Interleaved Concatenated Coding for Secrecy in the Finite Blocklength Regime

João P. Vilela, Marco Gomes, Willie K. Harrison, Dinis Sarmento, Fábio Dias

***Abstract*—We propose a systematic concatenated coding scheme based on the combination of interleaving with powerful channel codes and jamming for wireless secrecy under the practical assumption of codes in the finite blocklength regime. The basic idea lies in generating a short random key that is used to shuffle/interleave information at the source, Alice. This key is then sent to the legitimate receiver, Bob, during a brief period of advantageous communication over the eavesdropper Eve (e.g., due to more interference from a jammer). Finally, the key is decoded at Bob to properly deinterleave the original information. Bob receives a better quality version of the interleaving key, therefore having the needed advantage over Eve. Information reliability is provided by a strong inner code, while security against Eve results from the proper selection of the outer code and interference levels over the key. We propose a methodology for selection of the outer code with reliability and security constraints. For that, we introduce bit error complementary cumulative distribution function metrics, suitable for security and reliability analysis of error correcting codes.**

***Index Terms*—wireless, secrecy, finite blocklength, coding, interleaving, jamming.**

I. Introduction

Physical-layer security [1] is emerging as a promising approach that relies on the physical characteristics of wireless channels to enhance the secrecy level of these networks. This area has its roots in a contribution by Wyner [2] that showed in 1975 that there exist codes (wiretap codes) simultaneously guaranteeing reliable communication to Bob and secrecy against Eve. Wyner's work was based on the assumption of Eve observing a degraded version of the information being transmitted. The need for such an advantage over the adversary, along with the appearance of major cryptographic techniques, left this work in a dormant state until recently.

Wireless networks brought a renewed interest in this area, with possible sources of advantage over an adversary eavesdropper coming from (a) a better signal quality due to the varying nature of wireless channels [3], or (b) the use of cooperative relays [4] or friendly jammers [5]; enabling to either improve the signal quality of Bob or cause interference to Eve. However, building wiretap codes for these types of networks remains a formidable challenge; it was only recently that the first practical codes were discovered [6], and current designs still suffer from shortcomings and limiting assumptions. For example, most codes are designed to meet secrecy criteria only in the asymptotic blocklength regime; and thus, in real systems with finite blocklength, wiretap code performance is not guaranteed. Moreover, in spite of efforts towards analytical study of coding schemes over more realistic channel models [7], these efforts have proven elusive to construction and analysis of coding schemes under the finite blocklength regime [8]. This led to more empirical metrics (such as based on the bit error rate (BER)), that do not satisfy information-theoretic security requirements, but simplify system design over practical channels. An interesting recent advance [9], [10] provides a mechanism for bounding the equivocation rate of finite blocklength codes over the BPSK-constrained AWGN channel for specific coding schemes. In a similar fashion, results in [11] provide bounds for worst-case error rates over finite blocklength codes.

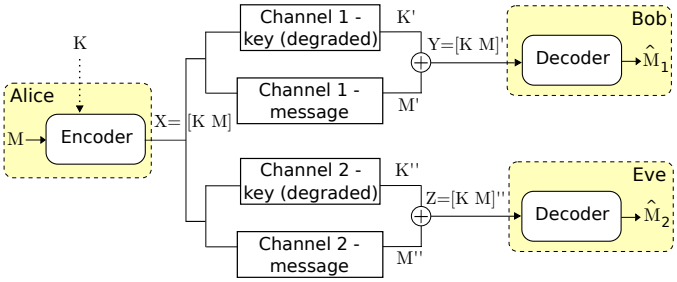

Fig. 1. Wiretap channel variant where an interleaving key K is sent with the original message M. The key is sent during a period in which a jammer is active, hence the degraded channels during the transmission of the key.

Most explicit constructions for realistic channels rely on non-systematic coding approaches, such as punctured low-density parity-check (LDPC) codes [12] and scrambling of information bits [13], to avoid directly exposing the secret information bits. Klinc et al. [12] introduce the concept of security gap, i.e., the ratio between Bob and Eve's channel quality required to achieve a desired level of physical-layer security, and propose a coding scheme in which messages are transmitted over punctured bits to hide information from eavesdroppers, thus leading to a small security gap. In [14] the puncturing concept is extended to random puncturing with a pattern that is kept secret from the eavesdropper, and analyzed over binary erasure channels. In [13], Baldi et al. propose further reducing the security gap by scrambling information bits over blocks of concatenated frames. When Eve's channel is not worse than Bob's channel, a feedback automatic repeat request (ARQ) mechanism is shown to provide secrecy at the cost of retransmissions and increased latency. Some authors have attempted to address reliability and security requirements of wiretap codes over simple channel models in a concatenated

João P. Vilela (jpvilela@dei.uc.pt) is with CISUC, Dep. of Informatics Engineering, University of Coimbra, Portugal. Marco Gomes (marco@co.it.pt), Dinis Sarmento and Fábio Dias ({dinis.pereira,dias.fabio}@student.uc.pt) are with Instituto de Telecomunicações, Department of Electrical and Computer Engineering, University of Coimbra, Portugal. Willie Harrison (wharriso@uccs.edu) is with the Department of Electrical and Computer Engineering, University of Colorado Colorado Springs, USA. This work was partially funded by the iCIS project under grant CENTRO-07-ST24-FEDER-002003, and FCT (Fundação para a Ciência e Tecnologia) projects PTDC/EEI-TEL/3684/2014 (SWING2) and Instituto de Telecomunicações PEst-UID/EEA/50008/2013 (pluriannual funding and project WINCE).

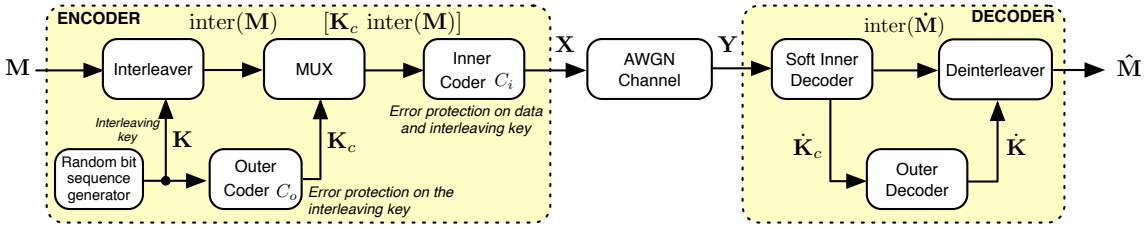

Fig. 2. Encoder and decoder processes of random-key interleaved coding for secrecy.

coding approach so that the parameters of the inner code can be adjusted to maintain both security against Eve and reliability for Bob at the outer code [15], [16]. Concatenated coding for secrecy may yield significant results if allowances can be made for more practical channels.

In this work, we propose a concatenated coding scheme for secrecy under the assumption of finite blocklength codes over practical channels. Our scheme is based on the combination of interleaving with powerful channel codes and jamming for secrecy, where a strong inner code is used to provide typical levels of data reliability. The proper selection of an outer code and interference levels over a transmitted interleaving key warrants reliability to Bob and secrecy against Eve.

II. System and Attacker Model

Consider the Gaussian wiretap channel system model variant depicted in Fig. 1, where Alice wants to send a message M to Bob while Eve is overhearing information. Unlike the typical setup, a different interleaving key K is generated and concatenated with each message M and fed to the encoder before being sent to the channel by Alice with transmit power P_a. We additionally consider the presence of a jammer that causes interference (extra additive white Gaussian noise) with transmit power $P_j = \alpha P_a$ (a fraction α of the transmit power of Alice). The jammer is active only during the transmission of the interleaving key with the goal of inducing a degraded channel for the eavesdropper, but can also cause interference to the key on its way to Bob (hence a degraded channel for both). Means to achieve a temporary degradation of the eavesdropper include, for example, a signaling scheme [17] that enables the temporary trigger of jammers during a transmission. The negative effect of jamming on legitimate communication can be addressed, for example, through the use of directional-antenna jammers to degrade communication outside a given area of legitimate devices (e.g., a warehouse) [18], or near-field communication with a jamming receiver that may be able to mitigate its self-generated interference [19]. Our work does not require full channel-state information at the transmitter; it is sufficient to guarantee a known advantage over Eve (e.g., Eve lying outside a given physical area).

Let $\dot{X}$ represent a block of data X (e.g., message M or key K) that has been decoded, while $\hat{X}$ corresponds to an approximation of the original data X obtained at the destination. K_c represents the coded version of an interleaving key K, and $\mathcal{S}_x$ the size of X. Finally, we consider interleaving and deinterleaving functions inter$(\cdot)$ and deinter$(\cdot)$ that perform a random permutation of the information received. The random permutation is performed by having the set of symbols/bits of the message rearranged according to a permutation table defined by the key K, which is chosen at random for each new message from one of the $\mathcal{S}_m!$ possible permutations.

We consider a passive eavesdropper adversary with equal capabilities as the legitimate receiver. In particular, the eavesdropper is aware of the encoding and decoding processes and is able to decode the original information if data is received with sufficiently low noise levels.

III. Interleaved Coding for Secrecy (ICS)

Fig. 2 details the encoder and decoder processes. The encoder and decoder are the same for Bob and Eve, the only difference being the quality of the channels. The scheme works to ensure both reliability for Bob and secrecy against Eve by exploiting these channel differences, some of which are due to nature (during the message transmission), and some of which are due to jamming (during the transmission of the key).

Reliable transmission (i.e., robust to channel errors) is assured by employing a powerful systematic inner code C_i with dimensions (η_i, κ_i). A different random binary interleaving key K, with size $\mathcal{S}_k$, is generated per message M, with size $\mathcal{S}_m$, and is used to shuffle/interleave the contents of M before being sent through the channel. Due to its importance to deshuffle M at the destination, the interleaving key K is additionally protected by an outer code C_o with dimensions (η_o, κ_o), therefore producing a coded version of the key, K_c, with size $\mathcal{S}_{k_c} = \eta_o$. The concatenated block $[K_c \text{ inter}(M)]$ is then encoded by C_i producing the codeword X that is sent through an additive white Gaussian noise (AWGN) channel.

On the decoder end, Bob (respectively Eve) performs typical soft iterative decoding of the received word Y (Z for Eve) producing an estimate of the interleaved message, inter$(\dot{M})$ and of the coded key $\dot{K}_c$. The correct determination of the interleaving key is critical to deshuffle inter$(\dot{M})$ and obtain $\hat{M}$; because the mapping between keys and permutations is random, a different key produces an approximation $\hat{M}$ completely different from the original message M for a correctly received inter(M). For that, the key goes through an additional decoding step with the outer code C_o, therefore producing a better estimate $\dot{K}$ of the original interleaving key to deshuffle the original message and produce $\hat{M}$.

The use of a systematic inner code C_i enables a jammer to cause interference only during the short period of the transmission of the coded interleaving key K_c. Practical security is then achieved at the cost of a slight decrease on the information rate with the useful code rate being $R_u = \frac{\kappa_i - \eta_o}{\eta_i}$ (where $\eta_o = \mathcal{S}_{k_c} \ll \kappa_i$). Due to the jammer's short activity period ($\eta_o \ll \eta_i$), the energy cost of jamming over the key is also small and can be measured as the jammer energy per information bit, E_{Jb}, normalized to Alice's energy per

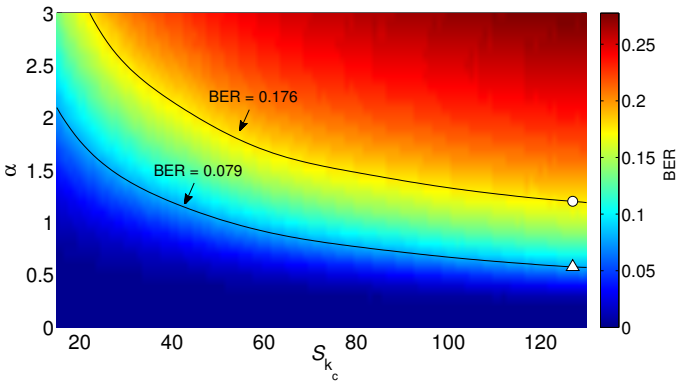

Fig. 3. BER on the interleaving key portion of $[K_c \text{ inter}(M)]$ as function of varying jamming power $P_j = \alpha P_a$ and key size $\mathcal{S}_{k_c}$, for C_i an LDPC$(1056, 880)$ code that provides a BER = 10^{-5} for decoding a transmission over an AWGN channel at SNR = 6.38 dB. For B&W visualization, the gradient on the right bar follows the same order as in the plot.

information bit, E_b, as follows

$$E_{Jb}/E_b = \frac{\eta_o P_j}{\kappa_i - \eta_o} \div \frac{\eta_i P_a}{\kappa_i - \eta_o} = \alpha \cdot \frac{\eta_o}{\eta_i} \ . \tag{1}$$

IV. Outer Code Selection Methodology

The selection of a proper outer code C_o is instrumental to guarantee reliability to Bob and confidentiality against Eve. C_o must be strong enough so as to correct expected key errors on Bob and not too strong so as not to correct key errors at Eve. For that, we consider BCH (Bose-Chaudhuri-Hocquenghem) codes, but any other t-error correcting code can be applied.

Let us assume that an inner code C_i (e.g., LDPC or turbo-code) was selected to provide a desirable reliability level (e.g., BER = 10^{-5}) for communication of an arbitrary data block X between Alice and Bob at a given signal-to-noise ratio (SNR). We then consider X as the concatenation of the coded key with the interleaved message, i.e., $[K_c \text{ inter}(M)]$. To determine how many errors the outer code C_o must be able to correct in order to return a correct deinterleaving key K, we can analyze the BER of C_i over the portion of X corresponding to K_c alone as a function of varying jamming power α and key size $\mathcal{S}_{k_c}$ for that selected SNR level. Fig. 3 presents those results with C_i as an LDPC $(1056, 880)$ code that provides a 10^{-5} BER at a selected SNR = 6.38 dB.

An outer code with dimensions (η_o, κ_o) that is able to correct up to t errors can successfully decode a BER $\leq t/\eta_o$, assuming an uniform error distribution. For example, a BCH(127,64) code under bounded-distance decoding corrects up to 10 errors, therefore being able to recover from a BER of $\frac{10}{127} \approx 0.079$. For Eve to obtain a BER higher than that, a jamming power of $\alpha \geq 0.6$ is required, as marked by the triangle in Fig. 3.

However, with the BER being an average metric, in practice we may have at times fewer than t errors, which is compensated by having at other times more than t errors. Therefore, we look instead to the distribution of errors of K_c and propose the Bit Error Complementary Cumulative Distribution Function (BE-CCDF) as an alternative metric for selecting the code C_o or adjusting the jamming power α.

Definition 1 (Bit Error Complementary Cumulative Distribution Function): The bit error complementary cumulative distribution function, BE-CCDF($t, \mathcal{S}_k, \alpha, C$,SNR), is the probability of having more than t errors, $\mathbb{P}\{E > t\}$, as a function of the jamming power α for a key of size $\mathcal{S}_k$, considering a code C operating at a given SNR.

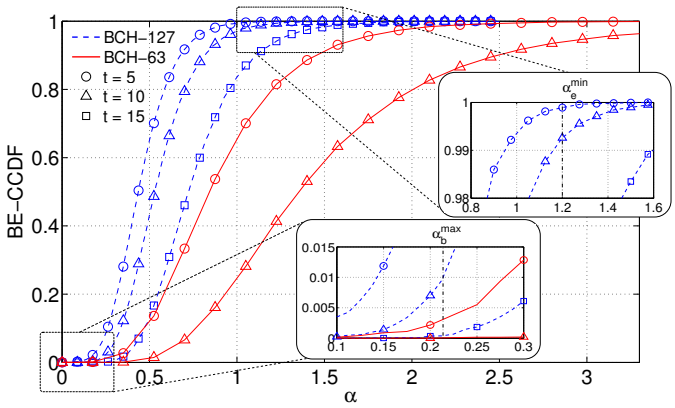

Fig. 4. BE-CCDF of K_c as a function of a jamming power of $P_j = \alpha P_a$ applied over K_c, for C_i an LDPC$(1056, 880)$ decoding at the selected SNR of 6.38 dB for reliability. We consider two key sizes $\mathcal{S}_{k_c} = [127, 63]$ that relate to BCH codes of those lengths ($\mathcal{S}_{k_c} = \eta_o$). The different markers correspond to the number of errors $t = [5, 10, 15]$ that the BCH codes $(127, [92, 64, 36])$ and $(63, [36, 18])$ can correct.

Due to the complexity of analysis of LDPC codes, we evaluate the BE-CCDF through Monte Carlo simulation of the probability of errors over a large number of random blocks.

The BE-CCDF allows us to determine the amount of jamming power that is needed so that the probability of having more than t errors (and hence being unable to decode the key, if under bounded-distance decoding) is greater than a desired security threshold. We present this distribution in Fig. 4 for the same LDPC inner code and C_o the BCH(127,64) that corrects up to 10 errors under bounded-distance decoding. This figure shows that for an $\alpha = 0.6$, $\mathbb{P}\{E > 10\}$ is just around 0.65, meaning that one would still be able to obtain the interleaving key more than 1/3 of the time.

We argue that the BE-CCDF metric can be used to fine tune the security and reliability levels of the system. For example, for the BCH(127,64) code, if we wanted a reliability level of at least 0.99, i.e., $\mathbb{P}\{E > 10\} < 0.01$, Bob would have to suffer a level of interference below $\alpha_b^{\max} \approx 0.21$. For a security level of $\mathbb{P}\{E > 10\} > 0.99$, Eve would have to suffer a level of interference above $\alpha_e^{\min} \approx 1.2$. In this case we would have a BER ≈ 0.176 (circle in Fig. 3), but, more importantly, a 99% probability of having more than 10 errors and being unable to decode the interleaving key, which is far more acceptable from a security perspective. This threshold can be adjusted to become closer to 100% with a corresponding penalty in the required jamming power over Eve. This change in how the BER is used to analyze security in a system, enables stronger guarantees (e.g., on the 1st percentile or more) on error rates of secrecy codes in the finite blocklength regime.

This leads to the methodology for selecting the outer code of Table I. In the first case (A), we fix the outer code (e.g., one that leads to a small penalty in the useful code rate) and design the system to provide the required interference over the eavesdropper to guarantee a prescribed level of security. In the second case (B), the system setup is already fixed and we determine a proper code to guarantee a desired level of

TABLE I
OUTER CODE SELECTION METHODOLOGY

(A) Fix the outer code and design the system so as to provide the necessary advantage (extra interference) over the eavesdropper:

1) select a systematic inner code C_i with dimensions (η_i, κ_i);
2) select an outer code C_o with dimensions (η_o, κ_o) and error correction capability of t errors;
3) generate the BE-CCDF curve for number of errors $E > t$ and a given SNR, for varying jamming power α;
4) define the desired security threshold for Eve τ_e and reliability threshold for Bob τ_b s.t. $\mathbb{P}\{E > t\} > \tau_e$ and $\mathbb{P}\{E > t\} < \tau_b$;
5) determine the minimum level of interference over Eve, $\alpha_e^{\min}$, and maximum level of interference over Bob, $\alpha_b^{\max}$, from the BE-CCDF and design the system appropriately to guarantee them.

(B) Fix the system parameters (expected interference) and select an appropriate outer code:

1) select a systematic inner code C_i with dimensions (η_i, κ_i);
2) obtain the minimum level of interference expected at Eve, $\alpha_e^{\min}$, and the maximum level of interference expected at Bob, $\alpha_b^{\max}$;
3) define the desired security threshold for Eve τ_e and reliability threshold for Bob τ_b;
4) generate BE-CCDF curves for several BCH codes that correct up to t errors under bounded-distance decoding;
5) from the set of considered codes, select an outer BCH code that guarantees $\mathbb{P}\{E > t\} > \tau_e$ and $\mathbb{P}\{E > t\} < \tau_b$.

security. In both cases, either the system or the code must be chosen to provide low probability of errors to Bob.

Note that although we have presented specific codes with bounded-distance decoding to illustrate the concept, our scheme can accommodate more powerful codes or decoding algorithms (e.g., soft-decision decoding) by varying the number of errors t that the code can correct. Of course, higher error correcting capabilities at Eve will necessarily lead to higher jamming power requirements over the interleaving key.

V. SECURITY EVALUATION

We now present security results for our coding scheme following the design of the previous section, i.e., with an outer BCH$(127, 64)$ code and an inner LDPC$(1056, 880)$ code. According to the BE-CCDF metric, this leads to a reliability level of $\mathbb{P}\{E > 10\} < 0.01$ for Bob and security level of $\mathbb{P}\{E > 10\} > 0.99$ for Eve, under maximum and minimum interference levels of 0.21 and 1.2, respectively.

Fig. 5(a) depicts the relation between the interference level (α) over the interleaving key and the achieved BER of our coding scheme (where a BER of 0.5 for Eve is deemed desirable). The different curves show the degradation of BER on the message M with increasing transmit power of a jammer ($P_j = \alpha P_a$) that is active only during the exchange of the interleaving key. Reliability to Bob (e.g., BER$= 10^{-5}$) can be achieved with little E_b/N_0 loss as long as the interference is limited (e.g., $\alpha \leq 0.2$). The drawback of the BER as a security metric for short blocklengths becomes apparent when, for example, for $\alpha = 1.2$ with $E_b/N_0 = 9.5$ dB the average BER is ≈ 0.45 (left plot); yet, looking at the distribution of BER values obtained we observed that roughly 10% of the blocks present an error rate below the average BER of 0.45.

To address this issue, we resort to a new metric, the BER-CCDF, based on the entire distribution of errors. This metric allows us to guarantee decoder failure with high probability, in addition to a high BER at the output of the decoder. Let $\hat{P}_b$ be an estimate of the proportion of bits in error of the message

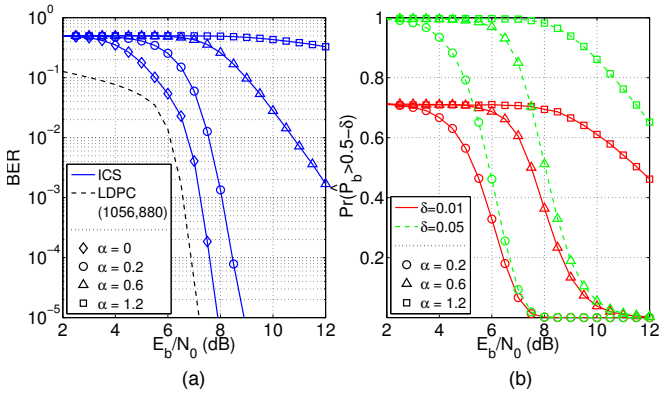

Fig. 5. Figures (a) and (b) show the variation of the BER and BER-CCDF^{ac} (respectively) with E_b/N_0 of our scheme (ICS) for different levels of jamming transmit power ($P_j = \alpha P_a$) on the interleaving key. The codes C_i and C_o employed were respectively an LDPC$(1056, 880)$ and a BCH$(127, 64)$ (useful code-rate ≈ 0.71). For reference, the curve for the operation of the LDPC alone (considering a BPSK transmission and using the sum product algorithm for decoding) is provided in Fig. (a).

at the output of the decoder.

Definition 2 (Bit Error Rate-CCDF): The Bit Error Rate-Complementary Cumulative Distribution Function, BER-CCDF$^{ac}(\delta,\ \alpha,\ \mathcal{S}_b,\ \mathcal{C})$ is the quantity $\Pr(\hat{P}_b > 0.5 - \delta)$ calculated over $\mathcal{S}_b$ estimated message bits for a code $\mathcal{C}$ as a function of the jamming power α, where $\mathcal{C}$ may be the concatenation of an inner code $\mathcal{C}_i$ and an outer code $\mathcal{C}_o$.

Applying the BER-CCDF metric at the output of the outer code C_o, we can see in Fig. 5(b) that for $\delta = 0.05$ our scheme ensures a $\Pr(\hat{P}_b > 0.5 - \delta)$ close to 1 for a wide range of E_b/N_0 values, when Eve is affected by a jamming signal with $\alpha = 1.2$. We further note that for $\delta = 0.01$, this probability never goes to 1. The BER-CCDF metric is further explored in [11], where it is showed that

$$\lim_{E_b/N_0 \to -\infty} \Pr(\hat{P}_b > 0.5 - \delta) = \mathcal{Q}\left(-2\delta\sqrt{\mathcal{S}_b}\right), \qquad (2)$$

where $\mathcal{Q}(\cdot)$ is the usual Q function. This indicates that there is a fundamental limit to how high this probability can go that is a function of only δ and $\mathcal{S}_b$. Thus, we can set $\mathcal{S}_b$ appropriately to attain any guarantees on BER over $\mathcal{S}_b$ bits that we desire.

The energy-cost of jamming the key defined in (1) is negligible, reaching maximum values of $E_{Jb}/E_b = -8.4$ dB when jamming the interleaving key with power of $\alpha = 1.2$.

VI. CONCLUSION

We proposed a concatenated coding scheme for secrecy in which an inner code is used to provide typical levels of information reliability, while security of a transmitted key against Eve results from the proper selection of the outer code and interference levels over that key. This key is then used to conceal the original message before being sent through the channel. Our scheme provides confidentiality through a methodology for choosing an outer code that provides lower bound probabilistic guarantees of error rates to an eavesdropper that suffers a prescribed level of interference only during the transmission of an interleaving key (thus considerably reducing the energy cost of jamming). Results show that an advantage during a small period used for key exchange suffices to ensure reliable and confidential communication.

REFERENCES

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

[2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[4] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, September 2008.

[5] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 256–266, June 2011.

[6] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, August 2007.

[7] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, "Semantically secure lattice codes for the gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 60, no. 10, pp. 6399–6416, 2014.

[8] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 41–50, September 2013.

[9] C. W. Wong, T. F. Wong, and J. M. Shea, "LDPC code design for the BPSK-constrained Gaussian wiretap channel," in *Proc. IEEE GLOBECOM (Workshops)*, Dec. 2011, pp. 898–902.

[10] M. Baldi, G. Ricciutelli, N. Maturo, and F. Chiaraluce, "Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel," in *IEEE ICC 2015 Workshop on Physical-Layer Security*, June 2015.

[11] W. K. Harrison, D. Sarmento, J. P. Vilela, and M. Gomes, "Analysis of Short Blocklength Codes for Secrecy," *ArXiv e-prints*, Sep. 2015, [Online]. Available at http://arxiv.org/abs/1509.07092.

[12] 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, Sept 2011.

[13] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and harq for the awgn wire-tap channel: A security gap analysis," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 883–894, 2012.

[14] J. Almeida and J. Barros, "Random puncturing for secrecy," in *Asilomar Conference on Signals, Systems and Computers*, California, USA, November 2013, pp. 303–307.

[15] Y. Cassuto and Z. Bandic, "Low-complexity wire-tap codes with security and error-correction guarantees," in *IEEE Information Theory Workshop (ITW)*, August 2010, pp. 1–5.

[16] V. Aggarwal, L. Lai, A. Calderbank, and H. Poor, "Wiretap channel type II with an active eavesdropper," in *IEEE Int. Symp. Information Theory (ISIT)*, June 2009, pp. 1944–1948.

[17] J. P. Vilela, P. C. Pinto, and J. Barros, "Position-based jamming for enhanced wireless secrecy," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 616–627, September 2011.

[18] S. Sankararaman, K. Abu-Affash, A. Efrat, S. D. Eriksson-Bique, V. Polishchuk, S. Ramasubramanian, and M. Segal, "Optimization schemes for protective jamming," *Mobile Networks and Applications*, vol. 19, no. 1, pp. 45–60, February 2014.

[19] 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, October 2013.