Full-Duplex Jamming for Enhanced Hidden-Key Secrecy

Zachary Dryer*, Adam Nickerl*, Marco A. C. Gomes†, João P. Vilela‡, and Willie K. Harrison*
*Department of Electrical and Computer Engineering, Brigham Young University, UT, USA
†Instituto de Telecomunicações, Department of Electrical and Computer Engineering, University of Coimbra, Portugal
‡CISUC and Department of Informatics Engineering, University of Coimbra, Portugal
Emails: zdryer0@byu.edu, nickerl2@byu.edu, marco@co.it.pt, jpvilela@dei.uc.pt, willie.harrison@byu.edu

***Abstract*—This paper presents a practical physical-layer security scheme based on coding methodologies combined with self-jamming to combat advantaged eavesdroppers, i.e., eavesdroppers that may possess an equal or even better channel than the legitimate receiver. We introduce a strengthened security gap notion, where reliability is assured by typical bit-error rate (BER) measurements, but secrecy is guaranteed by considering the entire distribution of messages upon reception, instead of average measures. Relying on this new security gap notion, we then propose a scheme that combines concatenated coding with self-jamming by the legitimate receiver for effective security and reliability even when eavesdroppers possess a channel with equal or better conditions than the legitimate receiver.**

***Index Terms*—physical-layer security, self-jamming, adaptive filtering**

I. Introduction

Physical-layer security (PLS) is a growing field that focuses on taking advantage of certain physical characteristics of a channel to securely transmit data. After Shannon proved the impracticality of the one-time pad, researchers have sought additional, improved methods of security [1]. In 1975, Wyner introduced the wiretap channel, in which an intended receiver (Bob), communicating with a legitimate transmitter (Alice), can guarantee secrecy over an eavesdropper (Eve) provided that he has an advantage over the eavesdropper [2]. More recent developments have been surveyed in [3], [4], [5], [6]. Although many of these follow a more theoretical approach (resorting to information-theoretic metrics such as strong, weak and semantic secrecy), attractiveness to practicality within PLS grows with the increasing pervasiveness of wireless communication systems [3]. This stresses the development of practical coding for secrecy schemes, and new practical security metrics capable of providing approximate information-theoretic security based on Monte-Carlo simulation measures [7]. This paper presents new contributions on both topics, and lays the basis for further research of practical coding schemes for secrecy employing full-duplex jamming.

This work was partially funded by the following entities and projects: the US National Science Foundation (Grant Award Number 1761280), the FLAD project INCISE (Interference and Coding for Secrecy), project SWING2 (PTDC/EEI-TEL/3684/2014), funded by Fundos Europeus Estruturais e de Investimento (FEEI) through Programa Operacional Competitividade e Internacionalização - COMPETE 2020 and by National Funds from FCT - Fundação para a Ciência e a Tecnologia, through projects POCI-01-0145-FEDER-016753 and UID/EEA/50008/2013.

A problem that was outlined in PLS after the introduction of the wiretap channel is the need for a tight security gap S_g between the legitimate receiver and the eavesdropper [8], [9]. If S_g is small enough, and Bob has even a slight advantage over Eve, then secure communications can be achieved. The security gap is a practical security metric usually defined as

$$S_g = SNR_{min}^{(B)} - SNR_{max}^{(E)} \quad \text{(dB)} \tag{1}$$

where $SNR_{min}^{(B)}$ is the minimum signal-to-noise ratio (SNR) above which Bob must operate to guarantee a bit-error rate (BER) below some reliability threshold (e.g., 10^{-6}), and $SNR_{max}^{(E)}$ is the maximum SNR for which Eve experiences BER ≈ 0.5, which is defined as the security threshold.

It is well known that high bit error rates and small security gaps fall well short of information-theoretic security guarantees [10], [7], but this does not necessarily render them useless. Considering only average BER may be dangerous, however, since the BER does not measure the correlation between signals. In this paper, we propose a new approach to the security gap that can strengthen security guarantees. Instead of using BER, the full probabilistic distribution of the messages upon reception is analyzed. Assuming there exists a practical coding scheme such that when $SNR < SNR_{max}^{(E)}$, the result is that all possible messages are received with equal probability independent of the one transmitted, then the communication can be considered secure. This idea is depicted in Fig. 1 and will be developed more in Section II where Kullback-Leibler (KL) divergence is used to fill the gap between practical secrecy and information-theoretic security.

The second contribution of this paper relates to the use of full-duplex jamming to enable very small, or even negative security gaps in practical coding schemes. Some existing schemes can already deliver small positive security gaps, e.g., interleaved and scrambled coding for secrecy schemes with hidden keys (ICSHK and SCSHK) [10], [11]. These schemes rely on the generation of a unique random interleaving/scrambling key that is used to shuffle a single message. The shuffled message and the key are then encoded together using a systematic error correcting code. The key is then removed/punctured (hidden) before transmission, which prevents an eavesdropper with a poor channel from obtaining/decoding the original information, but allows a legitimate receiver with a small advantage in signal quality to recover the message. More

recently a three-stage encoding scheme has been proposed [12], formed by the concatenation of a 1st-stage coset code [2], [13] with an ICSHK/SCSHK scheme[1] that approximates, upon decoding, a noiseless channel for Bob and a binary symmetric channel (BSC) for Eve between the output of the secrecy coder and the input of the corresponding secrecy decoder. The main limiting factor in most practical coding schemes is their inability to adapt, and thus, security and reliability are essentially hard-coded into the design with the choice of code parameters.

Recently, research in full-duplex jamming has been investigated using different methods such as those presented in [14], [15], [16] to provide secure wireless communications, and the adaptive digital self-interference cancellation technique applied in [17] shows the feasibility of full-duplex jamming. Furthermore, in [18] full-duplex self-jamming was employed to provide secure communications. The paper used pilot symbols known only to the legitimate receiver to estimate the self-interference channel and then remove it. Also, in [19], [20] full-duplex jamming and relaying has been investigated to improve secrecy and ensure reliability to the legitimate user, even for the case with an untrustworthy relay [20].

In this work, we aim to achieve smaller and more meaningful security gaps in practical secrecy coding schemes by resorting to a full-duplex jamming technique, where Bob acts as a jammer (self-jamming) while receiving Alice's transmission in tandem. The goal is to enable secure and reliable operation, even when Eve's channel is better than Bob's channel [21]. Since Bob controls the jamming power, he can also adjust to maximize security against Eve. Without loss of generalization, the three-stage encoding scheme for secrecy [12] is used in combination with full-duplex jamming for validation of the proposed approach, while also stressing the usefulness of the new security gap definition.

The remainder of the paper is organized as follows. Section II presents a new security gap metric that operates on KL divergence, and Section III gives background information on a previously invented scheme over which new ideas may be tested. Section IV introduces the system model for the paper, and self jamming at the receiver is highlighted as a means to secure transmitted information in Section V. An experimental setup of the scheme and results are given in Section VI, and Section VII concludes the paper and offers ideas for future work.

II. New Security Gap

Let M signify a secret message that Alice wishes to communicate to Bob. Alice codes the message and forms X^n a length-n codeword, which she transmits wirelessly to Bob, and Eve eavesdrops. Bob and Eve receive Y^n and Z^n, respectively, and attempt to decode the message. The decoder outputs for Bob and Eve are $\hat{M}$ and $\tilde{M}$, respectively. We assume that the messages are chosen uniformly at random from the message alphabet $\mathcal{M}$, and that Bob and Eves' decoders make hard decisions over the same alphabet.

We take the approach of [12] in measuring the secrecy of a practical coding scheme using the KL divergence. The KL divergence calculates a sort of a "distance" between two probability distributions, and can be used to evaluate statistical independence. The KL divergence between $p_{MA}(m,a)$ and $p_M(m)p_A(a)$ is given by

$$\mathbb{D}(p_{MA}||p_Mp_A) = \sum_{m\in\mathcal{M}}\sum_{a\in\mathcal{A}} p_{MA}\log_2\frac{p_{MA}}{p_Mp_A}, \qquad (2)$$

which approaches zero as $p_{MA}(m,a)$ approaches $p_M(m)p_A(a)$. Recall that the two distributions are equivalent if and only if M and A are independent, and $\mathbb{D}(p_{MA}||p_Mp_A) = \mathbb{I}(M;A)$. If we set A to the eavesdropper's observation Z^n, then we are working with a notion similar to strong information-theoretic security. The main difference is that we do not consider an asymptotic analysis as blocklength of an encoder gets large. For practical schemes over real-world channels, setting $A = Z^n$ does not tend to yield useful results, however, due to its difficulty to analyze [12]. In this paper, we set $A = \tilde{M}$. As long as Eve deploys best-practice decoding, meaningful security claims can still be made.

For practical coding schemes, an accurate estimation of KL divergence can be obtained from performing extensive Monte-Carlo simulations when $|\mathcal{M}|$ is small. Subsequent investigation of the joint probability distribution of messages and decoded messages [22], [12], thus enables a security analysis that is information-theoretic, although not identical to the traditional analysis of past information-theoretic security works.

The new security gap operates on $\mathbb{D}(p_{MA}||p_Mp_A)$, or equivalently $p_{\tilde{M}|M}(\tilde{m}|m)$ when $A = \tilde{M}$. Note that we can write the divergence so that

$$\mathbb{D}(p_{M\tilde{M}}||p_Mp_{\tilde{M}}) = \sum_{m\in\mathcal{M}}\sum_{\tilde{m}\in\mathcal{M}} p_{\tilde{M}|M}p_M\log_2\frac{p_{\tilde{M}|M}}{p_{\tilde{M}}}. \qquad (3)$$

When messages are assumed to be equally likely and channels are symmetric, then both $p_M(m)$ and $p_{\tilde{M}}(\tilde{m})$ are uniform distributions over the same message space. If $p_{\tilde{M}|M}(\tilde{m}|m)$ is also uniform for all m in the message alphabet, then the divergence is exactly zero, and no information about the message can be learned through $\tilde{M}$. Fig. 1 illustrates the new approach to defining a security gap with reference to this conditional distribution. We define our new lower security gap threshold to be the highest E_b/N_0 in Eve's reception such that

$$\mathbb{D}(p_{M\tilde{M}}||p_Mp_{\tilde{M}}) < \beta, \qquad (4)$$

where β is a small number chosen by the system designer. $(E_b/N_0)^{(E)}_{max}$ marks the edge of the secure zone for Eve, as shown in Fig 1. The new upper security gap threshold is similarly defined as the lowest E_b/N_0 in Bob's reception such that

$$\mathbb{D}(p_{M\hat{M}}||p_Mp_{\hat{M}}) \approx \delta, \qquad (5)$$

[1]The random interleaving/scrambling constitutes the 2nd stage, while the encoding with a systematic linear code followed by puncturing corresponds to the 3rd stage.

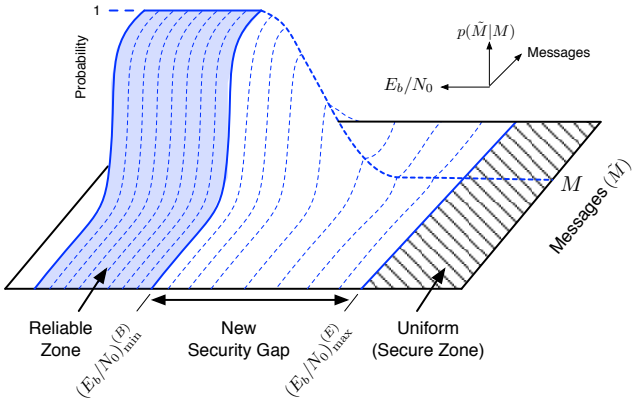


Fig. 1: The reliable zone shows where, with a high probability, messages received can be decoded correctly. The uniform region is where all possible messages are decoded uniformly no matter the transmitted message. The difference (measured in E_b/N_o dB) between the reliable zone in the legitimate receiver's curve and the uniform region in the eavesdropper's curve (sometimes the same curve as in this figure) is defined as the new security gap.

where δ is approximately $\mathbb{H}(M)$. $(E_b/N_0)^{(B)}_{min}$ marks the edge of the reliable zone for Bob. Note that, (5) corresponds in practice to a region of very low BER, thus instead BER measures can still be used to set up the reliability threshold $(E_b/N_0)^{(B)}_{min}$. Then

$$S_g = (E_b/N_0)^{(B)}_{min} - (E_b/N_0)^{(E)}_{max} \text{ dB}. \tag{6}$$

III. Background on the Three-Stage Encoding Scheme for Secrecy

This section presents the basic principles of the three-stage encoding scheme for secrecy proposed in [12]. This encoding scheme is formed by the concatenation of a coset-based code for secrecy [2], [13], with an ICSHK/SCSHK encoder [23], [10], [11]. The coset-based code can be optimized to guarantee information-theoretic security over a BSC, while the ICSHK/SCSHK technique, coupled with a Gaussian channel, generates an equivalent BSC for Eve, and an effectively noiseless channel for Bob [12].

A. Coset-based secrecy coding

The encoding procedure of an (n_1, k) coset-based code for secrecy can be described as follows. The encoder is given as

$$\dot{x}^{n_1} = \begin{bmatrix} m & m' \end{bmatrix} \begin{bmatrix} G \\ G^* \end{bmatrix}, \tag{7}$$

where $m \in \mathcal{M} = \{1, 2, \ldots, 2^k\}$ (but converted into binary), m' is a randomly chosen binary vector of length $(n_1 - k)$, G is the generator matrix of an $(n_1, n_1 - k)$ linear block code $\mathcal{C}$, and G^* is chosen so that $\begin{bmatrix} G \\ G^* \end{bmatrix}$ has full rank in GF(2). The cosets of $\mathcal{C}$ are $(C_1, C_2, ..., C_{2^k})$, where $\mathcal{C} = C_1$. The encoding operation in (7) allows m to choose the coset, and m' to choose a random codeword from the coset. Thus, the encoding process

TABLE I: Codebook structure for a $(4, 2)$ coset-based secrecy code.

M \ M'	0	1	2	3
0	0000	0011	1100	1111
1	0001	0010	1101	1110
2	1000	1011	0100	0111
3	1001	1010	0101	0110

of a given message involves simply choosing at random a codeword from its corresponding coset and transmitting it as $\dot{x}^{n_1}$. If $\dot{z}^{n_1}$ is a degraded version of $\dot{x}^{n_1}$ to the extent that there are enough flipped or erased bits of the message, Eve cannot reliably decode and recover the message m. Consider the example of a half-rate coset-based code of length $n_1 = 4$ presented in Table I. Say the message $m = 3$ is encoded and sent by Alice as the codeword $\dot{x}^{n_1} = \{0101\}$. If Eve receives the message as $\dot{z}^{n_1} = \{?101\}$, she is confused as to whether the original message was $m = 3$ or $m = 4$, as both $\{0101\}$ and $\{1101\}$ are options for decoding her received message and they are found in different cosets. Likewise, if Eve receives $\dot{z}^{n_1} = \{?10?\}$, she has no information about which message was sent, since a viable option is found in each of the four cosets.

B. ICSHK/SCSHK coding

The encoding procedure of an (n, n_1) ICSHK/SCSHK code can be described as follows. Per each input to the encoder $\dot{x}^{n_1}$, a random interleaving/scrambling key K of length n_k bits is generated. This key is used to shuffle the bits of $\dot{x}^{n_1}$, yielding $x_i^{n_1}$, which can be described as $\dot{x}_i^{n_1} = \dot{x}^{n_1} \times S_{f(K)}$, where $S_{f(K)}$ stands for an $(n_1 \times n_1)$ bit interleaving/scrambling matrix, which is a function of K. The key and the shuffled message are concatenated, and encoded with an $(n + n_k, n_1 + n_k)$ linear systematic code $\mathcal{C}'$, resulting into an $(n + n_k)$-length codeword $\ddot{x}^{n+n_k} = \begin{bmatrix} K^{n_k} & \dot{x}_i^{n_1} \end{bmatrix} G'$, where G' is the $(n_1 + n_k) \times n$ generator matrix of $\mathcal{C}'$. The final encoding step, corresponds to puncturing the key, resulting in the final codeword $x^n = \ddot{x}^{n+n_k} P$, where P is a $(n + n_k) \times n$ puncturing matrix. Therefore, the only knowledge about K in the transmitted data is encoded indirectly into the parity bits of x^n.

Upon decoding the procedure is reversed, with unknown values being set at the position of the punctured bits[2]. While soft-decoding can be carried upon decoding code $\mathcal{C}'$, a hard decision must be taken on the bits at this code's decoder output. This is true because an estimate of the key K is needed to deinterleave/unscramble the decoded message. It has been shown in [12] that when carrying transmission on the additive white Gaussian noise (AWGN) channel, the full chain from the input of ICSHK/SCSHK encoder to the decoder output can be modeled as a BSC.

IV. System Model

The top-level system model shown in Fig. 2 resembles a wiretap channel model. The transmitter Alice selects a

[2]Each unknown value is usually set to a zero log-likelihood ratio when soft-decoding is employed.

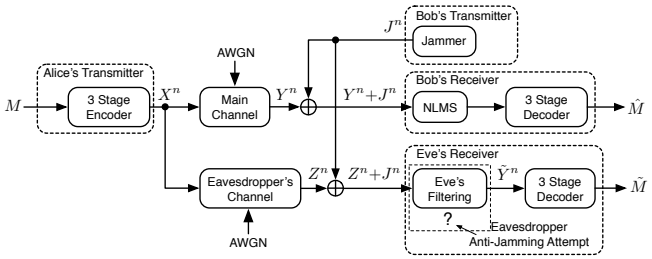


Fig. 2: System setup of an 3-stage encoder for secrecy with hidden key enhanced by the use of full-duplex jamming.

message $m \in (1, 2, ..., 2^k)$ with k number of message bits to pass through the three-stage encoder. After encoding the message, the length-n set of codewords X^n are sent through an additive white gaussian noise (AWGN) channel.

The legitimate receiver, Bob, obtains $Y^n + J^n$ whereas the eavesdropper, Eve, receives $Z^n + J^n$. The jamming noise J^n comes from Bob's transmitting antenna as an attempt to secure communications between Alice and Bob. The jamming transmitted provides a rise in the noise floor whereby Bob can obtain an advantage over Eve. The jamming noise continuously runs as long as Alice is transmitting the message.

We assume that Bob and Eve have equal computation capabilities, and both are equipped with a single receiving antenna. Further we assume that Eve's location is close enough to Bob that jamming significantly affects her. After Bob and Eve receive the message they try to recover X^n as closely as possible. They both apply noise estimation/cancellation signal processing techniques to get rid of the AWGN from the signals added by the channel and to synchronize their receivers to the messages obtained. However, the AWGN jamming forces a difference in the technique that Bob and Eve can use to regain an approximation on X^n. Bob uses a normalized least-mean squares (NLMS) adaptive filter to filter out his self generated jamming noise. Bob can use the NLMS filter because he has a reference jamming signal on which he can use to make an estimate on the jamming signal coming from his transmitting antenna. Real radio systems have used stochastic gradient descent algorithms to remove noise [24].

Eve has no reference signal like Bob since we assume Eve has one antenna. Therefore, this forces Eve to investigate other possible anti-jamming or filtering techniques. In our system model, we allow both Bob and Eve to apply the best practice decoder in their attempt to recover an approximation on the message.

V. Full-Duplex Jamming

Self-jamming has been tried on real radio systems to achieve secure communications [25]. We use a white Gaussian noise signal to jam because it is known to be the most penalizing jamming signal to a receiver [26]. Since the true communications channel also contributed AWGN, the effect of the jamming is to simply reduce the SNR at any receiver that does not have knowledge of the jamming signal [27].

There are many methods by which Bob could jam and all have trade-offs between conserving power and confusing Eve [28]. In this paper, for a matter of clarity on the principal of self-jamming, Bob employs a continuous jammer as Alice transmits. Then Eve's effective SNR is

$$\frac{E_b}{(N_o + \sigma^2)}, \tag{8}$$

where E_b is the energy per bit, N_o is the noise spectral density and σ^2 is the jammer's total instantaneous power, all measured at Eve's receiver. Thus, the jamming power σ^2 governs Eve's operating SNR along with the noise in the eavesdropper's channel [27].

A. Normalized Least-Mean Squares Filtering

Bob needs to estimate the transmitted jamming signal so that he can eliminate self-interference to ensure that he can reliably obtain Alice's message. We choose the NLMS technique to adaptively filter out the jamming noise because of Bob's knowledge of his self-generated signal. In practice, he cannot just simply subtract out the jamming because he will receive a signal with high correlation to the jamming noise that differs due to imperfections in the transmitting antenna.

The NLMS [29] filter is an adaptive filter that can determine the optimum filter coefficients to eliminate the jamming noise due to the fact that Bob has a reference with which to determine the optimal coefficients. The adaptive NLMS filter obtains the optimal filter coefficients by approximating the optimum Wiener-Hopf solution and the derivation shown in [30].

First, the signal Y^n is filtered to produce $\dot{Y}^n$, and the estimation error is calculated at time u by

$$e_u = j_u - \dot{y}_u, \tag{9}$$

where j_u is Bob's self-jamming signal at time u. The filter coefficients are then adapted to minimize the error signal E in the normalized least-mean square sense. As this occurs, the filter's characteristics change until the output signal is nearly devoid of the jamming signal altogether. Bob must select a step-size μ to govern the speed of the adaptation in the usual way [30]. Eve cannot use the NLMS algorithm because she lacks a priori knowledge of J.

VI. Evaluation

A. Experiment Setup

A (7,4) Hamming code provides the generator matrix for our coset-based secrecy encoder, while the ICSHK employs a $(1536, 1280)$ LDPC code from the WiMAX standard [31], and considers a random key of $n_k = 100$ bits, producing codewords X^n (see Fig. 2) of length 1436 bits after puncturing. Secrecy codewords at the output of coset-based code are buffered in order to provide proper input to the ICSHK coder. The resulting binary string is then sent over the AWGN channel.

While receiving messages, Bob transmits a continuous jamming signal. Different Gaussian variances are used in separate

simulations to represent the various levels of instantaneous power employed by the jammer. Bob implements NLMS filtering to cancel out jamming Gaussian noise interference. The five tap NLMS filter uses a variable step-size of 0.04 and 0.005 to obtain a fast yet stable approximation of its optimal filter coefficients.

B. Results

Before the results of the new security gap experiment can be presented, it is important that several quantities are expounded upon. In the experiments that follow, $SNR_{min}^{(B)}$ refers to the SNR at the point which the minimum amount of reliability required by Bob is met. The minimum reliability will be represented by the probability $P_{\tilde{M}|M=5}(\tilde{m}) > 0.99$. The SNR at which the minimum level of security is met will be represented by the quantity $SNR_{max}^{(E)}$. The minimum level of security will be represented by the probability $P_{\tilde{M}|M=5}(\tilde{m}) < 0.14$ and $P_{\tilde{M}|M=i}(\tilde{m}) \approx 0.12$ for $i \neq 5$.

The three-stage scheme presented in [12] performs well and assumes that the eavesdropper uses a best-practice decoder. Fig. 3a, provided in the results of [12], shows a steep probability change when E_b/N_o goes from 6.5 dB to 8 dB. The security gap here is the minimum amount of difference between E_b/N_o required to guarantee the Bob's security over Eve. A security gap of 2.5 dB exists at this range because if operating at 8 dB, Bob can obtain the correct message with $p_{\tilde{M}|M=5}(\tilde{m}) > 0.99$. However, if Eve operates at 6.5 dB, she can obtain the correct message with only $p_{\tilde{M}|M=5}(\tilde{m}) < \alpha$ where α is a very small number. Note that if both Bob and Eve operate at the same E_b/N_o then there does not exist a security gap.

The probability of the receiver's approximated message being the same as the transmitted message is the same for Bob and Eve when no jamming signal is transmitted. Fig. 3b shows the resulting graph for Bob. Eve's graph is not shown, as it is virtually indistinguishable from Bob's. Thus, if the SNR is the same for both Eve's channel and Bob's channels, and no jamming transmission is sent by Bob, then they will be able to recover the same amount of information about the sent message.

Fig. 4 shows the results of jammer transmitting from a Gaussian distribution with a variance of $\sigma^2 = \frac{1}{32}$. Scanning the $\frac{E_b}{N_o}$ range of 0 dB to 12 dB, it can be seen in Eve's probability curve in Fig. 4b (and verified in simulation results) that $SNR_{max}^{(E)} \approx 6.8$ dB. Based on Bob's probability curve in Fig. 4a, $SNR_{min}^{(B)} \approx 11$ dB. According to equation (1), the security gap of this transmission is therefore $S_g = 4.2$ dB, that is, Bob's SNR must be at least 4.2 dB higher than Eve's in order to achieve reliable communication and give Eve a very low chance of decoding the message correctly. Fig. 5 shows the results when the continuous jammer doubles its power from $\frac{1}{32}$ to $\frac{1}{16}$. Eve's probability curve shows that $SNR_{max}^{(E)} \approx 8.4$ dB. Based on Bob's probability curve in Fig. 4a, $SNR_{min}^{(B)} \approx 11$ dB. Thus, the security gap of this transmission is $S_g = 2.6$ dB, that is, Bob's SNR must be at least 2.6 dB higher than Eve's to achieve the reliability and security goals.

In Fig. 6, the jamming power of a transmission is again doubled to $\frac{1}{8}$. The secrecy threshold is $SNR_{max}^{(E)} > 12$ dB. The reliability threshold is $SNR_{min}^{(B)} \approx 11$ dB. So, in this case, the security gap $S_g < -1$ dB. This is a very interesting result, because it indicates that even if Eve has a *better* location to listen from, Bob can still receive his message reliably while a level of information-theoretic security is leveled against Eve.

It can be seen that the security gap decreases as Bob increases the power of his jamming transmissions. In Fig. 7, this relationship is shown. The new security gap is plotted with respect to the jamming power. Thus, using full-duplex jamming, Bob is able to create a significant advantage over Eve in terms of channel reliability.

As shown in [12], $\mathbb{D}(p(m, \tilde{m})||p(m)p(\tilde{m})) \to 0$ indicates no information leakage which happens when the probability curves tends to uniformity in the messages. The results show that with continuous self-jamming Bob can cause Eve to have a KL divergence that approaches zero faster than himself as seen in Fig. 5. The rapid decrease in receiving the correct message on Eve's end occurs from 12 dB to 8 dB. Whereas, for Bob the decrease occurs from 12 dB to 5 dB. Bob due to his NLMS adaptive filtering can operate at a near equal amount of $\frac{E_b}{N_o}$ ranges independent of the jamming powers observed in the simulations.

VII. Conclusion

In this paper, we present a new stronger security gap based on information-theoretic concepts, while assuming knowledge of Eve's decoder. Self-jamming with NLMS adaptive filtering is also shown to decrease the security gap for practical coding schemes over the Gaussian wiretap channel, like the three-stage coding scheme in [12]. Future work will address additional steps that can be taken by Eve to combat the jamming, such as blind source separation algorithms.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J*, vol. 28, pp. 656–715, 1948.

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

[3] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5g wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, April 2018.

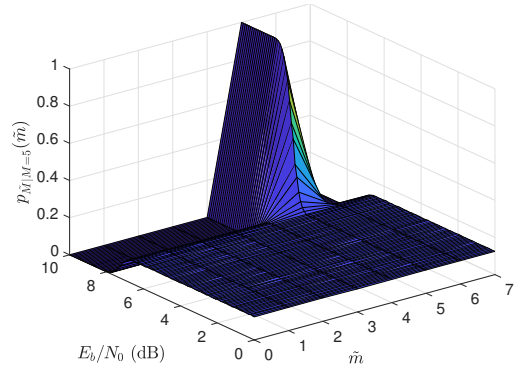
[4] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*, 1st ed. Springer Publishing Company, Incorporated, 2009.

[5] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

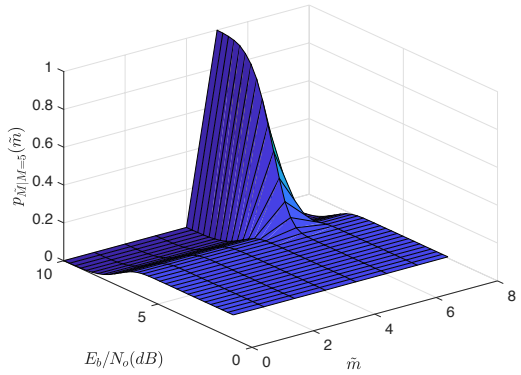
[6] Y. Liang, H. V. Poor, and S. S. (Shitz), "Information theoretic security," *Foundations and Trends® in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, 2009. [Online]. Available: http://dx.doi.org/10.1561/0100000036

[7] W. K. Harrison, D. Sarmento, M. A. C. Gomes, and J. P. Vilela, "Analysis of short blocklength codes for secrecy," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, Oct. 2018. [Online]. Available: https://doi.org/10.1186/s13638-018-1276-1

[8] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 532–540, 2011.

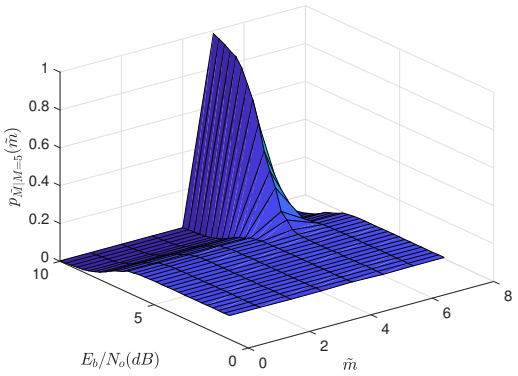


(a) The curve presented in [12].

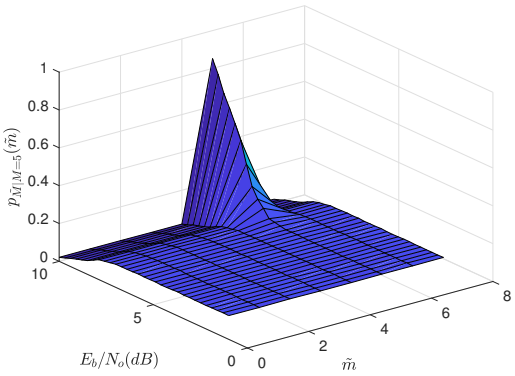


(b) The curve presented using our Simulink model.

Fig. 3: These curves show the probability of recovering a certain three-bit message across the SNR range of 0 to 10 dB without any jamming transmissions. Curve (a) was presented in [12]. Curve (b) is our Simulink replication of curve (a). Differences in the two figures are a result of different code parameters to each coding stage of the ICSHK.

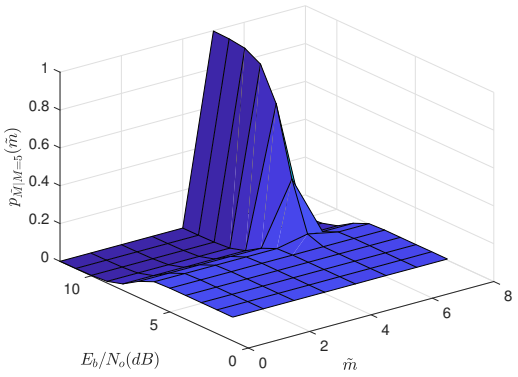


(a) Bob's curve.

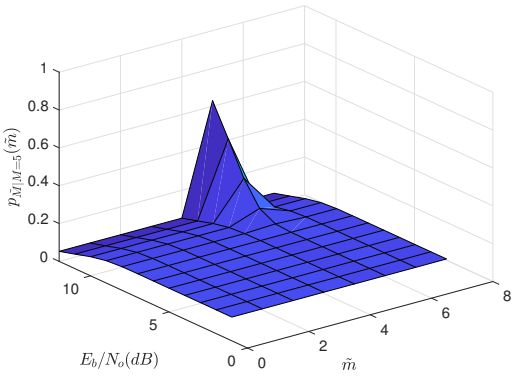


(b) Eve's curve.

Fig. 4: These curves show the probability of correctly receiving a three-bit message at a range of SNR values while Bob transmits a jamming signal with an instantaneous power of $\sigma^2 = 1/32$.



(a) Bob's curve.

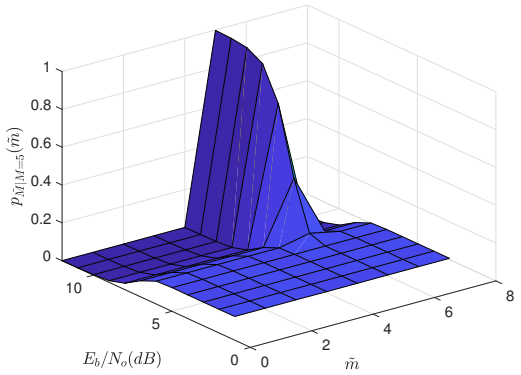


(b) Eve's curve.

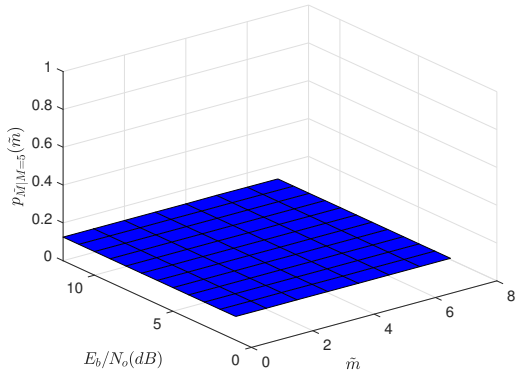
Fig. 5: These curves show the probability of correctly receiving a three-bit message at a range of SNR values while Bob transmits a jamming signal with an instantaneous power of $\sigma^2 = 1/16$.

[9] M. Baldi, G. Ricciutelli, N. Maturo, and F. Chiaraluce, "Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel," in *Proc. IEEE Int. Conf. Communication Workshop (ICCW)*, June 2015, pp. 435–440.

[10] J. P. Vilela, M. Gomes, W. K. Harrison, D. Sarmento, and F. Dias, "Interleaved concatenated coding for secrecy in the finite blocklength



(a) Bob's curve.



(b) Eve's curve.

Fig. 6: These curves show the probability of correctly receiving a three-bit message at a range of SNR values while Bob transmits a jamming signal with an instantaneous power of $\sigma^2 = 1/8$.

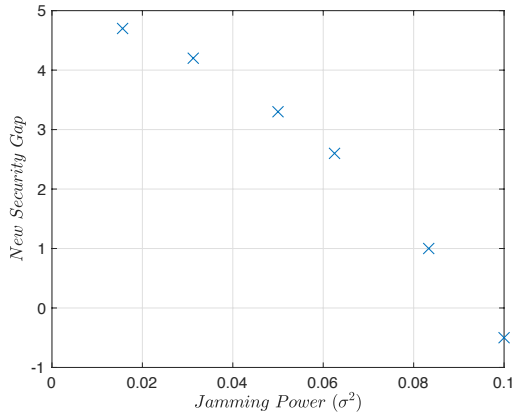


Fig. 7: Security gap as a function of jamming power.

regime," *IEEE Signal Processing Letters*, vol. 23, no. 3, pp. 356–360, Mar. 2016.

[11] C. Martins, T. Fernandes, M. Gomes, and J. Vilela, "Testbed implementation and evaluation of interleaved and scrambled coding for physical-layer security," in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, June 2018, pp. 1–6.

[12] W. K. Harrison, T. Fernandes, M. A. C. Gomes, and J. P. Vilela, "Generating a binary symmetric channel for wiretap codes," *IEEE Transactions on Information Forensics and Security*, (under submission).

[13] L. H. Ozarow and A. D. Wyner, "Wiretap channel II," *AT&T Bell Laboratories Tech. J.*, vol. 63, no. 10, pp. 2135–2157, December 1984.

[14] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, Oct 2013.

[15] N. H. Mahmood, I. S. Ansari, P. Mogensen, and K. A. Qaraqe, "On the ergodic secrecy capacity with full duplex communication," in *2017 IEEE International Conference on Communications (ICC)*, May 2017, pp. 1–6.

[16] I. T. Cummings, T. J. Schulz, J. P. Doane, S. A. R. Zekavat, and T. C. Havens, "Information-theoretic optimization of full-duplex communication between digital phased arrays," *Proc. IEEE Allerton Conference*, 2018.

[17] N. Li, W. Zhu, and H. Han, "Digital interference cancellation in single channel, full duplex wireless communication," in *2012 8th International Conference on Wireless Communications, Networking and Mobile Computing*, Sept 2012, pp. 1–4.

[18] S. Yan, X. Zhou, N. Yang, T. D. Abhayapala, and A. L. Swindlehurst, "Secret channel training to enhance physical layer security with a full-duplex receiver," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2788–2800, Nov 2018.

[19] H. Qi, Q. Wang, Y. Wang, and Y. Dong, "Secrecy rate and power allocation of full duplex relay network with full duplex hybrid relaying-and-jamming scheme," in *2016 19th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, Nov 2016, pp. 487–491.

[20] R. Nirala, S. S. Chauhan, and G. Verma, "Improving physical layer security in full-duplex relaying system," in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*, May 2017, pp. 997–1001.

[21] J. P. Vilela and J. S. Sousa, "Physical-layer security against non-degraded eavesdroppers," in *Global Communications Conference (GLOBECOM), 2015 IEEE*. IEEE, 2015, pp. 1–6.

[22] J. Pfister, M. Gomes, J. P. Vilela, and W. K. Harrison, "Quantifying equivocation for finite blocklength wiretap codes," in *Proc. IEEE Int. Conf. Communications (ICC)*, Paris, France, June 2017, pp. 1–6.

[23] D. Sarmento, J. Vilela, W. K. Harrison, and M. Gomes, "Interleaved coding for secrecy with a hidden key," in *2015 IEEE Globecom Workshops (GC Wkshps)*, Dec 2015, pp. 1–6.

[24] A. Quadri, M. R. Manesh, and N. Kaabouch, "Denoising signals in cognitive radio systems using an evolutionary algorithm based adaptive filter," in *2016 IEEE 7th Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*, Oct 2016, pp. 1–6.

[25] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *2011 Proceedings IEEE INFOCOM*, April 2011, pp. 1125–1133.

[26] S. N. Diggavi and T. M. Cover, "The worst additive noise under a covariance constraint," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 3072–3081, Nov 2001.

[27] R. Poisel, *Modern Communications Jamming: Principles and Techniques*. Artech House, 2011.

[28] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: A survey," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 17, no. 4, pp. 197–215, 2014.

[29] S. Haykin, *Adaptive Filter Theory (3rd Ed.)*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1996.

[30] N. Benvenuto and G. Cherubini, *Algorithms for communications systems and their applications*. John Wiley & Sons, 2002.

[31] *Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems - Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands*, IEEE Std. 802.16e, 2005.