m and changing the \( P_{FA} \) from \( 10^{-1} \) to \( 10^{-5} \) in Fig.4. When we take \( P_D \) in 0.9 level again, it can be said that the minimum SNR value of the received signal needs to be 14.5dB for \( P_{FA} \) level of \( 10^{-1} \). This limit is necessary to be able to detect the received signal with a certain accuracy. For \( P_{FA} \) levels of \( 10^{-2}, 10^{-3}, 10^{-4} \) and \( 10^{-5} \), the minimum SNR values are 15.7dB, 16.4dB, 17dB and 17.3dB at the same \( P_D \) level. At this point, it should be noted that as mentioned above, we plotted this figure for only one case which is when the illegitimate transmitter is in 20m. It is also apparent that if it is plotted for all cases, the curves would shift to the left or right with respect to the order seen in Fig.3. Fig.4 shows that choosing \( P_{FA} \) level high is better in terms of SNR value, but, it comes with a trade-off which is an increasing Type I Error. As we gave an example over a tumor detection for a patient above, if a tumor is diagnosed even though there is no in reality, the patient will have a very serious surgery unnecessarily. If this surgery is in a very sensitive part of a body such as brain, the patient might pass away. Therefore, it is important to choose the \( P_{FA} \) threshold appropriately. This depends on the application such as for radar application, it is generally chosen between \( 10^{-4} \) and \( 10^{-8} \) [12].

On the other hand, if the receiver chooses the threshold different for each transmitter, it can cause that the illegitimate transmitter would be considered as legitimate transmitter. As seen in Fig.4, when the \( P_{FA} \) level increases, minimum SNR value also increases. This shows that if \( P_{FA} \) is chosen differently for legitimate and illegitimate transmitters such as \( 10^{-5} \) and \( 10^{-1} \) when they are in 10m and 20m, respectively, the decision would be made wrong by the receiver. Because, the receiver is not able to differentiate the signal coming from illegitimate transmitter due to having similar SNR level with legitimate transmitter. Thus, the receiver should keep \( P_{FA} \) level constant for each case.

Fig.5 gives the receiver operating characteristics (ROC), i.e. the probability of false alarm vs. probability of detection with respect to distance of transmitters. \( P_D \) can be defined with
deflection coefficient, $d^2$ [11] as

$$P_D = Q(Q^{-1}(P_{FA}) - \sqrt{d^2}),$$

(17)

where

$$d^2 = \left(\bar{c}_1(\tau) - \bar{c}_0(\tau)\right)^2.$$  

ROC shows the visualization in $P_D$ improvement. If the curve is more bowed up, this indicates that higher $P_D$ can be achieved with small increase in $P_{FA}$. On the contrary, if the increase is high in $P_{FA}$, this means the slope on the curve is small. Therefore, it results with low $P_D$. To be able to obtain an important improvement in $P_D$, high $P_{FA}$ is needed. The disadvantage of this situation was mentioned above. Because we assumed that $\bar{c}(\tau) = 0$ for the legitimate transmitter, i.e. $\bar{c}_0(\tau) = 0$, deflection coefficient will simply be equal to SNR. Since SNR level reduces with the distance, when illegitimate transmitter is in 80m, it would have worse ROC.

IV. CONCLUSION

In this study, we identified the impersonation attacks in wireless communication. We assumed that the legitimate and illegitimate transmitters are in different distance from the receiver. This assumption is applicable, for instance, for health monitoring systems where transceiver pair is in very close in distance while illegitimate transmitter cannot come closer than legitimate transmitter. While the legitimate transmitter is static, illegitimate transmitter’s place was changed to observe the difference in terms of detectability on receiver side. To identify the signals coming from the different users, we looked at their delay profiles. Because PDP of both transmitters are different, we could differentiate undesired signal from desired signal by utilizing from the hypothesis test. The results in this test are described by observing the probability of false alarm and probability of detection of the signals. Our analysis showed that the further the illegitimate transmitter is from the receiver with respect to legitimate transmitter, the better the probability of detection is. On the other hand, selecting the probability of false alarm level has an effect on better detectability of the signal. When it increases, probability of detection also increases on the expense of increasing false alarm rate.

REFERENCES


