RESEARCH ARTICLE

Physical Layer Security based on Spread-Spectrum Watermarking and Jamming Receiver

Simone Soderi‡◇*, Lorenzo Mucchi†, Matti Hämäläinen‡, Alessandro Piva† and Jari Iinatti‡

‡ Centre for Wireless Communications, University of Oulu, Oulu, Finland
◇ Alstom Ferroviaria, Florence, Italy
† Department of Information Engineering, University of Florence, Florence, Italy

ABSTRACT

Wireless communications' infrastructures are frequently selected as a cable replacement in many applications giving an immediate advantage on the wireless investment. However, the worldwide proliferation of wireless local area network (WLAN) imposed large investments on the network security. In the early days of Internet, its layered protocol stack did not consider security as a primary concern. Since then a significant amount of literature has been published. This paper proposes a watermark-based blind physical layer security (WBPLSec) utilizing a jamming receiver in conjunction with the spread spectrum watermarking technique. The outage probability of the secrecy capacity is analytically derived, regardless of the eavesdropper position. The theoretical analysis let us draw a secure region around the legitimate receiver. Results indicate how the WBPLSec aims to be a valuable technique for deploying physical layer security. Authors utilized two performance metrics, the outage probability of secrecy capacity for assessing the secure communication effectiveness and the error probability for evaluating the watermark extraction process. Finally, the proposed protocol improves the secrecy capacity performance if compared to other protocols and moreover it has a lower energy consumption.

*Correspondence

Centre for Wireless Communications, University of Oulu, Oulu, Finland, email: soderi@ieee.org

1. INTRODUCTION

1.1. Related work

Worldwide proliferation of wireless communications imposed the development of the *security engineering* as multidisciplinary field. N owadays, s kills r equired for security range from cryptography and computer science through hardware and embedded systems [1]. Typically, security is implemented through cryptography at upper layers in the open system interconnection (OSI) model. Recently coding for secrecy has been applied and it seems to be a valuable solution for low power sensor networks [2]. On the other hand, in the few past years several techniques based on signal processing have been utilized to secure communications at physical layer and those are promising methods where standalone security solution is needed [2, 3].

Security services included in wireless communications are: authentication, confidentiality, integrity and availability [1]. In this scenario, a set of possible attacks is given as for example [4].

Confidentiality attack: unauthorized interception of private information. This attack damages the privacy leaving intact the confidential data (e.g., eavesdropping and Man in the Middle (MitM)).

Integrity attack: modification of data in transit over the wireless network in order to mislead the receiver or facilitate another attack (e.g., denial of service (DoS), IEEE 802.11 data replay and frame injection).

Authentication attack: stealing of user identifies and credentials in order to gain the access to the network (e.g., WPA (Wi-Fi Protected Access) or WPA2-PSK (Pre-Shared Key) cracking and application log-in theft).

Availability attack: denying legitimate users to access WLAN resources (e.g., Queensland DoS and IEEE 802.11 beacon flood).

The idea proposed in this paper addresses countermeasures against the confidentiality attacks.

With his notable paper, Shannon in 1949 defined the metrics of information theoretic for secrecy systems [5] and he proved the perfect secrecy condition where the eavesdropper cannot pull out any information from the transmitted signal. Afterwards, Wyner introduced the wiretap channel model assuming that a secure

communication can be achieved when the eavesdropper receives a degraded version of the transmitted signal [6]. Wyner defined the *secrecy capacity* as the maximum transmission rate that is achievable whenever the eavesdropper's channel observations are more noisy than the legitimate user's channel [7]. Finally, Csiszár *et al.* extended Wyner's results to non-zero secrecy capacity when a non-degraded wiretap channel is utilized [8]. This model includes a transmitter, i.e. Alice, a legitimate receiver, i.e. Bob and a passive eavesdropper named Eve. Bob and Eve receive Alice's transmissions through independent channels as depicted in Figure 1, where *tr* indicates transmitter-receiver link, *te* is for transmitter-eavesdropper link and *je* is the jammer-eavesdropper link. As shown in Figure 1, we expanded this model introducing a receiver with jammer, whose utilization is explained in the rest of the paper.

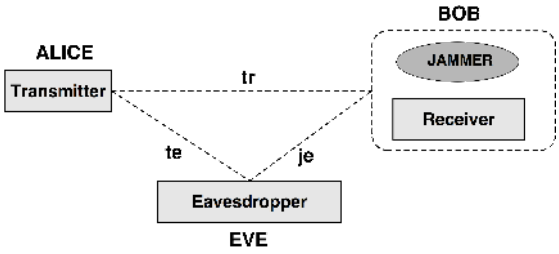

Figure 1. Block diagrams of the proposed protocol to analyse physical layer security

Today, there are two standard practices to secure communications. The first approach adds authentication and encryption to the existing protocols. The second, that is also the approach selected by authors for this paper, embeds security technologies at the physical layer. Bellare *et al.* proposed a new metric scheme that bridges the gap between these two approaches and combines privacy, normally used in cryptography, with error-correction exploited at physical layer [9].

Physical layer security has received recently many theoretical contributions because, due to their nature, wireless communications might suffer eavesdropping attacks. Bloch *et al.* proposed one-way protocol that exploits fading fluctuations and provides secure communication over quasi-static wireless channels [10]. In [11], Ko *et al.* introduced the ultra-wideband (UWB) signaling model to enhance security. Renna *et al.* proposed orthogonal frequency division multiplexing (OFDM) schema between Alice and Bob relaxing conventional assumptions on Eve's receiver structure [12]. Furthermore, other approaches describe how the secrecy capacity performances are improved adding artificial noise to the information [13].

Theoretical results have also shown that the secrecy capacity can be improved exploiting channel variations [14–16]. In literature there are several contributions that deals also with jamming because it can be used to damage wireless communications [17] or exploited as fundamental part in original ideas for security in cooperative networks [18]. Vilela *et al.* described the friendly jamming as a powerful tool to increase the secrecy of wireless systems [19]. Since these schemes are mainly applicable in mobile environment, a channel independent protocol called iJAM was introduced [20]. Let us now describe in more detail the iJAM approach.

1.2. iJAM protocol

The fundamental iJAM operating principle is shown in Figure 2. Alice, i.e. the sender, transmits two times each symbol and Bob, i.e. the receiver, randomly jams complementary samples over the two symbols. In this scheme, only the legitimate receiver knows which samples it jammed. Later, Bob is able to get a clean signal by discarding all corrupted complementary samples in the original signal and its repetition. In contrast, the eavesdropper cannot remove the interference because he does not have any information about the jamming characteristics. In order to make jammed samples indistinguishable, iJAM exploits a basic property of OFDM transmission in combination with jamming signal with Gaussian distribution. On the other hand, iJAM requires phase correction between sender and receiver to work, otherwise symbols are completely undecodable [20].

The major weakness of iJAM is that it implements physical layer security cutting the data-rate by half. Motivated by this observation a new full-rate protocol is proposed.

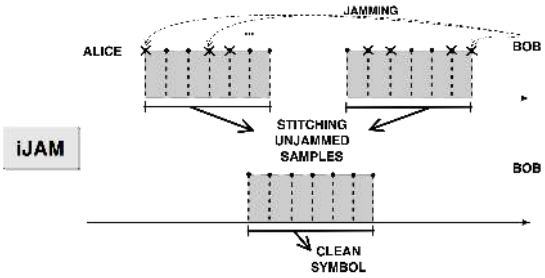

Figure 2. iJAM's operating principle

1.3. Our contribution

The primary goal of this study is to develop a new transceiver architecture to ensure secure communication combining *watermarking* with *jamming receiver*. Two performance metrics are investigated for assessing the system model presented here. The proposed scheme is partially based on iJAM's concept and the paper provides also the information theory analysis for the evaluation of this new approach. First, authors utilize *outage probability of the secrecy capacity* to evaluate the effectiveness of this secure communication. Second, with this architecture part of the information is conveyed by

means of watermarking technique and the *error probability* measures the watermark extraction process.

This paper proposes the watermark-based blind physical layer security (WBPLSec) as a valuable method to secure communication without neither assumptions on eavesdropper's channel nor jamming from third-party nodes. Authors exploit the watermarking concept to increase system performance in terms of outage probability of the secrecy capacity, data-rate and energy cost utilizing one spreading code between Alice and Bob in addition to a jamming receiver. We assume that Alice and Bob have perfect channel side information (CSI) about main and jamming channels, while Eve has CSI on the wiretap channel. In addition, we make no assumption about the eavsedropper's computing power. In other words, even if the adversary would have enough power to recover the watermark information, we will show that it contains only incomplete symbol's samples making that information useless. The WBPLSec protocol is then benchmarked against iJAM protocol.

In the multimedia context the *digital watermarking* process is utilized to hide or embed a desired signal into another signal, e.g. pictures and videos. This process has a lot of similarities with traditional communications. Spread-spectrum (SS) watermarking techniques are frequently utilized to implement physical layer security [21] and we adopt the second paradigm for watermarking described by Cox *et al.* [22], where the information to be embedded is modified prior to insertion, exploiting hidden data.

The truly innovative process for deploying a physical layer security consists of four important parts as follows

1. *Spread-Spectrum watermarking*: the message to be transmitted is first modulated with a spreading sequence and then embedded into the host signal;
2. *Jamming Receiver*: as shown in Figure 1, the jammer is implemented inside the receiver and utilized to jam the Alice's transmission;
3. *Selective jamming*: Bob jams only part of the received signal and knowing which samples are jammed, the receiver is able to rebuild a clean symbol;
4. *Data decomposition method*: the proposed method transmits the information through two independent paths but implementing a data decomposition policy. The information is sent via a narrow-band signal and a spread-spectrum signal. The SS signal implements the watermark. The narrow-band signal is partially jammed by Bob, but the watermark in the SS signal is utilized to re-compose the entire symbol.

The WBPLSec can be successfully applied in those scenarios where mobile devices are equipped with several air interfaces. A definite upward trend in the number of air interfaces for each terminal has defined two possible approaches. At first, multi-modality uses different chip solutions to implement air interfaces diversity. On the other hand, flexible air interfaces implemented via software defined radio (SDR) enables the opportunistic use of spectrum [3, 23]. The multiple air interface device can support the system model presented in Section 2.

Actually, low-power sensors network is an area where physical layer security can provide awesome advantages in terms of number of computations than cryptography [2]. This study shows that the proposed architecture can enhance device's battery life thanks to a better energy consumption compared with iJAM.

Authors propose technique which is acting at the physical layer level, and not in higher layers, like the symmetric encryption protocol does. Basically the goal is to improve the communication system compared to those with crypto-protocols in the same way as any other technique that can fall into the definition of physical-layer security. Physical layer security can be used together with and not in competition with the conventional cryptographic protocols. In our particular case, we aim at improving the iJAM technique, which also requires a shared secret (the symbol repetition code, i.e., in which slot time the symbol is repeated) without paying the cost of reducing the data rate. In order to obtain the goal authors use watermarking technique, known as spread-spectrum watermarking. The PN code in our case is used to decorrelate the host signal with the watermark. As in many wireless systems which use direct sequence spread spectrum (DSSS) code division multiple access (CDMA) as communication technique, e.g. universal mobile telecommunications system (UMTS) and IEEE 802.11x, the code is normally associated to each user.

The rest of this paper is organized as follows: Section 2 describes the WBPLSec system model introducing transmitter and receiver architectures. Section 3 introduces the outage probability the of secrecy capacity of a jamming receiver. Section 4 describes the watermark extraction implemented. Then, in Section 5 an energy cost comparison is presented. Finally, the paper is concluded in Section 6.

2. WBPLSEC SYSTEM MODEL

In this paper, authors address the general problem of physical layer security presented in [10] in which any secure communications shall handle secrecy to avoid confidentiality attacks. The WBPLSec system model is shown in Figure 3, where the jamming receiver together with the watermarking provides secrecy. Actually, the selected watermarking technique provides the needed information destroyed with the jamming.

A modified version of the non-degraded wiretap channel model [8] is used and it includes the so-called *jamming channel* utilized to jam the received signal and also the eavesdropper. The source message $(x_S)^N$ of length N is

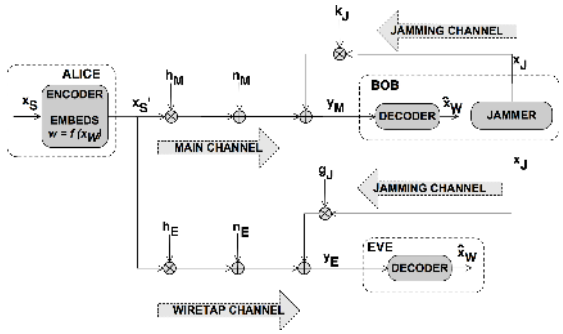

Figure 3. Non-degraded wiretap channel model with jamming receiver

encoded into codeword $(x'_S)^N$ of length N. In particular, the encoder embeds the watermark $(x_W)^{N_W}$ of length N_W into the host signal $(x_S)^N$. The legitimate user, i.e. Alice, transmits $(x'_S)^N$ to Bob through the *main channel*, which in this case, is assumed to be a discrete-time Rayleigh fading channel. The i-th sample of the signal received by Bob is given by

$$y_M(i) = h_M(i)x'_S(i) + k_J(i)x_J(i) + n_M(i), \tag{1}$$

where $h_M(i)$ and $k_J(i)$ represent main channel's and jamming channel's complex Gaussian fading coefficients, $n_M(i)$ is the complex zero-mean Gaussian noise and $x_J(i)$ denotes the jamming signal, which is generated by Bob.

Figure 3 shows how the eavesdropper, i.e. Eve, is capable to observe Alice's transmission over an independent discrete-time Rayleigh channel, i.e. *non-degraded wiretap channel*. The i-th sample of the signal received by Eve is given by

$$y_E(i) = h_E(i)x'_S(i) + g_J(i)x_J(i) + n_E(i), \tag{2}$$

where $h_E(i)$ is the wiretap channel's complex Gaussian fading coefficient between Alice and Eve, $n_E(i)$ is the complex zero-mean Gaussian noise, $g_J(i)$ is the jamming channel complex Gaussian fading coefficient. It is assumed that all channels are quasi-static fading channels, which mean that, the channel gain coefficients remain constant during the transmission of a codeword: $h_M(i) = h_M$, $h_E(i) = h_E$, $k_J(i) = k_J$ and $g_J(i) = g_J$, $\forall i = 1, ..., N$.

2.1. Transmitter

In accordance with the *data decomposition method* proposed in Section 1, Alice conveys the information by means of two independent paths. The information is sent to legitimate user by means of a narrowband signal and on the other hand, Alice also embeds a SS watermark in the host narrowband signal. The watermark conveys part of the information at the legitimate user, i.e. Bob, through a secondary channel.

In accordance with the framework presented by Cox *et al.* [24], transmitter combines the original modulated signal with a SS watermark, with an embedding rule defined as

$$x'_S(i) = x_S(i) + \mu w(i), \tag{3}$$

where $x_S(i)$ is the i-th sample of the amplitude shift keying (ASK) transmitted signal, μ is the scaling parameter and $w(i)$ is SS watermark. Without loss in generality, in the rest of the paper we use the direct sequence spread spectrum for watermarking. On the other hand, the same mechanism developed in WBPLSec can be implemented throughout OFDM. Correspondingly to iJAM, the utilization of OFDM ensure the jammed samples are indistinguishable from the clean samples*.

The host ASK modulated signal x_S can be expressed as

$$x_S(i) = \begin{cases} A_a\sqrt{\dfrac{2}{T_{hs}}} \cdot cos(2\pi f_{hs} i), & \text{for } 0 \le i \le T_{hs}, \\ 0, & \text{elsewhere} \end{cases} \tag{4}$$

where A_a is the amplitude, T_{hs} is the symbol time and f_{hs} is the frequency of the modulated signal.

We propose as proof-of-concept the utilization of DSSS signal for watermarking as

$$w(i) = \sum_{k=-\infty}^{+\infty} \sum_{j=0}^{N_c-1} g(i - kT_b - jT_c)(c_W(i))_j (x_W(i))_k, \tag{5}$$

where $(x_W(i))_k$ is the k-th data bit of the watermark signal. $(c_W(i))_j$ represents the j-th chip of the orthogonal pseudo-noise (PN) sequence. $g(i)$ is the pulse waveform, T_c is the chip length and $T_b = N_c T_c$ is the bit length. The SS watermarking is shown in Figure 4, where c_W represents PN code which spreads the information, i.e. x_W, that has to be inserted in the host signal. With these assumptions the energy of the watermarked signal is given by

$$E'_S = \sum_{i=1}^{N} |x'_S(i)|^2 = \tag{6}$$

$$= \sum_{i=1}^{N} |x_S(i)|^2 + \mu^2 \sum_{i=1}^{N} |w(i)|^2 + 2\mu \sum_{i=1}^{N} |x_S(i)w(i)| =$$

$$= E_S + \mu^2 E_W, \tag{7}$$

where E_S is the energy of x_S signal and E_W is the energy of x_W. It is assumed that the host signal and its watermark in (4) and (5) are uncorrelated.

The signal watermarking is done utilizing the traditional spread spectrum based approach [25]. The main idea implemented in the watermark embedding phase is that the transmitter marks, utilizing SS, the host signal x_S utilizing its first N_W over N samples. Then x_W is given by

$$x_W(i) = \begin{cases} x_S(i), & \text{for } 1 \le i \le N_W, \\ 0, & \text{elsewhere.} \end{cases} \tag{8}$$

*OFDM time samples approximate Gaussian distribution and if jamming signal has same distribution, the overall distribution after jamming does not modify the distribution of an OFDM signal [20].

Alternatively, the receiver can jam N_W discontinuous samples for each symbol but even if this randomness requires a wide-band jammer, e.g, UWB, the work presented in this paper is still valid. With $N_W < N$, the energy of the watermark is given by

$$E_W = \frac{N_W}{N} E_S. \tag{9}$$

Finally, the signal is mixed to carrier frequency f_c and radiated by the antenna. Figure 4 shows the block diagram of the transmitter.

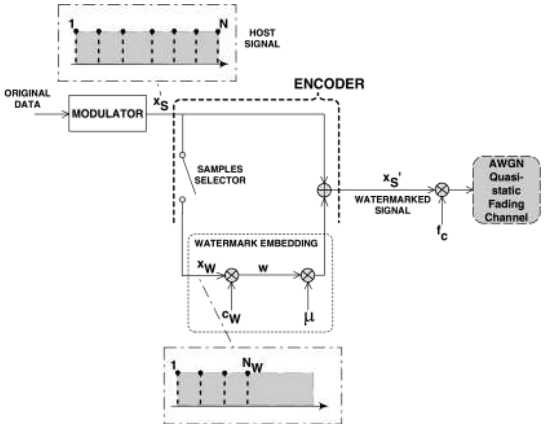

Figure 4. Transmitter structure for watermark-based blind physical layer security

2.2. Jamming receiver

In this paper, authors propose a different strategy to implement the jamming receiver's architecture when compared with iJAM [20]. Indeed, the proposed scheme of receiver works with jammed samples as well as the watermark extraction.

It is assumed that both the jamming signal and the host signal have the same energy over N samples as

$$E_S = \sum_{i=1}^{N} |x_S(i)|^2 = \sum_{i=1}^{N} |x_J(i)|^2. \tag{10}$$

Assuming N samples for symbol, as Bob jams M samples over N with $M < N$ the energy of the jamming signal is given by

$$E_J = \frac{M}{N} E_S. \tag{11}$$

The receiver structure is shown in Figure 5. In the WBPLSec, the legitimate receiver can jams at most $M = N_W$ samples because N_W samples are the information transmitted through SS watermark. The received signal after the antenna is down-converted to the baseband by the carrier frequency f_c and then processed by the original signal demodulator to recover data exchanged through channel. Due to jamming, the signal after the low pass filter (LPF), i.e. $\hat{x}_S$, is corrupted and unusable alone. In order to stitch un-jammed sampled and create a clean symbol, in parallel, the received signal is led to an additional DSSS demodulator used to recover the watermark x_W. Afterwards, as in the iJam protocol [20], the receiver replaces corrupted samples in $\hat{x}_S$ with non-jammed samples that in our solution are taken from $\hat{x}_W$. In the end, the clean symbol x_S is achieved and then demodulated.

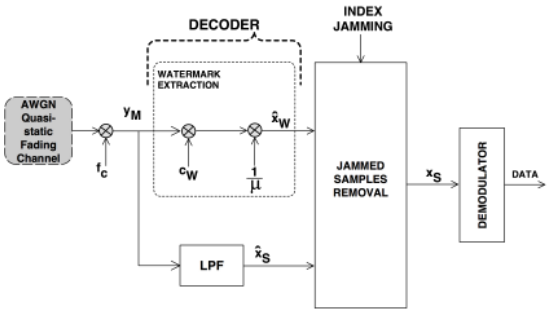

Figure 5. Receiver structure for watermark-based blind physical layer security

2.3. Secrecy metrics

In Section 1.1, authors presented the standard metrics used to measure the secrecy of communications. With reference to the notation used in Figure 3, Shannon defined a system that operates with *perfect secrecy* if the mutual information between the message $(x_S)^N$ and the encoder output $(x'_S)^N$ is zero [5]. This can be expressed as

$$I\Big((x_S)^N; (x'_S)^N\Big) = 0. \tag{12}$$

Together with the introduction of the wiretap channel, Wyner suggested the utilization of the *weak secrecy*, in which the amount of the information leaked about the message $(x_S)^N$ by the eavesdropper when he observes $(y_E)^N$, is asymptotically zero [6], i.e.,

$$\lim_{N\to\infty} \frac{1}{N} I\Big((x_S)^N; (y_E)^N\Big) = 0. \tag{13}$$

Some applications can not accept any information leakage and Maurer *et al.* defined the *strong secrecy* as follows [26]

$$\lim_{N\to\infty} I\Big((x_S)^N; (y_E)^N\Big) = 0. \tag{14}$$

Strong secrecy is hard to design and weak secrecy preserves a practical interest [2]. Authors recall that the secrecy capacity of the legitimate link is defined as the maximum rate that is achievable with strong secrecy [27]. The objective of physical layer security is to implement a reliable secure communication between Alice and Bob, at a target secure rate, leaking the least possible number of bits. Moreover, when the secrecy capacity is equal to zero Alice

can decide not to transmit, thus avoiding to disclosure any information. Reasonably, authors selected the outage probability (P_{out}) to describe the secrecy capacity in the modified wiretap channel model depicted in Figure 3. P_{out} is defined as the probability that the secrecy capacity is less than a target secrecy rate $R_s > 0$ [28].

2.4. Secrecy capacity of WBPLSec

Win *et al.* [29] utilized a general wireless propagation model to characterize network interference in wireless systems. In accordance with that model the received power, i.e. P_{rx}, is $\propto {}^{P_{tx}}/_{d_n^{2b}}$ where P_{tx} denotes the transmitted power, d_n the distance between the two nodes and b is the amplitude loss exponent [30].

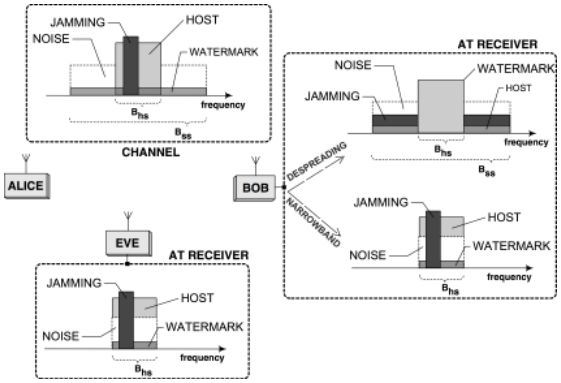

Figure 6. Power spectra densities of proposed blind physical layer security

The power spectra densities of the signals discussed above are illustrated in Figure 6. As shown in Figure 5, the received signal by Bob is split in two arms, the first despreads and extract the watermark. The latter filters the received signal in order to limit the bandwidth before the signal recovery [31]. The ideal LPF rejects a large fraction of the SS watermark and the magnitude of the residual watermark power density is given by

$$E'_W = \frac{B_{hs}}{B_{ss}} E_W = \frac{E_W}{G_p} \tag{15}$$

where $B_{hs} = {}^1/_{T_{sa}}$ is the bandwidth of the host signal, T_{sa} is the host signal symbol length, $B_{ss} = {}^1/_{Tc}$ is the bandwidth of SS signal and $G_p = {}^{T_{sa}}/_{T_c}$ is the processing gain. E'_W interferes with the narrowband demodulator and G_p is defined as the inverse of E_W reduction factor [31].

Therefore, the instantaneous signal-to-interference-plus-noise ratio (SINR) at the legitimate receiver, i.e. γ_M, is given by

$$\gamma_M = \frac{\frac{|h_M|^2 E'_S}{d_{tr}^{2b}}}{N'_0 + |k_J|^2 E_J} = \frac{\alpha \gamma'_{tr}}{1 + \tilde{\alpha} \gamma'_{jr}}, \tag{16}$$

where both $\alpha = |h_M|^2$, $\tilde{\alpha} = |k_J|^2$ follow an exponential distribution, $N'_0 = N_0 + E'_W$, $\gamma'_{tr} = {}^{E'_S}/_{(N'_0 d_{tr}^{2b})}$ and $\gamma'_{jr} = {}^{E_J}/_{N'_0}$. Due to the proposed jamming receiver architecture, the E_J does not undergo any attenuation at the legitimate receiver. Channels are power limited and it is assumed that $P = {}^{E'_S}/_N$ is the average transmit power, $P_J = {}^{E_J}/_M$ is the average jamming power when Bob jams M samples over N with $M < N$. Moreover, it is assumed that n_M and n_E have the same noise spectral density, i.e. N_0.

The instantaneous SINR at eavesdropper, i.e. γ_E, is given by

$$\gamma_E = \frac{\frac{|h_E|^2 E_S}{d_{te}^{2b}}}{N'_0 + \frac{|g_J|^2 E_J}{d_{je}^{2b}}} = \frac{\beta \gamma_{te}}{1 + \tilde{\beta} \gamma_{je}}, \tag{17}$$

where both $\beta = |h_E|^2$ and $\tilde{\beta} = |g_J|^2$ follow an exponential distribution, $N'_0 = N_0 + E'_W$, $\gamma_{te} = {}^{E_S}/_{(N'_0 d_{te}^{2b})}$ and $\gamma_{je} = {}^{E_J}/_{(N'_0 d_{je}^{2b})}$.

When Bob has a better channel realization than Eve, i.e. $\gamma_M > \gamma_E$, the secrecy capacity (C_s) of legitimate link is defined as follows for non-degraded Gaussian wiretap channel [8]

$$C_s = \max\{C_M - C_E, 0\}, \quad \text{where} \tag{18}$$

$$C_M = \frac{1}{2}\log_2(1+\gamma_M) \qquad \text{bit/transmission}$$

$$C_E = \frac{1}{2}\log_2(1+\gamma_E) \qquad \text{bit/transmission}$$

where C_M is the channel capacity from Alice to Bob, i.e. main channel, and C_E is the channel capacity from Alice to Eve, i.e. wiretap channel exploited by the eavesdropper. Otherwise, if Eve has a better SINR than Bob, C_s is set to 0. In (18) author assumed that the noise plus the interference is still Gaussian.

In presence of the Rayleigh channel, the secrecy capacity is conditioned to h_M, h_E, k_J, g_J, and without loss in generality in the rest of the paper we impose $E[h_M^2] = E[h_E^2] = E[k_J^2] = E[g_J^2] = 1$, [32].

The lower bound of the C_s is defined as the secrecy rate (R_s). R_s is given by the difference of the channel capacities from Alice to Bob and from Alice to Eve [6].

2.5. Secrecy capacity of iJAM

In the iJAM, each symbol is transmitted twice. The receiver with jammer, randomly jams complementary samples in the original signal and its repetition. The receiver knows which are the corrupted samples and then, the clean symbol is achieved by stitching together un-jammed samples.

The SINR at the legitimate receiver is given by [32]

$$\gamma_M^{iJAM} = \frac{|h_M|^2 E'_S}{d_{tr}^{2b} N_0} = \alpha \gamma'_{tr}, \tag{19}$$

where in order to facilitate the comparisons between the two protocols it is assumed to transmit the same energy, i.e. E'_S When iJAM is utilized, the γ_E is still given by (17).

Figure 7 shows how in the iJAM the sender repeats its transmission and then halves the data-rate when compared with the WBPLSec proposed in this paper. In particular, iJAM has to transmit twice the same symbol to get a clean signal whereas WBPLSec does not. Authors compared iJAM and WBPLSec assuming the same energy per symbol.

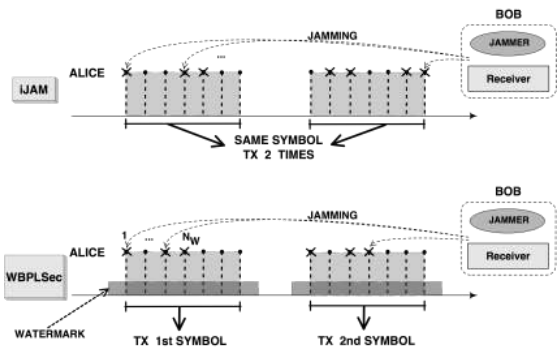

Figure 7. Comparison between iJAM and WBPLSec

In the scenario of the iJAM and assuming that iJAM and WBPLSec have the same bandwidth, the C_s is given by

$$C_s^{iJAM} = \max\{C_M - C_E, 0\}, \quad \text{where} \tag{20}$$

$$C_M = \frac{1}{4}\log_2\left(1+\gamma_M^{iJAM}\right) \quad \text{bit/transmission}$$

$$C_E = \frac{1}{4}\log_2(1+\gamma_E) \quad \text{bit/transmission}$$

As done in (18), the C_s^{iJAM} is conditioned to the Rayleigh channel's coefficients, i.e. h_M, h_E, g_J, and without loss in generality in the rest of the paper we impose $E[h_M^2] = E[h_E^2] = E[g_J^2] = 1$, [32]. In (20) author assumed that the noise plus the interference is still Gaussian.

3. OUTAGE PROBABILITY OF SECRECY CAPACITY OF A JAMMING RECEIVER

The outage probability of the secrecy capacity was defined by Bloch *et al.* [10] as

$$\begin{aligned} P_{out} &= P[C_s < R_s] = \\ &= P\left[\frac{1}{2}\log_2\left(\frac{1+\gamma_M}{1+\gamma_E}\right) < R_s\right] = \\ &= P\left[\alpha < p(1+\tilde{\alpha}\gamma_{jr}) + q\beta\left(\frac{1+\tilde{\alpha}\gamma_{jr}}{1+\tilde{\beta}\gamma_{je}}\right)\right] \end{aligned} \tag{21}$$

where R_s is the target secrecy rate, $p = (2^{4R_s}-1)/\gamma_{tr}$ and $q = (2^{4R_s}\gamma_{te})/\gamma_{tr}$. Therefore, in the case of WBPLSec, the results follow from simple algebra and can be expressed as [19]

$$\begin{aligned} P_{out} =& 1 - \iiint_0^\infty e^{-p(1+\tilde{\alpha}\gamma_{jr})-q\beta\left(\frac{1+\tilde{\alpha}\gamma_{jr}}{1+\tilde{\beta}\gamma_{je}}\right)} \cdot \\ & e^{-\tilde{\alpha}} e^{-\beta} e^{-\tilde{\beta}} d\tilde{\alpha} d\beta d\tilde{\beta} = \\ =& 1 - \frac{1}{(\gamma_{je}\gamma_{jr}p + \gamma_{je} - \gamma_{jr}q)^2} \cdot \\ & e^{-p}\left(-q\Omega\left(\frac{q+1}{\gamma_{je}}\right)(\gamma_{je}(\gamma_{jr}p+\gamma_{jr}+1) - \gamma_{jr}q) - \right. \\ & \Omega\left(\frac{(q+1)(\gamma_{jr}p+1)}{\gamma_{jr}q}\right)\left(\gamma_{je}\gamma_{jr}p - (\gamma_{je}+1)\gamma_{jr}q + \right. \\ & \left.\left. \gamma_{je}\right) + \gamma_{je}(\gamma_{je}\gamma_{jr}p + \gamma_{je} - \gamma_{jr}q)\right), \end{aligned} \tag{22}$$

where $\Omega(x) = e^x E_1(x)$, $E_1 = \int_0^\infty (e^{-t}/t)dt$ is the exponential integral. It is assumed that the fading channels' coefficients are zero-mean complex Gaussian random variables (RVs). The proof that α, $\tilde{\alpha}$, β and $\tilde{\beta}$ are exponential distributed is given in Appendix A.

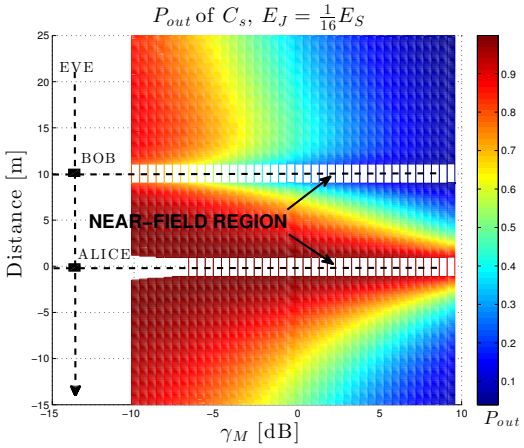

Figure 8. Outage probability versus γ_M when Eve moves from Bob to Alice.

Figure 8 shows the outage probability of the C_s versus γ_M for different Eve's positions. The eavesdropper moves along the line that connects Alice with Bob. The selected wireless propagation model accounts for far-field propagation [29]. We considered the near-field region limit at 1 m around Alice and Bob [32] as shown in Figure 8. With this model Eve cannot be closer than 1 m to both Alice and Bob.

In order to compare the proposed protocol against the iJAM, we computed the P_{out}^{iJAM} as

$$P_{out}^{iJAM} = 1 - \int_0^{\infty}\int e^{\left(-v - k\frac{\beta}{1+\tilde{\beta}\gamma_{je}}\right)} e^{-\beta} e^{-\tilde{\beta}} d\tilde{\beta} d\beta = \\ = 1 - \frac{e^{-v}\left(\gamma_{je} - k\Omega\left(\frac{k+1}{\gamma_{je}}\right)\right)}{\gamma_{je}^2 \gamma_{te}}. \quad (23)$$

Figure 9 shows the comparison between the WBPLSec and the iJAM with equal energy per symbol, i.e. E'_S. Observe that the proposed protocol has better P_{out} than iJAM. On an average, WBPLSec has P_{out} two times better than iJAM, comparing curves in Figure 9 with same E_J. Moreover, the higher is the E_J, the lower is P_{out} that yields to increase the performance of the proposed protocol. The scenario depicted in Figure 9 assumed Eve in the middle between Alice and Bob.

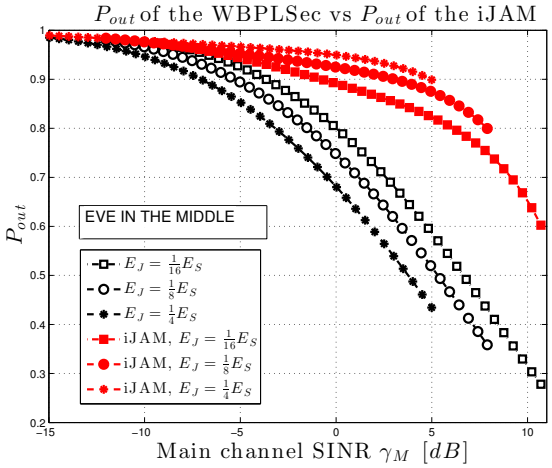

Figure 9. Protocol's comparison of P_{out} versus γ_M for a selected Eve's position.

Due to the jamming strategy implemented in the WBPLSec, Figure 10 shows the effect over P_{out} varying the number of jammed samples. Once more, the Figure depicts also the P_{out} for the same scenario achieved with iJAM, i.e., when $M = N_W = 1024$ samples are jammed, that yields to have $E_J = E_W = {}^{E_S}/_4$. As illustrated in Figure 10, the more jammed samples per symbol exist, i.e. higher E_J, the less is the P_{out}. Thus, controlling the value of E_J the receiver can control the target secrecy level.

3.1. Simulations scenario for secrecy capacity

Table I lists the parameters used for simulations. For each distance of the eavesdropper among the transmitter and the jamming receiver, the C_s was simulated with a different number of jammed samples per symbol. The outage probability of the C_s was calculated transmitting a watermarked signal with 50 dBJ energy. The watermark varies energy from 20 to 40 dBJ and a scaling parameter until 0.9. All the scenarios simulated refer to free-space.

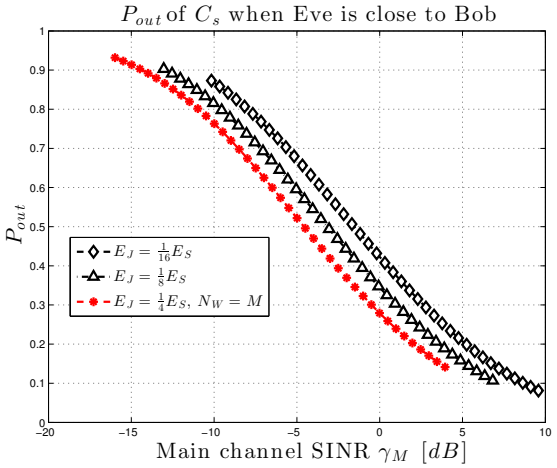

Figure 10. Outage probability of the C_s versus γ_M varying the jamming energy when Eve is close to Bob.

Table I. C_s scenario parameters

Parameter	Value
d_{tr} [m]	10
d_{je} [m]	-15 ÷ 25 [3]
d_{te} [m][1]	25 ÷ -15 [3]
Number of samples (N) per symbol	4096
Number of jammed samples (M) per symbol	256, 512, 1024
Number of samples (N_W) per watermark symbol	1024
E'_S [dBJ]	45
E_W [dBJ]	20 ÷ 40
Watermarking scaling parameter (μ)	0.7, 0.9
DSSS Processing Gain (G_p)	16, 64
AWGN spectral density (N_0) [dBJ]	3, 9
Amplitude path loss exponent (b)	1.0[2]
Secrecy Rate (R_s)	0.1

[1] $d_{te} = d_{tr} - d_{je}$
[2] $b = 1$ for free-space
[3] Placing Alice at the origin of right-handed coordinate systems and Bob at the distance positive axis, when Eve moves also negative values occur.

In Figure 11, a comparison among three different eavesdropper's positions are shown, i.e., 1) Eve is close to Alice; 2) Eve is close to Bob; 3) Eve is in the middle. As illustrated in the Figure, the more there are the jammed samples per symbol, the less is the effect of the eavesdropper position. The WBPLSec creates a *security area* around Alice and Bob. As shown in Figure 12, if Alice and Bob shall implement a secure communication with a secrecy outage probability $P_{out} = 0.3$ and $\gamma_M = 10.6$ dB,

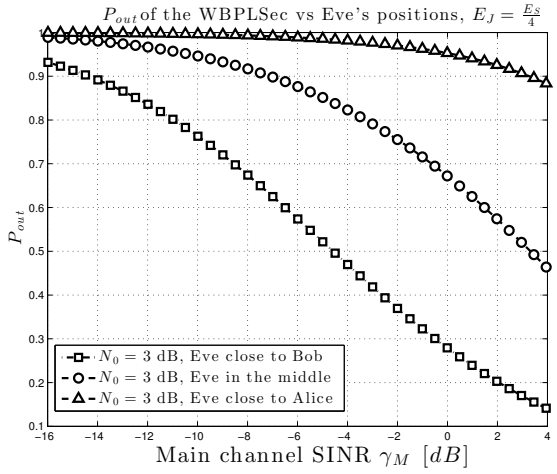

Figure 11. Outage probability versus γ_M for different Eve's positions.

then Eve should not be close to Alice, i.e., the unsecured region is 5 m radius around Alice. Legitimate nodes, i.e. Alice and Bob, might tune E_S and E_J implementing dedicated communication protocol strategies, e.g. three-way handshake, and then derive curves of P_{out} useful to define the needed security area. Furthermore, Figure 12 shows that with a lower γ_M the security area is getting worse because Eve shall move away from Alice to achieve the same P_{out}. In Figure 12, P_{out} is plotted for two different values of γ_M, and for $N_0 = 3$ dB. It can be seen that the effect of increasing the jammed samples leads to a lower P_{out} close to Alice. The Figure also shows the near-field regions around Alice and Bob.

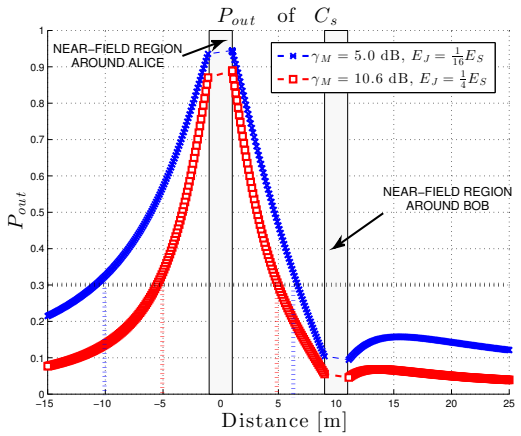

Figure 12. Outage probability versus the distance for fixed values of γ_M.

We have already shown that the secrecy outage probability depends on the eavesdropper position and on the number of jammed samples. In Figure 13 we have plotted P_{out} as function of the ratio E_J/E_W for three different positions of Eve. Reasoning about the increase of E_J up to $E_J = E_W$, the P_{out} is getting worse.

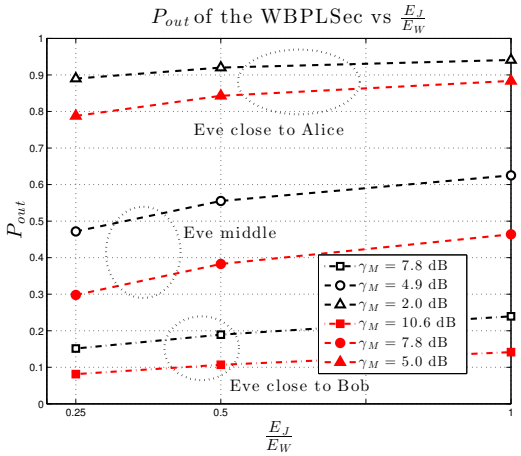

Figure 13. Outage probability as function of E_J/E_W

4. WATERMARK EXTRACTION

Many applications specify the desired error probability, i.e. P_e, and in this section we propose a theoretical analysis for watermark extraction performance. The achieved P_e for a certain ratio of E_J/E_S will give only a lower bound as we assumed AWGN negligible. In (1), the received signal by Bob is perturbed by AWGN and Rayleigh fading. Given the embedding rule showed in (3), the watermark extraction is performed by computing the normalized statistics as [25]

$$\begin{aligned} r \triangleq & \frac{\langle \boldsymbol{y_M}, \boldsymbol{c_W} \rangle}{\langle \boldsymbol{c_W}, \boldsymbol{c_W} \rangle} = \\ = & h_M \langle \boldsymbol{x_S}, \boldsymbol{c_W} \rangle + h_M \cdot \mu \cdot \boldsymbol{x_W} + \\ & k_J \langle \boldsymbol{x_J}, \boldsymbol{c_W} \rangle + \langle \boldsymbol{n_M}, \boldsymbol{c_W} \rangle = \\ = & \boldsymbol{r_S} + \boldsymbol{r_W} + \boldsymbol{r_J} + \boldsymbol{r_n}, \end{aligned} \tag{24}$$

where the inner product definition is $\langle \boldsymbol{u}, \boldsymbol{v} \rangle \triangleq \sum_{i=1}^{N} u(i)v(i)$ and it is assumed $\langle \boldsymbol{c_W}, \boldsymbol{c_W} \rangle = 1$, i.e. PN sequences have unit energy. The first term $\boldsymbol{r_S} = h_M \langle \boldsymbol{x_S}, \boldsymbol{c_W} \rangle$ and the third $\boldsymbol{r_J} = k_J \langle \boldsymbol{x_J}, \boldsymbol{c_W} \rangle$ are residual signals remaining after despreading and low pass filter as showed in Figure 5. $\boldsymbol{r_W} = h_M \cdot \mu \cdot \boldsymbol{x_W}$ is the signal of interest which we want to estimate. Then, $\boldsymbol{r_n} = \langle \boldsymbol{n_M}, \boldsymbol{c_W} \rangle$ is the uncorrelated noise after despreading.

The detector is the same introduced with the traditional spread spectrum watermarking [25] and the estimation of the embedded bit is given by

$$\hat{x}_W = sign(r). \tag{25}$$

Let us consider the case when $x_W = -1$. Then, an error occurs when $r' = r/(h_M \mu) > 0$ and the error probability p is

given by

$$p = Pr\{r' > 0 \mid x_W = -1\} = \\ = Pr\{r_1 + \xi \cdot r_2 - 1 > 0\} \quad (26)$$

where $r_1 = \langle \boldsymbol{x_S}, \boldsymbol{c_W} \rangle / \mu = \sqrt{E_S}/\mu G_p$, $r_2 = k_J/h_M$ is the ratio of two independent Rayleigh RVs and $\xi = \langle \boldsymbol{x_J}, \boldsymbol{c_W} \rangle / \mu = \sqrt{E_J}/\mu G_p$. Furthermore, assuming high SINR values the degradation due to AWGN is neglected. The same error probability can be achieved when $x_W = 1$, therefore the total error probability is given by

$$P_e = 2 \cdot Pr\left\{ r_2 > \frac{1 - r_1}{\sqrt{E_J}/\mu G_p} \right\} = \frac{2}{1 + \left(\frac{\frac{\sqrt{E_S}}{\mu G_p} - 1}{\frac{\sqrt{E_J}}{\mu G_p}} \right)} \quad (27)$$

where the pdf of r_2 is described in Appendix B. Without loss of generality we impose $E[h_M^2] = 1$ and $E[k_J^2] = 1$. The

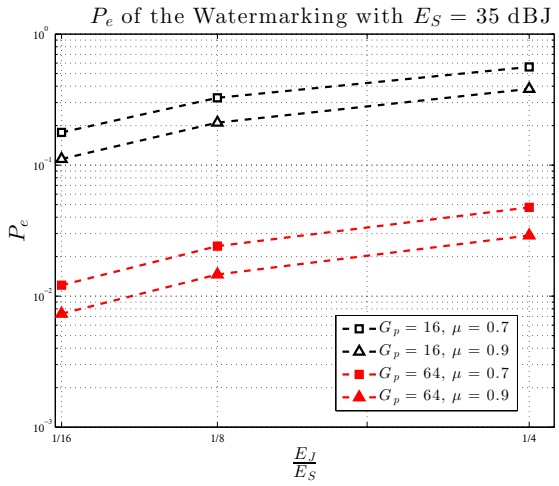

Figure 14. Error probability for watermark signal as function of E_J/E_S.

error probability as a function of the ratio E_J/E_S is given in Figure 14 and the watermark detection is more robust for higher values of G_p and μ. On the contrary to security task described in Section 3, the higher E_J the worse is the extraction of the watermark and thus the reliability task.

5. ENERGY COST

The physical layer security is one of the most promising techniques for low power sensor networks. The avoiding of upper layers' cryptography, makes the physical layer security attractive as standalone security solution that can improve also the battery life because it saves computation when compared to encryption [2].

Table II shows the evaluation of the energy cost when we compared WBPLSec and iJAM. In both scenarios, transmitters and jamming receivers spend energy but in

Table II. Energy cost comparison

		Energy Consum. WBPLSec	Energy Consum. iJAM
Tx ALICE		$E_S\left(1 + \frac{N_W}{N}\right)$	E_S
Tx BOB		$\frac{M}{N}E_S$	$\frac{3}{2}E_S$
TOTAL		$E_S\left(1 + \frac{N_W}{N} + \frac{M}{N}\right)$	$\frac{3}{2}E_S$
TOTAL for M	$M = 256$	$1.3125 \cdot E_S$[1]	$1.5 \cdot E_S$
	$M = 512$	$1.375 \cdot E_S$[1]	
	$M = 1024$	$1.5 \cdot E_S$[1]	

[1] $N_W = 1024$ and $N = 4096$

the WBPLSec's worst case, i.e. when $E_J/E_S = 1/4$ with $M = 1024$, the same system energy is spent. In all other cases, the WBPLSec has a lower energy consumption compared with iJAM.

6. CONCLUSIONS

In this paper, we propose a reliable physical layer solution, WBPLSec, against information disclosure attacks such as eavesdropping. The WBPLSec is trade-off between security and communication reliability because for a fixed symbol energy, E_S, increasing the jamming energy, E_J, a wider security area is achieved with a lower P_{out}. On the other hand, when E_J increases the watermark extraction is getting worse with a higher P_e. Furthermore, the proposed method exploits the non-degraded wiretap channel without any assumption on Eve's position and channel. One spreading code is utilized to implement SS watermarking. The wide utilization of SS communications in these days makes the sharing of one PN code acceptable for this implementation. The WBPLSec shares the same information in terms of spreading code when compared with a SS communication.

In comparison, with the iJAM, the proposed protocol offers the following advantages:

- it is full-rate protocol improving the major weakness of iJAM;
- it has P_{out} two times better than iJAM;
- it has a lower energy consumption.

The iJAM is an interesting protocol but it implements physical layer security with a split to half the data-rate. The proposed scheme is based on iJAM. Both protocols utilize SS techniques and even if authors implements DSSS for WBPLSec, the same concept can be applied using OFDM making jammed samples indistinguishable

from clean samples. The worldwide proliferation of SS communication makes the utilization of a spreading code for physical layer security reasonable for both iJAM and WBPLSec. Actually, the utilization of SS watermarking yields WBPLSec full rate. Furthermore, results show how the proposed protocol is a valuable technique for deploying security creating a secure region around the legitimate receiver.

Both theoretical analysis and simulation results prove the validity of the proposed method that for the first time combines watermarking techniques with a jamming receiver to develop a standalone physical layer security solution. Finally, in the case Alice and Bob would exchange secret keys they shall implement the jamming receiver and then apply the WBPLSec protocol.

REFERENCES

1. Anderson RJ. *Security engineering - a guide to building dependable distributed systems (2. ed.)*. Wiley, 2008.
2. Harrison W, Almeida J, Bloch M, McLaughlin S, Barros J. Coding for Secrecy: An Overview of Error-Control Coding Techniques for Physical-Layer Security. *IEEE Signal Processing Magazine* Sept 2013; **30**(5):41–50, doi:10.1109/MSP.2013.2265141.
3. Soderi S, Dainelli G, Iinatti J, Hamalainen M. Signal fingerprinting in cognitive wireless networks. *2014 9th International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)*, Oulu, 2014; 266–270.
4. List of Wireless Network Attacks. URL `http://www.brighthub.com/computing/smb-security/articles/53949.aspx`.
5. Shannon C. Communication theory of secrecy systems. *The Bell System Technical Journal* Oct 1949; **28**(4):656–715, doi:10.1002/j.1538-7305.1949.tb00928.x.
6. Wyner A. The wire-tap channel. *The Bell System Technical Journal,* Oct 1975; **54**(8):1355–1387, doi:10.1002/j.1538-7305.1975.tb02040.x.
7. Bloch M, Barros J. *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.
8. Csiszar I, Korner J. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory* May 1978; **24**(3):339–348, doi:10.1109/TIT.1978.1055892.
9. Bellare M, Tessaro S, Vardy A. A cryptographic treatment of the wiretap channel. *CoRR* 2012; **1201.2205**. URL `http://arxiv.org/abs/1201.2205`.
10. Bloch M, Barros J, Rodrigues M, McLaughlin S. Wireless information-theoretic security. *IEEE Transactions on Information Theory,* June 2008; **54**(6):2515–2534, doi:10.1109/TIT.2008.921908.
11. Ko M, Goeckel D. Wireless physical-layer security performance of uwb systems. *IEEE Military Communications Conference, MILCOM 2010*, 2010; 2143–2148, doi:10.1109/MILCOM.2010.5680483.
12. Renna F, Laurenti N, Poor H. Physical-Layer Secrecy for OFDM Transmissions Over Fading Channels. *IEEE Transactions on Information Forensics and Security,* Aug 2012; **7**(4):1354–1367, doi:10.1109/TIFS.2012.2195491.
13. Goel S, Negi R. Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications,* June 2008; **7**(6):2180–2189, doi:10.1109/TWC.2008.060848.
14. Mathur S, M N, Ye C, Reznik A. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. *In MobiCom '08*, 2008; 128–139.
15. Jana S, Premnath SN, Clark M, Kasera SK, Patwari N, Krishnamurthy SV. On the effectiveness of secret key extraction from wireless signal strength in real environments. *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking*, MobiCom '09, ACM: New York, NY, USA, 2009; 321–332, doi:10.1145/1614320.1614356. URL `http://doi.acm.org/10.1145/1614320.1614356`.
16. Jeon H, Kim N, Kim M, Lee H, Ha J. Secrecy capacity over correlated ergodic fading channel. *IEEE Military Communications Conference, 2008. MILCOM 2008.*, 2008; 1–7, doi:10.1109/MILCOM.2008.4753256.
17. Spuhler M, Giustiniano D, Lenders V, Wilhelm M, Schmitt J. Detection of reactive jamming in dsss-based wireless communications. *IEEE Transactions on Wireless Communications,* March 2014; **13**(3):1593–1603, doi:10.1109/TWC.2013.013014.131037.
18. Krikidis I, Thompson J, Mclaughlin S. Relay selection for secure cooperative networks with jamming. *IEEE Transactions on Wireless Communications,* October 2009; **8**(10):5003–5011, doi:10.1109/TWC.2009.090323.
19. Vilela J, Bloch M, Barros J, McLaughlin S. Wireless Secrecy Regions With Friendly Jamming. *IEEE Transactions on Information Forensics and Security* June 2011; **6**(2):256–266, doi:10.1109/TIFS.2011.2111370.
20. Gollakota S, Katabi D. Physical layer wireless security made fast and channel independent. *2011 Proceedings IEEE INFOCOM,*, 2011; 1125–1133, doi:10.1109/INFCOM.2011.5934889.
21. Li X, Yu C, Hizlan M, tae Kim W, Park S. Physical layer watermarking of direct sequence spread spectrum signals. *IEEE Military Communications Conference, MILCOM 2013*, 2013; 476–481, doi:10.1109/MILCOM.2013.88.
22. Cox IJ, Miller M, McKellips A. Watermarking as communications with side information. *Proceedings*

of the IEEE Jul 1999; **87**(7):1127–1141, doi:10.1109/5.771068.
23. Fitzek F, Katz M ((eds.)). *Cognitive Wireless Networks: Concepts, Methodologies and Visions Inspiring the Age of Enlightenment of Wireless Communications*. ISBN 978-1-4020-5978-0, Springer, 2007.
24. Cox IJ, Kilian J, Leighton F, Shamoon T. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing* Dec 1997; **6**(12):1673–1687, doi:10.1109/83.650120.
25. Malvar H, Florencio D. Improved spread spectrum: a new modulation technique for robust watermarking. *IEEE Transactions on Signal Processing* Apr 2003; **51**(4):898–905, doi:10.1109/TSP.2003.809385.
26. Maurer U, Wolf S. From weak to strong information-theoretic key agreement. *IEEE International Symposium on Information Theory, 2000. Proceedings.*, 2000; 18, doi:10.1109/ISIT.2000.866308.
27. Leung-Yan-Cheong S, Hellman M. The gaussian wire-tap channel. *IEEE Transactions on Information Theory* Jul 1978; **24**(4):451–456, doi:10.1109/TIT.1978.1055917.
28. Barros J, Rodrigues MRD. Secrecy capacity of wireless channels. *2006 IEEE International Symposium on Information Theory*, 2006; 356–360, doi:10.1109/ISIT.2006.261613.
29. Win M, Pinto P, Shepp L. A Mathematical Theory of Network Interference and Its Applications. *Proceedings of the IEEE* Feb 2009; **97**(2):205–230, doi:10.1109/JPROC.2008.2008764.
30. Goldsmith A. *Wireless Communications*. Cambridge University Press: New York, NY, USA, 2005.
31. Peterson RL, Ziemer RE, Borth DE. *Introduction to Spread Spectrum Communications*. Prentice-Hall: Englewood Cliffs, NJ, 1995.
32. Rabbachin A, Conti A, Win M. Intentional Network Interference for Denial of Wireless Eavesdropping. *2011 IEEE Global Telecommunications Conference (GLOBECOM 2011),*, 2011; 1–6, doi:10.1109/GLOCOM.2011.6134361.
33. Papoulis A. *Probability, Random Variables, and Stochastic Processes*. 3rd edn., MacGraw-Hill, 1991.
34. Shakil M, Ahsanullah M. Record Values of the Ratio of Rayleigh Random Variables. *Pakistan Journal of Statistics* 2011; **27**(3):307–325.

A. EXPONENTIAL DISTRIBUTION

$h = h_I + jh_Q$ denotes the channel complex Gaussian fading coefficients where h_I and h_Q are both Gaussian variables. $|h| = \sqrt{h_I^2 + h_Q^2}$ is RV that follows Rayleigh distribution

$$f_h(h) = \frac{2h}{E[h^2]} e^{-\frac{h^2}{E[h^2]}}, \tag{28}$$

where $|h|$ is RV that follow Rayleigh distribution. The instantaneous SINR is $\propto \alpha = |h|^2$ and in accordance to the fundamental theorem [33] its probability density function is given by

$$f_\alpha(\alpha) = \frac{1}{E[\alpha]} e^{-\frac{\alpha}{E[\alpha]}}, \tag{29}$$

it follows that α is exponentially distributed.

B. PDF OF THE RATIO RAYLEIGH RVS

Suppose h_1 and h_2 are independent RVs that follow Rayleigh distribution. The pdf of the ratio $v = {}^{h_1}/_{h_2}$ is given by [34]

$$f_v(v) = \frac{2E[h_1^2]E[h_2^2] \cdot v}{\left(E[h_2^2]v^2 + E[h_1^2]]\right)^2}. \tag{30}$$