Physical Communication 25 (2017) 14–25

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom

Review article

On physical-layer concepts and metrics in secure signal transmission[☆]

Ertuğrul Güvenkaya [a,*], Jehad M. Hamamreh [b], Hüseyin Arslan [a,b]

[a] *Department of Electrical Engineering, University of South Florida, Tampa, FL 33620, USA*
[b] *School of Engineering and Natural Sciences, Istanbul Medipol University, Istanbul 34810, Turkey*

ARTICLE INFO

Article history:
Received 23 March 2017
Received in revised form 12 August 2017
Accepted 12 August 2017
Available online 18 August 2017

Keywords:
Eavesdropping
PHY-security
Secrecy rate
Security gap
Wireless communications
Wireless fading channel

ABSTRACT

Communication secrecy in the wireless systems has unique challenges due to broadcasting nature of the radio waves, as compared to its wire-line counterpart. At the same time, different and independent perceptions of the transmitted signal by the legitimate receiver and the eavesdropper provide new opportunities for secure communication. The distinctness in the physical propagation environment, e.g., in received power, wireless channel, and location of the legitimate and illegitimate nodes, when coupled with random and unique signatures, can be exploited for secure communication without using secret keys. In this paper, fundamental stages as well as requirements of the physical layer (PHY) security in information transmission are reviewed from a novel perspective. Then, main performance metrics in secure communication are surveyed including from information theoretic measures to practical considerations along with associated generalizations. The presented comprehensive viewpoint of PHY security stages and metrics is helpful to better understand the techniques exploiting the physics to secure the information in the lowest layer of the communication system.

Contents

[☆] This paper is partially supported by the Scientific and Technological Research Council of Turkey (TUBITAK) under grant No. 114E244.

[*] Corresponding author.
E-mail addresses: ertugrul@mail.usf.edu (E. Güvenkaya), jmhamamreh@st.medipol.edu.tr (J.M. Hamamreh), arslan@usf.edu (H. Arslan).

http://dx.doi.org/10.1016/j.phycom.2017.08.011
1874-4907/

1. Introduction

The communication between distant entities requires exposing the message to outside world in some form of signal transmission. When the physical propagation medium between the transmitter and receiver is not perfectly secured, information transmission comes with confidentiality issues. That is, the transmitted signal is subject to be captured by an unintended third entity with not so good intention, i.e., eavesdropper. Security risk in the propagation can be due to protocol-based such as shared medium, or physical phenomenons such as wireless propagation of radio waves. In particular to wireless systems, although broadcasting nature of the radio waves provides benefits such as connectivity, support of mobility, and flexibility in communication distance, wireless transmission leads to security vulnerabilities due to the lack of physical boundaries preventing the eavesdroppers from capturing the transmitted message.

The key for achieving secure communication is to put the eavesdropper at a relative disadvantage compared to the legitimate receiver [1]. This can be performed by some cooperation between the transmitter and the receiver such as encryption/decryption, which has been a widespread method for securing the data in both storage and transmission phases. The other approach is to exploit the discrepancies in the physical characteristics of the propagation environment. Namely, nonidentical observations of the transmitted signal by the legitimate and illegitimate receivers, stemming from wireless channel, location, and antenna configurations can be the enabling factor for secure communication.

Fundamentals of the secure communication are laid by Claude Shannon [1]. He introduced the concept of perfect secrecy defined as the condition that observation of the signal by an eavesdropper does not provide any information about the secret message without any assumption on processing power and time. Shannon showed that this is achievable only if the secret key that is used for encryption is at least as large as the message itself. One-time pad cryptography is a well-known example of perfect secure system. This result is based on the assumption that the legitimate receiver and eavesdropper have identical observations of the signal. In other words, Shannon's limit is for the cryptographic approaches where all receiver nodes access the same signal without any additional effect [2]. The fact that cryptographic techniques reside in the upper layers of the communication stack supports this assumption since the data is assumed to be acquired from lower layer in an error-free manner [3].

When propagation medium is wireless channel, it is known that the signals captured by the legitimate receiver and eavesdropper follow different paths and experience distinct imperfections. After decades of Shannon's results, the secrecy under this condition was studied by Wyner [4]. Wire-tap channel is defined where the wire-tapper, i.e., the eavesdropper in wireless case, experiences a degraded version of the legitimate receiver's channel. Wyner revealed that it is possible to conduct a perfectly secure communication without using secrecy keys, but only when the main channel is relatively better than the eavesdropper's channel. Hence, the information theoretic notion of perfect secrecy has started the era of physical layer (PHY)-security, which is based on exploiting any form of physical characteristics in the nature of signal propagation in favor of legitimate nodes.

The path that Shannon and Wyner have opened in the secure communication constructs the theoretical limits on the secrecy of the systems. In other words, they follow the information-theoretic principles that focus on *how much one can secure the communication*, rather than *how to do it*. That is, practical aspects of the secure communication systems including secure transmission techniques, assumptions on the systems nodes, and practical metrics are also crucial along with the theoretical limits.

Recently, several elegant surveys on physical layer security have been introduced [5–7]. These surveys mostly focused on reviewing the studies and works performed in the literature comprehensively. Specifically, different organizational structures were adopted and followed in order to span and include the majority of the published security papers without much emphasis on the available secrecy metrics. However, in our paper, rather than intensely surveying the studies and techniques, we provide a conceptual and novel perspective on PHY security that can simplify its understanding to the researchers from one aspect and expand the domain of PHY security studies to include exploiting several reception stages from another aspect. Then, we comprehensively survey the secrecy performance metrics in a unified concept so that researchers can be aware of the available metrics, their meanings, and the differences among them. This will give freedom and flexibility to PHY security designers in choosing proper metrics to precisely evaluate the secrecy performance of their schemes.

In summary, this paper provides a comprehensive review for the fundamental stages of information transmission and corresponding requirements from the PHY layer security perspective in the presence of eavesdropper. These stages and requirements are explained by representing the information and the signals as points in the multidimensional message and signal spaces [8]. While eavesdropper can satisfy some of the requirements via having prior knowledge about the signal properties, the presented framework covers any type of knowledge level during the signal reception. Then, fundamental performance metrics for evaluating the security level along the mentioned stages are surveyed. We cover both information theoretic considerations and practical measures including both existing approaches and recent considerations. The outline of the paper is as follows: In Section 2, we explain the considered system model along with the preliminaries associated with a generic physical layer security scenario. Afterward, in Section 3, we present the fundamental stages that any receiver, in particular the eavesdropper, should pass for a successful reception. Then, main performance metrics for the physical security, including both information theoretic and practical measures are surveyed in Section 4. Finally, conclusions are given in Section 5.

2. System model and preliminaries

It is convenient here to define the structure of the system model and the communication entities considered in the security problem discussed in the paper. In the system model presented in Fig. 1, Alice is the legitimate transmitter that intends to confidentially send the secret message to the legitimate receiver, called Bob, in the presence of a third illegitimate node. The third node, which is a passive eavesdropper, called Eve, aims to obtain the secret message content from her own observations. Eve is generally assumed to have no limitations on its processing power

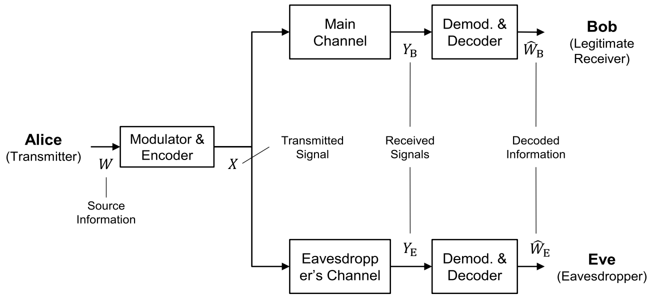

Fig. 1. Generic system model of the eavesdropping physical layer security problem, in which Alice tries to communicate confidentially with Bob without allowing Eve to get any useful information from the ongoing communication between the legitimate parties (Alice and Bob).

resources and computational capabilities. The confidential information message, W, is encoded into X of length n, and then sent through a wireless channel. The received signals at Bob and Eve are indicated by Y_B and Y_E, respectively. The entropy of the source information is given by $H(W)$, whereas the residual uncertainty (conditional entropy) for the eavesdropper's message is denoted by $H(W|Y_E)$. Now, based on the scenario and environment under consideration, the availability of channel state information (CSI) at the communication parties varies from complete to partial and even zero knowledge. However, in a practical wireless system, all communication parties can acquire some information about the channel between the transmitter and themselves. Moreover, Alice is assumed to have the CSI of the legitimate receiver by the means of exploiting the reciprocity of the channel in a time division duplex system or receiving CSI feedback from Bob. Furthermore, in spite of the fact that Alice has to practically be assumed to have no knowledge about Eve's channel as she is usually passive, one can find in the literature that Alice is sometimes assumed to know Eve's channel state [9–11]. This is justified by the fact that Eve can be considered a licensed user who has legal access to the network, but has a bad intention in eavesdropping the communication of other users in the network. One final notice to mention is the reality that Eve's and Bob's channels are usually assumed to be independent of each other due to the spatial de-correlation of the wireless channel response (i.e., channels de-correlate and become independent from each others if they are half wavelength apart).

3. Reception stages with eavesdropper

Information transmission can essentially be modeled as a series of transform operations. It includes mapping the information located in the message space to a waveform into the signal space at the transmitter. Then, the transmitted signal generally passes through multi-path and time varying channel. The multipath channel affects the signal selectively by warping the multidimensional space. For instance, frequency selective fading channels reshape the signal by changing the amplitude and phase of the signal along frequency domain. Similarly, any change in the propagation environment, in either small or large scale, creates selectivity in the time domain. These effects relocate the point in the signal space, i.e., signal, from its original location to another position. On top of that, any uncorrelated disturbance such as noise or interference creates uncertainty in the final position of the point. The additive uncertainty on the signal also defines the signal to noise plus interference ratio where the signal power is essentially the distance of the point to the origin. The receiver's task is to perform the reverse operation [8] as illustrated in Fig. 2. This representation can also be applied in the presence of an eavesdropper. When the security is concerned in transmission, making the demapping operation a hard task for the eavesdropper, along with effective transmission between the legitimate pair, becomes one of the main requirements.

As an adversary receiver, eavesdropper can possess different levels of prior knowledge on the legitimate signal transmission. For instance, Eve can have as much information as the legitimate receiver including transmission time, frequency, bandwidth, transmit filter, modulation format. On the other hand, she can have less information about the signal, e.g., only the spectral location and bandwidth, in other scenarios. Depending on the situation in this spectrum of knowledge levels, an eavesdropper has to satisfy certain conditions and pass through stages for a successful signal reception. In this section, we review the four main requirements, which an eavesdropper should already satisfy or attain via additional algorithms, as depicted in Fig. 3: Coverage, Detection, Interception, and Exploitation. Some examples for each stage are also summarized in the figure.

The motivation behind mentioning the stages required for successful reception is the fact that the leakage of channel and/or signal side information including transmission features to Eve [12] are critical factors for determining the secrecy level of a security scheme. Consequently, the assumption that Eve knows all the information about the signal except the message bits is somehow not a very realistic assumption and the impact of these details on the secrecy (Eve's uncertainty) may be significant in some practical scenarios. To support this, below we give several practical examples that demonstrate the significant importance of the stages presented in this paper:

(1) *Channel state information leakage to Eve*: This can significantly increase Eve's interception capability [13]. Most of the physical-layer security techniques highly depends on the fact that the forward link can be estimated from the reverse link by exploiting channel reciprocity (which is the case in TDD systems), making Eve unaware of the legitimate CSI, and thus unable to eavesdrop (intercept) the link. However, Eve may have the capability to know the legitimate CSI in some scenarios. For example, in practical FDD systems, CSI feedback from Bob to Alice is required, and since this feedback can be eavesdropped by Eve as it is usually sent publicly, the secrecy rate of the system is expected to decline.

(2) *Lack of channel state information knowledge at the transmitter alongside reciprocity mismatch*: In many security schemes proposed in the literature, some level of knowledge on Eve's CSI is required at Alice to achieve good secrecy rate. However, this rate is anticipated to decrease in practical scenarios, where Eve's CSI cannot be obtained at Alice due to her passive behavior [7]. Besides, channel reciprocity mismatch and outdated channel estimation of the legitimate and eavesdropper's links can have significant impact on the achievable secrecy level [14–16].

(3) *Channel estimation errors at Eve*: If the security scheme is designed in such a way to prevent Eve from estimating its channel correctly, then she cannot compensate the effect of severe fading on the received data, and thus she will not be able to intercept and perform the data detection process successfully [17–19]. Moreover, in [20], the authors proposed a discriminatory channel estimation (DCE) scheme to maximize the performance difference between Bob and Eve in MIMO wireless systems. The scheme utilizes a multistage training process and optimizes the performance of Bob's channel estimation, while degrading the performance of Eve's channel estimation. The basic idea is to take advantage of the channel estimates fed back from Bob to Alice in

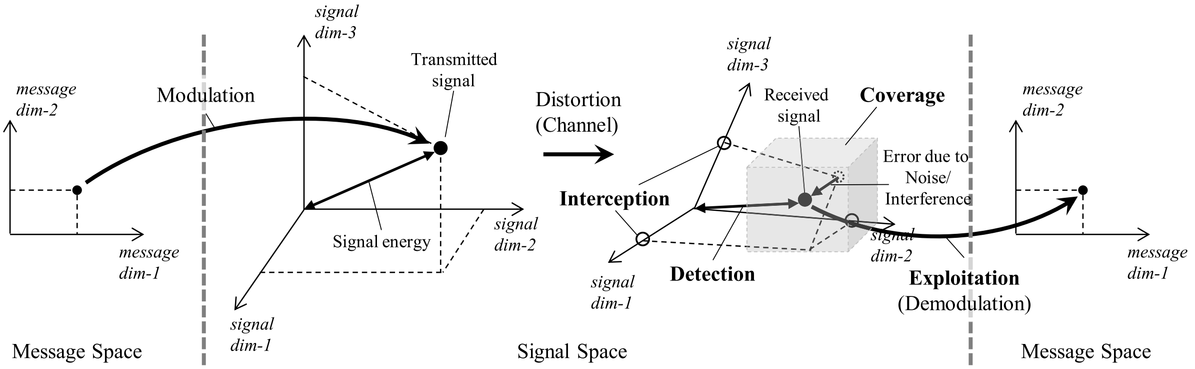

Fig. 2. Information transmission consists of mapping operations from message space to signal space at transmitter, channel effect with distortion via warping the signal space and addition of noise, and mapping back to message space at the receiver.

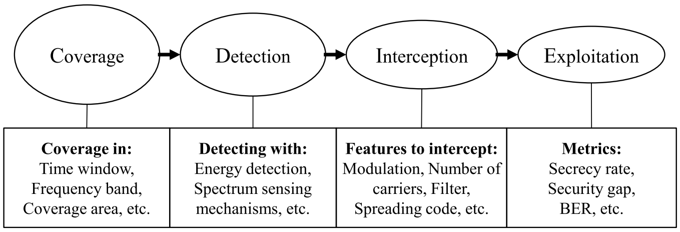
Coverage
Detection
Interception
Exploitation
Coverage in: Time window, Frequency band, Coverage area, etc.
Detecting with: Energy detection, Spectrum sensing mechanisms, etc.
Features to intercept: Modulation, Number of carriers, Filter, Spreading code, etc.
Metrics: Secrecy rate, Security gap, BER, etc.

Fig. 3. Stages of the overall reception mechanism at the eavesdropper.

order to enable the intelligent utilization of artificial noise (AN) in the training data sequence. Specifically, AN can deliberately be superimposed with the training sequence to degrade Eve's channel, while maintaining interference-free channel estimation at Bob. In [21], the authors introduced another scheme to improve upon their main discriminatory channel estimation (DCE) scheme proposed in [20], in which multiple stages of retraining and feedback were used. The idea of their improved scheme is basically to use a two-way training mechanism that allows the legitimate parties, Alice and Bob, to transmit training sequences to facilitate and ease channel estimation at both sides, while degrading Eve's channel. Both reciprocal and nonreciprocal channels were examined and a two-way DCE scheme was proposed for each scenario. In [22], a new two-way training method for DCE was proposed through exploiting a semi-blind method based on whitening-rotation. This enhanced scheme was shown to have two advantages over the existing schemes: first, it adopts a semi-blind strategy and achieves better DCE performance; and second, it is immune to the pilot contamination attack that can be launched and conducted by active eavesdroppers.

(4) *Hardware impairments*:

- *Synchronization errors*: It is possible to design the transmission technique in such a way that inhibits Eve from being able to synchronize with the time and frequency band of the transmitted packet. In such a scheme, Eve cannot compensate the effect of carrier frequency offset (CFO) and/or symbol time offset (STO) (caused by its local oscillator and sampling clock) on the received data, and thus severe performance degradation is expected due to the caused inter-symbol-interference (ISI) and inter-carrier-interference (ICI) in multi-carrier systems [23–25]. In [26], the cyclostationary feature of the cyclic prefix used for synchronization in OFDM was intentionally suppressed to provide secrecy by preventing Eve from detecting this feature accurately.
- *Non-linear conversion operation*: In [27], the nonideality of the eavesdropper's receiver was exploited to achieve security by ensuring the desired advantage that Bob has to have over Eve even when Eve can fully acquire the transmitted signal at its RF front end. Moreover, the power amplifier nonlinearity can be exploited for providing secrecy. Specifically, the transmitted signal can intelligently be designed in such a way to have large amplitude fluctuations at the input of the power amplifier at the adversary receiver, while having a smooth steady magnitude at the input of the legitimate receiver. Therefore, the amplified signal will exceed the saturation point (e.g., 1 dB compression point of the power amplifier), causing signal clipping and generating inter-modulation products. Thus, severe performance degradation in the BER and OOB emission leakage can occur as a result of PA impairments.
- *IQ imbalance and phase noise*. Authors in [28] illustrated the detrimental effects of IQ imbalance on the secrecy performance, and showed that IQ imbalance should be taken into account in the design of secure wireless systems. Moreover, it was demonstrated in [29] that phase noise can cause a significantly negative effect on the secrecy performance of the system. Thus, it has to intelligently be utilized in order to ban Eve from intercepting the transmitted signals, while guaranteeing minimum effect at the legitimate receiver.

In the light of the aforementioned practical examples, the following stages construct the framework for evaluating the wireless transmission and reception from information security perspective.

3.1. Coverage

The main task of a wireless transmitter is to map the source information in the message space to a particular signal in the signal space. Thus, a signal is represented as a point in the multidimensional space as shown in Fig. 2. This can also be regarded as electrospace, where each axis denotes time, frequency, space, code, etc.

The first requirement for an eavesdropper is to have a sufficient capability for capturing the transmitted signal. That is, Eve should be located within the coverage and in the direction of the transmitted signal. Also, the reception window of Eve needs to cover the signal of interest. As an example, the time window that eavesdropper is active must cover the frame of signal observed at the reception after passing through the channel. In addition to space and time, another domain of coverage is the spectrum. Receiver spectral window that is determined by the carrier frequency and the bandwidth should cover the transmitted signal band. In the multidimensional notion, this translates into the condition that the Eve's reception subspace, illustrated as shaded region in Fig. 2, should include the point which represents the signal after the channel. By satisfying this condition, eavesdropper can make observations that can result in a detection of the secret message. For the eavesdroppers with prior knowledge on signal properties regarding to coverage, this requirement is naturally satisfied via adjusting the reception parameters accordingly. Examples on techniques that exploit this stage to provide secrecy are: (1) antenna beam-forming, where the antenna beam (radiation pattern) is narrowed and oriented towards the location of the legitimate receiver only; (2) directional modulation [30], where the constellation points are defined only in the direction of the legitimate receiver, whereas the constellation points are distorted and scrambled in the other directions.

3.2. Detection

Knowing that the possible region of the signal under interest is covered, the next step is to decide if the signal is actually transmitted or not. The detection operation is a common problem in communication, specifically in cognitive radio systems that requires detection of other users' presence in the network via spectrum sensing mechanisms [31]. In general, detection can be connected to the energy of the signal that receiver examines via energy detection. In that respect, the detection performance is connected to the distance between the point representing the signal and the origin in the message space, which is illustrated in Fig. 2. Note that the power of the signal along a particular dimension in the signal space, compared to other dimensions, can be significantly different for the transmitted and received signals. This is because of the warping effect of wireless channel on the signal space. For instance, consider a broadband signal passing through a frequency-selective channel that can be represented as multiple orthogonal subchannels with flat fading [32]. In this case, each subchannel becomes a dimension in signal space in Fig. 2, and selective fading on each subchannel creates the effect of warping. Thus, the overall energy of the received signal determines the detectability of the existence of the signal in the presence of additional effects that create uncertainty in the exact position. That is, channel distortion is critical with noise and interference. The closer the point is located to the origin at Eve (and the farther for Bob), the lower probability for eavesdropper (the higher probability for Bob) to come with a successful binary decision about the signal's presence. A good example on techniques that exploit this stage to provide secrecy is Direct Sequence Spread Spectrum (DSSS), where the signal energy goes below the noise level, making Eve unable to detect the ongoing communication as the signals are hidden in the noise. It should be noted that this stage is closely related to the covert communication scenario, which has recently been discussed in detail from an information-theoretic perspective in [33].

3.3. Interception

After detection, further information about the transmitted signal is required for a reliable reception. The transmit filter type, modulation format, precoding matrix indicator (PMI), inter-leaver, number of subcarriers for multicarrier signaling, utilized code sequence for spread spectrum signals are all examples of signal features that the eavesdropper needs to intercept for a reliable decoding of the message. In other words, having prior knowledge on these properties can be considered as Eve having possible locations of the points in the multidimensional space. After detecting the signal covered by the receiver, these interception parameters provide the knowledge of all possible points that the signal resides in the signal space. The exact location of the corresponding point among other possibilities indeed provides the information content of the digitally modulated message. In spread-spectrum signals as an example, the knowledge of the spreading code clears the confusion of the receiver except possible locations in finite alphabet signal map, e.g., quadrature amplitude modulation constellation points. Another good practical example on exploiting this stage for providing secrecy is the secure waveform design presented in [34]. In this design, the information symbols in the message space are mapped to points (samples) in the signal space via using special expansion functions (transform bases), which are extracted form the channel of the legitimate receiver instead of using fixed exponential bases produced by IFFT and FFT as in OFDM. This makes Eve unable to perform the de-mapping operation correctly as her channel is different from Bob's channel.

It should be stated that the aforementioned signal features can be made adaptive based on the channel of the legitimate receiver only. In this case, a performance difference between Bob and Eve, resulting in a secrecy gap, is expected even if Eve can intercept the signal feature such as intercepting the selected PMI as was studied in [35].

3.4. Exploitation

The final stage is essentially a regular demodulation process with the assumption that all information about the signal is known except the modulated information. Hence, the exploitation of the signal at the end can be the decoding of the intercepted signal where conventional demodulation process, i.e., de-mapping the point from the signal space into message space as depicted in Fig. 2. The success in this stage is directly related to the amount of disturbance on the actual signal due to noise and interference. Thus, the aim in the secure transmission is to make the signal observed at the eavesdropper noisy, while keeping the distortion at the legitimate receiver minimum. As an example, a common technique is the insertion of artificial noise in the transmitted signal [36], by exploiting the dimension reduction at the receiver. The additional distortion component, artificial noise (AN), is selected from the nullspace of the intended receiver's channel, and hence, it disappears after passing through the wireless channel of the legitimate receiver. This eliminates the adverse effect on the reception performance for Bob. However, since AN is not aligned to the nullspace of the eavesdropper's channel, it creates uncertainty on the actual location of the transmitted signal. The concept of AN is illustrated in Fig. 4 in a 2×1 multiple-input single-output (MISO) transmission, where the transmitter has more antennas than each receiver in order to achieve a nonzero nullspace for the channels. In other words, the combination of the signals from two transmit antennas by a single antenna receiver corresponds to dimension reduction in the signal space from 2 to 1. Thus, the two dimensional signal in $d_1 - d_2$ plain is mapped to a point in one dimensional space. Then, after the channel, the main aim is to introduce additional distortion on the signal observed by Eve. In

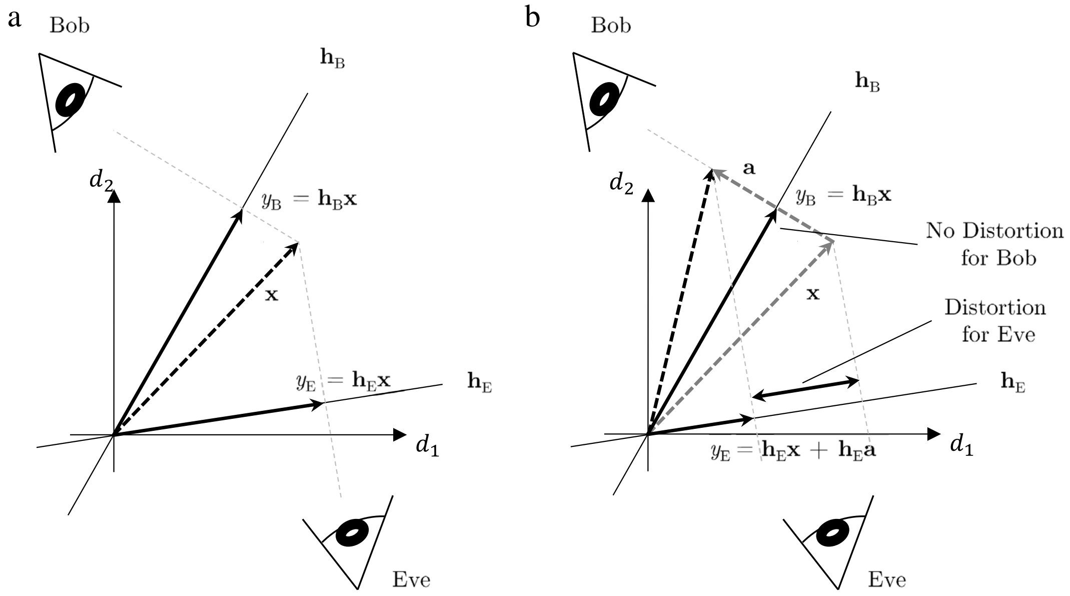
a
Bob
$\mathbf{h}_\mathrm{B}$
d_2
$y_\mathrm{B} = \mathbf{h}_\mathrm{B}\mathbf{x}$
$\mathbf{x}$
$y_\mathrm{E} = \mathbf{h}_\mathrm{E}\mathbf{x}$
$\mathbf{h}_\mathrm{E}$
d_1
Eve
b
Bob
$\mathbf{h}_\mathrm{B}$
$\mathbf{a}$
d_2
$y_\mathrm{B} = \mathbf{h}_\mathrm{B}\mathbf{x}$
No Distortion for Bob
$\mathbf{x}$
Distortion for Eve
$\mathbf{h}_\mathrm{E}$
$y_\mathrm{E} = \mathbf{h}_\mathrm{E}\mathbf{x} + \mathbf{h}_\mathrm{E}\mathbf{a}$
d_1
Eve

Fig. 4. (a) 2 × 1 MISO communication system where two dimensional transmitted signal $\mathbf{x}$ is mapped to one dimensional received signals y_B and y_E along the direction channels $\mathbf{h}_\mathrm{B}$ and $\mathbf{h}_\mathrm{E}$, respectively. (b) Artificial noise component $\mathbf{a}$ is selected along the orthogonal direction to the channel of Bob. Thus, the additional distortion is not observable by the legitimate receiver while it causes distortion at illegitimate receiver Eve.

other words, as two observers of the transmitted message in the signal space, the intended receiver exploits the signal effectively, while for the eavesdropper's demapping operation is much more challenging due to the additional uncertainty on the observed signal from her perspective.

Another example on techniques that utilize the exploitation stage is error control coding, which forms a substantial part in establishing reliable and secure communication when Eve's channel is a degraded version of Bob's one on average. After Wyner had proven the existence of channel codes that ensure both reliability and confidentiality as the block length tends to infinity, many researchers focused their efforts on the design and development of practical coding schemes that can achieve the secrecy capacity of various wiretap channels. Examples on these secrecy codes will be given alongside the information-theoretic secrecy metrics, surveyed in Section 4.

In general, the secrecy of the communication is measured from the exploitation perspective. This is because Eve is assumed to possess the same level of prior knowledge on the signal. Thus, the discrepancy between Bob and Eve is observable in the last stage. In the following sections, we will discuss the fundamental metrics used to measure the security in communication systems.

4. Metrics of secrecy in communication

Either for investigation of the limits of secrecy in a given system, or for the evaluation of the secrecy performance of a proposed scheme as well as for maximizing it, some numerical metrics have been developed most of which are adopted, or derived from the conventional communication metrics such as channel capacity, signal-to-noise ratio (SNR), and bit error rate (BER). The measures for the secrecy of the system can be considered under two main categories. The first type is information theoretic measures that do not specify a certain communication signaling and protocol, but generally consider the limits of the secrecy which are independent of the applications and underlying procedures. The second type is based on practical measures where the secrecy level is quantified by the metrics that can be observed in practical communication scenarios.

It should also be noted that in security design, the secrecy performance measure is highly related and dependent on the stage exploited for providing secrecy. More precisely, based on the stage (i.e., coverage, detection, interception, or exploitation) that a certain security technique exploits, specific secrecy metrics can be used to quantify the obtained secrecy performance properly. Interestingly, most of the secrecy metrics developed in the literature are related to the exploitation stage, i.e., which is the demodulation of the signal, heavily dependent on the assumption that all the details about the signal (i.e., prior knowledge) are known by Eve and Bob except the modulated information. Therefore, the secrecy of the communication is measured mainly from the exploitation perspective. For a particular design, focusing on the exploitation stage while keeping the assumptions for other stages as worst case can be acceptable. However, this might not be optimal in terms of overall communication system and can result in wasting resources. Therefore, more comprehensive secrecy metrics can be useful to better understand the practical system and considered design decisions with neither over-designs nor underestimations of Eve's capability. Thus, this Section discusses the fundamental metrics used to measure the security in communication systems, and substantiates the need for new metrics that can reflect the secrecy performance obtained by practical techniques that exploit the other stages like coverage, detection and interception.

4.1. Preliminaries

The principles of secret communication in information-theoretic sense are constructed by the Shannon's definition for information content, i.e., entropy, which quantifies the unpredictability of a signal as a random variable [37], and defined as

$$H(W) = \mathrm{E}[I(W)] = \mathrm{E}[-\ln(P(W))], \tag{1}$$

where $I(W)$ describes the information content of W. The relations between the information theoretic terms and the secrecy of the communication is illustrated in Fig. 5. For the main channel, the mutual information between the message and received signal, $I(W; Y_\mathrm{B})$, is the amount of information that Bob obtains about the message W by observing the received signal Y_B. This quantifies the reliability in the communication in terms of data rate, maximum of which is known to be the channel capacity [37]. For the eavesdropper channel, conditional entropy of the message W given that the received signal Y_E is known quantifies the amount of information needed to describe the message W. This is also referred to as *equivocation*, $H(W|Y_E)$, that corresponds to the confusion of eavesdropper on the received signal. Clearly, increasing the equivocation at Eve improves the security of the message. In other words, the unpredictability of Y_E, that is not originated from the message W, is the result of independent distortions on the signal such as noise and interference. Hence, increasing the level of distortion on Eve's side corresponds to increasing the amount of information needed to determine W from Y_E.

Therefore, the main goal in designing the communication system with secrecy constraints is to increase the mutual information between the transmitter and legitimate receiver which stands for the reliability in communication, while maximizing the uncertainty at the eavesdropper which paves the way for the security objectives.

4.2. Information-theoretic measures

4.2.1. Perfect secrecy

This measure defined by Shannon means that the mutual information leakage to Eve must be zero regardless of its processing power and capabilities. This notion serves as the most stringent secrecy measure as it ensures almost unity decoding error probability if the entropy of the message is very large. It can mathematically be expressed as $I(W; Y_E) = 0$, which implies that the entropy of the message is the same as the conditional entropy of the message given its observation at Eve (i.e., $H(W) = H(W|Y_E)$). In other words, perfect secrecy results in zero statistical dependence between the message and its observation at Eve. This can be guaranteed if and only if the entropy of the key used for encryption is as same as the entropy of the message itself. An example on a technique that can achieve perfect secrecy notion is the one-time pad scheme which was firstly invented by Miller [38] and later re-invented and patented by Vernam [39]. Another scheme that is proven to achieve perfect and ideal secrecy without using a shared key was proposed in [40]. In this scheme, the artificial noise is used as a one-time pad key aligned in the null space of the legitimate channel.

4.2.2. Weak secrecy

This notion defined by Wyner means that the asymptotic average mutual information rate goes to zero as the codeword length n goes to infinity. Thus, this notion does not strictly force mutual information leakage to be zero on each channel use, but rather on average. This can mathematically be denoted as $\lim_{n\to\infty} \frac{1}{n} I(W; Y_E) = 0$. The first practical coding scheme proposed to achieve the weak secrecy notion was introduced in [41]. Later on, a comprehensive study on coding techniques for wire-tap channels was given in [42]. Specifically, the authors first offered an alternative perspective on the proof of the fact that there do exist construction codes that can achieve the secrecy capacity of any arbitrary wiretap channel. As a particular case, they presented a secure coding scheme that can achieve the secrecy capacity when the main channel is noiseless and the wiretapper channel is binary erasure channel (BEC). It was stated that it is possible to use low-density parity-check (LDPC) codes to construct decodable secrecy codes that can achieve secrecy in the weak sense. Then, they extended their code construction to the scenario where both the main and wiretapper's channel are BECs, and showed evident connections between the codes threshold on graphs and security. Lastly, the authors considered the case when the main channel is noiseless and the wiretapper's channel is binary symmetric channel (BSC), where a coding solution of good error-detecting capability was provided.

4.2.3. Strong secrecy

This measure defined by Csiszar and Maurer implies that the asymptotic mutual information goes to zero as the codeword length n goes to infinity. Thus, this notion forces mutual information leakage to be zero on each channel use, but not on average as in weak secrecy. This can mathematically be written as $\lim_{n\to\infty} I(W; Y_E) = 0$. An example of coding schemes that can achieve strong secrecy notion was given in [43]. Specifically, a channel polarization-based coding scheme was introduced to achieve the strong secrecy capacity notion when the main channel is binary-input symmetric channel (BSC) and the wiretapper channel is degraded with respect to the main channel. The basic idea of their scheme is to send information bits over the sub-channels that are good for Bob but bad for Eve, random bits over the sub-channels that are good for both Eve and Bob, and zeros over the sub-channels that are bad for both Bob and Eve.

4.2.4. Semantic secrecy

In the strong secrecy notion, randomly uniform distribution of the messages is usually considered. This assumption is seen inappropriate from the key-based security perspective, since in many cases, messages are not completely random. This issue can be resolved by using the standard notion of semantic security [44,45] which requires that the probability that the eavesdropper can guess any function of the message given the cipher-text observation should not be higher than the probability of randomly guessing it without having access to the cipher-text. In other words, this basically means that it is asymptotically impossible to estimate any function of the message better than to randomly guess it without knowing or considering Eve's observations and over all message distributions. Mathematically, it is given as $\lim_{n\to\infty} \max_{p_W} I(W; Y_E) = 0$, where p_W represents all possible message distributions. It is clear from the mathematical representation that semantic security is equivalent to achieving strong secrecy for all message distributions. In [45], Lattice codes were proposed to achieve the semantic secrecy notion for Gaussian wiretap channels.

4.2.5. Distinguishing secrecy

It means that the channel output observations are asymptotically indistinguishable for different input information messages. This achieves strong secrecy over all message distributions. Therefore, distinguishing security is found out to be equivalent to semantic security at least for the discrete wiretap channel setup. Although the two notions are almost the same, distinguishing security is technically more convenient to deal with. Mathematically, it can be given as below

$$\lim_{n\to\infty} \max_{w,w'} \mathbb{V}(p_{\mathsf{Y}_E|\mathsf{W}=w}, p_{\mathsf{Y}_E|\mathsf{W}=w'}) = 0, \tag{2}$$

where w, w' are different input messages and $\mathbb{V}(p_\mathsf{X}, p_\mathsf{Y})$ is the statistical or variational distance, which can be given as

$$\mathbb{V}(p_\mathsf{X}, p_\mathsf{Y}) \triangleq \int_{\mathbb{R}^n} |p_\mathsf{X}(\mathbf{x}) - p_\mathsf{Y}(\mathbf{x})|\, d\mathbf{x}. \tag{3}$$

4.2.6. Channel resolvability-based metrics

Authors in [46] explored an alternative path to physical-layer security, by which secrecy is measured in terms of the statistical dependence between the transmitted messages and the observations at the eavesdropper. They proposed using channel resolvability [47] for constructing secrecy coding schemes instead of using capacity-based constructions. This requires the messages to be mapped to waveforms (bases or sub-codes), whose rates are just above the eavesdropper's channel resolvability rather than being just below the eavesdropper's channel capacity. Specifically,

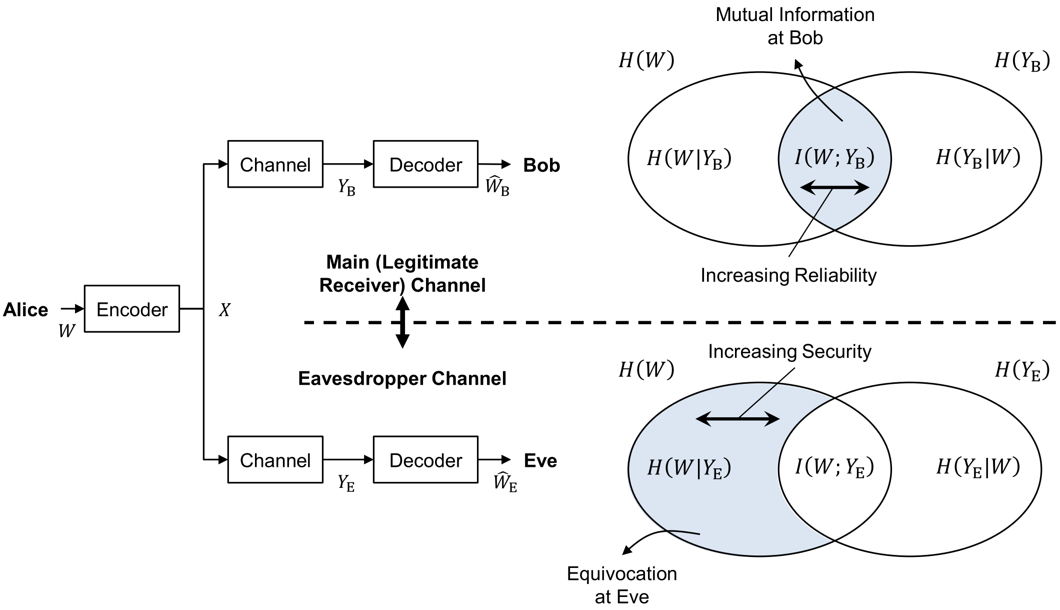

Fig. 5. Information-theoretic measures. The main aim is to increase the mutual information in main channel for reliability, while minimizing the mutual information (maximizing the equivocation) at Eve for security. Secrecy rate is the difference between mutual informations, which is desired to be maximized.

it was shown that for some channels like symmetric wire-tape channel, capacity-based constructions cannot fulfill the strong secrecy capacity conditions, whereas channel-resolvability-based constructions can provably achieve it. Thus, channel resolvability is considered as an appropriate mechanism, which can be utilized for constructing secrecy codes. Based on this concept, the authors suggested several new secrecy metrics, which are proven to be related to the conventional known secrecy capacity metric. In these metrics, it is found out that the average mutual information rate is actually equivalent to a normalized Kullback–Leibler divergence (a measure of the difference) between the product distribution $p_W p_{Y_E}$ and the joint distribution p_{WY_E}. The closeness of these two distributions can be measured by means of the variational distance, or the cumulative distribution function (CDF) of the random variable associated with the mutual information. Accordingly, the following metrics can be considered for analyzing secrecy:

- *Information divergence*: This metric uses Kullback–Leibler divergence to measure the statistical independence, and it can be represented as $\mathbb{S}_1\left(p_{WY_E}, p_W p_{Y_E}\right) \triangleq \mathbb{D}\left(p_{WY_E} \parallel p_W p_{Y_E}\right) = I\left(W; Y_E\right)$, where $\mathbb{D}(p_{WY_E} \parallel p_W p_{Y_E}) = \int_{-\infty}^{\infty} p_{WY_E} \log \frac{p_{WY_E}}{p_W p_{Y_E}} dx$, and all the probability distributions are functions of x.
- *Variational distance*: This metric employs variational distribution difference and it can be given as $\mathbb{S}_2\left(p_{WY_E}, p_W p_{Y_E}\right) \triangleq \mathbb{V}\left(p_{WY_E}, p_W p_{Y_E}\right)$, where $\mathbb{V}(p_X, p_Y)$ is given in (3).
- *CDF-based asymptotic independence*: This metric utilizes CDF as a probability measure, and it can be calculated as $\mathbb{S}_3\left(p_{WY_E}, p_W p_{Y_E}\right) \triangleq \mathbb{P}\left[I\left(W; Y_E\right) > \epsilon\right]$, where $\epsilon > 0$.

4.2.7. Secrecy rate/secrecy capacity

By using the identity that the total entropy of the signal is constituted by the mutual information and the equivocation at Eve, i.e., $H(W) = I(W; Y_E) + H(W|Y_E)$, the parameter that is desired to be maximized is the *secrecy rate* defined as

$$R_s = I(W; Y_B) - I(W; Y_E). \tag{4}$$

The maximum achievable secrecy rate over input distributions for the transmitted signal X, which is a function of the coding process, is given as the *secrecy capacity*. That is, the secrecy capacity can be represented as

$$C_s = C_B - C_E, \tag{5}$$

where C_B and C_E are the capacity of the Alice–Bob and Alice–Eve channels [4,48,49].

4.2.8. Secrecy outage probability

Randomness of the physical environment due to uncertainty in some factors such as the locations of nodes, shadowing and multipath-fading effect changes the signals observed by each node in a random manner. Thus, the aforementioned metrics become random variables as well. In such situations, statistical measures are generally adopted to represent the randomness of the environment itself on top of the information. For example, the secrecy outage probability can be defined as the probability that the instantaneous secrecy capacity falls below a target secrecy rate R_s^t, as

$$P_{\text{out}}(R_s^t) = P(C_s < R_s^t). \tag{6}$$

In such environments, where the randomness in the system parameters does not allow a deterministic secrecy metric, the performance of the system can be measured via outage probability [48], which is the better the lower for a given secrecy rate target.

4.2.9. Tight secrecy outage probability (TSOP)

In the conventional secrecy outage probability metric, the result is merely focused on evaluating the probability that the secrecy capacity is below a certain secrecy rate. However, this cannot always guarantee secrecy, especially when the CSI is not known at Alice. Particularly, this cannot ensure specific rates at either Bob or Eve. To address this issue, TSOP was proposed in [50] to constrain the information leakage to Eve, while guaranteeing a certain amount of information to Bob. Thus, TSOP can be given as follows: $P_{out}(R_s) = 1 - P(\{C_B \geq R_B\} \bigcap \{C_E < R_E\})$.

4.2.10. Secrecy throughput (ST)

This metric can measure the average confidential transmission rate (i.e., secrecy rate average) of the message and it can be given as $ST = R_s(1 - P_{out}(R_s))$. A much tighter definition for secrecy throughout is calculated as the average amount of information that is guaranteed to be transmitted both reliably and securely. Thus, tight secrecy throughput metric can be calculated as $TST = R_s(1 - P_{out}(R_s))(1 - P_{out}(R_B))$.

4.2.11. Fractional equivocation-based metrics

In spite of the fact that traditional secrecy outage probability has been extensively used in the literature for evaluating the security performance level of real wireless systems, it has got three main restrictions [51]. First, it cannot provide any insightful knowledge on the eavesdropper's capability to correctly decode the confidential messages. Second, it lacks the ability to characterize quantitatively the amount of information leakage to the passive eavesdroppers when outage secrecy occurs. Third, it cannot be linked with the QoS requirements of different services and applications. Motivated by these facts, authors in [51] proposed three new metrics based on the distribution of fractional equivocation (partial secrecy) given by $(\Delta = \frac{H(W|Y_E)}{H(W)})$ [52], which can be obtained from channel gains distributions. These metrics can be listed as below:

- *Generalized secrecy outage probability (GSOP)*: It takes into account the level of secrecy measured by equivocation, and hence establishes a relation between the concept of secrecy outage and the decodability of messages at the eavesdropper. The metric can be given as $p_{\text{out}} = \mathbb{P}(\Delta < \psi)$, where $\mathbb{P}(\ )$ indicates the probability measure and $0 < \psi < 1$ is the lowest allowable value of the partial secrecy.
- *Average fractional equivocation (AFE)*: This metric serves as an asymptotic lower bound on the eavesdropper's decoding error probability. Also, it provides a direct connection to error-probability-based secrecy metrics that are usually used for the practical design of security in wireless systems over fading channels. The fractional equivocation average can be given as $\bar{\Delta} = \mathbb{E}\{\Delta\}$, where $\mathbb{E}$ is the expectation operator.
- *Average information leakage rate (AILR)*: This secrecy metric enables evaluating and calculating the amount of confidential information leaked to the eavesdropper when conventional information-theoretic secrecy (i.e, perfect, strong, or week secrecy) is not achieved. Thematically, this metric can be given as $R_L = \mathbb{E}\left\{\frac{I(W;Y_E)}{n}\right\} = \mathbb{E}\left\{(1 - \Delta)R\right\}$, where R is the transmission rate of the message.

4.3. Practical measures

4.3.1. Security gap

Although secrecy capacity is a common metric for security of the communication, it is difficult to realize and measure in practical communication scenarios where non-Gaussian codes and finite block lengths are used. This is also the main reason for not having practical codes with finite length that achieve the secrecy capacity [53,54]. Thus, although the fact that both the secrecy capacity and equivocation rate provide important estimates of secrecy, when practical coding and modulation schemes are adopted, the metrics that can be mapped to easily measurable parameter, e.g., BER, emerge as valuable alternatives for measuring the security performance. After several decades of information-theoretic notion, a practical approach to determine a quantitative measure, *security gap*, is introduced in [55] and [56]. Although it does not address the information-theoretic measure, the security gap quantifies the secrecy level based on the BER performance at Bob and Eve, which is much easier to analyze in practice. In summary, the gap between the Bob's SNR (which is required to achieve reliable decoding for a certain service) and the Eve's SNR (which must be not sufficient enough to achieve reliable decoding for the same service) reflects the channel quality advantage that Bob has to have over Eve for satisfying the practical secrecy notion (i.e., security gap). The security gap is defined as

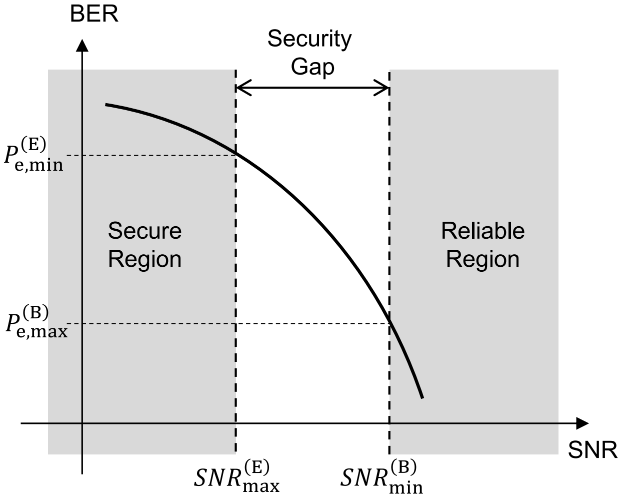
BER
Security Gap
$P_{\text{e,min}}^{(\text{E})}$
$P_{\text{e,max}}^{(\text{B})}$
Secure Region
Reliable Region
SNR
$SNR_{\text{max}}^{(\text{E})}$
$SNR_{\text{min}}^{(\text{B})}$

Fig. 6. Security gap when both receivers are assumed to have identical BER performance.

$$S_g = SNR_{\text{min}}^{(\text{B})} - SNR_{\text{max}}^{(\text{E})}, \tag{7}$$

which is the difference between the minimum SNR level of Bob to achieve reliable reception and the maximum SNR at Eve that guarantees a certain level of BER, which is generally desired to be close to 0.5. As illustrated in Fig. 6, two regions; reliability region where Bob operates with a certain maximum BER, $P_{\text{e,max}}^{(\text{B})}$, and secure region where Eve is desired to operate not to achieve a certain BER, $P_{\text{e,min}}^{(\text{E})}$, that can provide sufficient information about the original message. In other words, the gap between these two SNR levels denotes the channel quality advantage that Bob has to have over Eve for satisfying the practical notion of the secrecy in transmission.

In order to reduce the security gap for given reliability and security requirements, it is clear that the steepness of the BER curve needs to be increased. In other words, a remarkable increase in BER even with a small degradation in Eve's channel is desirable. Introducing coding with puncturing [55,56] and non-systematic coding with scrambling [57–60] are common approaches for increasing the steepness of BER curve resulting in smaller security gap.

As it can be seen in Fig. 6, identical BER performance profile for both legitimate receiver and the eavesdropper is generally assumed while determining the security gap. However, the error rate performance can possess different characteristics due to different perceptions of Bob and Eve. This can be due to natural effects such as different fading statistics with distinct multipath distribution for two receivers, e.g., line-of-sight (LOS) and non-LOS [61], or artificial effects such as AN differently effecting legitimate and illegitimate receivers [36]. Thus, the concept of security gap can be extended into general case where Bob and Eve experience different BER vs SNR characteristics. Note that since we consider fading, the SNR in the generalized case corresponds to mean SNR. As it is illustrated in Fig. 7, the security gap is determined by the SNR levels as a function of Bob's and Eve's own environmental conditions. It is worth noting that the security gap with this consideration can even be negative. In other words, the conditions that make secure communication possible when even Eve has better SNR than Bob can be represented in terms of the security gap.

Although BER-based metrics simplify the system design, they satisfy neither the weak nor the strong secrecy constraints. This

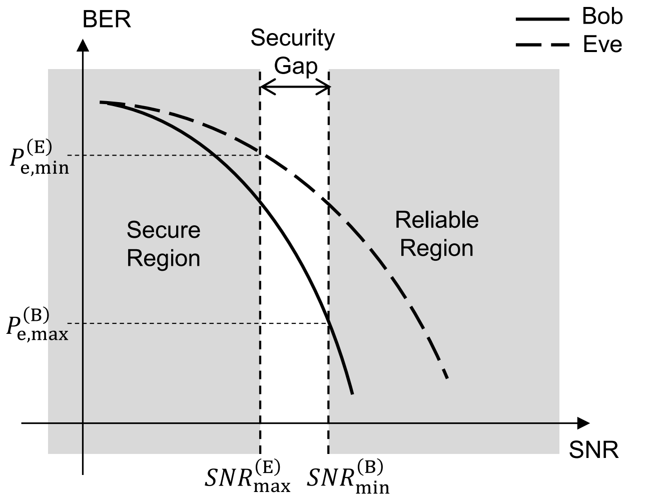

Fig. 7. Generalized security gap when Bob and Eve have different BER performances.

is due to the fact that strong or weak secrecy requires that the mutual information or rate of information leaked to the eavesdropper must asymptoticly vanish to zero as the length of the codeword goes to infinity (i.e., asymptotic statistical independence between the message and Eve's observation). This implies that the asymptotic decoding error probability at Eve must approach unity as the number of messages goes to infinity (very high entropy). However, since in a binary system only two possible message values exist (i.e., zero or one), the decoding error probability (which is equivalent to BER) can never be greater than half, which means that exactly half of the information will always be leaked to Eve. This means that neither the weak nor the strong secrecy constraints can be satisfied. Moreover, the secrecy analysis performed in [54] states that maximum BER cannot guarantee maximum equivocation rate at Eve, and thus cannot necessarily satisfy the weak or strong secrecy measures.

4.3.2. Bit error rate

Being a widespread measure for reliable communication, BER can also be used to quantify the security performance from a practical point of view. While various functions of BER can be set, a simple cost function as an example can be defined as

$$Cost = \frac{P_{\mathrm{e}}(\text{desired receiver})}{\min(P_{\mathrm{e}}(\text{undesired receiver}))} \tag{8}$$

which is a parameter to be minimized for increasing the security in the system. In the concept of directional modulation [62,63], the arguments of the error probabilities in (8) are considered for desired and undesired direction, respectively.

4.3.3. Secure packet error rate (SPER)

PER, which is equal to the ratio of the number of erroneously received packets to the total number of transmitted packets, was proposed as a practical security metric for cross layers (PHY/MAC) security design in [64]. Its use as a secrecy metric was justified by the following reasons: (1) it takes into account the effect of upper layers functionalities such as automatic-repeat-request (ARQ) on the system performance, (2) it can practically be measured by most wireless receivers thanks to cyclic redundancy check (CRC) process, (3) it can easily be linked and related to the Quality of Service (QoS) requirements of digital services such as video and voice. The goal here is to make sure that Eve operates above a certain PER level over all possible SNR values, while the PER value at the legitimate receiver is guarantied to be below a certain threshold so that it can decode the service under interest successfully. Therefore, the secrecy performance can be analyzed using the difference between Eve's PER denoted by PER^E and Bob's PER denoted by PER^B, where the exact PER gap difference between them can be determined. Mathematically, this measure can be given as $SPER = PER^E - PER^B$, where $0 \leq SPER \leq 1$. The ideal maximum value that $SPER$ can reach is one (which occurs when $PER^E = 1$, and $PER^B = 0$), while the minimum is zero. This metric implies that taking QoS requirements for various services into consideration during the design phase is an effective way for providing secure schemes. It should be mentioned that achieving maximum error rate at Eve (i.e., $PER^E = 1$), is equivalent to achieving the practical secrecy notion introduced in [65] (i.e., Eve's error probability is approaching unity).

It is also noteworthy that this formulated metric, i.e., $SPER$ is equivalent to secure throughput metric, denoted by η, and defined as the difference between Bob's throughput (η^B) and Eve's throughputs (η^E), i.e., $\eta = \eta^B - \eta^E$. Now, since the throughput metric itself can be defined as the complement of the packet error rate, η can be written in terms of PER^B and PER^E, i.e., $\eta = (1 - PER^B) - (1 - PER^E)$ and this can be simplified to $\eta = PER^E - PER^B$. This formulation establishes a direct and clear connection between error probability-based metrics from on side and capacity-based metrics from another side and clearly shows the inherent connection and relation between them.

4.3.4. Low probability of interception (LPI) / detection (LPD)

Considering the stages discussed in Section 3 as random events with associated success probabilities, the probability of a transmitted signal to be exploited by an eavesdropper can be given as

$$P(E) = P(E|I)P(I|D)P(D|C)P(C) \tag{9}$$

where $P(C)$ denotes the probability of coverage, $P(D|C)$, $P(I|D)$, and $P(E|I)$ are the conditional probabilities of; detection given that the signal is covered, interception given that the signal is detected, and exploitation given that the signal is intercepted, respectively. The task of PHY security techniques is minimizing the probability of exploitation, $P(E)$, via decreasing its one or more probability components, i.e., multiplicands in (9).

- *Probability of interception:* The probability that an eavesdropper locates this point, i.e., probability of interception, is another parameter for the security measure. As a general term, the interception can be considered in time–frequency dimension for spread-spectrum techniques [66,67] where the waveform features such as spreading or hopping sequence become the key for successful interception for eavesdropper. In directional signal transmission schemes, this can be in the space domain where the eavesdropper has to intercept in terms of angular location to be able to extract the message. When the mapping operation is tied to the multipath fading channel response, the knowledge of CSI between the transmitter and legitimate receiver can open the path to interception [68] in which the transmission is subject to LPI. Thus, in wireless systems where most of the parameters are random variables, the LPI on a domain based on the security technique stands for a general measure for the level of security. Functionally, probability of interception is analogous to the mutual information between the legitimate transmitter and eavesdropper, which is also desired to be minimized for achieving positive secrecy from the information-theoretic viewpoint [1].
- *Probability of detection:* The term low-probability-of-detection (LPD) is commonly defined as the probability of correctly detecting the presence of communication between the legitimate pairs. In other words, LPD is a function of covertness of the communication that is taking

place [69], and commonly referred with the concept of spread-spectrum where the power density of the signal is decreased with spreading and directional transmission techniques where the signal power for undesired directions is reduced [70].

It should be emphasized that some of the existing and previously discussed secrecy metrics may seem to have the ability to quantify the secrecy performance obtained by exploiting stages other than the final exploitation stage. However, this is not absolutely true and accurate for all possible scenarios and cases, especially when the designed secrecy scheme is not SNR-dependent. For instance, there are schemes that do not cause any difference in the SNR or even constellation and Eye diagrams between Bob and Eve, but still Eve cannot decode, while Bob can. This happens as a consequence of designing some prior information such as the interleaving sequence or precoder based on the channel of the legitimate receiver, which is different from Eve [16,71]. In such cases, secrecy capacity and secrecy outage probability are not applicable for quantifying the obtained secrecy. To avoid this problem, BER was used as a metric to measure secrecy as reported in [16,71] because there is no any other better alternative. Nevertheless, we advocate that BER alone is not a very accurate and suitable choice to be used as a metric in these special cases as it always points to bit error rate probability of 0.5 no matter what the SNR value is, which is the worst guess any receiver can randomly make. Therefore, defining new metrics that can better quantify the secrecy performance of some techniques that exploit different stages for providing confidentiality is a very important task that needs to be tackled and addressed in the future.

4.4. Ways to provide practical security design

The presented security framework, where the fundamental stages required by Eve to eavesdrop a communication link are determined, constitutes a novel perspective and much more generic overview on physical layer security. This not only strengthens and facilitates comprehending physical layer security concepts, but also helps inspire new physical layer security ideas by exploiting the inevitable stages used during the reception process. For instance, the practical examples, presented in Section III to demonstrate the significant importance of the stages discussed in this paper, can serve as a starting point in the direction of generalizing security concept to other stages. More specifically, in these practical examples, we have shown that the assumption that Eve knows all the information about the signal except the message bits is somehow not a very realistic assumption and the impact of these details on the secrecy (Eve's uncertainty) may be significant in some practical scenarios. This motives exploiting not only the wireless channel for secrecy, but also most types of hardware impairments in the transceiver chain. Moreover, the comprehensive review on the state of the art secrecy performance metrics including both information theoretic and practical measures can serve as a reference source for security researchers. It makes researchers aware of all the metrics that can be used for secrecy analysis at different reception stages. It also enables designers to choose proper metrics that can reflect the secrecy level of their proposed security schemes. Besides, the paper inspires defining new metrics that can reflect the secrecy performance obtained by techniques that utilize not only the final exploitation stage, but also the other stages like coverage, detection and interception.

5. Conclusions

Securing the information transmission when the medium is wireless is both challenging and, at the same time, provides additional degrees of freedom thanks to different perceptions of the received signal by legitimate receivers and eavesdroppers. Fundamental signal reception stages in secure signal transmission are presented from a different perspective along with practical security design examples from the literature. The metrics which are used to measure the secrecy of the communication are surveyed by connecting with transmission stages and techniques. New approaches to the existing performance metrics such as security gap, secrecy throughput, fractional equivocation-based metrics, secure packet error rate, etc. are presented. The detailed review on secrecy performance metrics is intended to help and make researchers aware of the available metrics, their meanings, and the differences among them. This will also provide flexibility to PHY security designers in selecting suitable metrics to accurately investigate and reflect the secrecy performance of their proposed techniques. The concepts in secure signal transmissions are exemplified with existing PHY layer techniques. The paper puts a step towards understanding the nature of secrecy in wireless communication from different perspectives and exploring new opportunities by exploiting different reception stages for providing secrecy.

References

[1] C.E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J. 28 (1949) 656–715.

[2] J. Massey, An introduction to contemporary cryptology, Proc. IEEE 76 (5) (1988) 533–549.

[3] U. Maurer, Secret key agreement by public discussion from common information, IEEE Trans. Inform. Theory 39 (3) (1993) 733–742.

[4] A.D. Wyner, The wire-tap channel, Bell Syst. Tech. J. 54 (1975) 1355–1387.

[5] A. Mukherjee, S.A.A. Fakoorian, J. Huang, A.L. Swindlehurst, Principles of Physical layer security in multiuser wireless networks: A survey, IEEE Commun. Surv. Tutor. 16 (3) (2014) 1550–1573.

[6] Y. Zou, J. Zhu, X. Wang, L. Hanzo, A survey on wireless security: technical challenges, recent advances, and future trends, Proc. IEEE 104 (9) (2016) 1727–1765.

[7] Y. Liu, H.H. Chen, L. Wang, Physical layer security for next generation wireless networks: theories, technologies, and challenges, IEEE Commun. Surv. Tutor. 19 (1) (2017) 347–376.

[8] C.E. Shannon, Communication in the presence of noise, Proc. IRE 37 (1949) 10–21.

[9] W.C. Liao, T.H. Chang, W.K. Ma, C.Y. Chi, QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-aoise-aided approach, IEEE Trans. Signal Process. 59 (3) (2011) 1202–1216.

[10] M. Li, S. Kundu, D.A. Pados, S.N. Batalama, Waveform design for secure SISO transmissions and multicasting, IEEE J. Sel. Areas Commun. 31 (9) (2013) 1864–1874.

[11] H. Reboredo, J. Xavier, M.R.D. Rodrigues, Filter design with secrecy constraints: The MIMO gaussian wiretap channel, IEEE Trans. Signal Process. 61 (15) (2013) 3799–3814.

[12] H. Rahbari, M. Krunz, Secrecy beyond encryption: obfuscating transmission signatures in wireless communications, IEEE Commun. Mag. 53 (12) (2015) 54–60.

[13] T.Y. Liu, P.H. Lin, S.C. Lin, Y.W.P. Hong, E.A. Jorswieck, To avoid or not to avoid CSI leakage in physical layer secret communication systems, IEEE Commun. Mag. 53 (12) (2015) 19–25.

[14] Z. Rezki, A. Khisti, M.-S. Alouini, On the secrecy capacity of the wiretap channel with imperfect main channel estimation, IEEE Trans. Commun. 62 (10) (2014) 3652–3664.

[15] A. Hyadi, Z. Rezki, M.S. Alouini, An overview of physical layer security in wireless communication systems with csit uncertainty, IEEE Access 4 (2016) 6121–6132.

[16] J.M. Hamamreh, H.M. Furqan, H. Arslan, Secure pre-coding and post-coding for OFDM systems along with hardware implementation, in: 2017 13th International Wireless Communications and Mobile Computing Conference, IWCMC, 2017, pp. 1338–1343.

[17] J.P. Cheng, Y.H. Li, P.C. Yeh, C.M. Cheng, MIMO-OFDM PHY integrated (MOPI) scheme for confidential wireless transmission, in: 2010 IEEE Wireless Communication and Networking Conference, 2010, pp. 1–6.

[18] M. Soltani, T. Bayka, H. Arslan, Achieving secure communication through pilot manipulation, in: 2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications, PIMRC, 2015, pp. 527–531.

[19] S.H. Wang, F.P.C. Lin, C.P. Li, Secure channel estimation method in TDD OFDM systems, in: 2016 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting, BMSB, 2016, pp. 1–4.

[20] T.H. Chang, W.C. Chiang, Y.W.P. Hong, C.Y. Chi, Training sequence design for discriminatory channel estimation in wireless MIMO systems, IEEE Trans. Signal Process. 58 (12) (2010) 6223–6237.

[21] C.W. Huang, T.H. Chang, X. Zhou, Y.W.P. Hong, Two-way training for discriminatory channel estimation in wireless MIMO systems, IEEE Trans. Signal Process. 61 (10) (2013) 2724–2738.

[22] J. Yang, S. Xie, X. Zhou, R. Yu, Y. Zhang, A semiblind two-way training method for discriminatory channel estimation in MIMO systems, IEEE Trans. Commun. 62 (7) (2014) 2400–2410.

[23] M. Yusuf, H. Arslan, Controlled inter-carrier interference for physical layer security in OFDM systems, in: IEEE Vehicular Technology Conference, VTC-Fall, 2016.

[24] J. Zhu, D.W.K. Ng, N. Wang, R. Schober, V. Bhargava, Analysis and design of secure massive MIMO systems in the presence of hardware impairments, IEEE Trans. Wirel. Commun. PP (99) (2017) 1.

[25] A. Sheikholeslami, D. Goeckel, H. Pishro-nik, Artificial intersymbol interference (ISI) to exploit receiver imperfections for secrecy, in: 2013 IEEE International Symposium on Information Theory, 2013, pp. 2950–2954.

[26] Z.E. Ankarali, H. Arslan, Cyclic feature suppression for physical layer security, Phys. Commun. (2016).

[27] A. Sheikholeslami, D. Goeckel, H. Pishro-Nik, Everlasting secrecy by exploiting non-idealities of the eavesdropper's receiver, IEEE J. Sel. Areas Commun. 31 (9) (2013) 1828–1839.

[28] A.A.A. Boulogeorgos, D.S. Karas, G.K. Karagiannidis, How much does I/Q imbalance affect secrecy capacity? IEEE Commun. Lett. 20 (7) (2016) 1305–1308.

[29] J. Zhu, R. Schober, V.K. Bhargava, Physical layer security for massive MIMO systems impaired by phase noise, in: 2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications, SPAWC, 2016, pp. 1–5.

[30] M.P. Daly, J.T. Bernhard, Directional modulation technique for phased arrays, IEEE Trans. Antennas Propag. 57 (9) (2009) 2633–2640.

[31] T. Yucek, H. Arslan, A survey of spectrum sensing algorithms for cognitive radio applications, IEEE Commun. Surv. Tutor. 11 (1) (2009) 116–130.

[32] E. Biglieri, J. Proakis, S. Shamai, Fading channels: information-theoretic and communications aspects, IEEE Trans. Inform. Theory 44 (6) (1998) 2619–2692.

[33] M.R. Bloch, Covert communication over noisy channels: A resolvability perspective, IEEE Trans. Inform. Theory 62 (5) (2016) 2334–2354.

[34] J.M. Hamamreh, H. Arslan, Secure orthogonal transform division multiplexing (OTDM) waveform for 5G and beyond, IEEE Commun. Lett. PP (99) (2017) 1.

[35] J.M. Hamamreh, E. Guvenkaya, T. Baykas, H. Arslan, A practical physical-layer security method for precoded OSTBC-based systems, in: 2016 IEEE Wireless Communications and Networking Conference, 2016, pp. 1–6.

[36] S. Goel, R. Negi, Guaranteeing secrecy using artificial noise, IEEE Trans. Wirel. Commun. 7 (6) (2008) 2180–2189.

[37] C.E. Shannon, A mathematical theory of communication, Bell Syst. Tech. J. 27 (1948) 379–423, 623–656.

[38] S.M. Bellovin, Frank miller: Inventor of the one-time pad, Cryptologia 35 (3) (2011) 203–222.

[39] G. Vernam, Secret Signaling System, Patent, Jul. 22, 1919, US Patent 1,310,719. [Online]. Available https://www.google.com/patents/US1310719.

[40] S. Liu, Y. Hong, E. Viterbo, Unshared secret key cryptography, IEEE Trans. Wirel. Commun. 13 (12) (2014) 6670–6683.

[41] L.H. Ozarow, A.D. Wyner, Wire-tap channel II, Bell Syst. Tech. 63 (1984) 2135–2157.

[42] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, J.-M. Merolla, Applications of LDPC codes to the wiretap channel, IEEE Trans. Inform. Theory 53 (8) (2007) 2933–2945.

[43] H. Mahdavifar, A. Vardy, Achieving the secrecy capacity of wiretap channels using polar codes, IEEE Trans. Inform. Theory 57 (10) (2011) 6428–6443.

[44] S. Goldwasser, S. Micali, Probabilistic encryption, J. Comput. System Sci. 28 (2) (1984) 270–299.

[45] C. Ling, L. Luzzi, J.C. Belfiore, D. Stehl, Semantically secure lattice codes for the gaussian wiretap channel, IEEE Trans. Inform. Theory 60 (10) (2014) 6399–6416.

[46] M.R. Bloch, J.N. Laneman, Strong secrecy from channel resolvability, IEEE Trans. Inform. Theory 59 (12) (2013) 8077–8098.

[47] T.S. Han, S. Verdu, The resolvability and the capacity of AWGN channels are equal, in: Proc. IEEE Int. Symp. Information Theory, 1994, p. 463.

[48] J. Barros, M.R.D. Rodrigues, Secrecy capacity of wireless channels, in: Proc. IEEE Int. Symp. Information Theory, 2006, pp. 356–360.

[49] I. Csiszar, J. Korner, Broadcast channels with confidential messages, IEEE Trans. Inform. Theory (1978) 339–348.

[50] K. Morrison, D. Goeckel, Secrecy rate pair constraints for secure throughput, in: 2014 IEEE Mil. Commun. Conf., IEEE, 2014, pp. 479–484.

[51] B. He, X. Zhou, A.L. Swindlehurst, On secrecy metrics for physical layer security over quasi-static fading channels, IEEE Trans. Wirel. Commun. 15 (10) (2016) 6913–6924.

[52] S. Leung-Yan-Cheong, M. Hellman, The gaussian wire-tap channel, IEEE Trans. Inform. Theory 24 (4) (1978) 451–456.

[53] M. Baldi, G. Ricciutelli, N. Maturo, F. Chiaraluce, Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel, in: 2015 IEEE International Conference on Communication Workshop, ICCW, 2015, pp. 435–440.

[54] A. Wickramasooriya, I. Land, R. Subramanian, Comparison of Equivocation Rate of Finite-Length Codes for the Wiretap Channel, in: SCC 2013; 9th International ITG Conference on Systems, Communication and Coding, 2013, pp. 1–6.

[55] D. Klinc, J. Ha, S. McLaughlin, J. Barros, B.-J. Kwak, LDPC codes for physical layer security, in: IEEE Global Telecommunications Conference, GLOBECOM, 2009, pp. 1–6.

[56] D. Klinc, J. Ha, S. McLaughlin, J. Barros, B.-J. Kwak, LDPC Codes for the Gaussian Wiretap Channel, IEEE Trans. Inf. Forens. Secur. 6 (3) (2011) 532–540.

[57] M. Baldi, M. Bianchi, F. Chiaraluce, Non-systematic codes for physical layer security, in: IEEE Information Theory Workshop, ITW, 2010, pp. 1–5.

[58] M. Baldi, M. Bianchi, F. Chiaraluce, Increasing physical layer security through scrambled codes and ARQ, in: IEEE International Conference on Communications Workshops, ICC, 2011, pp. 1–5.

[59] M. Baldi, M. Bianchi, F. Chiaraluce, Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis, IEEE Trans. Inf. Forens. Secur. 7 (3) (2012) 883–894.

[60] N. Maturo, M. Baldi, M. Bianchi, F. Chiaraluce, Security gap assessment for the fast fading wiretap channel, in: 20th International Conference on Telecommunications, ICT, 2013, pp. 1–5.

[61] J.G. Proakis, M. Salehi, Digital Communications, fifth ed., McGraw-Hill, New York, 2008.

[62] M. Daly, J. Bernhard, Directional modulation technique for phased arrays, IEEE Trans. Antennas Propag. 57 (9) (2009) 2633–2640.

[63] M. Daly, E. Daly, J. Bernhard, Demonstration of directional modulation using a phased array, IEEE Trans. Antennas Propag. 58 (5) (2010) 1545–1550.

[64] J.M. Hamamreh, M. Yusuf, T. Baykas, H. Arslan, Cross MAC/PHY layer security design using ARQ with MRC and adaptive modulation, in: 2016 IEEE Wireless Communications and Networking Conference, 2016, pp. 1–7.

[65] S. Liu, Y. Hong, E. Viterbo, Practical secrecy using artificial noise, IEEE Commun. Lett. 17 (7) (2013) 1483–1486.

[66] R. Scholtz, The origins of spread-spectrum communications, IEEE Trans. Commun. 30 (5) (1982) 822–854.

[67] G. Prescott, Performance Metrics for Low Probability of Intercept-communication System, Tech. Rep., Air Force Office of Scientific Research, 1993.

[68] A. Hero, Secure space-time communication, IEEE Trans. Inform. Theory 49 (12) (2003) 3235–3249.

[69] F.A.P. Petitcolas, R. Anderson, M. Kuhn, Information hiding-a survey, Proc. IEEE 87 (7) (1999) 1062–1078.

[70] E. Ghashghai, Communications Networks to Support Integrated Intelligence, Surveillance, Reconnaissance, and Strike Operations, Tech. Rep., RAND Corporation, 2004.

[71] H. Li, X. Wang, J.Y. Chouinard, Eavesdropping-resilient ofdm system using sorted subcarrier interleaving, IEEE Trans. Wirel. Commun. 14 (2) (2015) 1155–1165.

Ertuğrul Güvenkaya received the B.Sc. (summa cum laude) degree in Electrical and Electronics Engineering from Middle East Technical University (METU), Turkey in 2011; M.S. and Ph.D. degrees in Electrical Engineering from University of South Florida, FL in 2013 and 2015 respectively. He has been with Maxlinear, Carlsbad, CA, USA, as Staff Communication Systems Engineer since 2016. His research interests include multicarrier waveform design, digital signal processing and physical layer security in wireless communications.