entropy

MDPI

Article

Semantic Security with Practical Transmission Schemes over Fading Wiretap Channels †

Linda Senigagliesi, Marco Baldi * and Franco Chiaraluce

Dipartimento di Ingegneria dell'Informazione (DII), Università Politecnica delle Marche, Ancona 60131, Italy; l.senigagliesi@pm.univpm.it (L.S.); f.chiaraluce@univpm.it (F.C.)

* Correspondence: m.baldi@univpm.it; Tel.: +39-071-2204894

† This paper is an extended version of our paper published in the proceedings of the IEEE Global Conference on Signal and Information Processing (GlobalSIP 2016)—Symposium on Information Theoretic Approaches to Security and Privacy, Greater Washington, DC, USA, 2016; pp. 964–969.

Received: 17 July 2017; Accepted: 9 September 2017; Published: 13 September 2017

Abstract: We propose and assess an on–off protocol for communication over wireless wiretap channels with security at the physical layer. By taking advantage of suitable cryptographic primitives, the protocol we propose allows two legitimate parties to exchange confidential messages with some chosen level of semantic security against passive eavesdroppers, and without needing either pre-shared secret keys or public keys. The proposed method leverages the noisy and fading nature of the channel and exploits coding and all-or-nothing transforms to achieve the desired level of semantic security. We show that the use of fake packets in place of skipped transmissions during low channel quality periods yields significant advantages in terms of time needed to complete transmission of a secret message. Numerical examples are provided considering coding and modulation schemes included in the WiMax standard, thus showing that the proposed approach is feasible even with existing practical devices.

Keywords: all-or-nothing transforms; coding; fading channels; mutual information security; physical layer security; semantic security; wireless channels; wiretap channel

1. Introduction

Designing schemes for secure wireless transmissions is a challenging task in telecommunications [1], even in the case of advanced applications like smart grids [2] and green data transmissions [3]. Two trends are prevalent in this context: using classical cryptographic solutions, and exploiting the emerging paradigm of physical layer security (PLS) [4]. Cryptographic techniques aim to obtain *computational security* [5], which means that the overall security of the system depends on the computational resources available to attackers. In recent years, the technological progress and the growing computing power have made it increasingly difficult for cryptographic techniques to resist new attacks. On the other hand, *information theoretic security* deals with the achievement of *unconditional security*, only based on the intrinsic characteristics of the communication channel in the presence of a wiretapper [6], since different users experience different channel conditions. In this case, the secrecy of a message does not rely on any pre-shared secret, and is also independent of the eavesdropper's computational power. Unfortunately, PLS is still barely used in practical systems, mostly because of the inability to achieve perfect secrecy under realistic assumptions, such as discrete modulations and finite code lengths. Based on the above considerations, a recent trend in research is to combine computational and physical layer security, thus taking advantage of the benefits of both paradigms.

In line with this approach, in [7] we have proposed a protocol based on coding for physical layer security and all-or-nothing transforms (AONTs), the latter being classical computational security solutions. In this paper, we improve and extend such a protocol, by also taking advantage of fictitious

packet transmissions. From now on, for the sake of convenience, we will denote the message sender as Alice, the receiver as Bob and the eavesdropper as Eve. According to our protocol, Alice transmits a codeword only when the channel towards Bob has sufficiently high signal-to-noise ratio (SNR) to allow reliable communication. Conversely, when Bob's channel SNR is below some threshold, Alice sends a fake packet to Bob, i.e., a block of randomly generated bits. In our original proposal of this protocol [7], instead, Alice skips transmission when Bob's channel SNR is insufficient for reliability, waiting some time before attempting transmission again. As often occurs in PLS, this protocol relies on the assumption that Alice's and Bob's channel estimates are consistent, i.e., that the SNR value resulting from their measurements is the same. This issue was not faced in [7], whereas in this paper we introduce a suitable reconciliation mechanism of their SNR estimates. With respect to [7], where only Rayleigh fading channels were considered, we also extend the analysis to the more general case of channels affected by *Nakagami-m* fading.

Our aim is to propose a protocol that is feasible in practice, possibly exploiting low cost devices. Therefore, we focus on state-of-the-art coding and modulation schemes which are included in standards for wireless communications, and already implemented in commercial transceivers, such that existing hardware and software can easily be reused. Moreover, we consider short codes and high order modulation schemes, like quadrature amplitude modulation (QAM), which are desirable to cope with the channel variability. In fact, we consider channels subject to fading effects in order to model practical wireless transmissions. Unlike classical approaches to PLS, where asymptotic conditions like infinite block length and continuous modulations are assumed, we need security metrics working in the finite block length and discrete modulation regime. For this reason, the metric we use to estimate the PLS levels is the wiretapper's total equivocation about the message. The concept of equivocation is related to that of *partial secrecy* [8]. In fact, measuring the wiretapper's total equivocation allows us to obtain a lower bound on the size of a list to which the eavesdropper can reliably limit the message. Obviously, Eve's total equivocation depends on Eve's channel mutual information. As in our analysis we do not make any assumption on the message distribution and consider the maximum of Eve's channel mutual information over all possible distributions, the security notion we use for PLS is *mutual information security* (MIS) according to [9]. In [10], we have proposed some tools to study the levels of MIS achievable by practical transmission schemes over Rayleigh fading channels. In this paper, we start from those tools and extend them to the more general case of channels with Nakagami-*m* fading. Then, the estimated level of MIS is used as a substrate for our protocol to achieve some level of *semantic security* (SS) through cryptographic tools like AONTs.

In fact, if we only resort to PLS stemming from the communication channel and measured through MIS, it is still possible for Eve to discover some part of the message with less attempts than those estimated through her total equivocation. To avoid this, we propose to pre-process the secret data through an AONT prior to transmission. AONTs are obtained through algorithms based on cryptographic primitives [11] and therefore achieve some level of computational security. Using an AONT to transform the secret data prior to transmission prevents Eve from gathering any information on each secret message with less attempts than those required to recover the full message, as measured by MIS. Therefore, when AONTs are used, we achieve SS [12]. More recently, SS has also been considered as a metric in the PLS scenario, and it has been shown that MIS and SS are asymptotically equivalent [9]. The chance of achieving SS through PLS techniques in the finite block length regime has been discussed in the literature for the binary erasure wiretap channel [13], but its extension to wireless wiretap channels with fading is still an open issue [14]. In this paper, we propose an approach to achieve SS by using coding and AONTs over additive white Gaussian noise (AWGN) channels affected by Nakagami-*m* fading in the finite length regime and in practical conditions.

1.1. Related Work

Many previous works have been devoted to the study of PLS over fading wiretap channels (see, for example, [15–18] and references therein). However, they are mostly focused on asymptotic secrecy

targets and consider ideal conditions (like capacity achieving codes and continuous modulations). Moreover, suitably designed coding schemes for the wiretap channel are commonly considered [13], while our aim is to exploit classical coding schemes to achieve some level of PLS in practical conditions.

Some literature also exists on protocols in which the transmission of each packet depends on the occurrence of a certain channel condition, known as *on–off schemes*. Examples can be found in some recent papers [19–21]. The use of fake packets has already been introduced in [22], where the author considers the deliberate transmission of random message blocks when Bob's channel quality is poor. The use of dummy messages has also been considered in previous works concerning hybrid automatic repeat request (HARQ) protocols for secure transmissions [23,24]. All these approaches, however, consider asymptotic notions of secrecy (like the secrecy capacity, the secrecy throughput or the ergodic secrecy rate) with an underlying notion of weak secrecy, and do not take into account either practical constraints or SS as a metric. Moreover, they focus on optimal codes specifically designed for the wiretap channel and do not consider practical modulation formats, thus being still far from practical applications. On the contrary, our goal is to propose and assess an on–off scheme able to provide some level of SS at the physical layer by exploiting practical and simple coding and modulation schemes.

The paper is organized as follows. In Section 2 we describe the system model and the protocol we propose. In Section 3 we show how to assess security and design the protocol parameters in order to achieve some desired level of SS. In Section 4 we provide some examples considering standard codes and fixed security levels. In Section 5 we provide some conclusive remarks.

2. System Model and Protocol Description

As mentioned above, in the model we consider, a legitimate sender (Alice) wishes to transmit some secret data to a legitimate receiver (Bob) over a fading wireless channel in the presence of a passive eavesdropper (Eve). The protocol we propose to achieve this target under reliability (towards Bob) and security (against Eve) constraints exploits a special processing of the message prior to transmissions that relies on three main functions: encryption (with padding), slicing and encoding. Then, transmission is performed according to an *on–off transmission* (OOT) scheme based on channel quality estimates. All of these elements of the protocol are described next.

2.1. Encryption

Let us denote as M the private data that Alice wishes to securely transmit to Bob. First of all, she transforms M into X through an AONT. The concept of AONT was introduced by Rivest in [11] and can be seen as a random-like transformation that is infeasible to invert, even partially, unless the transformed data is completely available. Therefore, an AONT-processed message cannot be recovered, even in part, if some part of it is missing. In the original proposal [11], the message is divided in blocks of fixed length and a random encryption key is generated and used to encrypt each block through some symmetric block cipher. The random key is necessary to feed the symmetric cipher, but it does not represent a secret to be shared between legitimate users. Then, a cryptographic hash function is used to compute the digests of all blocks, that are XORed together and with the random key. This way, a last block is obtained that is appended to the transformed message. Therefore, the AONT can be easily inverted (by inverting the above procedure) by anyone retrieving the entire amount of transformed data, without the need of any prior knowledge of the random key (since it is embedded with the transformed data). The procedures of AONT encryption and decryption are schematically described in Figure 1. This first implementation of an AONT relies on cryptographic primitives, and hence follows a computational security paradigm. However, it has been shown in [25] that it is also possible to define AONTs with unconditional security.

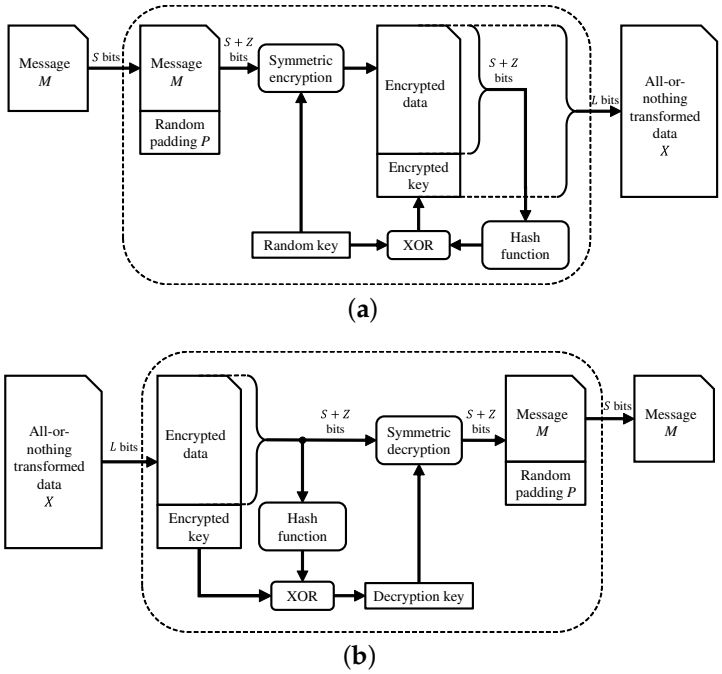

Figure 1. Block diagram of: (**a**) AONT encryption and (**b**) AONT decryption of a secret message M.

Coherent with the figure, let us denote the length of M in bits as S and the length of X in bits as L. Before application of the AONT, the message M is concatenated with a random padding string P having length $Z \geq 0$, i.e., $X = \text{AONT}([M|P])$, where $|$ denotes concatenation. We have $L \geq S + Z$ and the value of Z is chosen such that L is a multiple of an integer k coincident with the dimension of the binary linear block code $C_1(n,k)$ used in the encoding step (see Section 2.3).

2.2. Slicing

As shown in Figure 2a, X is split into N blocks which are then separately encoded. Each block is called slice and is k bits long. The length k coincides with the dimension of the linear block code $C_1(n,k)$ used in the subsequent encoding phase, and the number of slices is $N = L/k$. As also shown in Figure 2a, we denote the i-th block as x_i, $i = 1, 2, 3, \ldots, N$.

2.3. Encoding

Each block is encoded through $C_1(n,k)$, where n denotes the code length and k is the code dimension. This way, Alice obtains a set of n-bit codewords c_i, $i = 1, 2, 3, \ldots, N$, which are then modulated and serially transmitted to Bob over the wireless channel.

When these codewords are received, they are decoded into x_i, $i = 1, 2, 3, \ldots, N$, through the decoder of $C_1(n,k)$. This way, X can be recovered and the AONT can be inverted. Then, the random padding P is discarded and the secret message M is re-obtained. The whole procedure for transforming a secret message M into a set of n-bit codewords c_i, $i = 1, 2, 3, \ldots, N$, to be transmitted through an ideal error-free channel using the proposed protocol and its inverse is schematically depicted in Figure 2.

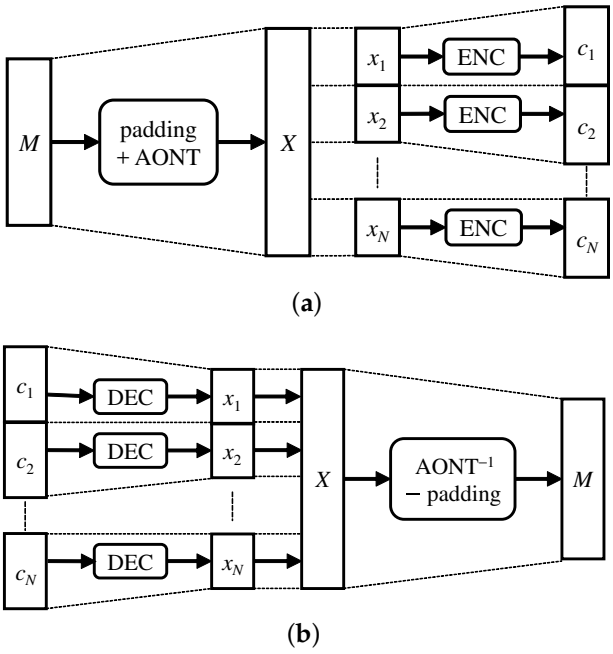

Figure 2. Block diagram of: (**a**) the procedure for transforming a secret message M into a set of n-bit codewords c_i, $i = 1, 2, 3, \ldots, N$, to be transmitted and (**b**) its inverse.

2.4. Transmission

The OOT transmission scheme we consider works as follows. Transmission is synchronous, i.e., organized in time slots, each slot having the duration of n bits. This coincides with the length of a codeword c_i, $i = 1, 2, 3, \ldots, N$. Each transmission starts at the beginning of a time slot and lasts for n bits or less. Before transmitting any data packet, the following preliminary steps are performed:

1. Alice sends a request to send (RTS) message to Bob containing some known string.
2. Based on the received string, Bob estimates the channel SNR, noted as γ_{AB}.
3. Bob sends γ_{AB} to Alice after syndrome encoding through a second binary linear block code $C_2(f, b)$, as explained next. The length of the syndrome is $z = f - b$. Bob's reply is protected through a third, ultra-reliable binary linear block code $C_3(n, z)$ such that all channel errors can be corrected with very high probability. This can be achieved by designing the system parameters in such a way that the rate of $C_3(n, z)$ is much smaller than the rate of $C_1(n, k)$, that is, $z \ll k$.
4. Alice decodes Bob's message through the decoder of $C_3(n, z)$ and recovers its original content, that is, the syndrome of γ_{AB}.
5. By comparing the decoded data with the received signal, Alice estimates the channel SNR, noted as γ_{BA}.
6. Alice reconciliates her estimate (γ_{BA}) with that of Bob (γ_{AB}) by exploiting the procedure explained next.

The aim of the reconciliation phase is to allow γ_{BA} to converge to γ_{AB}, i.e., allow Alice to obtain the same information of Bob as regards the channel SNR. Noting by γ_B this common value, if $\gamma_B \geq \gamma_B^*$, where γ_B^* is a prefixed threshold, Alice will then transmit a codeword c_i containing valid data. Otherwise, Alice will transmit a fake packet, which is recognized as such by Bob and hence discarded. The aim of the fake packet transmission is to confuse Eve. The entire procedure is summarized in Figure 3. In the following, this protocol will be named *on–off transmission with fake packets* (OOT-FP).

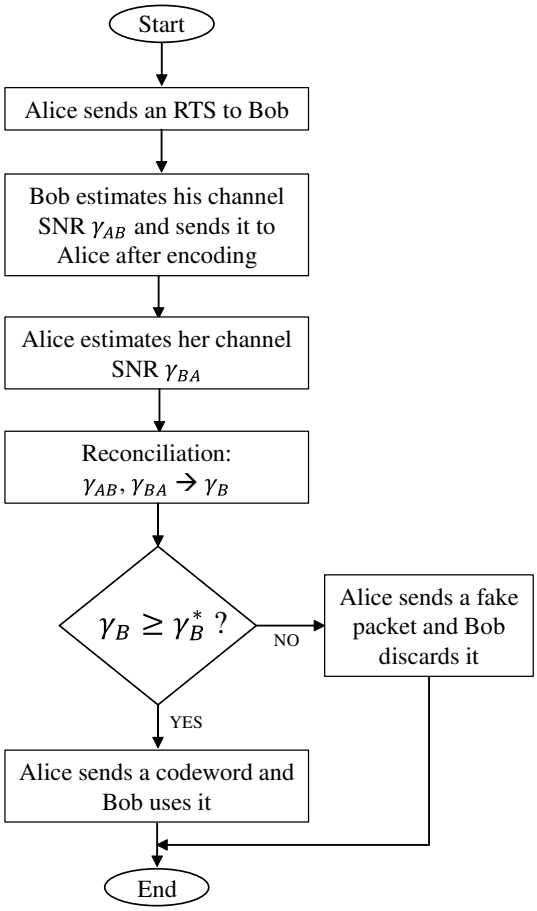

Figure 3. Flow chart of the transmission of a packet according to the OOT-FP protocol.

2.5. Reconciliation

As mentioned above, the main purpose of the reconciliation phase is to find a common estimate of the channel SNR, in order to allow both Alice and Bob to verify if this value overcomes the threshold γ_B^* or not. For this purpose, let us suppose that Alice represents γ_{BA} with a $[1 \times f]$ binary string s_A. Similarly, Bob represents γ_{AB} with a $[1 \times f]$ binary string s_B. Since, in general, $\gamma_{AB} \neq \gamma_{BA}$ the same will be for the two binary strings, i.e., $s_B \neq s_A$. The binary representation used by Alice and Bob, that can be the result of a quantization followed by a suitable mapping, must be chosen such that the following requirements are fulfilled:

- s_A and s_B must be two dense binary vectors, that is, their Hamming weights $w_H(s_A)$ and $w_H(s_B)$ must be on the order of $f/2$.
- Noted by e the binary sum of s_A and s_B (that is, $e = s_A \oplus s_B$, where $\oplus$ denotes the XOR operation), with a very high probability, it must be $w_H(e) \leq t \ll f$, being t a parameter chosen in advance. In other terms, the binary representation used for the SNR values must be chosen in such a way that small differences between γ_{AB} and γ_{BA} translate into low-weight difference vectors between s_A and s_B. Practical binary representations with this feature can be easily devised.

The reconciliation phase exploits the binary linear block code $C_2(f, b)$ having length f and rate b/f, able to correct t errors or less. Contrary to $C_1(n, k)$, that uses soft-decision decoding, $C_2(f, b)$ exploits hard-decision syndrome decoding. As an example, a classical Bose–Chaudhuri–Hocquenghem (BCH) code provided with Berlekamp–Massey hard-decision decoding [26] can be used as C_2. Its $z \times f$ parity-check matrix is denoted by H in the following. A detailed description of the operations

performed during the reconciliation phase is provided next. After having estimated γ_{AB} and converted it into the binary string s_B, Bob computes the syndrome h_B, which is a $1 \times z$ vector obtained as

$$h_B^T = H \cdot s_B^T, \tag{1}$$

where $\cdot$ denotes the matrix-vector multiplication and T denotes transposition. Bob then encodes h_B through the ultra-reliable low-rate binary linear block code $C_3(n, z)$ mentioned above and sends it to Alice. This ultra-reliable code should allow Alice to correct all transmission errors through decoding. The rare cases in which this does not occur are commented next. When Alice receives h_B without errors, she computes

$$h^T = h_B^T \oplus H \cdot s_A^T = H \cdot s_B^T \oplus H \cdot s_A^T = H \cdot (s_A \oplus s_B)^T = H \cdot e^T. \tag{2}$$

Since $w_H(e) \leq t$, Alice is able to recover e from h through syndrome decoding of $C_2(f, b)$. Finally, by knowing e, Alice can easily compute

$$s_B = s_A \oplus e. \tag{3}$$

At this point, both Alice and Bob know the same SNR value $\gamma_B = \gamma_{AB}$ and, by comparing it with γ_B^*, they can consistently decide whether the packet must be an information packet (if $\gamma_B \geq \gamma_B^*$) or a fake packet (if $\gamma_B < \gamma_B^*$). In the rare cases in which Alice is unable to correct all errors on h_B, she obtains $\tilde{h}_B \neq h_B$ and computes

$$\tilde{h}^T = \tilde{h}_B^T \oplus H \cdot s_A^T = H \cdot \tilde{s}_B^T \oplus H \cdot s_A^T = H \cdot (s_A \oplus \tilde{s}_B)^T = H \cdot \tilde{e}^T. \tag{4}$$

For the properties of syndromes, $\tilde{s}_B$ is generally significantly different from s_B. Therefore, $\tilde{e}$ has a large weight, yielding a failure in syndrome decoding that is detected by Alice. Hence, Alice becomes aware of the failure and can restart the procedure. Being a rare event, for the sake of simplicity, this fact will be not considered in the following.

Concerning Eve, after receiving Alice's RTS through her channel, she estimates a value γ_{AE} of the SNR of her channel, and represents it through a $1 \times f$ vector s_E, which, however, is different from s_B. Thus, even if we assume that Eve (who can use the same decoders of the legitimate users) can correctly recover the syndrome h_B transmitted by Bob:

- She cannot recover s_B since $w_H(s_B)$ largely exceeds the correction capability of $C_2(f, b)$ under hard-decision syndrome decoding. On the other hand, the values of the parameters are such to prevent that Eve successfully decodes s_B even with more powerful soft-decision decoders. Moreover, soft-decision decoding is practically infeasible for several families of classical codes (like BCH codes) unless their length is very short.
- She could try to exploit (2) with s_E in place of s_A, but we suppose that her channel is independent of Bob's one and different enough, so that $w_H(s_E \oplus s_B) = w_H(e') > t$, such that syndrome decoding does not permit Eve to recover e' from $h_B^T \oplus H \cdot s_E^T$. The meaning and applicability of this assumption will be further discussed in Section 2.6.

Therefore, Eve is not able to discover γ_B and, consequently, she has no information to decide whether the packet flowing from Alice to Bob after reconciliation is an information packet or a fake packet.

In order to measure the advantage coming from the use of fake packets, in the following we will compare the performance of the OOT-FP protocol with that of a basic version of it without fake packets, simply denoted as OOT. As in the OOT-FP protocol, in OOT Alice and Bob perform the initial estimate and reconciliation phases. After reconciliation, Alice compares γ_B with γ_B^* and, when $\gamma_B < \gamma_B^*$, instead of sending a fake packet, she simply skips transmission and restarts the procedure at the next time slot. Indeed, we have introduced a slightly different version of this protocol in [7], where fake packets are not considered and the possible mismatch between Alice and Bob estimates of the

SNR is faced through a different approach. In fact, in the protocol in [7], Bob still estimates $\gamma_B = \gamma_{AB}$ and compares it with the threshold γ_B^*. However, differently from the setting we consider in this paper, Bob sends to Alice a clear to send (CTS) message if $\gamma_B \geq \gamma_B^*$, or a not available (NA) message otherwise. Therefore, Alice decides whether to transmit a codeword or to skip transmission based on Bob's reply. This has the advantage of reducing complexity by avoiding computations needed for reconciliation of Alice's and Bob's estimates of the SNR. On the other hand, the broadcast transmission of CTS packets provides Eve with a clear indication of which time slots Alice is going to use to transmit valid codewords.

As a performance metric, in the following we use the number of time slots needed to transmit a message M with a given security level. In this respect, ignoring the processing times required at Bob's and Alice's premises (this is a reasonable assumption, since the processors' speed is usually orders of magnitude greater than the transmitters' speed), the protocol in [7] is perfectly equivalent to the OOT protocol described above. In fact, in both protocols, three time slots per packet are needed, the difference being in the fact that the second time slot is filled with a CTS/NA packet according to [7] or with SNR estimation/reconciliation data according to the OOT protocol we consider. Therefore, in the following analysis, performance results denoted as OOT may be equally referred to both protocols. We then compare the performances of OOT and OOT-FP protocols, showing that the introduction of fake packets yields significant improvements in performance.

2.6. Applicability of the Protocol

From the description given in Section 2.4, it immediately follows that the feasibility of the proposed protocol is conditioned on the following hypotheses:

1. Eve's channel SNR is significantly different from that of the main channel between Alice and Bob, so that its binary representation is also significantly different.
2. The main channel between Alice and Bob remains stationary during the execution of the steps required by the protocol for transmitting each packet (this means we are considering *slow fading).*

Concerning Hypothesis 1, we can rely on it because we assume that the main and eavesdropper's channels fade independently. Moreover, in the following analysis we often consider that Eve's channel is significantly degraded (with an SNR penalty in the order of 3 dB or more) with respect to the main channel. In those cases in which this does not occur, that are also of interest in practice, we have that the secret message is spread on a long sequence of (50 ore more) packets. The latter condition means that, even if in this case Eve could successfully attack the reconciliation phase of some packet transmissions, this is very unlikely to occur for all the packets of a sequence, and the use of AONTs prevents Eve from gathering any partial information about the secret message.

Hypothesis 2 instead depends on the channel and transmission characteristics. Since we focus on short packets, it is likely that the channel can be considered stationary during each execution of the protocol. For the sake of simplicity, we will denote each three-way protocol execution as a *single packet session* in the following. In general terms, the assumption of stationary channels during each single packet session requires the use of codes with short length (i.e., small values of n) and high order modulations. Therefore, when missing, such a condition can be restored by changing the data rates, the coding rates and/or the modulation order.

Security of the proposed protocol will be discussed in detail in Section 3. Qualitatively, however, we can say that the addition of fake packets causes an additional difficulty for Eve. In fact, in the absence of fake packets, her challenge is to reconstruct the codeword transmitted by Alice from the noisy data she eavesdrops from the channel, while with fake packets she also needs to understand if any packet she intercepts is a valid or a fake packet. We also observe that Eve cannot mount active attacks, like transmitting fictitious RTS packets or impersonating Bob, since these would be detected by Alice and Bob, due to the broadcast nature of the wireless channel.

On Bob's side, the whole set of codewords must be received and decoded into the vectors x_i, $i = 1, 2, 3, \ldots, N$. Then, such vectors are used to reconstruct X and to invert the AONT to recover M. Due to the presence of the AONT, the message M can be recovered only on condition that all its corresponding codewords are correctly received and decoded, such that the AONT can be inverted. This means that, in the proposed protocol, reliability is not less important than security.

In the next sections, we show that it is possible to achieve some desired level of SS through this protocol even when the average SNR of Bob's channel is lower than the average SNR of Eve's channel. This is somehow in contrast with previous results concerning the wiretap channel, where it has been shown that in such conditions there cannot be secrecy unless some retransmission scheme is exploited [23]. Indeed, there is no contradiction with our results, since we adopt a different notion of secrecy with a different target, that is, SS against passive attackers with computational constraints. The following analyses also show that the OOT-FP protocol achieves transmission of an S-bit message by requiring a significantly smaller number of time slots with respect to the OOT protocol, though maintaining the same security level.

2.7. Channel Model

In order to model the fading nature of the channels, we consider the Nakagami-m distribution [27], which is a consolidated mathematical model for small-scale fading in high-frequency radio wave propagation. We consider this type of distribution for our channel model since it is a versatile statistical distribution that can be used to model a variety of fading environments, including one sided Gaussian fading (for $m = 1/2$) and Rayleigh fading (for $m = 1$). It also gives an approximation of the Rician fading that is amenable for mathematical manipulations.

According to the Nakagami-m distribution, the probability density function (p.d.f.) of the signal-to-noise ratio γ can be written as

$$p_\Gamma(\gamma) = \begin{cases} \frac{1}{\Gamma(m)} \left(\frac{m}{\bar{\gamma}}\right)^m \gamma^{m-1} e^{-\frac{m}{\bar{\gamma}}\gamma}, & \text{for } \gamma \geq 0, \\ 0, & \text{for } \gamma < 0, \end{cases} \tag{5}$$

where $\bar{\gamma}$ is the average SNR and $\Gamma(\cdot)$ is the Gamma function.

The parameter m represents the "shape factor" of the distribution, and it controls the severity, or intensity, of fading. Values of m lower than 1 correspond to a fading more severe than Rayleigh fading, while values higher than 1 lead to a less severe fading.

For $m = 1$, which is the particular case considered in [7], the p.d.f. of γ, corresponding to the Rayleigh's model, is given by

$$p_\gamma(\gamma) = \begin{cases} \frac{1}{\bar{\gamma}} e^{-\frac{\gamma}{\bar{\gamma}}}, & \gamma \geq 0, \\ 0, & \gamma < 0. \end{cases} \tag{6}$$

It is useful to calculate a primitive of the p.d.f. in (5), i.e., a solution of the integral

$$I = \int \frac{1}{\Gamma(m)} \left(\frac{m}{\bar{\gamma}}\right)^m \gamma^{m-1} e^{-\frac{m}{\bar{\gamma}}\gamma} d\gamma. \tag{7}$$

Indeed, this integral can be solved by exploiting the properties of the Gamma function, thus obtaining

$$I = -\frac{\Gamma\left(m, \frac{m}{\bar{\gamma}}\gamma\right)}{\Gamma(m)} + a, \tag{8}$$

where a is a constant and $\Gamma(\cdot, \cdot)$ is the incomplete Gamma function.

3. Security Level

We focus on practical, already implemented coding and modulation schemes, hence we consider classical deterministic coding instead of random coding or coset coding, which are often invoked in the literature for this kind of systems. Therefore, each k-bit block of data x (subscript is omitted for the sake of simplicity) is univocally mapped into a codeword c, differently from coding schemes specifically designed for the wiretap channel, which usually exploit random binning based on coset coding. Let us denote by c_E the noise corrupted vector received by Eve upon transmission of the codeword c. Then, noting by $H(\cdot)$ the entropy function, $s = H(c|c_E) = H(x|c_E)$ is Eve's total equivocation about the transmitted codeword, that is, the conditional entropy of c given c_E. As in general the input messages are not i.i.d., we have $H(c) = H(x) = k' \leq k$. When $s = k'$, we have perfect secrecy in Wyner's sense [6]. Instead, if $0 < s < k'$, perfect secrecy is not achieved; however, Eve still has to perform 2^s attempts on average in order to correctly decode c from c_E. The source entropy rate is $R_h = \frac{k'}{n} \leq \frac{k}{n} = R_c$, being R_c the code rate. Eve's equivocation can be expressed as

$$s = H(c|c_E) = H(c) - I(c; c_E), \tag{9}$$

where $I(c; c_E)$ denotes the mutual information between c and c_E. The dependence of $I(c; c_E)$ on the distribution of x and c can be removed by resorting to the upper bound $I(c; c_E) \leq \frac{n}{q} C_E$, where C_E is Eve's channel capacity and q is the number of bits per transmitted symbol. As we consider generally distributed messages and take the maximum of Eve's channel mutual information over all message distributions, we are under a MIS notion according to [9].

Let us denote by $R_e = \frac{s}{n}$ Eve's equivocation rate. By using the above upper bound on $I(c; c_E)$ and taking into account that Eve's equivocation cannot be negative, we have

$$R_e \geq \max\left\{0, \frac{1}{n}\left[k' - \frac{n}{q} C_E\right]\right\} = \left[R_h - \frac{C_E}{q}\right]^+. \tag{10}$$

Then, normalizing to the code rate, we obtain

$$\bar{R}_e \geq \frac{\left[R_h - \frac{C_E}{q}\right]^+}{R_c} = \widetilde{R_e}, \tag{11}$$

and, finally,

$$s = nR_e = k\bar{R}_e \geq n\left[R_h - \frac{C_E}{q}\right]^+ = \widetilde{s}. \tag{12}$$

Let us consider the lower bound on s at the right-hand-side (r.h.s.) of (12). In the OOT-FP protocol, the total equivocation on a packet can be obtained as the sum of two contributions as follows: $\widetilde{s}_{tot} = \widetilde{s}_e + \widetilde{s}_{fk}$. The term $\widetilde{s}_e$ represents Eve's equivocation due to her channel, and it is the only contribution present in the OOT protocol. The term $\widetilde{s}_{fk}$ represents Eve's equivocation due to the presence of the fake packets, that, in turn, depends on Bob's channel. $\widetilde{s}_e$ will be studied in Section 3.2, while the value of $\widetilde{s}_{fk}$ is discussed next.

Let us denote by p_{fk} the probability to have a fake packet, i.e., the probability that the channel SNR between Alice and Bob is below some prefixed threshold γ_B^*. Since Eve's and Bob's channels are independent, Eve's equivocation about the valid or fake nature of each packet can be written as the binary entropy following from p_{fk}, that is,

$$\widetilde{s}_{fk} = -p_{fk}\log_2 p_{fk} - (1 - p_{fk})\log_2(1 - p_{fk}). \tag{13}$$

The value of p_{fk} can be easily computed as

$$\begin{aligned} p_{fk} &= \Pr\{\gamma_B < \gamma_B^*\} = 1 - \Pr\{\gamma_B \geq \gamma_B^*\} \\ &= 1 - \frac{1}{\Gamma(m)} \left(\frac{m}{\bar{\gamma}_B}\right)^m \int_{\gamma_B^*}^{\infty} \gamma_B^{m-1} e^{-\frac{m}{\bar{\gamma}_B}\gamma_B} d\gamma_B. \end{aligned} \tag{14}$$

Let us express the average SNR experienced by Bob in terms of the threshold γ_B^* as follows:

$$\bar{\gamma}_B = \gamma_B^* \cdot \Omega, \tag{15}$$

that is, Ω is the ratio of Bob's channel average SNR to its threshold value. The last integral in (14) can be solved exploiting (8), thus obtaining

$$p_{fk} = 1 - \left[-\frac{\Gamma\left(m, \frac{m}{\bar{\gamma}_B}\gamma_B\right)}{\Gamma(m)} \right]_{\gamma_B^*}^{\infty} = 1 - \frac{\Gamma\left(m, \frac{m}{\Omega}\right)}{\Gamma(m)}. \tag{16}$$

Eve's maximum equivocation about the valid or fake nature of each packet occurs when p_{fk} is equal to 0.5. In fact, in this case, we have $\widetilde{s}_{fk} = 1$, since the occurrence of a valid or a fake packet is equally probable. The value of Ω that yields $p_{fk} = 0.5$ can be obtained from (16). As an example, for $m = 1$, it results in $\Omega = \frac{1}{\ln 2} = 1.44$, i.e., about 1.58 dB. However, the choice of $\bar{\gamma}_B$ is influenced also by Bob's error probability, i.e., reliability requirements. For this reason, in the following, we do not assume to be in the optimal situation with $\widetilde{s}_{fk} = 1$, but we compute the value of $\widetilde{s}_{fk}$ following from the required γ_B^* through (16) and (13). Then, we consider the same ratio Ω for all modulation formats and code rates.

3.1. Approximate Input-Constrained Capacity

Based on (12), we have a simple tool to assess the minimum of Eve's total equivocation on each transmitted block. However, in order to compute it, we need to know the value of Eve's channel capacity C_E, which depends on the modulation order $M = 2^q$ and on Eve's channel SNR. Actually, C_E can be computed through classical formulations of the input-constrained channel capacity. However, though providing exact estimates, such formulations are not in closed form, and therefore not amenable to manipulate. For this reason, we exploit the following approximation based on simple logarithmic functions

$$C(\gamma) \approx \begin{cases} \alpha_1 \log_2\left(\frac{1+\alpha_2\gamma}{1+\alpha_3\gamma}\right), & \text{for } \gamma \leq \gamma_{\max}, \\ q, & \text{for } \gamma > \gamma_{\max}, \end{cases} \tag{17}$$

where C is the input-constrained capacity and γ is the channel SNR. The values of the parameters α_1, α_2, α_3 and $\gamma_{\max}$ for the cases of binary phase shift keying (BPSK), 4-QAM and 16-QAM have been found through a least-squares fitting procedure and are reported in Table 1. The corresponding curves are shown in Figure 4, as functions of γ, and compared with their exact counterparts. From the figure, we observe that, for these cases, the approximation provided by (17) is very tight.

Table 1. Parameters used in (17) to compute the approximate input-constrained capacity for BPSK, 4-QAM and 16-QAM.

Modulation	α_1	α_2	α_3	$\gamma_{\max}$ [dB]
BPSK	10.4798	1.4095	1.3007	5.36
4-QAM	15.1700	0.7823	0.7034	9.17
16-QAM	11.7634	0.3150	0.2441	16.43

The availability of (17) allows us to characterize the p.d.f. of the approximate input-constrained capacity through a classical random variable analysis. More precisely, starting from (5) and (17), the following closed form expression can be easily obtained

$$p_C(C) = \begin{cases} \beta \gamma_f(C)^{m-1} e^{-\frac{m}{\bar{\gamma}}\gamma_f(C)} + \theta\delta(C-q), & 0 \le C \le q, \\ 0, & \text{otherwise}, \end{cases} \tag{18}$$

where

$$\gamma_f(C) = \frac{2^{C/\alpha_1} - 1}{\alpha_2 - \alpha_3 2^{C/\alpha_1}} \tag{19}$$

is the inverse of the r.h.s. of (17) for $\gamma \le \gamma_{\max}$, $\beta = \frac{1}{\Gamma(m)}\left(\frac{m}{\bar{\gamma}}\right)^m \frac{\ln(2)(1+\alpha_2\gamma_f(C))(1+\alpha_3\gamma_f(C))}{\alpha_1(\alpha_2-\alpha_3)}$, $\theta = \frac{1}{\Gamma(m)}\Gamma\left(m, \frac{m}{\bar{\gamma}}\gamma_{\max}\right)$ and $\delta(x)$ denotes the Dirac delta function in $x = 0$.

For $m = 1$, the Nakagami-m model reduces to a Rayleigh fading model, and (18) becomes [7,10]

$$p_C(C) = \begin{cases} \xi e^{-\frac{\gamma_f(C)}{\bar{\gamma}}} + e^{-\frac{\gamma_{\max}}{\bar{\gamma}}}\delta(C-q), & 0 \le C \le q, \\ 0, & \text{otherwise}, \end{cases} \tag{20}$$

where $\xi = \frac{\ln(2)(1+\alpha_2\gamma_f(C))(1+\alpha_3\gamma_f(C))}{\bar{\gamma}\alpha_1(\alpha_2-\alpha_3)}$.

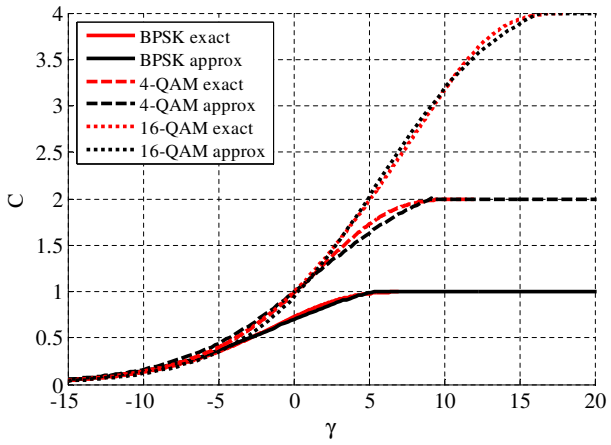

Figure 4. Exact and approximate input-constrained capacity for BPSK, 4-QAM and 16-QAM, as a function of the SNR γ.

3.2. Wiretapper's Equivocation under Outage Constraints

In this section, we estimate the wiretapper's equivocation $\widetilde{s}_e$ which is due to the quality of the Alice–Eve channel, expressed by the SNR value γ_E. Indeed, $\widetilde{s}_e$ is the only contribution present in the OOT protocol, while, in the case of OOT-FP, it sums up with the contribution $\widetilde{s}_{fk}$, due to the inclusion of the fake packets, in order to obtain the total equivocation $\widetilde{s}_{tot}$.

Since we are considering wireless channels affected by fading, Eve's channel capacity C_E is represented by a random variable described by the p.d.f. $p_C(C)$ in (18), with $C = C_E$. Consequently, $\widetilde{s}_e$ is a random variable as well, and we can derive its p.d.f. through classical transformations of random variables. This way we obtain

$$p_{\widetilde{s}_e}(\widetilde{s}_e) = \begin{cases} \frac{q}{n} p_{C_E}(\tau) + \phi\delta(\widetilde{s}_e), & 0 \le \widetilde{s}_e \le k', \\ 0, & \text{otherwise}, \end{cases} \tag{21}$$

where $\tau = q\left(R_h - \frac{\widetilde{s}_e}{n}\right)$ and $\phi = \Pr\{C_E > qR_h\} = \int_{qR_h}^{q} p_{C_E}(C_E)dC_E$.

Let P_o denote the equivocation outage probability, i.e., the probability that $\widetilde{s}_e$ falls below some lower threshold $\widetilde{s}_{\min} > 0$. Once having fixed the total equivocation $\widetilde{s}_{tot}$, according to the desired security level, the value of $\widetilde{s}_{\min}$ results as $\widetilde{s}_{\min} = \widetilde{s}_{tot} - \widetilde{s}_{fk}$. Obviously, for the OOT protocol, $\widetilde{s}_{fk} = 0$ and $\widetilde{s}_{\min} = \widetilde{s}_{tot}$. By definition, we have

$$P_o = \int_0^{\widetilde{s}_{\min}} p_{\widetilde{s}_e}(\widetilde{s}_e)d\widetilde{s}_e = 1 - \int_{\widetilde{s}_{\min}}^{k'} p_{\widetilde{s}_e}(\widetilde{s}_e)d\widetilde{s}_e. \tag{22}$$

Equivalently, $1/P_o$ is the number of channel realizations within which $\widetilde{s}_e \leq \widetilde{s}_{\min}$ occurs once, on average. Thus, taking into account possible outage events, we must impose $1/P_o \geq 2^{\widetilde{s}_{\min}}$ or, explicitly,

$$\log_2\left(\frac{1}{P_o}\right) \geq \widetilde{s}_{\min}, \tag{23}$$

which fixes the MIS level.

Since $\widetilde{s}_{\min} > 0$, we have

$$\begin{aligned}\int_{\widetilde{s}_{\min}}^{k'} p_{\widetilde{s}_e}(\widetilde{s}_e)d\widetilde{s}_e &= \int_{\widetilde{s}_{\min}}^{k'} \frac{q}{n} p_{C_E}(\tau)d\widetilde{s}_e \\ &= \int_0^{q\left(R_h - \frac{\widetilde{s}_{\min}}{n}\right)} p_{C_E}(\tau)d\tau.\end{aligned} \tag{24}$$

By replacing (18), with $C = C_E$ and using (8), we obtain

$$P_o = \frac{1}{\Gamma(m)}\Gamma\left(m, \frac{m}{\bar{\gamma}_E}\eta\right), \tag{25}$$

where $\bar{\gamma}_E$ is the average SNR of the channel between Alice and Eve, and $\eta = \gamma_f\left(q\left(R_h - \frac{\widetilde{s}_{\min}}{n}\right)\right)$.

Through (23) and (25), we can compute the value of $\bar{\gamma}_E$ required to reach a given value of $\widetilde{s}_{\min}$. Because of the presence of the incomplete Gamma function, this value is not easily obtainable in closed form. In essence, the problem consists of calculating $\bar{\gamma}_E$ such that

$$\Gamma(m)2^{-\widetilde{s}_{\min}} \geq \Gamma\left(m, \frac{m}{\bar{\gamma}_E}\eta\right). \tag{26}$$

We must note that $\widetilde{s}_{\min}$ appears on both sides of this inequality: explicitly at the left-hand-side (l.h.s.) and implicitly in the computation of η at the r.h.s. According to our target, however, the unknown variable is the upper bound on $\bar{\gamma}_E$. Thus, we set $y = \frac{m}{\bar{\gamma}_E}\eta$ and we evaluate the inverse incomplete Gamma function. Once having found the value of y, $\bar{\gamma}_E$ is easily computed as

$$\bar{\gamma}_E \leq \frac{m}{y}\eta = \bar{\gamma}_E^*. \tag{27}$$

If we consider the special case of Rayleigh fading, it is easy to verify that $y = \widetilde{s}_{\min}\ln(2)$, so that (27) becomes [7]

$$\bar{\gamma}_E \leq \frac{\eta}{\widetilde{s}_{\min}\ln(2)} = \bar{\gamma}_E^*. \tag{28}$$

Based on (27) and (28) (for the special case), we can define the conditions under which some given level of MIS is achieved.

3.3. Design Criteria

Equation (27) defines the upper threshold $\bar{\gamma}_E^*$ that must be imposed on Eve's channel quality in order to meet the security requirements. More precisely, imposing such an upper threshold ensures that Eve must perform $2^{\widetilde{s}_{\min}}$ attempts, on average, to fully recover a transmitted codeword. This must be considered in addition to the lower threshold γ_B^* on Bob's channel quality, which instead is required to achieve some reliability target for transmission from Alice to Bob. These two thresholds can be collected into the parameter

$$S_g = \frac{\gamma_B^*}{\bar{\gamma}_E^*}, \tag{29}$$

which represents the minimum SNR gap between Bob's and Eve's channels that is required to achieve both the reliability and the security targets.

As explained in Section 2, however, we still need to avoid that Eve is able to gather some (even small) part of a transmitted codeword with less attempts than $2^{\widetilde{s}_{\min}}$. This is achieved by pre-processing the messages through the AONT. The use of the AONT also allows for concatenating together N data blocks before transmission, which are processed together through the AONT itself. This way, Eve needs to correctly recover all the N codewords corresponding to those blocks before being able to invert the AONT. Therefore, $2^{N\widetilde{s}_{tot}}$ attempts are required on average by Eve to correctly recover the whole set of packets and invert the AONT to recover the secret bits. In other words, the use of the AONT allows us to achieve SS from MIS, while this form of concatenation allows us to tune the security level according to the desired target. Numerical examples are given in the next section.

4. Numerical Examples

In order to assess the performance of the protocols we consider, let us compute the number of time slots required to achieve a given security level, i.e., a prefixed value of $\widetilde{s}_{\min}$, as a function of the SNR gap. This way, we can also compare the performance of the OOT protocol with that of the OOT-FP protocol. For the sake of fairness, the comparison assumes the same value of S, that is, the length of the secret message M. Instead, based on Eve's equivocation achieved by each protocol, the resulting length of the random padding Z may be different. Considering that the handshaking phase between Alice and Bob, i.e., the exchange of initial messages and the subsequent reconciliation, involves the same number of time slots in the two protocols, the following analysis will be focused on the number of single packet sessions required to successfully transmit a message under given reliability and security constraints.

In order to refer to a significant, practical example concerning wireless transmissions, we suppose that the code $C_1(n,k)$ is one of the low-density parity-check (LDPC) codes included in the WiMax standard [28], and we consider modulation schemes compliant with the same standard. In WiMax, four code rates (1/2, 2/3, 3/4, 5/6) and several code lengths for each code rate are supported. As an example, we focus on codes with length $n = 2304$, but the analysis can be obviously extended to the other code lengths. Since our protocol relies on the hypothesis that the channel does not vary during each single packet session between Alice and Bob, for a given transmission bandwidth we suppose that the modulation order and the channel symbol rate are chosen in such a way that the channel coherence time is longer than a single packet session. The chance to actually meet this constraint depends on any specific setting. In the following numerical examples, we suppose that such a condition is met with $n = 2304$ and $q = 1, 2, 4$, but the analysis could be obviously repeated by assuming shorter codes and higher order modulations.

According to the model described in Section 3, and denoting the desired security level as SL (expressed in bits), the number of codewords that is necessary to transmit for achieving SL-bit security is easily obtained as

$$N = \frac{SL}{\widetilde{s}_{tot}}, \tag{30}$$

where $\widetilde{s}_{tot} = \widetilde{s}_{\min} + \widetilde{s}_{fk}$ for the OOT-FP protocol and $\widetilde{s}_{tot} = \widetilde{s}_{\min}$ for the OOT protocol. Although a direct comparison with a complete WiMax system is not possible (since we focus on one instance of the physical layer and neglect higher layer features like channel adaptivity of coding and modulation techniques), we observe that N represents an upper bound on the overhead introduced by our method with respect to plain transmission. Such an upper bound is reached when data to be transmitted are so few that they are contained in a single codeword, while all the other $N-1$ codewords must be filled with encoded padding bits. In this case, the overhead introduced by our protocol might be large. However, we must consider that this is an upper bound, while the average overhead depends on the statistical features of the source, whose consideration is out of the scope of this paper.

Once having fixed the average quality required for the main channel and the resulting threshold γ_B^*, the value of p_{fk} can be determined from (16), and then that of $\widetilde{s}_{fk}$ follows from (13). For a range of $\widetilde{s}_{\min}$ values, the values of $\bar{\gamma}_E^*$ can then be computed according to (27). The number of single packet sessions finally results as

$$N_{sps} = \frac{N}{1 - p_{fk}}, \tag{31}$$

and can be plotted as a function of S_g.

The numerical values obtained depend on the particular choices made for the degrees of freedom of the system. Indeed, the performance of the codes we consider with several modulation formats over different channels has been assessed in [29]. In order to provide some significant examples, let us fix the reliability requirement in terms of a decoding error probability $\leq 10^{-4}$ experienced by Bob. We note that the decoding error probability, that is the complement of the probability of successful transmission, is an input of our model since the target reliability of the system is fixed beforehand. The corresponding values of γ_B^* obtained from [29] are reported in Table 2. Let us also consider a ratio $\Omega = 3$ dB of the average quality of the main channel to its threshold value. According to (15), this fixes the value of Bob's average SNR.

Table 2. Values of γ_B^* (in dB) required to achieve decoding error probability $\leq 10^{-4}$ for LDPC codes with $n = 2304$ and several rates and modulation schemes compliant with WiMax.

R_c	1/2	1/2	1/2	2/3	2/3	2/3
Mod.	BPSK	4-QAM	16-QAM	BPSK	4-QAM	16-QAM
γ_B^*	−1.26	1.75	7.16	0.58	3.59	9.55
R_c	3/4	3/4	3/4	5/6	5/6	5/6
Mod.	BPSK	4-QAM	16-QAM	BPSK	4-QAM	16-QAM
γ_B^*	1.63	4.64	10.47	2.76	5.77	12.12

In Figures 5 and 6, we compare the results obtained using the OOT-FP protocol (continuous line) with those achieved by the OOT protocol (dashed line), for two different modulation formats, namely BPSK and 16-QAM, and a couple of WiMax code rates. The figures report the values of N_{sps}, that is the number of single packet sessions, required to achieve a decoding error probability $\leq 10^{-4}$ (towards Bob) and a semantic security of 128 bits (against Eve). The independent variable is the ratio S_g, defined by (29). Moreover, as an example, we fix k' equal to $0.9k$. In order to match binary coding with non-binary modulations, we follow a pragmatic approach, according to which coding is applied first and modulation acts downstream on groups of encoded symbols.

As it is reasonable and expected, independently of the protocol used, the values of N_{sps} become smaller and smaller for increasing S_g. In the figures we consider channels with different fading intensity: from $m = 0.5$, which is the minimum value allowed for the Nakagami-m distribution, to $m = 5$, which represents a more stationary channel. The case with $m = 1$, coinciding with the Rayleigh fading model, is considered as well.

From these figures, we observe that, interestingly, the proposed protocol is able to achieve 128-bit SS even when the average SNR of Eve's channel is comparable to or even slightly better than that

of Bob's channel, although this is obviously paid in terms of an increased number of single packets sessions needed to achieve such a security level. Finally, and very important, we observe that the use of fake packets provides a significant improvement in performance, since Alice needs to transmit for a shorter time, measured in time slots, in order to reach 128-bit SS.

Also the value of m has a relevant impact, both in absolute terms and as regards the comparison between the two protocols. In particular, we must consider that strong fading, as described by low values of m, yields to a greater number of fake packet transmissions that hence dominate Eve's equivocation. On the contrary, more stationary channels yield less fake packet transmissions. This reflects on higher values of N_{sps} when Eve's channel is better (or, at least, not significantly worse) than Bob's channel, since fake packets are those responsible for Eve's equivocation in these conditions.

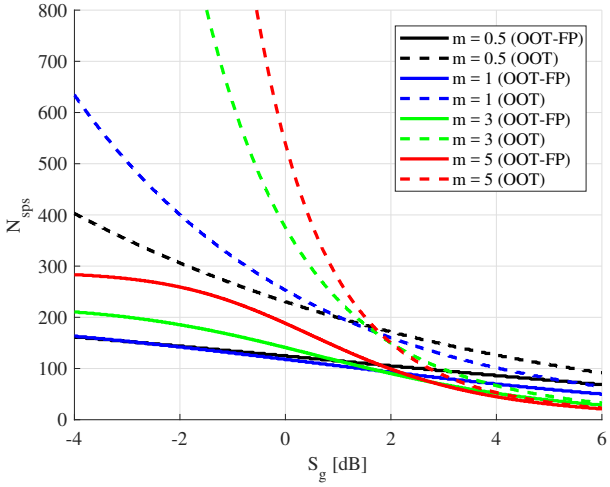

Figure 5. Number of single packet sessions needed to achieve 128-bit SS versus SNR gap with WiMax LDPC codes having length $n = 2304$, rate $R_c = 1/2$ and BPSK, for the case of $k' = 0.9k$.

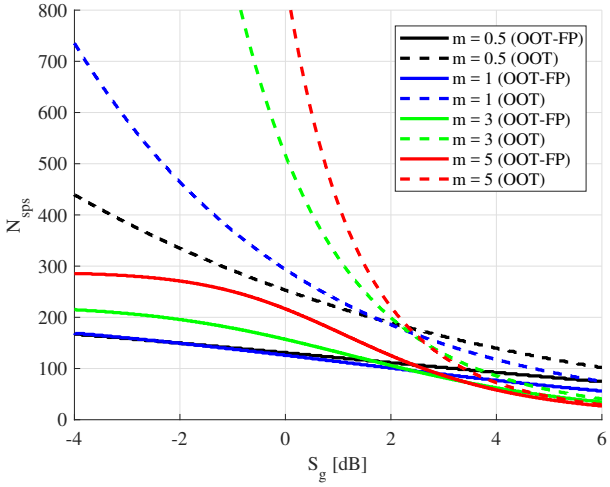

Figure 6. Number of single packet sessions needed to achieve 128-bit SS versus SNR gap with WiMax LDPC codes having length $n = 2304$, rate $R_c = 5/6$ and 16-QAM, for the case of $k' = 0.9k$.

Figures 7 and 8, in turn, highlight the differences in terms of performance between various code rates and modulation formats, respectively. In this case, the analysis has been repeated for different values of k'. The value of the shape factor has been fixed to $m = 3$. Although the variations are almost negligible, we can observe from Figure 7 that using high rate codes permits us to achieve the target

security level with a smaller number of time slots with respect to low rate codes. Instead, from Figure 8, we see that using high order modulation schemes is not beneficial from the number of time slots standpoint. 16-QAM, in particular, always requires the largest amounts of single packet sessions to achieve the target security level. It must be said that high order modulation schemes may be needed in order to ensure that the channel can be considered stationary during each single packet session. In these cases, using high order modulations still allows for achieving the desired SS level with a moderate increase in the number of required single packet sessions.

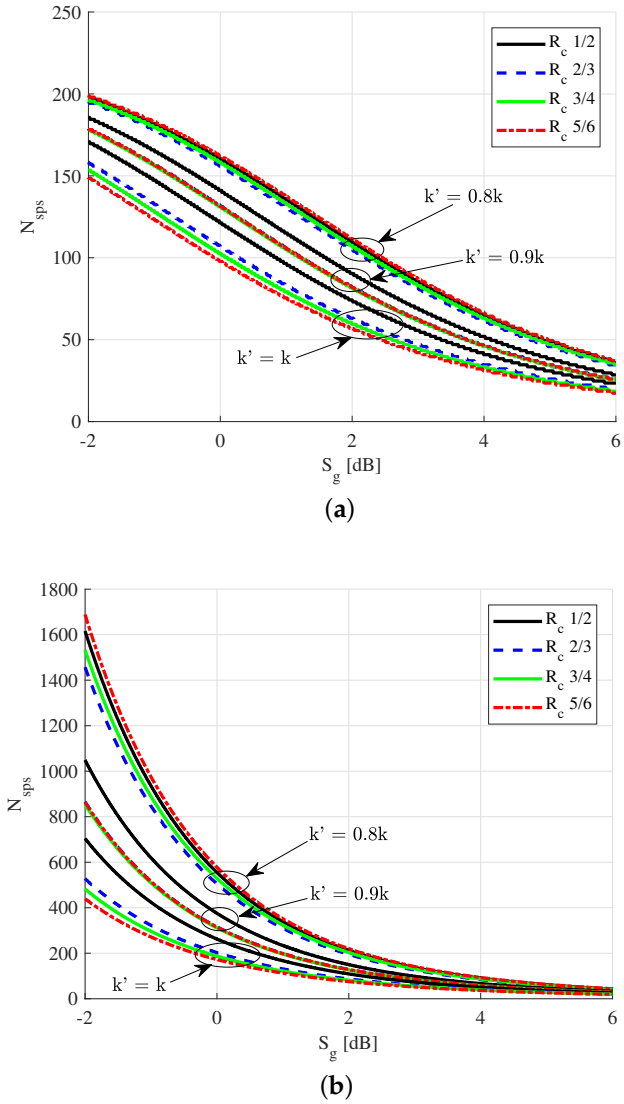

Figure 7. Number of single packet sessions needed to achieve 128-bit SS in terms of SNR gap with WiMax LDPC codes having length $n = 2304$, BPSK and different rates, for the cases of $k' = 0.8k$, $k' = 0.9k$ and $k' = k$, and shape factor $m = 3$, using: (**a**) the OOT-FP protocol and (**b**) the OOT protocol.

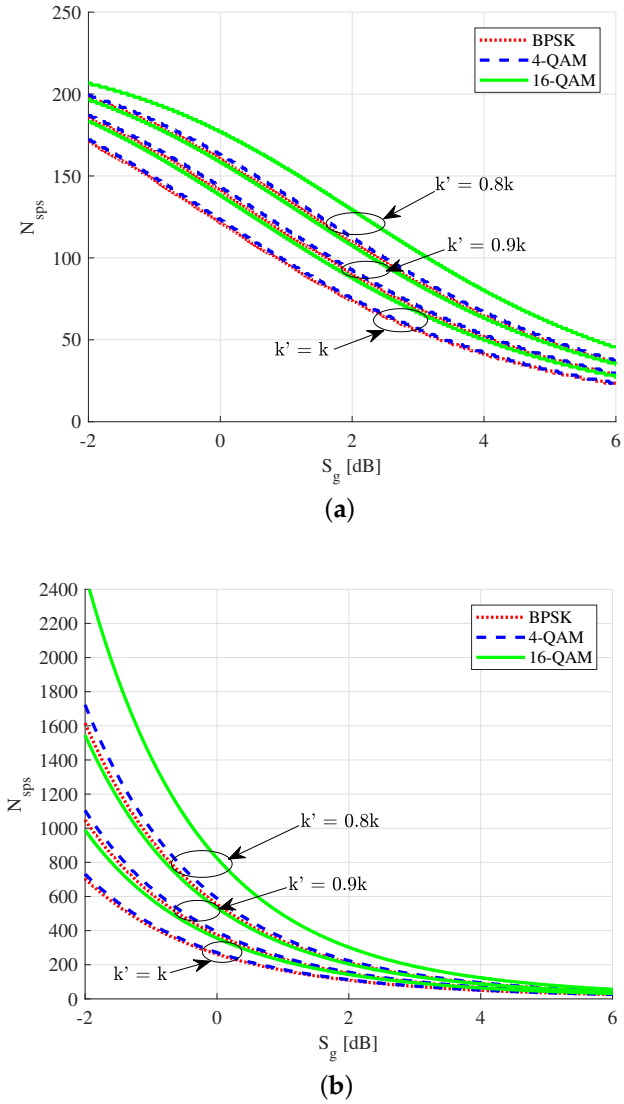

Figure 8. Number of single packet sessions needed to achieve 128-bit SS in terms of SNR gap with WiMax LDPC codes having length $n = 2304$, rate $R_c = 1/2$ and three different modulations, for the cases of $k' = 0.8k$, $k' = 0.9k$ and $k' = k$, and shape factor $m = 3$, using: (**a**) the OOT-FP protocol and (**b**) the OOT protocol.

5. Conclusions

We have proposed an OOT protocol based on coding and AONTs to achieve some desired level of SS over fading wiretap channels by using classical and practical transmission techniques. We have introduced the use of fake packets in the proposed protocol and assessed the resulting benefits in terms of performance. Fading has been modeled by means of the Nakagami-m distribution, this way representing a number of different scenarios. The feasibility of the proposed approach has been demonstrated through numerical examples considering coding and modulation schemes compliant with the WiMax standard. Our results show that satisfactory SS levels are achievable with practical coding and modulation schemes, even when the average quality of the eavesdropper channel is not worse than that of the main channel.

Author Contributions: Marco Baldi, Franco Chiaraluce and Linda Senigagliesi contributed equally to this work.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proc. IEEE* **2016**, *104*, 1727–1765.
2. Su, H.; Qiu, M.; Wang, H. Secure wireless communication system for smart grid with rechargeable electric vehicles. *IEEE Commun. Mag.* **2012**, *50*, 62–68.
3. Zhang, Z.J.; Lai, F.C.; Chao, H.C. A green data transmission mechanism for wireless multimedia sensor networks using information fusion. *IEEE Wirel. Commun.* **2014**, *21*, 14–19.
4. Bloch, M.; Barros, J. *Physical-Layer Security: From Information Theory to Security Engineering*, 1st ed.; Cambridge University Press: Cambridge, UK, 2011.
5. Katz, J.; Lindell, Y. *Introduction to Modern Cryptography*; CRC Press: Boca Raton, FL, USA, 2014.
6. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387.
7. Baldi, M.; Senigagliesi, L.; Chiaraluce, F. Achieving semantic security without keys through coding and all-or-nothing transforms over wireless channels. In Proceedings of the IEEE Global Conference on Signal Processing (GlobalSIP2016), Washington, DC, USA, 7–9 December 2016; pp. 964–969.
8. Cuff, P. A framework for partial secrecy. In Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM 2010), Miami, FL, USA, 6–10 December 2010.
9. Bellare, M.; Tessaro, S.; Vardy, A. Semantic security for the wiretap channel. In *Advances in Cryptology— CRYPTO 2012*; Lecture Notes in Computer Science; Savafi-Naini, R., Canetti, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7417, pp. 294–311.
10. Baldi, M.; Senigagliesi, L.; Chiaraluce, F. On the security of transmissions over fading wiretap channels in realistic conditions. In Proceedings of the IEEE International Conference on Communications (IEEE ICC 2017), Paris, France, 21–25 May 2017.
11. Rivest, R.L. All-or-nothing encryption and the package transform. In *Fast Software Encryption*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1997; Volume 1267, pp. 210–218.
12. Goldwasser, S.; Micali, S. Probabilistic encryption. *J. Comput. Syst. Sci.* **1984**, *28*, 270–299.
13. Bloch, M.; Hayashi, M.; Thangaraj, A. Error-control coding for physical-layer secrecy. *Proc. IEEE* **2015**, *103*, 1725–1746.
14. Harrison, W.K.; Sarmento, D.; Vilela, J.P.; Gomes, M. Analysis of short blocklength codes for secrecy. *arXiv* **2015**, arXiv:1509.07092.
15. Gopala, P.K.; Lai, L.; El Gamal, H. On the secrecy capacity of fading channel. *IEEE Trans. Inf. Theory* **2008**, *54*, 4687–4698.
16. Liang, Y.; Poor, H.V.; Shamai (Shitz), S. Secure communications over fading channels. *IEEE Trans. Inf. Theory* **2008**, *54*, 2470–2492.
17. Renna, F.; Laurenti, N.; Poor, H.V. Physical layer secrecy for OFDM transmissions over fading channels. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1354–1367.
18. Poor, H.V.; Schaefer, R.F. Wireless physical layer security. *Proc. Natl. Acad. Sci. USA* **2017**, *114*, 19–26.
19. He, B.; Zhou, X. Secure on–off transmission design with channel estimation errors. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1923–1936.
20. Hu, J.; Yang, W.; Yang, N.; Zhou, X.; Cai, Y. On-off-based secure transmission design with outdated channel state information. *IEEE Trans. Veh. Technol.* **2016**, *65*, 6075–6088.
21. Mu, P.; Li, Z.; Wang, B. Secure on–off transmission in slow fading wiretap channel with imperfect CSI. *IEEE Trans. Veh. Technol.* **2017**, doi:10.1109/TVT.2017.2703861.
22. Choi, J. On channel-aware secure HARQ-IR. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 351–362.
23. Tang, X.; Liu, R.; Spasojevic, P.; Poor, H.V. On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels. *IEEE Trans. Inf. Theory* **2009**, *55*, 1575–1591.
24. Tomasin, S.; Laurenti, N. Secure HARQ with multiple encoding over block fading channels: Channel set characterization and outage analysis. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 1708–1719.
25. Stinson, D.R. Something about all or nothing (transforms). *Des. Codes Cryptogr.* **2001**, *22*, 133–138.
26. Massey, J.L. Shift-register synthesis and BCH decoding. *IEEE Trans. Inf. Theory* **1969**, *15*, 122–127.
27. Nakagami, M. The m-Distribution: A General Formula of Intensity Distribution of Rapid Fading. In *Statistical Methods in Radio Wave Propagation*; Hoffman, W., Ed.; Pergamon Press: Elmsford, NY, USA, 1960; pp. 3–36.

28. IEEE. *802.16e 2005: IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems—Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands*; IEEE: New York, NY, USA, 2005.
29. Yang, R. LDPC-Coded Modulation for Transmission over AWGN and Flat Rayleigh Fading Channels. Master's Thesis, Université Laval, Ville de Québec, QC, Canada, 2010.