Joint PHY/MAC Layer Security Design Using ARQ with MRC and Null-Space Independent, PAPR-Aware Artificial Noise in SISO Systems

Article *in* IEEE Transactions on Wireless Communications · July 2018

DOI: 10.1109/TWC.2018.2855163

CITATIONS
20

READS
420

2 authors:

Jehad Hamamreh
Antalya Bilim University
63 PUBLICATIONS **620** CITATIONS

SEE PROFILE

Huseyin Arslan
University of South Florida & Istanbul Medipol University
444 PUBLICATIONS **12,004** CITATIONS

SEE PROFILE

Joint PHY/MAC Layer Security Design Using ARQ With MRC and Null-Space Independent PAPR-Aware Artificial Noise in SISO Systems

Jehad M. Hamamreh and Huseyin Arslan, *Fellow, IEEE*

***Abstract*— Automatic-repeat-request (ARQ) as a MAC layer mechanism and artificial noise (AN) as a physical layer mechanism along with the help of maximal ratio combining (MRC), are jointly designed to achieve secrecy. Basically, a special AN, which does not require null-space in the channel, is designed based on the quality of service requirements and the channel condition between the legitimate parties and injected to the data packet. If the same packet is requested by the legitimate receiver (Bob), an AN canceling signal is properly designed and added to the next packet. Then, an AN-free packet is obtained by using MRC process at Bob, while deteriorating the eavesdropper's performance. Furthermore, two simple closed-form expressions of the achievable secure throughput are derived. The first one is given in a closed-form for the case of ARQ scheme without AN, while the second one is given in an upper-bound form for the case of ARQ with AN. Moreover, this paper addresses two critical security-associated problems: 1) the joint design of secrecy, reliability, throughput, delay and the tradeoff among them, and 2) the increase in the peak-to-average power ratio (PAPR) due to the added AN. Finally, the proposed design is extended to OFDM to demonstrate its capability in not only enhancing the secrecy due to the frequency selectivity of the channel, but also in reducing the PAPR and out-of-band emission of OFDM-based waveforms, while maintaining secrecy.**

***Index Terms*— Cross PHY/MAC layer security, automatic-repeat-request (ARQ), peak-to-average power ratio (PAPR), out-off-band emission (OOBE), artificial noise (AN), maximum ratio combining (MRC), quality of service (QoS), throughput, secure throughput, delay, perfect secrecy, packet error rate (PER).**

I. Introduction

THE demand for wireless communication services is continuously increasing as a consequence of the massive spread in wireless devices with wide variety of applications. Since wireless communication is becoming the dominant access type for most of the Internet-based services, serious security risks appear on the wireless signals due to their broadcast nature. Therefore, security ensuring precautions emerge as a critical need for wireless services. Specifically, users require confidential transmission for their wireless data such as private messages, voice calls, videos, financial transactions, etc. As a matter of fact, secure communication systems are desirable without just relying on the traditional encryption and key-sharing methods. To this end, physical-layer (PHY) security emerges as a promising and revolutionizing concept. This has been motivated by four main security problems in practical scenarios. *First*, the key generation, distribution, and management processes between the legitimate parties are extremely challenging, especially in large-scale heterogeneous and decentralized wireless networks. *Second*, longer key length results in more waste of resources, apart from the fact that implementing security methods with Shannon's perfect secrecy is impractical in today's data volume. *Third*, the fast developments and advances in computing and processing devices reveal the fact that current secret key-based techniques can be cracked, no matter how much mathematically complex they are, especially when quantum computing becomes a reality. *Fourth*, cryptographic-based security adds extra delay and complexity to the Tactile communication applications such as autonomous driving, remote surgery, controlling unmanned aerial vehicles (UAVs), etc. These applications require utmost secure communication with minimal latency.

To mitigate the effect of the aforementioned problems, key-less information-theoretic-based schemes have attracted the research community's attention due to their desirable features. In Wyner's paper [1], it was stated that confidential communication between legitimate users is possible without secret key sharing if the channel of the eavesdropper (Eve) is worse than the channel of the intended receiver (Bob). Motivated by the same study [1], the achievable secrecy capacity from an information-theoretic point of view was studied for various communication scenarios and channels, which were surveyed in [2]–[4]. In particular, information-theoretic secrecy under channel coding and automatic-repeat-request (ARQ) was studied for the case where Eve's signal-to-noise ratio (SNR) is lower than that of Bob in [5]–[9].

Manuscript received October 25, 2017; revised March 8, 2018 and May 16, 2018; accepted July 9, 2018. Date of publication July 20, 2018; date of current version September 10, 2018. This work was supported by the Scientific and Technological Research Council of Turkey (TÜBITAK) under Grant 114E244. The associate editor coordinating the review of this paper and approving it for publication was S. K. Jayaweera. *(Corresponding author: Jehad M. Hamamreh.)*

J. M. Hamamreh is with the Department of Electrical and Electronics Engineering, Istanbul Medipol University, 34810 Istanbul, Turkey (e-mail: jmhamamreh@st.medipol.edu.tr; jehad.hamamreh@gmail.com).

H. Arslan is with the Department of Electrical and Electronics Engineering, Istanbul Medipol University, 34810 Istanbul, Turkey, and also with the Department of Electrical Engineering, University of South Florida, Tampa, FL 33620 USA (e-mail: huseyinarslan@medipol.edu.tr; arslan@usf.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2018.2855163

However, in practical scenarios, due to the random, location-dependent, and broadcast nature of the wireless channel; Eve's channel condition including its received SNR can be comparable to or even better than Bob's one [10]. Therefore, well-advanced and practical security techniques are extremely needed to ensure the secrecy for legitimate users. In the literature, various PHY security methods have been proposed and comprehensively surveyed in [2], [3], and [4]. To the best of our knowledge, most of these methods mainly depend on exploiting one or more of the following approaches: 1) the channel variations and its reciprocity with the assistance of diversity to extract shared secret keys [11], [12]; 2) space diversity such as MIMO, relays, and large scale networks to, for instance: inject artificial noise (AN) [13], perform precoding, shape antenna patterns (beam-forming) towards trusted users [14], etc.; 3) specific features in certain systems such as cyclic prefix, pilots, hardware impairments, and synchronization to disrupt Eve's reception [15]–[19]. However, when these degrees of freedom are not available, PHY security becomes extremely hard to achieve. Despite of all these constraints, security can still be provided by exploiting some already existing features in MAC layer, which are linked with the quality of service (QoS) requirements. For instance, employing (ARQ/HARQ) protocol, that takes an advantage of the fact that only intended recipients can request retransmissions, can be used to enhance security [20]. In [21], authors studied the optimal power allocation sequence over the HARQ rounds that maximizes the outage probability of Eve, without considering the effect of the transmission parameters. They assumed that the statistical knowledge of Eve's channel and SNR levels are available at the transmitter. However, such an assumption might be impractical since Eve is usually a passive receiver in reality [2], [22]. Additionally, they considered that the channel exhibits quasi-static fading, which is not necessarily the case in many practical scenarios [23], [24]. Without relying on the aforementioned assumptions, we in [25] investigated the exact practical secrecy gap between Bob and Eve due to adopting a special design of ARQ. It was shown that although ARQ scheme can provide secrecy, it fails to deliver enough of it at high SNR values or when Eve's SNR is higher than that of Bob, making Eve able to decode the packet correctly from the first round [25]. To mitigate this problem, adaptive modulation was proposed to enhance the obtained secrecy. However, the enhancement was not significant enough and not applicable over all SNRs [25].

In this paper, a new joint PHY/MAC layer security method that exploits ARQ with maximal ratio combining (MRC) process alongside a special design of AN is proposed to provide secrecy even if Eve's SNR is higher than that of Bob. Under realistic assumptions, it is shown that the information-theoretic perfect secrecy notion[1] can practically be achieved by the proposed method. Furthermore, the method preserves its applicability for the worst security scenario, where the legitimate channel is flat (not providing much randomness) and the transmitter is equipped with only a single antenna. On the other hand, it is also noticed that perfect secrecy is not always needed to provide a perfectly secure service. In reality, each service has different QoS requirements than the others, and if we ensure that Eve is operating below these requirements, then practical secrecy can be guaranteed. **The main contributions** of this paper can be summarized as follows:

- The exact secure throughput, resulting from the implicit adaptivity, caused by using ARQ scheme with MRC employed on a symbol level basis, is determined and quantified by analysis and simulations, and then used as a benchmark for comparison purposes with the performance of the next proposed design.
- A new security method based on ARQ mechanism with null-space-independent AN that exploits the receiver structure of MRC is developed to ensure security for various data services such as voice and video. Thus, instead of relying on the null-space created by the degree of freedom that exists in the case of multiple antennas [13], [14], cooperative relays [26], frequency-selective channel [15], or cyclic prefix feature in OFDM [16], for AN generation; in this work, ARQ with MRC is exploited for the first time in the literature for producing null-space-independent AN to safeguard transmission against eavesdropping attacks. Basically, AN is designed based on the quality of service (QoS) requirements and the channel condition between the legitimate parties and injected to the data packet. If the same packet is requested by Bob, an AN canceling signal is designed based on the legitimate user's channel and added to the next packet. Then, an AN free packet is obtained by using MRC process, whereas the AN severely deteriorates the eavesdropper's performance.
- Closed form expressions of the achievable secure throughput for voice, video, and delay-tolerant services are derived, which can be used by designers to quantify the secrecy performance of the proposed design.
- Two important security-related problems are addressed: 1) the combined practical design of secrecy, reliability, throughput, delay, and the trade-off among them; 2) the peak-to-average power (PAPR) increase, resulting from the structure of the added AN.
- The scheme is extended to multi-carrier systems (OFDM) over a frequency selective channel to demonstrate how a designer can exploit and optimize the added AN to not only improve secrecy, but also to reduce the PAPR and out-of-band emission (OOBE) in OFDM systems.

The merits of the proposed scheme can be stated as follows:

- It is structurally simple but very effective, and it does not require to be supported by a complicated transceiver architecture. More importantly, it does not require any changes or extra processing at the receiver side thanks to the proper design of the added AN, which can be perfectly canceled during the MRC process.
- It can provide prefect secrecy with the aid of the added AN. This ensures zero information leakage to Eve even if Eve's SNR is higher than Bob's one.
- It can provide secrecy in one of the most challenging scenario, where there is no spatial degree of freedom

[1]Perfect secrecy means that the mutual information leakage to Eve is equal to zero (i.e., the decoding error probability of Eve must go to unity).

(no null-space) and the channel is flat fading (i.e., no much randomness).

- The proposed design creates an extra degree of freedom in the power domain due to the added AN, which can be utilized not only to enhance secrecy, but also for other purposes alongside secrecy such as reducing PAPR and mitigating OOBE of OFDM-based systems. In other words, the scheme increases the system design flexibility.
- It can serve as an alternative solution for the jamming-aided eavesdropping problem presented in [27]. In this problem, Eve jams Bob to force him to ask for retransmission so that she can get more copies of the same packet, and thus increasing her decoding capability. However, since in our scheme AN is added to each retransmission round, this will prohibit Eve benefiting from the retransmitted copies of the same packet. Interested readers can refer to [27] for more details.
- The maximum benefit and best operating condition of the proposed scheme can be obtained when it is used with OFDM-based waveforms over dispersive channels. This is due to two reasons: 1) the AN vector's randomness becomes not only a function of the generated signal at the source, but also of the dispersive channel randomness; 2) the possibility of redesigning the AN to solve some of the major drawbacks of OFDM, as it will be shown in Section V.

The remainder of the paper is ordered as follows: Section II gives the details of the system model and the main adopted assumptions. Section III provides the description and explanation of the proposed security design. The analytical analysis of the achievable secure throughput is presented in Section IV. The extension of the proposed scheme to OFDM is explained in Section V, where two new optimization problems related to PAPR and OOBE are formulated and solved numerically. Section VI exhibits and discusses the simulation results of the developed method. Finally, conclusion and future works are drafted in Section VII.

Notations: Vectors are denoted by bold-small letters, whereas matrices are denoted by bold-large letters. Norm-2 and norm-infinity are defined by $\|\cdot\|_2$ and $\|\cdot\|_\infty$, respectively. $\mathbf{I}_N$ is the $N \times N$ identity matrix. The transpose, conjugate transpose, inverse, and absolute value (amplitude) are symbolized by $(\cdot)^T$, $(\cdot)^H$, $(\cdot)^{-1}$, and $|\cdot|$, respectively.

II. System Model and Preliminaries

We consider a single-input single-output (SISO) communication system employing ARQ protocol as briefly presented in Fig. 1. In particular, a source node (Alice) is communicating with a legitimate user (Bob) in the presence of a passive eavesdropper (Eve), who tries to intercept the source information of a service, communicated between the legitimate parties (Alice and Bob). The transmission mechanism of ARQ without AN, as shown in the lower part of Fig. 2 and before connecting the adaptive artificial noise (AAN) block, works as follows. First, Alice encodes the information bits using cyclic redundancy check (CRC), maps the bits into symbols using M-ary phase shift keying (M-PSK) and then forms a data packet

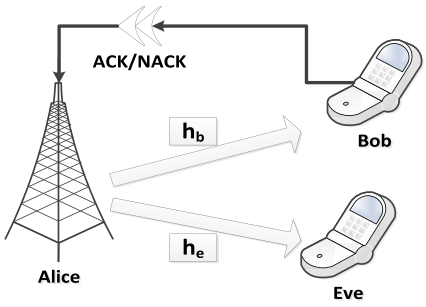


Fig. 1. Concise and simple model of the considered security scenario.

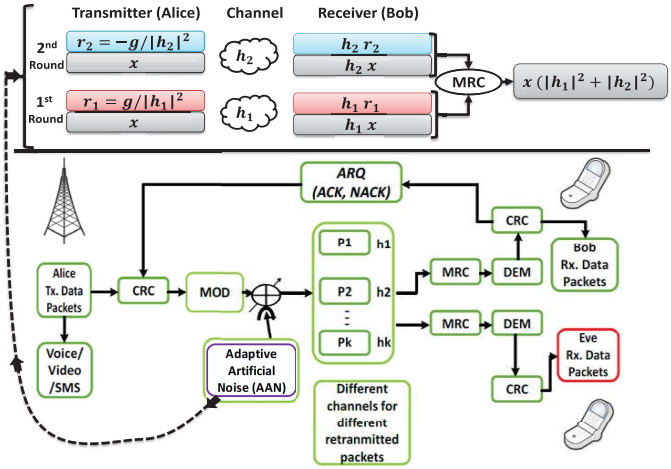


Fig. 2. The detailed system model of the proposed security scheme.

$\mathbf{x} = [x_1\ x_2\ \cdots\ x_N]^T \in \mathbb{C}^{N\times 1}$ of N number of modulated symbols, to be sent to Bob. After receiving the transmitted packet, which passes through a Rayleigh fading channel and affected by additive white Gaussian noise (AWGN), Bob demodulates and then decodes the packet using CRC. Based on the decoding result of the CRC, Bob decides success or failure of packet decoding by sending back to Alice an ACK or NACK messages through an error-less feedback channel, which is accessible by Eve as well. If a NACK is received by Alice and the current retransmission value is less than the maximum number of allowable retransmissions (L), Alice resends the same data packet with identical transmission parameters to the first round, i.e., same power and modulation during each retransmission. The receiver then uses MRC on a symbol level basis (before demodulation process) to combine the last received data packet with the previously erroneous received ones, which are stored in a buffer (i.e., soft-combing is used). If ACK is received by Alice or L is reached, Alice stops retransmitting the current same packet and instead transmits a new data packet. In each retransmission round, both Bob and Eve try to detect the transmitted packet by combining the received data from all preceding retransmissions of the same packet via MRC. If Bob cannot extract the packet after L rounds, then Bob records a packet error. This transmission mechanism is referred to in the literature (e.g., [24], [28]) as chase combining ARQ (CC-ARQ) scheme. Note that adaptive artificial noise (AAN) block is initially excluded from the

system and the explanation of this block is left for the next section.

The following assumptions are also adopted: 1) Both channels, Alice-to-Bob (h_b) and Alice-to-Eve (h_e) are considered to be independent and identically distributed (i.i.d.) block Rayleigh fading with constant gain over each ARQ round, but independent across ARQ rounds [23], [24], [28]. 2) A maximum of L ARQ rounds is allowed which limits both complexity and delay. 3) Alice has no knowledge on Eve's channel since Eve is a passive node. 4) Alice has the normal feedback information about Bob such as ACK/NACK signals [25]. Also, in the case of ARQ with AN scheme, Alice has knowledge on h_b, but not h_e [24]. 5) The channel reciprocity property is adopted, where the downlink channel can be estimated from that of the uplink in a time division duplexing (TDD) system. Thus, Eve does not know the channel of the legitimate link [29]. 6) The worst (most difficult) security scenario is considered, where the channel is not providing much randomness (one tap channel) and Eve is aware of the retransmission process by accessing the feedback messages and also uses MRC (optimal receiver structure) similar to Bob [25]. 7) Each one of the communicating parties (Alice and Bob) is equipped with a single antenna as well as Eve [21]. 8) Both Bob and Eve experience independent channel realizations because the wireless channel response is dependent on the positions of the communicating parties as well as the environment [15], [22].

III. The Proposed Security Design

Here, we divide our work into two parts: the first is dedicated to studying and investigating CC-ARQ scheme before adding AN as explained in Section II, which will be used as a benchmark for comparison purposes; while the second is devoted to developing a new security method based on ARQ with MRC and AN. For the first part, as explained earlier, Alice transmits data packet $\mathbf{x}$ with average power at the k^{th} round denoted by P_k. The received signal vectors, whose sizes are the same as $\mathbf{x} \in \mathbb{C}^{N\times 1}$, at both Bob and Eve in the k^{th} round are modeled as

$$\mathbf{y}_{i,k} = h_{i,k}\mathbf{x} + \mathbf{w}_{i,k}, \quad k = 1, 2, \cdots L, \quad i \in \{b, e\}, \tag{1}$$

where the subscripts b and e indicate the parameters for Bob and Eve. Thus, when $i = b$ and $i = e$, we will have $h_{b,k}$ and $h_{e,k}$, which are the block-fading Rayleigh channel realizations of Alice-to-Bob and Alice-to-Eve links over the k^{th} round, respectively; whereas $\mathbf{w}_{b,k}$ and $\mathbf{w}_{e,k}$ are the complex additive white Gaussian noise vectors with power spectral density of $N_{b,k}$ and $N_{e,k}$ at Bob and Eve, respectively. Additionally, we define $\gamma_{i,k}$ and $\bar{\gamma}_{i,k}$ to be the instantaneous and average received SNR of both Bob and Eve at k^{th} round, which are given by $\gamma_{i,k} = \frac{P_k|h_{i,k}|^2}{N_{i,k}}$ and $\bar{\gamma}_{i,k} = \frac{P_k}{N_{i,k}}$, respectively. As mentioned before, in this scheme, MRC is performed on a symbol level basis before demodulation, where each version of the received signal at each round is multiplied by the corresponding channel realization conjugate $(*)$ and thus the net combined received signal at Bob/Eve after L rounds can be expressed as

$$\hat{\mathbf{y}}_i = \sum_{k=1}^{L} \mathbf{y}_{i,k} \times h_{i,k}^* \tag{2}$$

$$= \sum_{k=1}^{L} (h_{i,k}\mathbf{x} + \mathbf{w}_{i,k}) \times h_{i,k}^* \tag{3}$$

$$= \sum_{k=1}^{L} |h_{i,k}|^2\mathbf{x} + \mathbf{w}_{i,k}h_{i,k}^*. \tag{4}$$

For the case of voice service, where $L = 2$, the above formula can be reduced to the below form

$$\hat{\mathbf{y}}_i = \mathbf{y}_{i,1}h_{i,1}^* + \mathbf{y}_{i,2}h_{i,2}^* \tag{5}$$

$$\hat{\mathbf{y}}_i = \mathbf{x}\left(|h_{i,1}|^2 + |h_{i,2}|^2\right) + \hat{\mathbf{w}}_i, \tag{6}$$

where $\hat{\mathbf{w}}_i = \mathbf{w}_{i,1}h_{i,1}^* + \mathbf{w}_{i,2}h_{i,2}^*$, and the detected data packet $\hat{\mathbf{x}}$ is given as

$$\hat{\mathbf{x}} = \mathbf{x} + \frac{\hat{\mathbf{w}}_i}{(|h_{i,1}|^2 + |h_{i,2}|^2)}. \tag{7}$$

Now, since Bob's channel is independent of Eve's one, the implicit adaptation process resulting from ARQ mechanism and controlled by Bob will be in favor of him, but not Eve because the retransmission happens according to Bob's channel condition, but not Eve's one. In other words, there are cases where Eve requires two rounds to be able to decode due to her possible bad channel conditions, but Bob may require only one round to decode as he may have a good channel gain in the first round. Since Bob controls the retransmission process, a second retransmission, which may be needed for Eve to decode, will not be triggered as Bob is able to decode successfully from the first round. Consequently, Eve's packet error rate (PER) will be significantly affected not only by the channel conditions but also by the number of occurred retransmission. Simulation results exhibit that the use of ARQ in the described way can provide a significant PER secrecy gap between Bob and Eve and thus secure throughput at a specific SNR region, which will be accurately identified in the forthcoming sections.

However, CC-ARQ scheme alone, as described before, is not sufficient to provide eavesdropping-resilient services at any SNR Eve may have. In fact, insecure transmission occurs in two cases. The first case happens when Eve is closer to the transmitter than Bob, in this situation, Eve will be able to decode the packet from the first round due to experiencing high average SNR, resulting in zero secrecy gap [18], [30]. Thus, with respect to Eve, there is no need for extra retransmissions. The second case occurs when both Bob and Eve have a very high signal quality, thus, both of them will be able to decode the packet successfully from the first round. Consequently, the adaptivity process, which was in favor of Bob and giving him better performance than Eve is no longer applicable. These two intuitive factual issues, which are verified by our performed results as it will be shown later, substantiate the key motivation for the next proposed design.

To overcome the problem of insecure transmission in the aforementioned scenarios, especially for those cases where

perfect secrecy is required over all expected SNRs, we propose a new, simple, practical and very effective security scheme, by which ARQ along with MRC is exploited for the first time in the literature for generating null-space independent artificial noise that can be automatically canceled at only the legitimate user without any extra processing. Particularly, an interfering signal (i.e, AN) based on the channel gain and QoS requirements of the legitimate user, is added on top (in the power domain) of the transmitted data signal $\mathbf{x}$ in each retransmitted round as shown in the upper part of Fig. 2. The added interfering AN signals[2] are designed in such a way that when they get combined at the receiver side using MRC process, they will compensate each other at the Bob's side only, while Eve will suffer a severely degraded performance. To achieve this, the designed AN, which does not depend on having null-space in the channel as opposed to the existing AN-based security schemes in the literature (e.g., [13], [16]), is properly added on top (power domain) of the time[3] domain signal vector to the first and second retransmission rounds, making the newly received signal vectors in the first and second rounds appear as

$$\mathbf{y}_{i,1} = h_{i,1}\left(\mathbf{x}+\mathbf{r}_1\right)+\mathbf{w}_{i,1} \tag{8}$$

$$\mathbf{y}_{i,2} = h_{i,2}\left(\mathbf{x}+\mathbf{r}_2\right)+\mathbf{w}_{i,2}, \tag{9}$$

where $\mathbf{r}_1 \in \mathbb{C}^{N\times 1}$ and $\mathbf{r}_2 \in \mathbb{C}^{N\times 1}$ are the added AN vectors to the first and second rounds, respectively. After MRC at the receiver side, $\hat{\mathbf{y}}_i$ becomes

$$\hat{\mathbf{y}}_i = \mathbf{y}_{i,1}h^*_{i,1}+\mathbf{y}_{i,2}h^*_{i,2} \tag{10}$$

$$\hat{\mathbf{y}}_i = \mathbf{x}\left(|h_{i,1}|^2+|h_{i,2}|^2\right) + \mathbf{r}_1|h_{i,1}|^2+\mathbf{r}_2|h_{i,2}|^2+\hat{\mathbf{w}}_i. \tag{11}$$

From (11), we find that it is possible to design $\mathbf{r}_1$ and $\mathbf{r}_2$ at the transmitter in such a way that ensures full cancellation of the added AN at only Bob as graphically depicted in the upper part of Fig. 2. To achieve this, $\mathbf{r}_1$ and $\mathbf{r}_2$ are designed to be a function of the legitimate user's channel power ($|h_{b,k}|^2$)

[2]For services other than voice, i.e., for the case of $L > 2$, we perform AN addition as follows. We first check whether L is odd or even, if it is even, we add AN with each retransmission round based on the corresponding channel responses, but if it is odd, then two design options can be used. Option I: we leave the last retransmission round without adding AN so that a balance in the added AN can be achieved and then AN can be canceled without changing the receiver structure. Option II: we add to the last retransmission round the opposite of the added AN in the first round; however, the legitimate receiver structure needs some modification in this case to properly cancel the added AN. Specifically, the second received round has to be combined with the first one using MRC and saved in buffer I, then the third received round has to also be combined with the first one using MRC and saved in buffer II. Finally, the content of buffer I can be added to that of buffer II in order to get an AN-free packet at the legitimate receiver. In this paper, we adopt using option I as it does not require receiver structure modification and can serve as the worst security scenario for the proposed scheme.

[3]It is important to note here that in a **multicarrier** system with multi-tap (frequency selective) channel, the AN signal will be added on top of the **frequency** domain of the transmitted signal. In this case, the received vector signals at both Bob and Eve in the k^{th} round can be modeled as $\mathbf{y}_{i,k} = \mathbf{H}_{i,k}\left(\mathbf{x}+\mathbf{r}_k\right)+\mathbf{w}_{i,k}$, where $\mathbf{H}_{i,k} \in \mathbb{C}^{N\times N}$ is the diagonal frequency response matrix of a multitap channel. The added AN signals will cancel each others at only Bob by using MRC in the frequency domain.

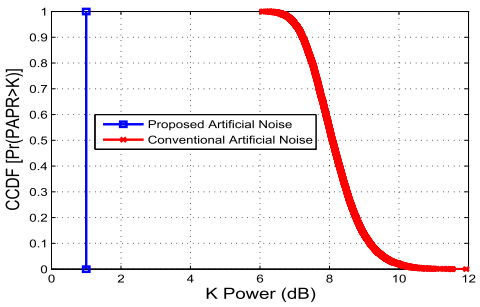


Fig. 3. Baseband peak-to-average power ratio (PAPR) comparison between the conventional AN-based methods with Gaussian distribution and our proposed AN design with uniform distribution.

and a random AN vector $\mathbf{g}$ as follows:

$$\mathbf{r}_1 = \frac{\mathbf{g}}{|h_{b,1}|^2}, \quad \mathbf{r}_2 = \frac{-\mathbf{g}}{|h_{b,2}|^2} \tag{12}$$

$$\mathbf{g} = \sqrt{\frac{\varphi}{2}}\left((2\mathbf{u}-1)+j(2\mathbf{q}-1)\right), \tag{13}$$

where $\mathbf{g} = [g_1\ g_2\ \cdots\ g_N]^T \in \mathbb{C}^{N\times 1}$ can be seen as an AN vector, whose samples change independently from one symbol to another according to a certain distribution. Therefore, $\mathbf{g}$ can also be perceived as a one-time pad key [31], whose length is equal to the message length with entropy equals to that of the message, and does not require to be shared with the receiver. It should be emphasized that although the AN vector in our scheme is perceived to be similar to one-time pad key in the sense that it can achieve perfect secrecy notion as described by Shannon with zero information leakage to Eve; it is however fundamentally different in the sense that the key (i.e., AN in our case) is not known to the receiver. It is also worth mentioning that the design of $\mathbf{g}$ gives freedom in: 1) modifying the structure (or distribution) of the added AN; 2) adjusting the power of the added AN, which is done based on the QoS requirements; and 3) controlling the PAPR problem resulting from the added AN by designing it to have a constant envelope with a uniform phase distribution. In the proposed scheme, $\mathbf{g}$ is deliberately designed to have a *uniform* phase distribution with a constant envelope (like a QAM signal) as in (13), in which φ is the power (variance) of the added AN vector and it is optimized based on the QoS requirements as well as the targeted security level as it will be shown later. Without loss of generality, $\mathbf{g}$ is properly designed so that PAPR problem can be avoided as uniform phase distribution has a constant envelope, resulting in a zero increase in the PAPR. To achieve this, the samples of $\mathbf{u}$ and $\mathbf{q}$ vectors are chosen to be Bernoulli-distributed random variables with values of ones and zeros. It should also be emphasized that most of the AN-based security methods existing in the literature are merely using Gaussian distributed noise, which leads to a significant increase in the PAPR as it does not have a constant envelope. To the best of our knowledge, PAPR problem has generally been ignored in the existing AN-based security methods, while this work sheds the light on this problem and proposes a practical solution to address this issue. Fig. 3 is drawn to show the huge difference

in the baseband PAPR between the conventional Gaussian distributed AN and the proposed uniformly distributed AN. It is evident from Fig. 3 that the proposed one, colored by a blue line, has a constant unity PAPR, while the PAPR of the conventional one is ranging from 6 dB to 12 dB (very high values causing power amplifier problems). Note that the proposed AN design has unity PAPR because oversampling and pulse shaping are not included in our design. However, the PAPR of a QPSK signal in passband (when up-sampling with pulse shaping is considered) will not be unity, but rather twice that of the baseband PAPR. It should also be mentioned that Fig. 3 shows only the PAPR of the added AN signal instead of the PAPR of the combination of the added AN signal and the original signal. The reason for that is the fact that adding the proposed AN signal to an M-PSK modulated signal of a constant amplitude will not affect the PAPR of the combined signal. However, in Section V, we will consider the PAPR of the combined signal because the AN vector there will be added to an OFDM signal of variable amplitude (not M-PSK signal of constant amplitude).

Aside from PAPR, having a uniform distribution is more desirable from a security perspective than Gaussian, because it has larger variance and creates complete randomness as well as full uncertainty in the added AN samples. Particularly, each sample value in $\mathbf{g}$ has equal probability and thus very high entropy, which is the same as the property of good secret keys [32].

At the receiving sides, the detected data signal vectors at both Bob and Eve become, respectively, as follows:

$$\hat{\mathbf{x}}_b = \mathbf{x} + \frac{\hat{\mathbf{w}}_b}{(|h_{b,1}|^2 + |h_{b,2}|^2)} \tag{14}$$

$$\hat{\mathbf{x}}_e = \mathbf{x} + \frac{\hat{\mathbf{w}}_e + \mathbf{r}_1|h_{e,1}|^2 + \mathbf{r}_2|h_{e,2}|^2}{(|h_{e,1}|^2 + |h_{e,2}|^2)}. \tag{15}$$

It should be clear that when the values of $\mathbf{r}_1$ and $\mathbf{r}_2$ are substituted in (11), the intentionally added AN gets totally canceled. Thus, the detected $\hat{\mathbf{x}}$ packet shown in (14) is the same as that in (4). This means that Bob's packet error rate (PER) performance will not be affected after employing this method whatsoever. Looking back at Eve's side, one can infer that since Eve neither knows the channel of Alice (due to using sounding techniques to estimate the channel in TDD systems) nor the added AN vector $\mathbf{g}$ (due to not sharing it with any communication party), a considerable degradation will occur whether Eve is using MRC or not. If she employs MRC, then an additional interfering noise resulting from non-zero subtraction process will affect her PER. On the other hand, if she does not employ MRC, then the AN added to each retransmission round will automatically affect her PER. It should be stated that the secrecy is enhanced by the proposed scheme because of 1) the added AN vector $\mathbf{g}$, and 2) the asymmetric CSI availability and the independence of channel states between Bob and Eve from one side and between different rounds from another side. Moreover, an additional source of secrecy can be obtained when the channel is not flat fading, but rather dispersive in time, frequency, or both. The details and investigation of the scheme in dispersive channels is beyond the scope of this paper and left for future works.

TABLE I

QoS LOOKUP TABLE [33] WITH POWER (φ) OF AAN REQUIRED TO ACHIEVE SECRECY

Service	Delay	L	PER_t	SNR_t^e	φ
Voice	100 ms	2	10^{-2}	30 dB	0.01
Video	150 ms	3	10^{-3}	40 dB	0.001

Although this method provides a good practical security performance against Eve without affecting the reliability (i.e., PER) of Bob, it is observed that this performance is achieved at the expense of extra retransmission rounds, causing small delay and slight throughput reduction, which can be fully controlled according to the secrecy and QoS requirements. This reduction happens since the first round of each transmitted packet might be received in error even at high SNR due to the added AN. Thus, a second retransmission is usually needed to compensate the intentionally introduced error (uncertainty) in the first round. In fact, this throughput degradation problem occurs due to most Wyner's secrecy codes proposed in the literature [3]–[7]. On the other hand, it was mentioned in the latest state-of-the-art security survey paper [3] that the joint design of secrecy, reliability, and throughput with delay are challenging tasks to be studied and hopefully resolved in the future as the three factors are coupled and influencing each other. To the best of our knowledge and based on the surveys in [2], [3], and [4], such an issue has not been comprehensively investigated from a practical perspective. Thus, besides the proposed design, this work also comes to put a step forward towards studying the mutual effect of these factors on each other, and to also find out the best trade-off that can ensure security without exceeding the QoS requirements determined by PER, delay, and throughput.

To mitigate the aforementioned throughput degradation's problem, we redesign the AN to be not only based on the channel of Bob but also on the QoS requirements of the requested service. Thus, adaptive AN (AAN) is added with just enough power to degrade Eve's reception, while trying to keep Bob's performance the same as it was before introducing the AN. The following steps summarize how to perform and employ the proposed security method in the context of LTE and future 5G and beyond networks:

1) The transmitter (Enode-B) determines which service the legitimate wireless user is intending to use.
2) According to the requested service, Enode-B (Alice) determines a PER threshold (PER_t) from a look-up table, as presented in Table I, which is required to reliably accommodate a legitimate user with the requested service.
3) Based on the determined PER and from the extensive off-line PER simulation results obtained for Eve, Enode-B identifies the corresponding required SNR for Eve (SNR_t^e) to eavesdrop the service reliably. It should be noted that SNR_t^e is determined from the off-line simulation results, which are shown in Fig. 5 (a) and Fig. 6 (a). Particularly, we determine the value of SNR_t^e at which Eve's PER becomes less than PER_t, which is required to use a certain service reliably.

4) From the found SNR, Enode-B calculates a rough numerical value of the needed noise power to sufficiently degrade Eve's performance using this formula, $\varphi = 10^{\frac{-SNR_t^e(dB)+10}{10}}$.
5) A uniformly distributed noise with the previously calculated power, is intentionally added on top of the transmitted packet in the first and second retransmission round in such a way that they will cancel each other after they get combined at only the intended receiver as explained before.

According to this method, it is noticed that in many daily used services such as voice and video, we do not actually need to have perfect secrecy to obtain a completely secure communication. That is because this method imposes Eve to operate in such a way that she is not able to achieve the QoS requirements necessary to intercept these services and use them reliably. Thus, there is no way to benefit from the undergoing service. Although we have targeted from the beginning to provide a good trade-off among reliability, throughput, delay and secrecy, our method shows that perfect secrecy can be achieved to provide fully secure messaging service at the expense of only half-throughput degradation. This is attained by making sure that the first packet transmission in the first round is always received in error, while the retransmitted packet in the second round can entirely cancel the noise added in the first round by sending an appropriate noise power. It is found by using extensive simulation that this can be achieved by making the variance of the added AN equal to the Bob's SNR value (i.e., $\varphi = SNR_{dB}$).

IV. Analytical Analysis of the Achievable Secure Throughput

Finding exact formula for the achievable secure transmission efficiency or secure throughput ($S\eta$) under the proposed ARQ scheme with and without AN would be useful and helpful to security designers in quantifying the exact achievable secrecy performance. In this work, $S\eta$ is determined by calculating the difference between Bob's throughput η^b and Eve's one η^e, where the throughput (η) itself is basically defined as the ratio of the number of information Packets Received Successfully (PRS) to the Total number of Transmitted Packets (TTP) including the retransmitted ones [23]. Thus, throughput (η) can be regarded as the complement of packet error rate (PER). The retransmitted packets are included in the throughput calculation in order to take the effect of the retransmission process on the average delay. Additionally, our analysis takes into consideration the implicit adaptivity process of ARQ along with MRC process. Also, practical discrete M-PSK signaling is considered in the analysis instead of the impractical Gaussian signaling in order to limit the peak transmission power and preserve low receiver complexity [16]. Given the aforementioned practical conditions, $S\eta$ can mathematically be defined as [30]

$$S\eta = \eta^b - \eta^e = \frac{PRS^b}{TTP} - \frac{PRS^e}{TTP} \tag{16}$$

$$= (1 - PER_L^b) - (1 - PER_L^e) \tag{17}$$

$$= PER_L^e - PER_L^b. \tag{18}$$

It is evident that all what we need to do now is to find Bob's average PER (PER_L^b) and Eve's one (PER_L^e) after L retransmission rounds, and then substitute them in (18) to find the net secure throughput. However, calculating PER of ARQ scheme analytically is not feasible as stated in the literature [23]. Although an approximate expression for the average PER of CC-HARQ after L^{th} round was recently given and discussed from the reliability and optimal power allocation perspectives in [24], but unfortunately it is not accurate at low SNR regimes. Moreover, from security point of view, Eve's performance comes into the picture, therefore, finding $S\eta$ requires not only finding exact Bob's PER, but also Eve's one. Motivated by all these factual challenges, we strive to find a simple closed-form expression for $S\eta$, which can practically reflect the achievable performance of the proposed security scheme.

By assuming that the effective SNR of the received combined signals at k^{th} round (i.e., accumulated SNR from all the retransmission rounds until the current k^{th} round) is defined by $\gamma_{b,\Sigma k} = \sum_{l=1}^{k}(\gamma_{b,l})$, whose joint probability density function (PDF) is given by $g_{\gamma_b}(\gamma_{b,\Sigma k})$; and by defining error probability relating function as $f(\gamma_{b,\Sigma k})$, PER_L^b can be expressed as [24]

$$PER_L^b = \int_0^\infty \cdots \int_0^\infty f(\gamma_{b,\Sigma 1}) \cdots f(\gamma_{b,\Sigma L}) \, g_{\gamma_b}(\gamma_{b,1}) \cdots g_{\gamma_b}(\gamma_{b,L}) d\gamma_{b,1} \cdots d\gamma_{b,L}. \tag{19}$$

According to [24], (19) can be simplified as follows:

$$PER_L^b = \int_0^\alpha g_{\gamma_b}(\gamma_{b,\Sigma L})\, d\gamma_b, \;\; \alpha = \int_0^\infty f(\gamma_b)\, d\gamma_b. \tag{20}$$

The difficulty of finding exact PER analytically is simplified when the effects of the retransmission parameters such as modulation, coding and combination are represented by a single transmission parameter. That is because α, which is called in the literature the waterfall threshold, can be taken from the simulation results of Bob's PER. Furthermore, α is related to a certain well-defined system model, which should be as close as possible to what happens in reality and the adopted parameters in the system design. Thus, α is a function of the transmission parameters, and is related to the instantaneous spectral efficiency (i.e. the accumulated information over a total number of transmitted information [λ]). Based on proposition (1) given in [24], PER_L^b can be written in terms of the cumulative distribution function (CDF) as

$$PER_L^b = F_{\gamma_b}^L(\alpha) = Pr\left(\sum_{k=1}^{L} \gamma_{b,k} < \alpha\right), \tag{21}$$

where $Pr()$ is the probability function, and $\sum_{k=1}^{L}\gamma_{b,k}$ is the sum of L statistically i.i.d. exponential random variables. More precisely, $\sum_{k=1}^{L}\gamma_{b,k}$ can be expanded as follows:

$$\sum_{k=1}^{L}\gamma_{b,k} = \gamma_{b,1} + \gamma_{b,2} + \cdots + \gamma_{b,L} \tag{22}$$

$$= \bar{\gamma}_{b,1}|h_{b,1}|^2 + \bar{\gamma}_{b,2}|h_{b,2}|^2 + \cdots + \bar{\gamma}_{b,L}|h_{b,L}|^2 \tag{23}$$

where, $\bar{\gamma}_{b,1} = \bar{\gamma}_{b,2} = \cdots = \bar{\gamma}_{b,L}$, since equal modulation and power allocation during retransmission process are adopted. Also, the power of the channel gain ($|h_{b,k}|^2$) in Rayleigh fading environment at k^{th} round follows an exponential distribution with PDF $f(x) = \frac{1}{\bar{\gamma}} e^{-x/\bar{\gamma}}$.

Hence, the distribution of the sum given in (23) follows a Gamma distribution, $\Gamma(L,\gamma) \equiv \text{Gamma}(L,\gamma)$, and if k is a positive integer, which is always the case in our system, then the distribution turns out to be Erlang with CDF given as

$$F^L_{\bar{\gamma}_b}(\alpha) = 1 - \sum_{m=0}^{L-1} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_b}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}. \tag{24}$$

By substituting (24) into (21), we get the accurate generic PER^b_L formula as follows:

$$PER^b_L(\bar{\gamma}_b, \alpha) = 1 - \sum_{m=0}^{L-1} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_b}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}. \tag{25}$$

For the case of $L = 2$, Bob's PER becomes as below

$$PER^b_L(\bar{\gamma}_b, \alpha) = 1 - e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)} - \frac{\alpha}{\bar{\gamma}_b} e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}, \tag{26}$$

where α is derived numerically from the extensive simulation results, that we have performed at different modulation orders (M) and different L values [25]. Next, we carried out fitting methods on the obtained simulation results to get a simple formula for α, which can be represented as

$$\alpha = 2^{\lambda} - 1, \quad \lambda = L \times \log_2(M) - 0.5, \ \lambda \geq 2.5. \tag{27}$$

The details of the simulation results used to perform curve fitting can be found in [25].

In the following, we present the analysis of Eve's PER denoted by PER^e_L first for the most two practical cases when $L = 2$ (related to voice service) and $L = 3$ (related to video service), and then in general for any L value. For voice service with $L = 2$, Eve's decoding error occurs when either 1) Eve's SNR in the first round is below the decoding threshold α, while Bob's one is above; or 2) when the accumulated SNR at Eve in the second round is still below the decoding threshold α, while Bob was below that threshold in the first round. Thus, Eve's PER can mathematically be written as

$$\begin{aligned} PER^e_L(\bar{\gamma}_e, \bar{\gamma}_b, \alpha) &= \underbrace{\left(F^1_{\bar{\gamma}_e}(\alpha)\right)}_{\text{Eve is in error at } k=1} \times \underbrace{\left(1 - F^1_{\bar{\gamma}_b}(\alpha)\right)}_{\text{Bob is in success at } k=1} \\ &+ \underbrace{\left(F^2_{\bar{\gamma}_e}(\alpha)\right)}_{\text{Eve is still in error at } k=2} \times \underbrace{\left(F^1_{\bar{\gamma}_b}(\alpha)\right)}_{\text{Bob was in error at } k=1}. \end{aligned} \tag{28}$$

It is obvious from (28) that Eve's PER not only depends on her channel condition, but also on Bob's channel and his success in decoding the packet before Eve is able to do so. After substituting the corresponding formulas of the CDFs into (28), Eve's PER becomes as

$$\begin{aligned} PER^e_L(\bar{\gamma}_e, \bar{\gamma}_b, \alpha) &= \left(1 - e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right) \times \left(e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right) \\ &+ \left(1 - \sum_{m=0}^{L-1} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_e}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right) \\ &\times \left(1 - e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right), \quad L = 2. \end{aligned} \tag{29}$$

Finally, by substituting PER^e_L given in (29) and PER^b_L given in (25) into (18), we get the achievable secure throughput ($S\eta$) for the adaptive ARQ scheme without adding AN as follows:

$$\begin{aligned} S\eta &= \left(1 - e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right)\left(e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right) \\ &+ \left(1 - \sum_{m=0}^{L-1} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_e}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right)\left(1 - e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right) \\ &- 1 + \sum_{m=0}^{L-1} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_b}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}, \quad L = 2. \end{aligned} \tag{30}$$

For the case of video service with $L = 3$, Eve's PER can mathematically be written as

$$\begin{aligned} PER^e_L(\bar{\gamma}_e, \bar{\gamma}_b, \alpha) &= \left(F^1_{\bar{\gamma}_e}(\alpha)\right) \times \left(1 - F^1_{\bar{\gamma}_b}(\alpha)\right) \\ &+ \left(F^2_{\bar{\gamma}_e}(\alpha)\right) \times \left(F^1_{\bar{\gamma}_b}(\alpha)\right) \times \left(1 - F^2_{\bar{\gamma}_b}(\alpha)\right) \\ &+ \left(F^3_{\bar{\gamma}_e}(\alpha)\right) \times \left(F^2_{\bar{\gamma}_b}(\alpha)\right), \quad L = 3. \end{aligned} \tag{31}$$

After substituting the corresponding formulas of the CDFs into (31), Eve's PER becomes as

$$\begin{aligned} &PER^e_L(\bar{\gamma}_e, \bar{\gamma}_b, \alpha) \\ &= \left(1 - e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right) \times \left(e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right) \\ &+ \left(1 - \sum_{m=0}^{L-2} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_e}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right) \\ &\times \left(1 - e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right) \times \left(\sum_{m=0}^{L-2} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_b}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right) \\ &+ \left(1 - \sum_{m=0}^{L-1} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_e}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right) \\ &\times \left(1 - \sum_{m=0}^{L-2} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_b}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right), \quad L = 3. \end{aligned} \tag{32}$$

Finally, by substituting PER^e_L given in (32) and PER^b_L given in (25) into (18), we can get the achievable secure throughput ($S\eta$) of the video service with $L = 3$.

For any service with any general L value, the generic formula of Eve's PER is also derived and given in the Appendix.

To get $S\eta$ under the adaptive AN-based method, we need to find the exact resulting distribution of γ_e, as well as to deliberately adjust the derived formula of α given in (27) by using fitting methods and according to the extra increase in the number of retransmissions caused due to the intentionally added AN. However, since finding the distribution of γ_e with AAN is extremely tedious and complex, we confine our

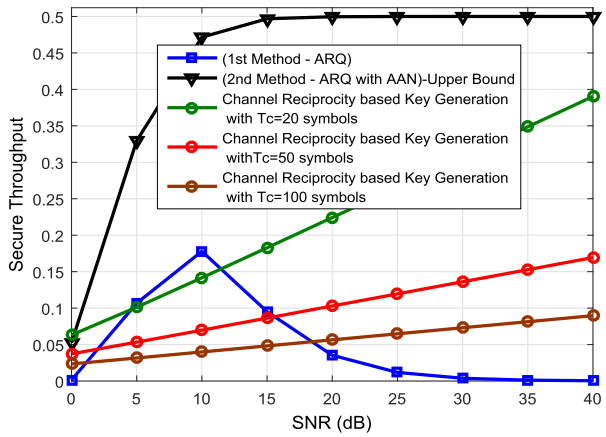


Fig. 4. The achievable secure throughput using the derived analytical results for voice service for $\alpha = 4.66$, which corresponds to BPSK with $L = 2$ over a block Rayleigh fading channel. The curve colored with blue represents Eq. (30), while the one colored with black represents Eq. (33). In addition, a comparison with channel reciprocity-based key generation approach [34] at different coherence block length (T_c) is drawn.

analysis for the case of perfect secrecy, which holds when sufficient AN power is allocated so that Bob can decode the packet successfully only at the second retransmission round, i.e., $\eta^b_{new} = \frac{1}{2}\eta^b$, while Eve is kept unable to decode any information packets, i.e., $\eta^e = 0$. This can be achieved by assigning sufficient power to the added AN, as discussed in the previous section ($\varphi = SNR_{dB}$). The upper bound of the achievable $S\eta$ for voice service ($L = 2$) can be given as

$$S\eta = \frac{1}{2}\eta^b = \frac{1}{2}\sum_{m=0}^{L-1}\frac{1}{m!}\left(\frac{\alpha}{\bar{\gamma}_b}\right)^m\left(e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right), \quad L = 2. \tag{33}$$

It is of importance to notice here that the secure throughput is exactly equal to the legitimate user's throughput as perfect secrecy is achieved in this case, where Eve's throughput approaches zero while Bob can cancel the AN vectors and thus correctly decode the signal only in the second round. Fig. 4 shows the achievable secure throughput using the derived equations in (30) and (33). It is shown that ARQ with AAN method significantly outperforms that of ARQ alone due to the added AN. Besides, since we assume that the channel randomness is securely shared between only the legitimate parties (which is practically possible in TDD systems by utilizing the property of channel reciprocity), it is insightful to compare our proposed scheme with those strategies that can be implemented under this assumption by mapping the shared random variable (i.e., channel realizations) to secret keys using schemes introduced in [34]. For this purpose, we provide a comparison with the channel reciprocity-based key generation approach [34] with coherence block-length (T_c) fixed at 20, 50, and 100 symbols. It is observed that our proposed scheme not only outperforms the channel-based key generation approach, but also its secrecy performance is more robust and immune to the coherence block-length, where T_c in our scheme is set to 432 symbols (i.e., equal to the packet size N); whilst the performance of the channel-based key generation approach is highly affected by T_c value as shown in Fig. 4.

V. Reducing PAPR and OOBE Besides Enhancing Secrecy in OFDM

The main objective of this section is to demonstrate how the new degree of freedom created by our proposed scheme in the power domain can intelligently be utilized to solve two major problems in the OFDM setup, while maintaining secrecy. As explained in Section III, to achieve secrecy, ARQ with MRC is exploited to add channel-based, QoS-guaranteeing, and null-space-independent AN that can inherently be canceled out at only the legitimate receiver by MRC. Besides secrecy, the added AN can be further exploited to attain other benefits. Specifically, the structure of the added AN can judiciously be redesigned to not only provide security, but also to reduce the PAPR and mitigate the OOBE in OFDM systems. Here, we reveal two new designs that can achieve the aforementioned goals. In the first design, the AN signal is optimized to reduce the PAPR subject to a certain secrecy constrain defined by the power level of the added AN; while in the second design, the AN signal is redesigned to minimize the OOBE subject again to a certain power level that indirectly represents a well-defined secrecy constraint.

Also, it is worth mentioning that the deployment of the proposed security method in multi-carrier systems makes the method more resilient to eavesdropping as multi-path frequency selective channels in OFDM bring more randomness. Specifically, the randomness of the added channel-based AN in the OFDM case does not only come from the randomly generated samples at the transmitter, but also from the randomness of the multi-path frequency selective channel.

A. Joint PAPR Reduction and Physical Layer Security Design

In a basic OFDM, the transmitted time domain signal can be modeled as

$$\mathbf{d} = \mathbf{G}\mathbf{F}^H\mathbf{s} \in \mathbb{C}^{[(N+T-1)\times 1]}, \tag{34}$$

where $\mathbf{s} \in \mathbb{C}^{[N\times 1]}$ is a set of QAM symbols in frequency domain, $\mathbf{F}^H$ is the N-point inverse discrete Fourier transformation (DFT) matrix, and $\mathbf{G} \in \mathbb{C}^{[(N+T-1)\times N]}$ is the CP addition matrix, where T is the number of channel taps. Unlike [16] and [35], which adds the AN in the time domain of the signal by exploiting the channel's null-space, in the proposed design, the newly designed AN signal $\mathbf{z} \in \mathbb{C}^{[N\times 1]}$ is added on top of the data symbols in the **frequency** domain by exploiting ARQ with MRC process, which is performed in the **frequency** domain too. Thus, the newly proposed transmitted signal can be written as

$$\mathbf{d} = \mathbf{G}\mathbf{F}^H(\mathbf{s} + (\mathbf{H}_f\mathbf{H}_f^H)^{-1}\mathbf{z}) \in \mathbb{C}^{[(N+T-1)\times 1]}, \tag{35}$$

where $\mathbf{H}_f \in \mathbb{C}^{[N\times N]}$ is the diagonal matrix of the channel frequency response with diagonal entries $\{H_1, H_2, \cdots, H_N\} \in \mathbb{C}^{[1\times N]}$. The baseband PAPR of the above-transmitted signal is the ratio between the maximum transmitted power and the average power, which can be given as

$$PAPR = \frac{\|\mathbf{G}\mathbf{F}^H(\mathbf{s} + (\mathbf{H}_f\mathbf{H}_f^H)^{-1}\mathbf{z})\|^2_\infty}{\frac{1}{N+T-1}\|\mathbf{G}\mathbf{F}^H(\mathbf{s} + (\mathbf{H}_f\mathbf{H}_f^H)^{-1}\mathbf{z})\|^2_2}. \tag{36}$$

The problem here reduces to finding the optimal AN vector $\mathbf{z}$ that can reduce the PAPR. Thus, the optimization problem to be solved can be formulated as follows:

$$\mathbf{z} = \arg\min_{\mathbf{z}} \ \|\mathbf{G}\mathbf{F}^H(\mathbf{s} + (\mathbf{H}_f\mathbf{H}_f^H)^{-1}\mathbf{z})\|_\infty^2$$
$$subject\ to \rightarrow \|\mathbf{z}\|_2^2 \leq \frac{\lambda \times \|\mathbf{s}\|_2^2}{\|(\mathbf{H}_f\mathbf{H}_f^H)^{-1}\|_2}, \quad (37)$$

where the percentage of the power used by the AN signal is controlled by $\lambda \in [0, 1]$ to achieve a certain pre-defined secrecy level, while making the PAPR as minimal as possible.[4] The objective function shows that we have a convex optimization problem that can numerically be solved by one of the advanced and powerful optimization solvers such as MOSEK. In this case, to obtain a precise numerical solution to (37), we adopt using YALMIP, a handy optimization package that can smoothly be integrated with MOSEK and MATLAB to solve complex optimization problems. The PAPR performance results of this design will be shown in Section VI.

B. Joint OOBE Reduction and Physical Layer Security Design

Now, we turn our attention to reduce the OOB power leakage by redesigning and optimizing the AN structure subject to a secrecy constraint defined by the power level of the added AN. Before we start with the design, we need first to determine the main signal spectrum and the interfering part of the signal. The spectrum of the transmitted OFDM signal can be given as

$$\mathbf{S}_{\zeta N} = \|\mathbf{F}_{\zeta N}\left(\mathbf{G}\mathbf{F}^H\mathbf{M}(\mathbf{s} + (\mathbf{H}_f\mathbf{H}_f^H)^{-1}\mathbf{z})\right)\|_2^2, \quad (38)$$

where, $\mathbf{M} \in \mathbb{C}^{N \times N_s}$ is a sub-carrier mapping matrix containing the N_s columns of $\mathbf{I}_N$ corresponding to the active data sub-carriers. Also, $\mathbf{F}_{\zeta N}$ is an $\zeta N \times (N + T - 1)$ DFT matrix, in which ζ is the oversampling factor used optionally to increase the resolution of the measured spectrum. Now, if we consider that there are ν sub-carriers, which are deactivated from the edge band of the OFDM signal spectrum, then the interference in the edge band can be given as

$$\mathbf{I}_\nu = \|\mathbf{F}_\nu\left(\mathbf{G}\mathbf{F}^H\mathbf{M}(\mathbf{s} + (\mathbf{H}_f\mathbf{H}_f^H)^{-1}\mathbf{z})\right)\|_2^2, \quad (39)$$

where $\mathbf{F}_\nu$ is a sub-matrix of $\mathbf{F}_{\zeta N}$, and comprised of only the rows that are related to the sub-carriers set as a guard band, or occupied by an edge user. To minimize the interference leakage in the edge band, we formulate the following optimization problem that has to be solved for $\mathbf{z}$

$$\mathbf{z} = \arg\min_{\mathbf{z}} \ \|\mathbf{F}_\nu\left(\mathbf{G}\mathbf{F}^H\mathbf{M}(\mathbf{s} + (\mathbf{H}_f\mathbf{H}_f^H)^{-1}\mathbf{z})\right)\|_2^2$$
$$subject\ to \ \rightarrow \|\mathbf{z}\|_2^2 \leq \frac{\lambda \times \|\mathbf{s}\|_2^2}{\|(\mathbf{H}_f\mathbf{H}_f^H)^{-1}\|_2}. \quad (40)$$

[4]It should be emphasized that the optimization problem can be reformulated in another way, i.e., to design the AN that maximizes the secrecy performance subject to a certain PAPR constraint. However, since the resulting problem formulation in this case would be non-convex (has no solution) and also may seem impractical as it requires Eve's channel, we instead formulate the problem of minimizing the PAPR (which is a hardware limiting factor, where it may impede the implementation of the security technique if it does not comply with it) subject to a certain power constraint on the added AN, which indirectly resembles the targeted secrecy performance.

TABLE II
SYSTEM SPECIFICATIONS

Parameter	Setting Value
Maximum number of retransmission (L)	2 (for voice), 3 (for video)
Packet size	432 symbols
CRC Size	32 bits
Modulation	BPSK
Receiver structure	MRC on a symbol level basis
Channel type	Block Rayleigh fading, where retransmitted packets experience independent channel gains [7]

The solution to this problem can numerically be obtained using efficient optimization solvers. Here, we again select MOSEK as our solver due to its efficiency and accuracy.

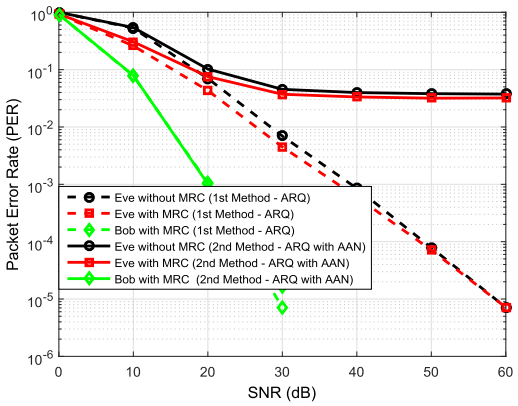
The effectiveness of the proposed optimization problems in reducing PAPR and OOBE of OFDM will be exhibited in the next section by using computer simulations. Future work regarding this section can include conducting thorough investigation and analysis alongside finding analytical closed-form solutions for the above formulated problems.

VI. SIMULATION SCENARIO AND RESULTS

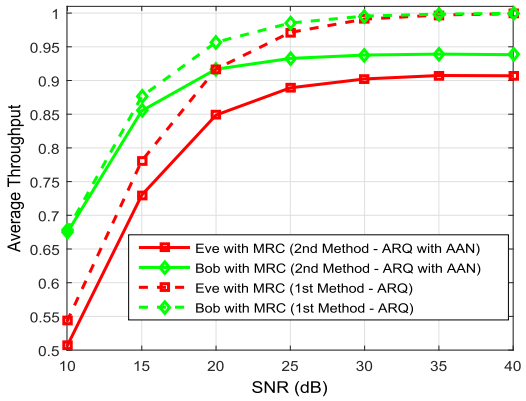
The simulation results are divided into three phases: the first is related to ARQ with MRC; the second is associated to ARQ with MRC and AN; whereas the third is concerned to PAPR and OOBE in OFDM system using the aforementioned formulated optimization problems that are based on the proposed ARQ with AN design. The adopted system specifications for the first two phases are listed in Table II.

To investigate the obtained performance; average PER as well as average throughput of both Bob and Eve, secure throughput, and the delay caused by the adopted ARQ scheme; are all evaluated and characterized. Thus, a comprehensive picture of the whole system performance is drawn, which eventually helps not only in quantifying the achievable performance, but also in understanding the trade-off among the different service requirements in terms of secrecy, reliability, throughput, and delay.

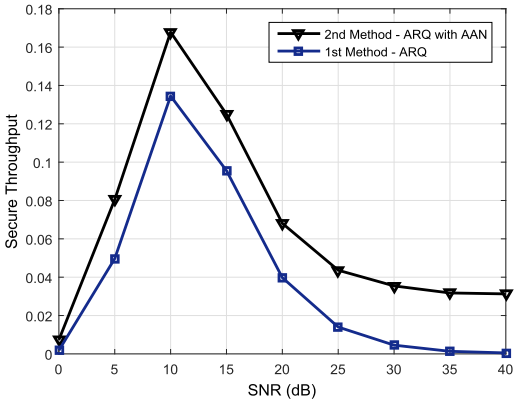
In Fig. 5 (a), voice service with $L = 2$ is targeted to be secured. It is evident that there is a PER secrecy gap between Bob and Eve at comparable SNRs due to the implicit adaptivity resulting from ARQ along with MRC, which is basically in favor of Bob but not Eve as explained earlier. This happens because Bob can ask for retransmission according to his channel conditions, while Eve cannot. Although ARQ with MRC can provide a noticeable PER secrecy gap, it is insufficient for providing a secure voice service at high SNRs because Eve's PER becomes less than a certain threshold needed for using the voice service reliably. More specifically, at SNR values above 30 dB, Eve's PER becomes less than 10^{-2}, therefore voice service becomes insecure as Eve can reliably decode the service. To combat this problem, the proposed method, ARQ with AAN, is used, where we add to the data packet an AAN that is designed based on the QoS and the channel between the legitimate parties. Thus, in the second part of our simulations, the AAN block shown in Fig. 2 is switched on. Now, AAN



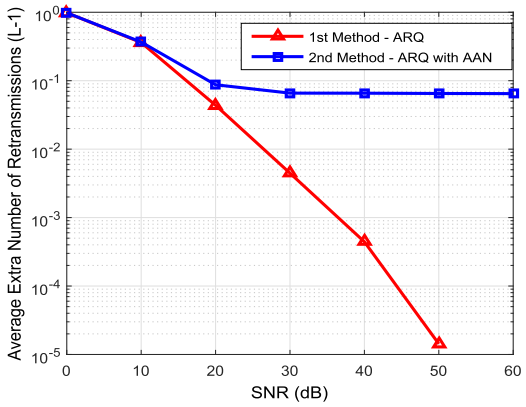
(a) Packet Error Rate (PER) vs SNR



(b) Average Throughput vs SNR



(c) Secure Throughput vs SNR



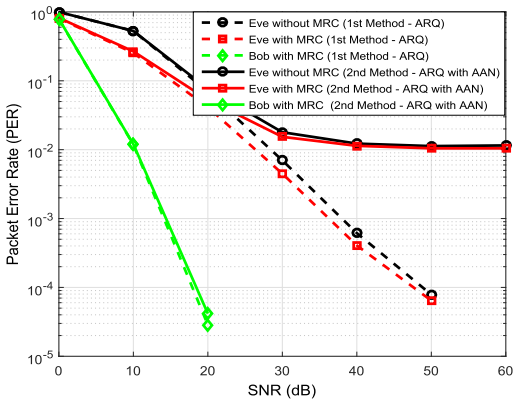
(d) Delay (L-1): Average retransmission percentage vs SNR

Fig. 5. Reliability, security and throughput performance comparison between ARQ without and with AAN with $\varphi = 0.01$ for providing a secure voice service ($L = 2$).

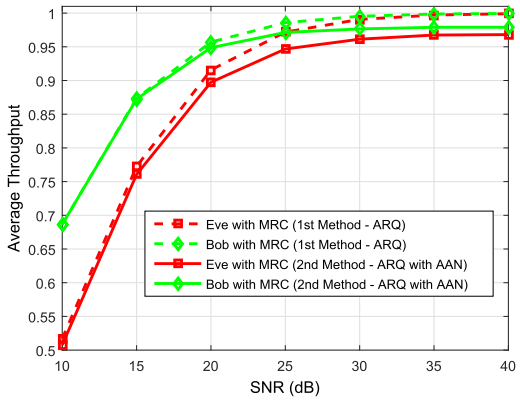
is added according to the QoS requirements of the voice service, which is determined (as reported in LTE standard) in terms of PER being $\leq 10^{-2}$ and L being ≤ 2 as presented in Table I, where packet delay budget is determined to be less than 100 ms [33]. Fig. 5 (a) shows the PER performance of the new proposed method. It is clear that the gap between Bob and Eve is significantly increased. Consequently, voice service is now secured at any SNR Eve may have (i.e., at any distance Eve may be located from the base station). However, Fig. 5 (b) shows that the proposed AAN-based method is accompanied by a slight throughput degradation due to the tiny increase in the average extra number of retransmissions ($L-1$). This can be explained by the fact that adding AN will mostly cause receiving the first transmission round of each packet in error, which will force Bob to ask for retransmission to cancel the added AN. Fig. 5 (c) depicts that ARQ with AAN method not only increases secrecy, but also ensures it at high SNR values unlike ARQ alone. Fig. 5 (d) presents the exact effect of the proposed method on increasing the average extra number of retransmissions, where it is exhibited that the resulting gain in the secure throughput comes at the expense of a tiny increase in the percentage of the retransmitted packets, which anyway lies within the QoS requirements of the voice service.

Fig. 6 is devoted to illustrate the exact obtained performance using the proposed design for conversational (live streaming) video service ($L = 3$) [33]. Here, we add AN only to the first and second rounds, while the third round is left free of noise. It is made like this to balance the added AN so that it gets canceled after MRC process. In Fig. 6 (a), it is exhibited that Bob's PER is kept $<10^{-3}$ with respect to the QoS requirement of the video service as presented in Table I, while Eve's PER is kept $>10^{-3}$, resulting in a secure video service at any SNR. Fig. 6(b) shows that the throughput degradation in case of video service is less than that of voice since lower AN power is added ($\varphi = 0.001$). Fig. 6 (c) confirms that secrecy has been maintained even at high SNR. Fig. 6(d) shows the extra small delay caused in case of using the second method. It is depicted that at SNR $\geq$ 30 dB, the receiver asks the retransmission of only one packet out of each 100 packets[5] to cancel the effect of the added AN so that secure video service can be achieved. Thus, security is achieved without exceeding the QoS requirements of the targeted service.

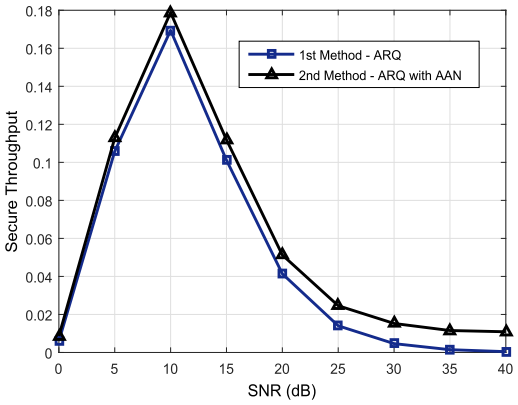
[5]This is because the power of the added AN is so small ($\varphi = 0.001$ from Table I) that it does not even harm Bob's reception in most of the cases, while it is significantly impacting Eve's performance.



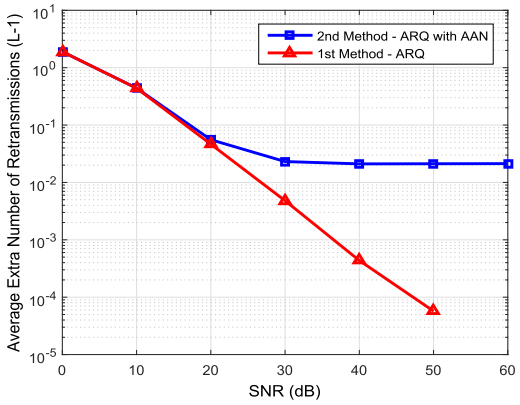
(a) Packet Error Rate (PER) vs SNR



(b) Average Throughput vs SNR

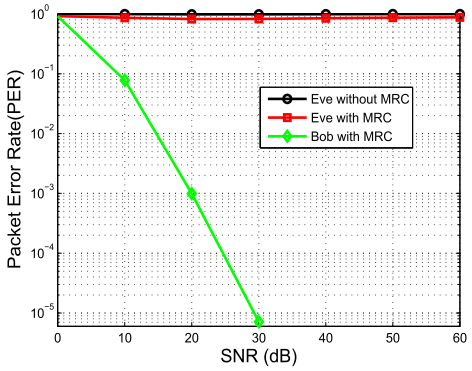


(c) Secure Throughput vs SNR

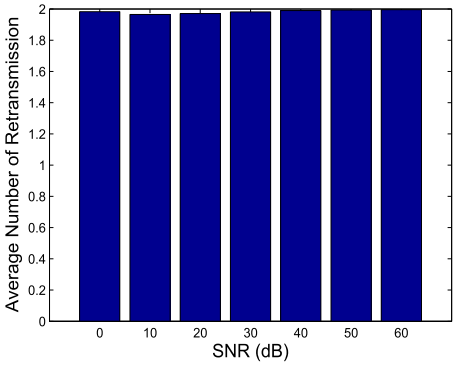


(d) Delay (L-1): Average retransmission percentage vs SNR

Fig. 6. Reliability, security and throughput performance comparison between ARQ without and with AAN with $\varphi = 0.001$ for providing secure video service ($L = 3$).



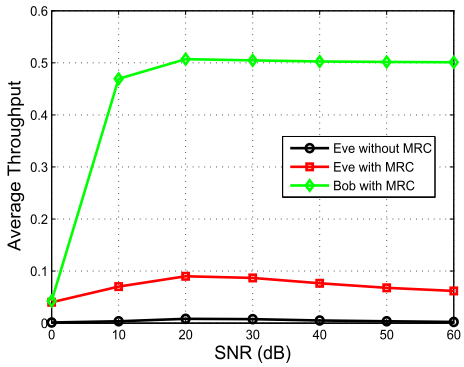
(a) Packet Error Rate (PER) vs SNR



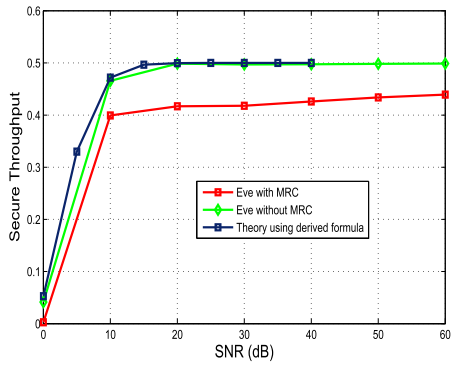
(b) Average number of retransmissions (L)

Fig. 7. Reliability performance comparison between Bob and Eve when sufficient AN power is added to provide close to perfect secrecy at ($L = 2$).

Fig. 7 and Fig. 8 present the comprehensive performance of the proposed method in case of TCP-based services such as web browsing, E-mail, chatting, messaging, FTP, P2P file sharing, etc. Since the content of all these services is basically text, it is highly desirable from a practical point of view to perfectly secure it. This is because of the fact that any information leakage will explicitly cause disclosing some text content to the eavesdropper, who is capable of doing complex processing to guess what was the content. To achieve this, Eve's PER should be as close as possible to unity (worst performance), which results in zero throughput to Eve, i.e., perfect secrecy. Such a target is shown to be achievable by our proposed method through allocating sufficient noise power ($\varphi = SNR_{dB}$) to the two rounds ($L = 2$). Specifically, Fig. 7 (a) shows the PER performance comparison between Bob and Eve. It is clear that Eve's PER is exactly one without MRC, and around 0.9 (very close to one) with MRC. In Fig. 7 (b), it is pictured that the average number of retransmissions (L) for all SNR



(a) Average Throughput vs SNR



(b) Secure Throughput vs SNR

Fig. 8. Throughput and security performance comparison between Bob and Eve using sufficient AN power to provide perfect secrecy at ($L = 2$).

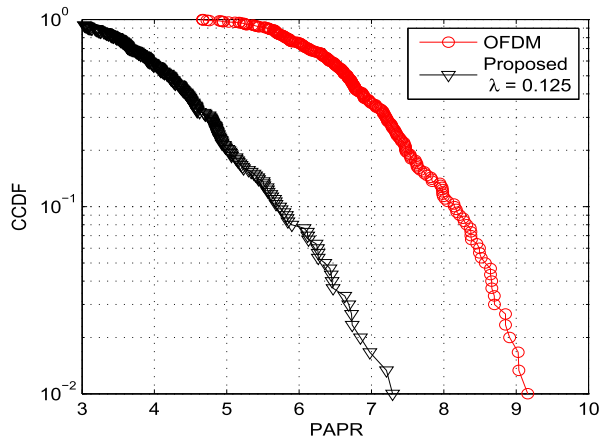


Fig. 9. CCDF of baseband PAPR, where the proposed security design is exploited for reducing PAPR.

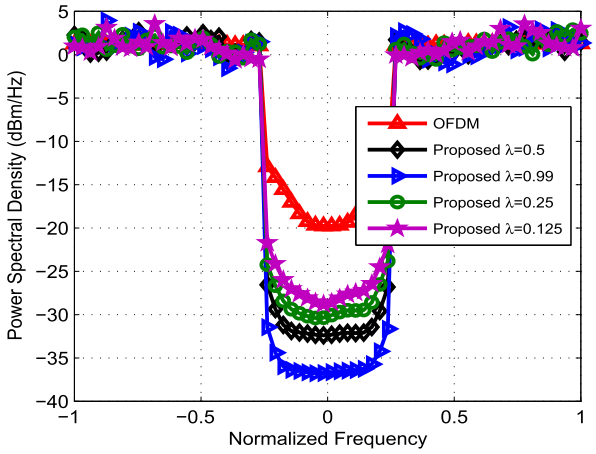


Fig. 10. Out-off-band emission (OOBE) reduction performance at different λ values, where the proposed security design is utilized to reduce OOBE. The number of deactivated sub-carriers (ν) is one forth of the total number of sub-carriers (N).

values is almost 2 as expected due to the added high AN power. On the other hand, throughput and secrecy performance comparison between Bob and Eve is drawn in Fig. 8, where it is evident that the secure throughput performance shown in Fig. 8 (b) is almost the same as Bob's average throughput shown in Fig. 8 (a). From these comparisons, it is obvious that the degradation in the legitimate receiver's throughput turns out to be a secure throughput in the case of perfect secrecy, which is needed for messaging and web services. Moreover, Fig. 8 (b) exhibits that the analytically derived equation of the upper bound secure throughput given in (33) matches the obtained simulation results. Thus, without exceeding L set by the protocol nor degrading PER performance of the legitimate user, a practically perfect secure service transmission is achieved.

Finally, to show the effectiveness of the proposed method in mitigating PAPR and OOBE besides security in multi-carrier systems, the method is used and simulated in a standard OFDM system. In this system, the number of sub-carriers is set to 64 and the CP length is set to be equal to the channel spread length. Fig. 9 shows the PAPR performance of the OFDM system that uses the proposed joint MAC/PHY design of ARQ with AN compared with a conventional OFDM that does not use the proposed AN design. Note that the AN vector in this case is obtained from the solution of the optimization problem formulated in (37). It is clear that there is a remarkable PAPR reduction due to the adoption of our proposed method.

In order to evaluate the capability of the proposed method in reducing OOBE, we assume that there is an adjacent user transmitting its OFDM signal over 16 subcarriers located at the edge of the OFDM transmission band. Fig. 10 shows the OOBE performance of an OFDM scheme that uses the proposed ARQ with AN design, compared with the conventional OFDM. Note that the AN vector in this case is obtained from the solution of the optimization problem formulated in (40). It is clear that there is a significant reduction in OOBE due to the adoption of our proposed method. It is also shown that as we increase λ (the power of the added AN signal with respect to the power of the transmitted OFDM signal), the OOB interference reduces more.

VII. Conclusion

A practical, effective, and cross PHY-MAC layer security method is proposed for securing any service requested by legitimate users. Particularly, ARQ along with MRC and AN have jointly been exploited to develop an eavesdropping-resilient

system. This has been achieved by intentionally adding a properly well-designed channel amplitude-dependent, null-space-independent, PAPR-aware, and QoS-based (adaptive) AN on top (superimposed in the power domain) of the transmitted data packets in such a way that the added AN vectors cancel each other at only the legitimate receiver, while severely deteriorating Eve's performance. It has been shown that without exceeding the QoS requirements set by the current LTE standard, and without degrading PER performance of the legitimate user, perfect secure service transmission can be achieved. For some services such as voice and video, it is observed that secure transmission can be attained by just forcing Eve to operate below the defined QoS requirements (unsatisfied QoS for Eve). Thus, security is guaranteed without sharing a secret key, nor imposing any changes in the receiver structure, making it a very suitable candidate technique for future 5G and beyond wireless networks as well as for low complexity Internet of Thing (IoT) devices. Besides, the proposed scheme is shown to help reduce the PAPR and OOBE of OFDM-based waveforms.

APPENDIX

For the case of general L, which corresponds in practice to any type of delay-tolerant services such as web-browsing, chatting, FTP, etc., the generic formula of Eve's PER can be given as

$$\begin{aligned} &PER_L^e(\bar{\gamma}_e, \bar{\gamma}_b, \alpha) \\ &\quad = \left(F^1_{\bar{\gamma}_e}(\alpha)\right) \times \left(1 - F^1_{\bar{\gamma}_b}(\alpha)\right) \\ &\qquad + \sum_{v=1}^{L-2} \left(F^{v+1}_{\bar{\gamma}_e}(\alpha)\right) \times \left(F^{v}_{\bar{\gamma}_b}(\alpha)\right) \times \left(1 - F^{v+1}_{\bar{\gamma}_b}(\alpha)\right) \\ &\qquad + \left(F^{L}_{\bar{\gamma}_e}(\alpha)\right) \times \left(F^{L-1}_{\bar{\gamma}_b}(\alpha)\right). \end{aligned} \tag{41}$$

After substituting the corresponding formulas of the CDFs into (41), Eve's PER becomes as

$$\begin{aligned} &PER_L^e(\bar{\gamma}_e, \bar{\gamma}_b, \alpha) \\ &\quad = \left(1 - e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right) \times \left(e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right) \\ &\qquad + \sum_{v=1}^{L-2} \left(1 - \sum_{m=0}^{v} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_e}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right) \\ &\qquad \times \left(1 - \sum_{m=0}^{v-1} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_b}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right) \\ &\qquad \times \left(\sum_{m=0}^{v} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_b}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right) \\ &\qquad + \left(1 - \sum_{m=0}^{L-1} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_e}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_e}\right)}\right) \\ &\qquad \times \left(1 - \sum_{m=0}^{L-2} \frac{1}{m!} \left(\frac{\alpha}{\bar{\gamma}_b}\right)^m e^{\left(-\frac{\alpha}{\bar{\gamma}_b}\right)}\right). \end{aligned} \tag{42}$$

Finally, by substituting PER_L^e given in (42) and PER_L^b given in (25) into (18), we can get a generic formula for the achievable secure throughput ($S\eta$) for any service with any L value. Note that the generic expression of Eve's PER given in (42) reduces to (29) when $L = 2$, and to (32) when $L = 3$.

ACKNOWLEDGMENT

The authors would like to deeply thank Dr. Z. Esat Ankarali, Haji M. Furqan, and the anonymous reviewers for their detailed, helpful comments and thoughtful, constructive suggestions that undoubtedly helped enhance the quality of the paper.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[3] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[4] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.

[5] Z. Mheich, M. Le Treust, F. Alberge, P. Duhamel, and L. Szczecinski, "Rate-adaptive secure HARQ protocol for block-fading channels," in *Proc. EUSIPCO*, 2014, pp. 830–834.

[6] M. Le Treust, L. Szczecinski, and F. Labeau, "Secrecy & rate adaptation for secure HARQ protocols," in *Proc. IEEE Inf. Theory Workshop*, Sep. 2013, pp. 1–5.

[7] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1591, Apr. 2009.

[8] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 883–894, Jun. 2012.

[9] S. Tomasin and N. Laurenti, "Secure HARQ with multiple encoding over block fading channels: Channel set characterization and outage analysis," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 10, pp. 1708–1719, Oct. 2014.

[10] C. W. Wong, J. M. Shea, and T. F. Wong, "Secret sharing in fast fading channels based on reliability-based hybrid ARQ," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, Nov. 2008, pp. 1–7.

[11] C. Thai, J. Lee, and T. Q. S. Quek, "Physical-layer secret key generation with colluding untrusted relays," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1517–1530, Feb. 2016.

[12] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secret key generation using channel quantization with SVD for reciprocal MIMO channels," in *Proc. Int. Symp. Wireless Commun. Syst.*, Sep. 2016, pp. 597–602.

[13] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[14] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[15] E. Guvenkaya and H. Arslan, "Secure communication in frequency selective channels with fade-avoiding subchannel usage," in *Proc. IEEE Int. Conf. Commun. Workshop (ICC)*, Jun. 2014, pp. 813–818.

[16] H. Qin *et al.*, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2717–2729, Jun. 2013.

[17] Z. E. Ankarali and H. Arslan, "Cyclic feature suppression for physical layer security," *Phys. Commun.*, vol. 25, pp. 588–597, Dec. 2016.

[18] J. M. Hamamreh and H. Arslan, "Secure orthogonal transform division multiplexing (OTDM) waveform for 5G and beyond," *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1191–1194, May 2017.

[19] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Secure pre-coding and post-coding for OFDM systems along with hardware implementation," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 1338–1343.

[20] J. Choi, "On channel-aware secure HARQ-IR," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 2, pp. 351–362, Feb. 2017.
[21] S. Kundu, D. A. Pados, and S. N. Batalama, "Hybrid-ARQ as a communications security measure," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, May 2014, pp. 5681–5685.
[22] J. M. Hamamreh, E. Guvenkaya, T. Baykas, and H. Arslan, "A practical physical-layer security method for precoded OSTBC-based systems," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2016, pp. 1–6.
[23] H. Mukhtar, A. Al-Dweik, M. Al-Mualla, and A. Shami, "Low complexity power optimization algorithm for multimedia transmission over wireless networks," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 1, pp. 113–124, Feb. 2015.
[24] S. Ge, Y. Xi, S. Huang, and J. Wei, "Packet error rate analysis and power allocation for CC-HARQ over Rayleigh fading channels," *IEEE Commun. Lett.*, vol. 18, no. 8, pp. 1467–1470, Aug. 2014.
[25] J. M. Hamamreh, M. Yusuf, T. Baykas, and H. Arslan, "Cross MAC/PHY layer security design using ARQ with MRC and adaptive modulation," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2016, pp. 1–7.
[26] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 2067–2076, Dec. 2011.
[27] D. Wang, P. Ren, Q. Du, Y. Wang, and L. Sun, "Secure cooperative transmission against jamming-aided eavesdropper for ARQ based wireless networks," *IEEE Access*, vol. 5, pp. 3763–3776, 2017.
[28] T. V. K. Chaitanya and E. G. Larsson, "Optimal power allocation for hybrid ARQ with chase combining in I.I.D. Rayleigh fading channels," *IEEE Trans. Commun.*, vol. 61, no. 5, pp. 1835–1846, May 2013.
[29] J. M. Hamamreh, E. Basar, and H. Arslan, "OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services," *IEEE Access*, vol. 5, pp. 25863–25875, 2017.
[30] E. Güvenkaya, J. M. Hamamreh, and H. Arslan, "On physical-layer concepts and metrics in secure signal transmission," *Phys. Commun.*, vol. 25, pp. 14–25, Dec. 2017.
[31] S. Liu, Y. Hong, and E. Viterbo, "Unshared secret key cryptography," *IEEE Trans. Wireless Commun.*, vol. 13, no. 12, pp. 6670–6683, Dec. 2014.
[32] C.-Y. Wu, P.-C. Lan, P.-C. Yeh, C.-H. Lee, and C.-M. Cheng, "Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1687–1700, Sep. 2013.
[33] *Policy and Charging Control Architecture*, document TS 23.203 V11.6.0, 3GPP, 2012.
[34] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.
[35] A. Tom, A. Sahin, and H. Arslan, "Suppressing alignment: Joint PAPR and out-of-band power leakage reduction for OFDM-based systems," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1100–1109, Mar. 2016.

Jehad M. Hamamreh received the B.Sc. degree in electrical and telecommunication engineering from An-Najah University, Nablus, in 2013. He is currently pursuing the Ph.D. degree with the Communications, Signal Processing, and Networking Center, Istanbul Medipol University, Turkey. Previously, he was a Trainee Researcher with the Department of Electrical and Computer Engineering, Texas A&M University at Qatar. His current research interests are in wireless physical and MAC layers security, including the design of advanced secure waveforms, new modulation techniques, and multiple access schemes for future 5G and beyond wireless systems.

Huseyin Arslan (S'95–M'98–SM'04–F'15) received the B.S. degree from Middle East Technical University, Ankara, Turkey, in 1992, and the M.S. and Ph.D. degrees from Southern Methodist University, Dallas, TX, USA, in 1994 and 1998, respectively. From 1998 to 2002, he was with the Research Group, Ericsson Inc., NC, USA, where he was involved in several projects related to 2G and 3G wireless communication systems. He was a part-time consultant for various companies and institutions, including Anritsu Company, Morgan Hill, CA, USA, and the Scientific and Technological Research Council of Turkey (TÜBITAK). Since 2002, he has been with the Electrical Engineering Department, University of South Florida, Tampa, FL, USA. He has also been the Dean of the College of Engineering and Natural Sciences, Istanbul Medipol University, since 2014. His research interests are in physical layer security, mm-wave communications, small cells, multicarrier wireless technologies, co-existence issues on heterogeneous networks, aeronautical (high-altitude platform) communications, *in vivo* channel modeling, and system design.

He has served as the technical program committee chair, the technical program committee member, the session chair and a symposium organizer, and the workshop chair of several IEEE conferences. He has also served as a member of the Editorial Board for the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, the Journal of *Physical Communication* (Elsevier), the *Journal of Electrical and Computer Engineering* (Hindawi), and the Journal of *Wireless Communication and Mobile Computing* (Wiley). He is currently a member of the Editorial Board for the IEEE SURVEYS AND TUTORIALS and the IEEE SENSORS JOURNAL.