Walls Have Ears! Opportunistically Communicating Secret Messages Over the Wiretap Channel: from Theory to Practice

Qian Wang[†]
qianwang@whu.edu.cn

Kui Ren[‡,§]
kuiren@buffalo.edu

Guancheng Li[†]
sunatum@whu.edu.cn

Chenbo Xia[†]
microwall@whu.edu.cn

Xiaobing Chen[†]
chenxb002@whu.edu.cn

Zhibo Wang[†], Qin Zou[†]
{zbwang,qzou}@whu.edu.cn

[†]State Key Lab of Software Engineering, School of Computer Science, Wuhan University, P. R. China
[‡]Dept. of Computer Science and Engineering, The State University of New York at Buffalo, USA
[§]College of Information Science and Technology, Jinan University, P. R. China

ABSTRACT

Physical layer (PHY) security has aroused great research interest in recent years, exploiting physical uncertainty of wireless channels to provide communication secrecy without placing any computational restrictions on the adversaries under the information-theoretic security model. Particularly, researches have been focused on investigating Wyner's Wiretap Channel for constructing practical wiretap codes that can achieve simultaneous transmission secrecy and reliability. While theoretically sound, PHY security through the wiretap channel has never been realized in practice, and the feasibility and physical limitations of implementing such channels in the real world are yet to be well understood. In this paper, we design and implement a practical opportunistic secret communication system over the wireless wiretap channel for the first time to our best knowledge. We show that, our system can achieve nearly perfect secrecy given a fixed codeword length by carefully controlling the structure of the parity-check matrix of wiretap codes to strike the proper balance between the transmission rate and secrecy. Our system is implemented and evaluated extensively on a USRP N210-based testbed. The experimental results demonstrate the physical limitations and the feasibility of building practical wiretap channels in both the worst channel case and the case where the sender has only the knowledge of instantaneous channel capacities. Our system design and implementation successfully attempts towards bridging the gap between the theoretical wiretap channel and its practice, alleviating the unrealistic and strong assumptions imposed by the theoretical model.

CCS'15, October 12–16, 2015, Denver, Colorado, USA.

DOI: http://dx.doi.org/10.1145/2810103.2813702.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: [General–*Security and Protection*]

Keywords

Wiretap channel; physical layer security; channel capacity; low-density parity check code

1. INTRODUCTION

Different from classical cryptography, information-theoret -ic security guarantees message secrecy without relying on the computational hardness of mathematical problems [9, 20]. Based on the information-theoretic security principles, physical layer (PHY) security places no computational restrictions on adversaries, and it can provide an additional layer of security besides cryptographic protocols implemented in the upper layers. Due to its unique properties, PHY security has aroused considerable research interest in recent years.

To achieve PHY security, there are two main research streams: generating secret keys from correlated observations between the legitimate sender and receiver [7, 3], and transmitting secret messages between the legitimate sender and receiver by leveraging their physical advantage over the eavesdropper's channel through wiretap coding [20, 9, 19]. By separately dealing with reliability and security constraints, secret key generation from correlated observations turns out to be a much simpler problem, and many effective key-agreement protocols have been proposed by exploiting the inherent randomness of wireless fading channels [13, 16]. The fundamental limits of secret key generation from source or channel models, however, are not as well understood as those of secret communications over wiretap channels, mainly due to harder analysis of two-way communications than the one-way paradigm. Meanwhile, wiretap codes capable of guaranteeing communication reliability and secrecy have been proved to exist. Consequently, over years researchers have put a great deal of effort into constructing practical wiretap codes to achieve asymptotic perfect secrecy [19, 11, 10]. Based on these codes, the secrecy (outage) capacity under different constraints, *e.g.*, transmission delay and power, have also been investigated recently [6, 12, 8].

While theoretically sound, so far PHY security through the wiretap channel has not been realized in practice due to its design and implementation challenges brought by strong assumptions made in theory and the dynamic feature of wireless channels, and the feasibility and physical limitations of implementing the wiretap channel in the real world are yet to be well understood.

Can we realize the theoretical wiretap channel in the real world? We answer this question in the affirmative by presenting a practical opportunistic secret communication system, letting the legitimate sender communicate secret messages right away over wireless channels under the wiretap channel model. The key advantage of our system over cryptographic solutions is in terms of information-theoretic physical-layer security. As an immediate application, it enables key exchange between two trusted parties without pre-knowledge of any shared secret or certificates to be set up a *priori*. We show that it is always possible to establish a secure message communication channel which has a "physical advantage" over the eavesdropper in wireless indoor environments. We, for the first time, design and implement a software defined secret communication system on a USRP N210 based testbed. Our system design has to address several challenges unique to the nature of multipath fading channels and the asymptotic assumptions made in theory. To this end, we present a novel and efficient technique to trade moderate transmission rate for high secrecy, which takes the advantage of the internal structure of wiretap code construction. Our experimental results show that there exist multiple "restricted zones", where if the eavesdropper locates, secret communications over the wiretap channel can be realized in the worst channel case. When the knowledge of the channel statistics are available at the sender, we estimate instantaneous channel capacities on the main channel and the eavesdropper's channel in terms of bits per channel use using measured bit error rates (BERs). To sum up, the main contributions of our work are as follows.

- We present the design of a secure and reliable secret communication system under the wireless wiretap channel. We investigate both the worst channel application scenario without dynamic knowledge of channel statistics and the scenario where channel statistics are available for dynamic code selection.
- We tackle the challenges of tuning the theoretical coding channel to the physical channel, alleviating unrealistic and strong assumptions imposed on the theoretical model, and accessing the instantaneously changing channel state information in practice.
- We present the implementation and an extensive evaluation of our system in a typical indoor environment. Our results provide a detailed characterization of the system and uncover the feasibility and constraints for realizing the wiretap channel in practice.

The remainder of the paper is organized as follows. We describe the system model and background in Section 2, and discuss the gap between theory and practice for wiretap channel in Section 3. We present the software defined design of the secret communication system in 4. Extensive evaluations using simulations are shown in Section 5. We implement the wiretap channel in the real world and evaluate its performance in Section 6. Finally, we conclude our paper in Section 7.

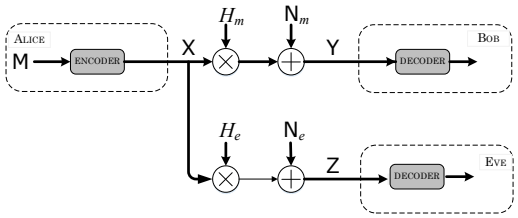


Figure 1: The wireless wiretap channel model.

2. SYSTEM MODEL AND BACKGROUND

2.1 System Overview

We design and implement a secret wireless communication system based on the classic wiretap channel model as illustrated in Fig. 1. In this model, a legitimate sender (Alice) transmits messages to a legitimate receiver (Bob) over a multipath fading channel (called the main channel), while an eavesdropper (Eve) passively listens to the messages over another independent multipath fading channel (called the eavesdropper's channel). For the multipath fading channel, we consider "approximately" quasi-static fading channels, where fading coefficients remain approximately constant over the transmission of two or more codewords. The time required to send a single symbol is much smaller than the duration of a coherence interval. The experimental results suggest that this theoretical model is most consistent with our system implementation in indoor environments.

In a slotted system, a codeword is transmitted over N channel uses. At the end of the transmission of codeword t, the observed signals at the receiver and at the eavesdropper are given by:

$$\mathsf{Y}(t) = H_m(t)\mathsf{X}(t) + \mathsf{N}_m(t) \text{ and } \mathsf{Z}(t) = H_e(t)\mathsf{X}(t) + \mathsf{N}_e(t), \quad (1)$$

respectively, where $\mathsf{X}(t) \in \mathcal{C}^N$ is the transmitted signal vector, $\mathsf{Y}(t) \in \mathcal{C}^N$ is the received signal vector by the legitimate receiver, and $\mathsf{Z}(t) \in \mathcal{C}^N$ is the received signal vector by the eavesdropper. The fading coefficient $H_m(t)$ of the main channel and the fading coefficient $H_e(t)$ of the eavesdropper accounts for the multipath interference in wireless transmissions. Furthermore, the processes $\{H_m(t)\}_{t\geq 1}$ and $\{H_e(t)\}_{t\geq 1}$ are mutually independent and i.i.d., and the square of the magnitude of the fading coefficients $G_m = ||H_m||^2$ and $G_e = ||H_e||^2$ are called fading gains.

The transmitted signals are corrupted by the noise vectors $\{\mathsf{N}_m(t)\}_{t\geq 1}$ and $\{\mathsf{N}_e(t)\}_{t\geq 1}$, which are i.i.d. complex Gaussian with $\mathsf{N}_m(t) \sim \mathcal{CN}(0, \sigma_m^2)$ and $\mathsf{N}_e(t) \sim \mathcal{CN}(0, \sigma_e^2)$ at the receiver and at the eavesdropper, respectively. Finally, the transmission of $\{\mathsf{X}(t)\}_{t\geq 1}$ is subject to a short-term power constraint $\frac{1}{N}\sum_{i=1}^{N} \mathbb{E}[\mathsf{X}^i(t)^2] \leq P$.

We consider two typical secret message transmission application scenarios in an indoor environment: with the noiseless main channel and with the noisy main channel. Our experimental results indicate that when Alice communicates to Bob in a room, the channel between them (*i.e.*, the main channel) is fairly good and is advantageous over Eve's channel (*i.e.*, the eavesdropper's channel), who hides at certain locations behind walls. In the theoretical model, Alice is always required to know the instantaneous channel state $\mathsf{H} = (H_m(t), H_e(t))$. The knowledge of $H_m(t)$ is reasonable since the legitimate transceivers can always cooperate to characterize the main channel. We show in Section 4 that, this assumption can be further eliminated when the

main channel is fairly good. When the knowledge of the channel statistics is necessary to Alice, we place multiple USRP N210-based sensors around the communicating area, facilitating channel capacity estimation in a practical setting. In the system, we also assume that Eve knows the coding scheme used by Alice.

For each codeword t, by the results in [9] the secrecy rate that can be achieved in additive white Gaussian noise (AWGN) channels is

$$\begin{aligned} C_s(t) &= [C_m(t) - C_e(t)]^+, \quad (2) \\ &= [B\log(1+\frac{\mathcal{P}(\mathsf{H})G_m}{\sigma_m^2}) - B\log(1+\frac{\mathcal{P}(\mathsf{H})G_e}{\sigma_e^2})]^+, \end{aligned}$$

where the channel bandwidth B can be normalized to 1, $C_m(t)$ and $C_e(t)$ denote the capacity of the main channel (instantaneous maximum achievable rate for the legitimate receiver) and the capacity of the eavesdropper's channel (instantaneous maximum achievable rate for the eavesdropper), respectively, $\mathcal{P}(\mathsf{H})$ is the power allocation function, and $[x]^+ = \max\{0, x\}$. The secrecy capacity is the maximum transmission rate that is achievable, *i.e.*, the number of bits the receiver can decode per second with no decodable bits at the eavesdropper. Theoretically, we can transmit messages securely and reliably with a non-zero transmission rate (called *secrecy rate*) whenever the eavesdropper's observation $\mathsf{Z}(t)$ is "noisier" than $\mathsf{Y}(t)$. Note that, in this paper, we take the first step towards the realization of secret communications under the wiretap channel model in practice, and we do not consider optimal power allocation with the variations of wireless channels in our system and assume that the transmit power remains constant during the protocol execution. Obviously, by jointly considering the power allocation the system performance can be further improved, and we leave it as our future work.

2.2 Wiretap Codes: Properties and Availability

To achieve secure and reliable transmission under positive secrecy rate (the transmission rate is equal to the secrecy rate when all transmissions are secured), we rely on channel coding techniques that asymptotically guarantee both reliability at the intended receiver and secrecy against the eavesdropper. Such codes are called *wiretap codes*. In the coding function, it is the local randomness introduced by the source (only available to the sender) that enables transmission secrecy. While reliability calls for the introduction of redundancy to mitigate the effect of channel noise, too much redundancy will affect the secrecy. These two seemingly contradictory requirements can be precisely controlled by carefully-designed codes. A typical wiretap code should satisfy two properties: i) the same message should be represented by multiple codewords uniquely and the choice of codewords should be random; ii) the codewords are a function of original messages M's and the local randomness R, which are independent with each other. Using the results in [2], in our paper we define the *information leakage* to the eavesdropper as

$$\begin{aligned} \mathbf{L}(\mathcal{C}_n) &= \mathbb{I}(\mathsf{M}; \mathsf{Z}^n|\mathcal{C}_n) \quad (3) \\ &= \mathbb{I}(\mathsf{X}^n; \mathsf{Z}^n|\mathcal{C}_n) - \mathbb{H}(\mathsf{R}|\mathcal{C}_n) + \mathbb{H}(\mathsf{R}|\mathsf{Z}^n\mathsf{M}\mathcal{C}_n). \end{aligned}$$

To achieve reliable communications in full secrecy, we must choose code $\mathcal{C}_n$ that at least ensures the *leakage rate* $\frac{1}{n}\mathbf{L}(\mathcal{C}_n) \leq \varepsilon$ for arbitrarily small $\varepsilon > 0$.

Note that, in this paper, we restrict ourselves to the design, the implementation and the evaluation of secret communications under the wiretap channel model other than the design of wiretap codes. In the following discussions, we introduce two efficient code constructions for our purpose.

2.2.1 Type-I Code: Secrecy Codes for Binary Erasure Eavesdropper's Channel

We first restrict ourselves to a wiretap channel model where the main channel is noiseless but the eavesdropper's channel is a binary erasure channel (BEC) with erasure probability ϵ. Thus, the resulting capacity of a BEC is $1-\epsilon$. In real life, this corresponds to the scenario where the legitimate sender and the legitimate receiver communicates to each other at a short range (*e.g.*, in a room). Due to the "favorable" main channel, it can be assumed that any codeword sent by the sender is correctly received by the receiver. The wiretap codes can be efficiently implemented as follows [19].

Let $\mathcal{C}_0$ be an $(n, n-k)$ low-density parity-check (LDPC) code with a generator matrix $\mathbf{G} \in GF(2)^{(n-k)\times n}$ and a parity-check matrix $\mathbf{H} \in GF(2)^{k\times n}$. Under a BEC channel, assume $\mathcal{C}_0$ with rate $r = \frac{n-k}{n}$ has a threshold $\epsilon^* \geq \epsilon$ to ensure reliability. The encoder maps a k-bit message M to a n-bit codeword X as $\mathsf{X} = (\mathbf{G}_1^T \ \mathbf{G}^T)\binom{\mathsf{M}}{\mathbf{V}}$, where $\mathbf{G}_1 \in GF(2)^{k\times n}$ is composed of k independent row vectors chosen from $\{0,1\}^n \backslash \mathcal{C}_0$, and $\mathbf{V} \in GF(2)^{n-k}$ is chosen uniformly at random. The decoder recovers the message as $\mathsf{M} = \mathbf{H}_1\mathsf{X}$, where $\mathbf{H}_1$ is generated from $\mathbf{H}$. As can be seen from the above encoding process, one coset code of $\mathcal{C}_0$ (which has 2^k coset codes) is chosen for every message M, and the use of $\mathbf{V}$ is to choose one codeword from this coset code. Obviously, 2^k possible M's are corresponding to 2^k possible coset codes. Given its observation Z, which is the erasured version of X, the eavesdropper's uncertainty about M can be ensured if all cosets of $\mathcal{C}_0$ are consistent with Z and they contain the same number of codewords that agree with Z in the unerased bits. It has been proved in [19] that when $\mathbf{G}$ is the parity-check matrix with an erasure threshold $\epsilon^* > 1-\epsilon$, the leakage rate to the eavesdropper is bounded by $\frac{1}{n}\mathbf{L}(\mathcal{C}_n) \leq \delta(n)$, where $\delta(n)$ approaches zero as n goes to infinity. It is easy to see that this wiretap code has a typical binning structure [19] and its security guarantee is consistent with $\frac{1}{n}\mathbf{L}(\mathcal{C}_n) \leq \varepsilon$. In coding theory, a code that satisfies $1 - r = \epsilon^*$ is called a *capacity-achieving* code. Note that this wiretap code established under the noiseless main channel does not rely on any capacity-achieving property. However, the price paid is that the rates arbitrarily close to the secrecy capacity cannot be achieved.

2.2.2 Type-II Code: Secrecy Codes for Binary Erasure Main Channel and Eavesdropper's Channel

We move on to another wiretap channel model, in which the main channel and the eavesdropper's channel are both binary erasure channels, with erasure probabilities ϵ_m and ϵ_e ($\epsilon_m < \epsilon_e$) respectively. In this application scenario, the legitimate sender and the legitimate receiver are not close enough to establish an error-free main channel. The wiretap code is constructed as follows [19].

Let $\mathcal{C}_2$ be an (n, nr_2) LDPC code with parity-check matrix $\mathbf{H}_2 \in GF(2)^{n(1-r_2)\times n}$, with rate satisfying $1 - r_2 \geq \epsilon_m^* \geq \epsilon_m$, where ϵ_m^* is the erasure threshold of $\mathcal{C}_2$. Let $\mathcal{C}_1$ be an

(n, nr_1) LDPC code with parity-check matrix $\mathbf{H}_1 = \binom{\mathbf{H}_2}{\overline{\mathbf{H}_2}} \in GF(2)^{n(1-r_1)\times n}$, satisfying $1 - r_1 \geq \epsilon_e^* \geq \epsilon_e \geq 1 - r_2$, where ϵ_e^* is the erasure threshold of $\mathcal{C}_1$. The encoder maps an $n(r_2 - r_1)$ message M to an n-bit codeword X_i ($i \in [1, 2^{nr_1}]$) which all satisfy $\binom{\mathbf{H}_2}{\overline{\mathbf{H}_2}}\mathsf{X}_i^T = \binom{\mathbf{0}}{\mathsf{M}^T}$, and chooses one codeword uniformly at random. The decoder first gets all the solution(s) of $\mathbf{H}_2\mathsf{Y}^T = 0$ (Y is the erasured codeword) and then calculates $\mathsf{M}^T = \overline{\mathbf{H}_2}\mathsf{X}^T$ to recover the message(s). As n goes to infinity, because $\epsilon_m^* \geq \epsilon_m$, the legitimate receiver gets only one message which is the original one. But the eavesdropper gets $2^{n(\epsilon_e-(1-r_2))} = 2^{n(r_2-r_1)}$ different messages which cover all possible messages if $\epsilon_e^* = \epsilon_e = 1 - r_1$. This means that $\mathcal{C}_1$ is a *capacity-achieving* code. The leakage rate to the eavesdropper is then $\frac{1}{n}\mathbf{L}(\mathcal{C}_n) = \lim_{n\to\infty}\frac{1}{n}\mathbb{I}(\mathsf{M};\mathsf{Z}^n|\mathcal{C}_n) = \lim_{n\to\infty}\frac{1}{n}\mathbb{I}(\mathsf{X}^n;\mathsf{Z}^n|\mathcal{C}_n) - \frac{1}{n}\mathbb{H}(\mathsf{R}|\mathcal{C}_n) + \frac{1}{n}\mathbb{H}(\mathsf{R}|\mathsf{Z}^n\mathsf{M}\mathcal{C}_n) = r_1 - \frac{1}{n}\log_2(2^{nr_1}) + 0 = 0$.

3. WIRETAP CHANNEL: THE GAP BETW -EEN THEORY AND PRACTICE

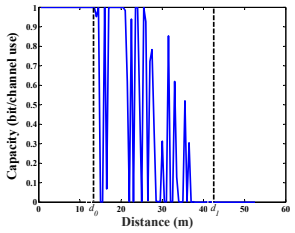
Over the years, the famous wiretap channel for providing information-theoretic secrecy of communications has been revisited by many researchers in literature. The results obtained so far are theoretically sound, but there exists a gap between the wiretap channel model and its secure and efficient implementation in practice. To bridge the gap, we have to contend with the limitations of unpractical assumptions in theory and the peculiarities of wireless communication medium.

3.1 Physical Channel Is More than A Coding Channel

While constructing codes capable of guaranteeing reliable communication and at the same time satisfying a secrecy condition is the key to the success of secret communications over the wiretap channel, secure and reliable message transmission in a wireless communication system is subject to many factors, such as data modulation, fading gain, power allocation, and shift recovering (including time, frequency and phase shifts) etc. The current state-of-the-art on wiretap channel are mainly focused on the construction of practical and efficient wiretap codes for very general channels to meet theoretic reliability and security criteria. We found that multipath channel fadings have a great impact on both the reliability and security constraints, and the requirement of optimal configurations in every step in the theory is hard to achieve in practice. These findings inform that the design and implementation of our secure communication system should carefully take into account all practical factors and integrate them in a systematic way.

3.2 Asymptotic Assumptions Are Not Easy to Achieve

Modern cryptography usually relies on mathematical problems assumed to be hard to solve. Different from the concept of computational security, information-theoretic security skillfully uses asymptotic notions to obtain security guarantee. As the wiretap channel model, the security and reliability of the theoretical construction are feasible only when the code length n of the wiretap codes tends to infinity. Besides, in some specific channels the communication security highly relies on capacity-achieving codes, the existence of which is also proved using the asymptotic notion theoretically. In the real world, however, the code length cannot be extremely long due to the efficiency concern. From the practical perspective, it is necessary to alleviate the strict and strong asymptotic assumptions, and our experimental findings inform the practicability of exploiting a small concrete code length and the relaxation of the strict requirement of capacity-achieving codes in the implementation.



(a) Capacity vs. distance

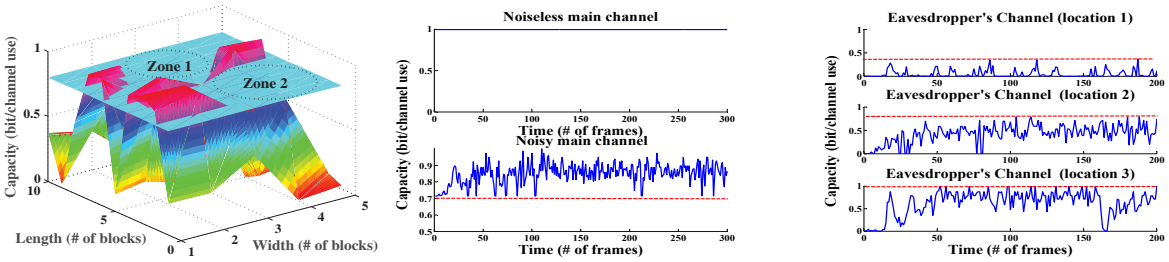
Figure 2: The average variations of capacity with the increase of communicating distance. Here, Alice and Bob are inside our lab, and Eve, which is behind a wall, is located and tested in different positions along the hallway.

3.3 The Accessibility of Changing Channel St -ate Information

In theory, for ease of analysis it is explicitly assumed that channel statistics are known a *priori*. From the practical perspective, the assumption that the statistics of the main channel are perfectly known can be reasonable because the legitimate transceivers can always cooperate to characterize their pairwise channel. However, the assumption that the eavesdropper's channel statistics are known ahead of time remains questionable. The good news is that theoretical results inform this stringent requirement can be somewhat alleviated for a class of stochastically degraded channels when the wiretap channel ensures *equivocation* for the worst channel case [2] (*i.e.*, the most favorable eavesdropper's channel from Eve's perspective). So, the question becomes does the "worst channel" exist in the real life? Also, as presented in Section 4.1.1, our experimental results show that the channel capacity at any fixed position varies quite fast from time to time. How to deal with the changing channel state information also poses a challenging problem to the practical and secure system design.

4. THE SOFTWARE DEFINED SECRET C -OMMUNICATION SYSTEM DESIGN

Our system implements a software defined radio for enabling secret communications between Alice and Bob. At the start of the communication, Alice first performs channel coding and adds barker code to help synchronize the encoded data. Then, she modulates the coded data into complex signals and scrambles them. Finally, Alice transmits the signals to Bob over the wireless channel. At the receiver end, Bob first executes shift recovering on the received channel-attenuated signals. Then, he uses the matched descrambler to descramble the signals and demodulates them into bit streams, from which barker codes are applied to generate data frames. Finally, Bob performs channel decoding to recover the original message. From the perspective of the eavesdropper, Eve follows exactly the same signal processing



(a) Restricted zones. (b) Capacity of the main channel. (c) Capacity of the eavesdropper's channel.

Figure 3: Characterization of restricted zones for Eve under the worst channel in indoor wireless environments. The right two figures demonstrate the feasibility of establishing a secret message transmission system over the wiretap channel. Here, each block on the floor is of $0.36m^2$, and each frame is the time interval between the transmission of two consecutive codewords.

procedures as Bob, but as a result of our wiretap codes, she is kept ignorant of the original message. Rather than describing the well-known aspects of wireless communications, in this section we focus on the whole design thoughts and solutions unique to our implementation.

4.1 Dealing with Dynamic Changes of Channel State Information

For short-range wireless communications in an indoor environment, there are mainly three circumstances. As can be seen in Fig. 2, when the distance d between two communicating parties is less than a threshold d_0, the signal that arrives at the receiver is strong enough for successfully recovering the original message, albeit with amplitude fluctuations due to the channel fading. When $d_0 \leq d \leq d_1$, the receiver receives the signal with weak strength such that it is more easily affected by noise interference. As the distance exceeds d_1, the original signal is overwhelmed by noise. Due to the changing wireless environment, the values of d_0 and d_1 may vary over a period of time.

The variation of wireless channels mainly comes from the path loss, reflection, diffraction, scattering and shadowing etc. Specific to the indoor wireless communication, walls have a great impact on signal blocking. Measures in [17] indicate that when the communicating parities operating at 900MHz are separated by a single wall/floor, the attenuation ranges from 10 to 20dB. Meantime, the signal propagation path is also changing frequently, and it directly affects the phase of the received signal. In our implementation, we choose carrier frequency $f_c = 850$MHz. When $d_0 \leq d \leq d_1$, the fast phase change causes the fluctuation of the strength of the combined signal. Accordingly, the effect of multipath fading is the significant cause for channel capacity variations. In our implementation, we use phase compensation algorithm [15] to alleviate the effect of phase variations. We also use the numerically-controlled oscillator and the phase-locked loop to combat frequency drift at the sender and the receiver, respectively.

In order to achieve the maximum secret rate, the coding matrix for channel coding is determined by channel capacities C_m and C_e, *i.e.*, the coding matrix should be dynamically generated with the variations of C_m and C_e (The implementation of Type-I and Type-II wiretap codes will be discussed in detail in Section 6). Obviously, the faster channel capacities change the higher efficiency requirements of matrix generation and wiretap channel coding. In practice, the dynamic matrix generation approach will be unacceptable if the coding matrix generation time is larger than the coherence time. In this subsection, we present and characterize our two designs through real world measurements on a USRP N210-based testbed.

4.1.1 *Characterizing Restricted Zones for Eve Under the Worst Channel*

The secrecy and reliability of wiretap channel coding are highly sensitive to the changes of C_m and C_e. To deal with the dynamic changes of channel capacity, our first idea is to choose the worst channels of both the main channel and the eavesdropper's channel for wiretap coding. Before presenting the scheme, we first illustrate the intuition behind this idea by looking at the following definition and propositions.

Definition 1. (Stochastically degraded channel [1, 4])$(\mathcal{X}, p_{Z|X}, \mathcal{Z})$ is stochastically-degraded with respect to $(\mathcal{X}, p_{Y|X}, \mathcal{Y})$ if there exists a channel $(\mathcal{Y}, p_{Z|Y}, \mathcal{Z})$ such that $\forall(x, z) \in \mathcal{X} \times \mathcal{Z}$, $p_{Z|X}(z|x) = \sum_{y\in\mathcal{Y}} p_{Z|Y}(z|y)p_{Y|X}(y|x)$.

Proposition 1. (Robustness of worst-case design [2]) Given a class of stochastically-degraded eavesdropper's channels, a wiretap code ensuring equivocation for the worst channel guarantees at least the same equivocation $\mathcal{E}$ for any eavesdropper's channel in the class.

Here, the eavesdropper's equivocation is the average uncertainty of Eve about message M. Proposition 1 tells us that a wiretap code that guarantees the security through an eavesdropper's channel can guarantee the security through any channel that is a degraded version with respect to this wiretap channel. The above theoretical results motivate us to seek the worst channel case (*i.e.*, the most favorable eavesdropper's channel from Eve's perspective) and validate if there exist a class of stochastically-degraded eavesdropper's channels physically.

Fig. 3 depicts the characterization of the capacity distribution for the eavesdropper's channel, on the basis of capacity measurements in our indoor environment. Specifically, Fig. 3 (b) shows the cases where C_m achieves the maximum capacity 1 for a noiseless channel, and it is above a threshold 0.7 for a noisy channel all over the time. Such favorable channels can be easily obtained when Alice and Bob communicates in a room, *e.g.*, as large as $97m^2$ in our test. For the eavesdropper behind a wall, Fig. 3 (c) shows that although C_e varies with time, there exist a number of locations where the capacity is always below a certain value, *e.g.*, 0.4 in the first location and 0.8 in the second location. This visible capacity difference between C_m and C_e can be leveraged to

build a secret message transmission system under the wiretap channel model. Our experimental results in Fig. 3 (a) further suggest that around Alice and Bob there exist certain "restricted zones", where the eavesdropper's channel capacities in this area are all below a threshold, denoted by $C_e^{max} \in (0, 1)$. That is, in such a restricted zone, no matter how channel state changes with the time-varying eavesdropper's channel, C_e will not exceed C_e^{max}. We call it the worst channel with respect to the eavesdropper's channel. On the other hand, the worst channel with respect to the main channel is the minimum channel capacity achieved by Alice and Bob in their communicating area, and we denote it by $C_m^{min} \in (0, 1]$. Obviously, $C_m^{min} = 1$ for a noiseless main channel. In practice, it is easy to obtain a reasonably high C_m^{min} when Alice and Bob are not far away. Once obtaining C_e^{max} and C_m^{min} satisfying $C_m^{min} - C_e^{max} > 0$, it is possible to provide the communication security and reliability guarantee no matter how the channel state changes over time. Note that, our experimental results also indicate that unless the environment changes dramatically, the movement of people and objects does not affect the thresholds much.

In the real world, potential eavesdroppers can always be considered to be located at some restricted areas, and the legitimate communicating parties are not likely to talk with each other unless the potential eavesdropper is kept at an alert area. As can be seen from the discussion above, the solution of characterizing restricted zones for Eve under the worst channel case does not require the knowledge of the eavesdropper's channel capacity in real time, which eliminates the strong assumption of knowledge of the instantaneous channel states.

4.1.2 *Enabling Dynamic Channel Capacity Feedback*

While the first solution to contend with time-varying channels requires the characterization of restricted zones for the eavesdropper, our second idea is to cover a wide range of area for communication security. To this end, Alice needs to obtain the instantaneous channel capacities C_m^{ins} and C_e^{ins} to dynamically adjust the coding strategy. As discussed before, Alice and Bob can always cooperate to characterize the main channel. To facilitate the acquisition of the instantaneous capacity of the eavesdropper's channel, we place multiple USRP N210-based sensors as the helper nodes to compute and feed back C_e^{ins} to Alice. Fig. 4 depicts the cumulative distribution function (CDF) of channel capacity differences over the transmission time of two codewords at different locations in our indoor environment. It can be seen that, for most of the time, the capacity difference is less than 0.3, which is applicable in our system implementation. Our results show that given an efficient wiretap code, it is sufficient to measure and utilize fed-back C_e^{ins} as the input of channel coding. Similar to the worst channel case, we can also adopt a conservative strategy to contend with the coding efficiency and the dynamic changes of channel capacity. To do so, the coding matrix corresponding to a specified capacity pair (C_m^{std}, C_e^{std}) can be pre-determined, and the secure transmission strategy works as follows: Alice transmits messages coded using the pre-determined coding matrix to Bob if and only if both $C_m^{ins} \geq C_m^{std}$ and $C_e^{ins} \leq C_e^{std}$ hold; otherwise Alice does not transmit anything.

The advantage of utilizing dynamic channel capacity feedback is to place no restrictions on the eavesdropper's locations. It applies to the application scenario where it is difficult to find the "worst case", *e.g.*, the worst channel capacity of the main channel C_m^{min} is too bad and/or the worst channel capacity of the eavesdropper's channel C_e^{max} is too good. In Section 6, we will implement and analyze both of the above two solutions.

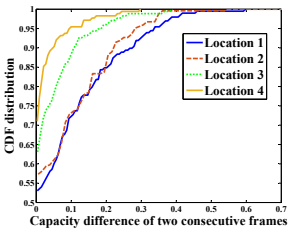


Figure 4: Capacity difference between two consecutive frames. A frame is approximately the time for one codeword transmission.

4.2 Estimating Channel Capacity for Dynamic Code Selection

As described in Section 4.1.2, our second solution requires the feedback of channel capacity updates to determine the message transmission strategy. In general, channel estimation is widely used in telecommunication systems to obtain the channel state information for counteracting the effect of multipath fading and/or facilitating optimal allocation of transmit power. Different from existing telecommunication systems, the channel statistics concerned in our system are channel capacities. In information theory, the notion of channel capacity is defined as the maximum of the mutual information between the input and the output of the channel, where the maximization is taken with respect to the input distribution

$$C = \sup_{p_{\mathsf{X}}(x)} \mathbb{I}(\mathsf{X}; \mathsf{Y}), \tag{4}$$

where the supremum is taken over all possible choices of $p_{\mathsf{X}}(x)$. Note that, if the channel is a binary input and output channel, C is measured as bits per channel use. As seen in Eq. (2), if specific to an AWGN fading channel, the capacity or the achievable rate can be written as

$$\begin{aligned} C &= B \log(1 + \mathsf{SNR}) \\ &= B \log(1 + \frac{\mathcal{P}(\mathsf{H}) G_m}{\sigma_m^2}), \end{aligned} \tag{5}$$

where the channel bandwidth B can be normalized to one and SNR is the signal-to-noise ratio. As for this metric, C is measured in bits per second if the logarithm is taken in base 2.

Note that, metric (5) is a special case of metric (4). With metric (5), we can make more use of the characteristics of wireless channels such as dynamically allocating transmission power by using fading coefficients and performing adaptive modulation, which will lead to a higher rate. However, for simplicity, we don't use metric (5) in our implementation. We leave the realization of dynamic power control and adaptive modulation as our future work.

Since quadrature phase shift keying (QPSK) leads to a symmetric error rate, we can abstract the wireless channel into the Binary Symmetric Channel (BSC). Then, the instantaneous bit error rate (BER) is the cross-over probability of the BSC. Now it is easy to get metric (4) through chan-

nel transfer matrix by using the formulation of the BSC capacity or iteration algorithms [14]. In order to obtain a more accurate estimation, we compute the instantaneous BER by transmitting training sequences before message transmission. Note that, our channel has been abstracted into the BSC, and thus no more than one bit message can be transmitted per channel use, causing the maximum capacity in bits per channel use to be one, which is more convenient for our coding design.

4.3 Achieving Practical Coding for the Wiretap Channel

Proposition 1 tells us that a wiretap code designed for a specific eavesdropper's channel can be used over any other eavesdropper's channel due to the stochastically-degraded channel property. The following proposition shows that all binary-input channels are stochastically degraded with respect to binary erasure channels with certain erasure probability.

Proposition 2. ([2]) A memoryless binary-input channel $(\{0,1\},\ p_{\mathsf{Y}|\mathsf{X}}, \mathcal{Y})$ is stochastically degraded with respect to an erasure channel with erasure probability

$$\epsilon \quad = \quad \int_y \big(\min_{u\in[0,1]} p_{\mathsf{Y}|\mathsf{X}}(y|u)\big) dy. \tag{6}$$

This implies that wiretap codes designed for an eavesdropper's BEC can be used over any binary-input channel by simply converting the channel into a stochastically-degraded version of BEC. This proposition gives the sufficient condition for realizing secret communications over non-BECs. As shown in Section 6, our experimental findings indicate that this proposition actually provides a conservative solution, and a much higher transmission rate can be achieved by properly overestimating the capacity of eavesdropper's channel.

As discussed in Section 2.2, in theory the existing available wiretap codes can asymptotically guarantee both secrecy and an arbitrarily small probability of error at the intended receiver. In a practical system, however, the codeword length n cannot be arbitrarily large. Our design and implementation restrict the codeword length n to an acceptable range, which is sufficient for achieving reliability and secrecy. Specifically, under a practically short codeword length n, we propose to sacrifice moderate amount of transmission rate for secrecy when the main channel is noiseless (using Type-I code) or noisy (using Type-II code). In the following discussion, we show how to achieve our goal through elaborate analysis.

Proposition 3. ([19]) Let an $(n, n-k)$ code $\mathcal{C}$ have a generator matrix $\mathbf{G} = [a_1, ..., a_n]$, where a_i is the i-th column of $\mathbf{G}$. Consider an instance of the eavesdropper's observation $\mathsf{Z} \in \{0,1,?\}^n$ with μ unerased positions given by $\{i : \mathsf{Z}_i \neq ?\} = \{i_1, i_2, ..., i_\mu\}$. Z is secured by $\mathcal{C}$ iff the matrix $\mathbf{G}_\mu = [a_{i_1}, a_{i_2}, ..., a_{i_\mu}]$ has rank μ.

Proposition 4. ([2]) Let $\mathbf{H}$ be the parity-check matrix of a length-n LDPC code selected uniformly at random in an ensemble whose block error probability threshold under belief-propagation decoding for the erasure channel is ϵ^*. Form a submatrix $\mathbf{H}'$ of $\mathbf{H}$ by selecting each column of $\mathbf{H}$ with probability $\epsilon < \epsilon^*$. Let the block error probability be P_e. Then, $\mathbb{P}[\mathsf{rank}(\mathbf{H}') = \epsilon n] = 1 - P_e = 1 - \delta(n)$.

Based on Propositions 3 and 4, we have the following theorem for Type-I wiretap code.

THEOREM 1. *For Type-I wiretap code, under a fixed codeword length n the information leakage $\boldsymbol{L}(\mathcal{C}_n)$ can be reduced by overestimating the capacity of the eavesdropper's channel C_e.*

PROOF. According to Propositions 4 and the construction of Type-I code, if we use the parity-check matrix $\mathbf{H}$ of a LDPC code with threshold ϵ^* as the generator matrix $\mathbf{G}$ and the capacity of the eavesdropper's channel $BEC(\epsilon_e)$ satisfies $1-\epsilon_e < \epsilon^*$, then for a fixed codeword length n, a submatrix formed by selecting each column of $\mathbf{H}$ with probability $1-\epsilon_e$ will have full rank with probability $1-\delta(n)$. According to Propositions 3, because the number of unerased bits is also $n(1-\epsilon_e)$, this is equivalent to say that Eve's observation Z is secured with probability $1-\delta(n)$.

Motivated by this observation, for Type-I wiretap code we can define the block leakage probability P_l, which denotes the probability that Z is not secured. That is to say, the information leakage $\mathbf{L}(\mathcal{C}_n) = nP_l$. Note that, a general LDPC code focuses on the reliability and thus uses the block error probability P_e as the performance metric, which denotes probability that the erased bits' corresponding columns in the generator matrix are not in full rank. Our Type-I wiretap code focuses on the secrecy and thus uses the block leakage probability P_l, which denotes the probability that the unerased bits' corresponding columns in the generator matrix are not in full rank. Inherently, P_e and P_l both denote the probability that the selected columns with a specific probability ϵ ($\epsilon \leq \epsilon^*$) from the generator matrix are not in full rank. When the two probabilities ϵ's are the same, which means the number of erased bits in the first case is the same as the number of unerased bits in the second case, they are equal in value. Obviously, we can have $\mathbf{L}(\mathcal{C}_n) = nP_l = n\delta(n)$, where n is fixed. Note that $\delta(n)$ not only approaches 0 as n goes to infinity but also does when C_e approaches 0. This is because when C_e approaches 0, the eavesdropper's channel becomes worse. Hence, with a fixed code, the leakage to the eavesdropper obviously becomes less, *i.e.*, P_l, which shares the same value as $\delta(n)$, approaches 0. In the extreme case, if we apply the code for $BEC(\epsilon_e)$ to the eavesdropper's channel with erasure probability 1, then $\delta(n) = 0$. So $\mathbf{L}(\mathcal{C}_n)$ is reduced to 0. This approach that applies codes used in C_e^+ to C_e ($C_e^+ > C_e$) is called an *overestimation* of eavesdropper's channel. That is, if we obtain an eavesdropper's channel with capacity C_e, we overestimate it as C_e^+, based on which we select the code with threshold $\beta^* > C_e^+ > C_e$. Then $\mathbf{L}(\mathcal{C}_n)$ is reduced. □

Remarks. While the overestimation of C_e reduces the information leakage, it also reduces the transmission rate simultaneously. Note that in this paper, the transmission rate is discussed in the context of secrecy, *i.e.*, the transmission rate is the secrecy rate when the message is transmitted at a rate lower than the secrecy capacity. The proof indicates that we can measure the tradeoff between the transmission rate and the secrecy by $\Delta = C_e^+ - C_e$ in our experiments for Type-I wiretap code.

In our implementation, we adopt fixed wiretap codes for the worst channel case. The idea of utilizing a fixed wiretap code (*i.e.*, keep the generation and parity-check matrices constant) can be considered as a conservative strategy when

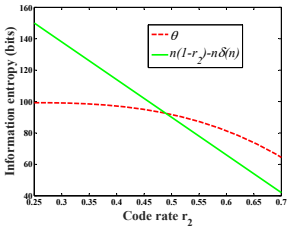


Figure 5: Control of equivocation/information entropy loss θ to approach $n(1-r_2)-n\delta(n)$. Here, codeword length $n = 120$, the erasure probability of the eavesdropper's channel $\epsilon_e = 0.75$ and the threshold $\epsilon^* = 0.25$.

there is no channel state information feedback. We find that the adoption of a fixed code is equivalent to the overestimation of C_e. For example, if the fixed code can only be suitable for the eavesdropper's channel with capacity less than or equal to 0.7, then we actually overestimate C_e when applying the code to the channel with C_e less than 0.7.

In wiretap coding approaches, capacity-achieving codes are more preferred due to their high efficiency. As discussed in Section 2.2.2, for Type-II wiretap code, $\mathcal{C}_1$ must be a capacity-achieving code to guarantee secrecy. Intuitively, it seems that selecting a capacity-achieving code as $\mathcal{C}_2$ is also the best choice. However, our following findings reveal that the use of a non-capacity-achieving code for $\mathcal{C}_2$ can enhance the security strength by sacrificing moderate transmission rate.

Lemma 1. Assume code $\mathcal{C}_2$ is a length-n LDPC code for a $BEC(\epsilon)$ with threshold ϵ^* and code rate r, $\mathbf{H}_2$ is the parity-check matrix of $\mathcal{C}_2$, Z the $BEC(\epsilon)$-attenuated version of transmitted codeword X, and θ is the equivocation loss/information entropy loss after decoding by $\mathbf{H}_2\mathsf{Z} = 0$. If $\epsilon^* \leq 1-r$, $\epsilon^* \leq \epsilon \leq 1$, then θ can be controlled in the range $n\epsilon^* \leq \theta \leq n(1-r)$ by adjusting the relationship between ϵ^*, ϵ and r.

Proof. When $\epsilon^* \leq \epsilon \leq 1$, θ increases with the increase of ϵ. The equivocation loss/information entropy loss θ after decoding is determined by the rank of columns corresponding to the erased bits in $\mathbf{H}_2$. Because $rank(\mathbf{H}_2) = n(1-r)$, we have $\theta \leq n(1-r)$. We next define two erasure channels $BEC(\epsilon_1)$ and $BEC(\epsilon_2)$ with $\epsilon_1 < \epsilon_2$. Because the average number of erased bits of $BEC(\epsilon_2)$ are more than those of $BEC(\epsilon_1)$, the number of columns corresponding to $BEC(\epsilon_2)$'s erased bits is larger than that of $BEC(\epsilon_1)$. Consequently, the average rank of randomly selecting $n\epsilon_2$ columns from $\mathbf{H}_2$ is larger than that of randomly selecting $n\epsilon_1$ columns from $\mathbf{H}_2$. This implies that the information entropy loss after decoding over $BEC(\epsilon_2)$ is definitely larger than that over $BEC(\epsilon_1)$.

We next determine the range of θ. If $\epsilon = \epsilon^*$, then $\theta = n\epsilon^*$ as n goes to infinity; if $\epsilon = 1$, then θ is obviously equal to $n(1-r)$. So, we can adjust the relationship between ϵ^*, ϵ and r to increase or decrease θ between $n\epsilon^*$ and $n(1-r)$. □

Remarks. In the above Lemma, we define θ as the information entropy loss other than information bits that can be recovered after decoding. Note that when $\epsilon < \epsilon^*$, both of them are equal to $n\epsilon$. In our Type-II wiretap code, we focus on the case $\epsilon > \epsilon^*$ for the eavesdropper's channel, where the reliability of decoding cannot be fully guaranteed. In this case, the possible decoded codeword is not unique, so we use θ to measure the results when errorless transmissions over the eavesdropper's channel are not available.

Theorem 2. *For Type-II wiretap code, under a fixed codeword length n, $\mathcal{C}_1$, $\mathcal{C}_2$ and $\overline{\mathcal{C}}_2$ have code rates r_1, r_2 and $r_2 - r_1$ and parity-check matrices $\boldsymbol{H}_1$, $\boldsymbol{H}_2$ and $\overline{\boldsymbol{H}}_2$, respectively. The information leakage $\mathbf{L}(\mathcal{C}_n)$ can be reduced by using a non-capacity-achieving code $\mathcal{C}_2$.*

Proof. Assume that the eavesdropper's channel has erasure probability ϵ_e, and the main channel has erasure probability ϵ_m. Then Y has $n\epsilon_m$ erased bits and Z has $n\epsilon_e$ erased bits. Let θ be the equivocation loss/information entropy loss after decoding by $\mathbf{H}_2\mathsf{Z} = 0$. As n goes to infinity, the leakage $\mathbf{L}(\mathcal{C}_n) = n(r_2 - r_1 - \epsilon_e) + \theta$. If $\mathcal{C}_1$ is a capacity-achieving code, then $\epsilon_e = 1 - r_1$. When $\theta \leq n(1-r_2)$, the leakage is zero. For a fixed codeword length n, the leakage will not be zero. We denote the leakage rate induced by a fixed codeword length n by $\delta(n)$. The leakage now increases to $n(r_2 - r_1 - \epsilon_e) + \theta + n\delta(n)$. We use a non-capacity achieving code $\mathcal{C}_2$ with threshold $\epsilon^* < 1 - r_2$ and a capacity-achieving code $\mathcal{C}_1$. Thus, we have $\epsilon_e = 1 - r_1$. Now the leakage becomes $n(r_2 - 1) + \theta + n\delta(n)$. If $(1-r_2) - \epsilon^*$ is large enough, by Lemma 1, we can make θ close to $n(1-r_2) - n\delta(n)$, then the leakage is approaching zero. As shown in Fig. 5, the equivocation loss θ can be carefully controlled to approach $n(1-r_2) - n\delta(n)$ by adjusting the code rate r_2. The intersection point indicates the leakage can be reduced to zero. However, if $\mathcal{C}_2$ is capacity-achieving, then $\epsilon^* = 1 - r_2$ and θ has only one value, *i.e.*, $n\epsilon^* = \theta = n(1-r_2)$. So, we have $\mathbf{L}(\mathcal{C}_n) = n\delta(n)$. When the codeword length n is fixed, then $\delta(n) > 0$ and the leakage $\mathbf{L}(\mathcal{C}_n)$ cannot be reduced to approach zero. □

Theorem 2 shows the information leakage can be reduced by using a non-capacity-achieving code $\mathcal{C}_2$. The following theorem shows that the strict requirement of the capacity-achieving property for $\mathcal{C}_1$ can be further relaxed.

Theorem 3. *For Type-II wiretap code, under a fixed codeword length n, secrecy can be guaranteed by using the non-capacity-achieving codes $\mathcal{C}_2$ and $\mathcal{C}_1$.*

Proof. Based on Theorem 2, when $\mathcal{C}_1$ is not a capacity-achieving code, we have $\epsilon_e < 1 - r_1$. Denote the difference between ϵ_e and $1 - r_1$ by μ, so $\epsilon_e + \mu = 1 - r_1$. Due to the use of a fixed code length n and a non-capacity-achieving code $\mathcal{C}_1$, the leakage $\mathbf{L}(\mathcal{C}_n) = n(r_2 - r_1 - \epsilon_e) + \theta + n\delta(n) = n(r_2 + \mu - 1) + \theta + n\delta(n)$. Similar to Theorem 2, when $\mathcal{C}_2$ is a non-capacity-achieving code and the difference $(1-r_2) - \epsilon^*$ is large enough, θ can be adjusted to make it close to $n(1 - r_2 - \mu) - n\delta(n)$. So, secrecy can be achieved without requiring $\mathcal{C}_1$ to be a capacity-achieving code given a fixed codeword length n. □

As can be seen, for Type-II wiretap code, the difference $(1-r_2) - \epsilon^*$ measures how much $\mathcal{C}_2$ is not capacity-achieving, so we measure the tradeoff between the transmission rate and the secrecy by $\Delta = (1-r_2) - \epsilon^* = (1-r_2) - \epsilon_m = C_m - r_2$ when $\epsilon^* = \epsilon_m$.

Theorems 1, 2 and 3 lay the foundations for trading transmission rate for secrecy (leakage reductions). In Section 6, we show the effectiveness of trade-offs for achieving nearly *perfect secrecy* given a fixed codeword length n.

5. SIMULATION RESULTS

In this section, we provide a comprehensive simulation study to evaluate the system performance. In the next section, we further implement the wiretap channel in a real system and report experimental performance results. The following metrics are used to evaluate the system performance in both simulation and experimental studies.

- Equivocation ($\mathcal{E}$): $\mathcal{E}$ is defined as the entropy of M_d, where M_d is a random variable representing the message decoded by the eavesdropper, and the original message set is denoted by $\mathcal{M}$. Therefore, $\mathcal{E} = \mathbf{H}(\mathsf{M}_d) = -\sum_{m\in\mathcal{M}} p_m \log p_m$, where p_m is the probability that $\mathsf{M}_d = m$.
- Bit Error Rate (BER): the ratio of the number of bits in the decoded message different from the original message to the total number of bits in the original message.
- Block Error Rate (BLER): the ratio of the number of decoded messages different from the original messages to the total number of the original messages.

Here, $\mathcal{E}$ and BLER are used to measure the system security performance and reliability performance, respectively. Note that, we can use BER to measure both the system security performance (with respect to the eavesdropper) and reliability performance (with respect to the legitimate receiver).

To evaluate the system performance, our strategy is to randomly generate a message, and then encode the message thousands of times to get thousands of wiretap codewords, which are transmitted over the main channel and the eavesdropper's channel. Note that, the number of times to encode and transmit a message increases exponentially with the increase of the message bit length k. As a result, it is extremely time-consuming to evaluate the system performance on the off-the-shelf machines when the message bit length is relatively large. Without loss of generality, to solve this problem and improve the practicality of the system, we limit k to be a small value in our simulations and experiments, say $10bits$. Note that the message length does not affect the evaluation of the system security and reliability performance.

5.1 Wiretap Code Implementation

In this subsection, we present the implementation details of wiretap codes introduced in Section 2.2.

Theoretically, we need to convert the BSC with cross-over probability $p(p < \frac{1}{2})$ into a degraded version of BEC, and then generate coding matrices by using the threshold ϵ^* of LDPC code and the erasure probability ϵ. While the conversion does help us to achieve nearly *perfect secrecy*, it does not make full use of channel characteristics [2], and therefore sacrificing too much transmission rate especially when the code threshold ϵ^* is much smaller than $1-r$. Our experiments demonstrate that we can transmit messages at a much higher rate by merely using the transmission rate tradeoff Δ (we proposed), rather than converting a BSC to a degraded version of BEC, to achieve nearly *perfect secrecy* performance.

In both Type-I and Type-II wiretap codes, we adopt regular LDPC codes and use Gallager's algorithm [5] for parity-check matrix generation and Message-Passing decoding algorithm [18] for LDPC decoding. To implement Type-I wiretap code, we first determine a suitable codeword length n through preliminary experimental results. Based on C_e, we overestimate it as C_e^+ according to Theorem 1, *i.e.*, $C_e^+ > C_e$. Then we can construct a $nC_e^+ \times n$ LDPC parity-check matrix $\mathbf{H}$ as the generator matrix $\mathbf{G}$ in $\mathsf{X} = (\mathbf{G}_1^T \ \mathbf{G}^T)\binom{\mathsf{M}}{\mathsf{V}}$. For a non-capacity-achieving LDPC code, we can determine $k = n(1-C_e^+)$. To obtain $\mathbf{G}_1$, we generate a $k_1 \times n$ $(k_1 > k)$ parity-check matrix, from which k rows are selected as $\mathbf{G}_1$'s k independent vectors $x_1, \ldots, x_k$ satisfying $\mathbf{H}_e x_i \neq 0$, where $\mathbf{H}\mathbf{H}_e^T = 0$, *i.e.*, $\mathbf{H}_e$ is the parity-check matrix of $\mathbf{H}$ when $\mathbf{H}$ is used as $\mathbf{G}$. To implement Type-II Wiretap Code, we also choose a fixed codeword length n. Based on C_m and C_e, we first construct an $n(1-r_1) \times n$ parity-check matrix $\mathbf{H}_1$ (we assume $\mathcal{C}_1$ is a capacity-achieving LDPC code for ease of exposition, however, according to Theorem 3 a non-capacity-achieving LDPC code can also be used for $\mathcal{C}_1$ without loss of privacy guarantee). So we have $r_1 = C_e$. Then, we select $n(1-r_2)$ rows from $\mathbf{H}_1$ as $\mathbf{H}_2$ (corresponding to a non-capacity-achieving LDPC code $\mathcal{C}_2$), where $C_m > r_2$ and $\mathbf{H}_2$ ensures the reliability at the receiver. Finally, the remaining $n(r_2 - r_1)$ rows constitute $\overline{\mathbf{H}}_2$.

In our system design, we introduce transmission rate tradeoffs to enhance the system security (*i.e.*, message secrecy) and make the Type-I and Type-II codes practical in real systems by alleviating the theoretical assumption of requiring a large codeword length n. In the simulation study, since we mainly focus on evaluating the effects of transmission rate tradeoff Δ on the system performance, the capacities of both the main channel and the eavesdropper's channel are assumed to remain constant over time.

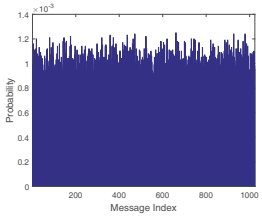
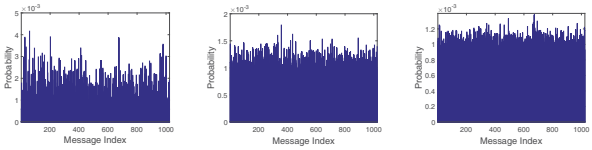


Figure 6: Distribution of uniformly randomly generated messages.



(a) $\Delta = 0.06$ (b) $\Delta = 0.16$ (c) $\Delta = 0.32$

Figure 7: Message distribution when $n = 60$.

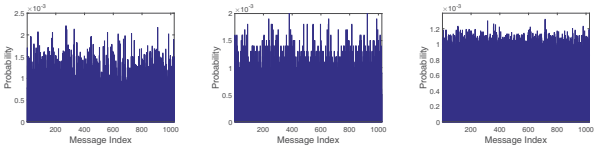
5.2 Performance Evaluation for the Noiseless Main Channel

When the main channel is noiseless, Type-I code is adopted for encoding. We only evaluate the secrecy performance since channel reliability is readily satisfied for a noiseless channel. We evaluate the performance under different codeword length n and transmission rate tradeoff Δ. Note that we keep the coding matrices (or say C_e^+) and message length unchanged but change the tradeoff value, the real capacity of the eavesdropper's channel will change correspondingly.

Fig. 6 shows the distribution of the uniformly randomly generated messages and its equivocation $\mathcal{E} = 9.9921$. We call this distribution as *perfect distribution*, which is used as the benchmark. Figs. 7, 8 and 9 show the distributions of

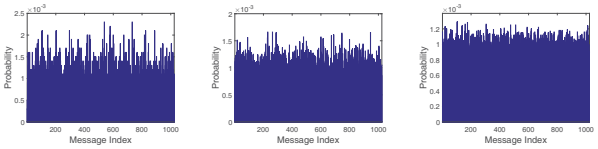
	Codeword length $n = 60$			Codeword length $n = 120$			Codeword length $n = 240$		
C_e^+	0.8332	0.8332	0.8332	0.9139	0.9139	0.9139	0.9563	0.9563	0.9563
Δ	0.06	0.16	0.32	0.06	0.12	0.19	0.02	0.04	0.06
C_e	0.7732	0.6732	0.5132	0.8539	0.7939	0.7239	0.9363	0.9163	0.8963
$\mathcal{E}$	9.9714	9.9917	9.9923	9.9902	9.9923	9.9928	9.9678	9.9915	9.9923
BER_e	0.4998	0.4996	0.5000	0.4994	0.4993	0.4998	0.5000	0.5000	0.4991

Table 1: Performance comparison under different n and Δ for Type-I code.



(a) $\Delta = 0.06$ (b) $\Delta = 0.12$ (c) $\Delta = 0.19$

Figure 8: Message distribution when $n = 120$.



(a) $\Delta = 0.02$ (b) $\Delta = 0.04$ (c) $\Delta = 0.06$

Figure 9: Message distribution when $n = 240$.

the received messages at the eavesdropper for different values of n and Δ, respectively. Generally speaking, the more similar between the distribution of the received messages and the *perfect distribution*, the higher message secrecy of the system.

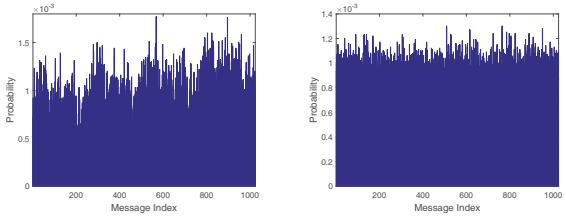
As can be observed, the distribution of received messages becomes more and more similar to the *perfect distribution* when the transmission rate tradeoff Δ increases for the same codeword length n. Accordingly, as shown in Table 1, the equivocation $\mathcal{E}$ increases as the value of transmission rate tradeoff Δ increases for the same codeword length n. It is shown that when $n = 60$ and $\Delta = 0.32$, the equivocation $\mathcal{E} = 9.9923$, which is very close to 9.9921, *i.e.*, the equivocation of *perfect distribution*. Therefore, we can conclude that the system achieves nearly *perfect secrecy* by introducing the transmission rate tradeoff. More importantly, it can be observed that the introduction of Δ can also weaken the influence of the codeword length n to the message secrecy performance. Meanwhile, by introducing the tradeoff the bit error rate BER_e is very close to 0.5, which also implies that the system achieves nearly *perfect secrecy*. Moreover, as expected, only a smaller Δ is required for a larger n to achieve the same equivocation.

It is worth noting that in theory the wiretap channel achieves *perfect secrecy* when the codeword length goes to infinity. However, with the help of the transmission rate tradeoff, the wiretap channel can also achieve nearly *perfect secrecy* even for a small codeword length, which validates the correctness of Theorem 1.

5.3 Performance Evaluation for the Noisy Main Channel

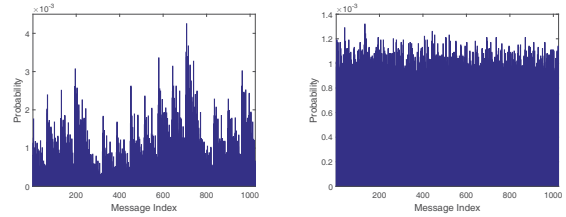
We next consider the second scenario where the main channel is noisy and Type-II wiretap code is adopted for message encoding. Note that we keep the message length unchanged but change r_2, and thus C_e and r_1 will change correspondingly.

Figs. 10, 11 and 12 show the distributions of received messages under different values of n and Δ. As in the noiseless



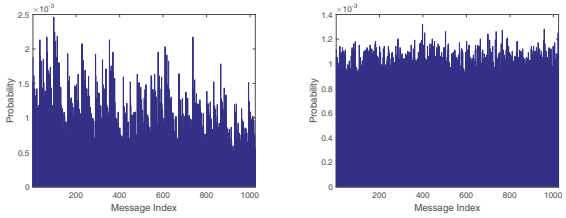
(a) $\Delta = 0.2667$ (b) $\Delta = 0.4167$

Figure 10: Message distribution when $n = 60$.



(a) $\Delta = 0.2083$ (b) $\Delta = 0.5491$

Figure 11: Message distribution when $n = 120$.



(a) $\Delta = 0.2748$ (b) $\Delta = 0.3552$

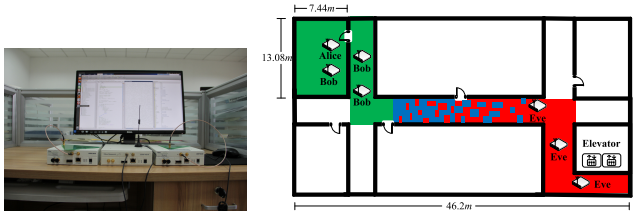
Figure 12: Message distribution when $n = 240$.

	$n = 60$		$n = 120$		$n = 240$	
Δ	0.2667	0.4167	0.2083	0.5491	0.2748	0.3552
C_m	0.8056	0.8056	0.8056	0.8056	0.8056	0.8056
C_e	0.3199	0.1699	0.4706	0.1298	0.4802	0.3998
$\mathcal{E}$	9.9623	9.9929	9.7384	9.9928	9.9037	9.9921
BER_e	0.4885	0.4996	0.5001	0.499	0.4664	0.4991
BER_m	0.0017	0	0.0005	0.000097	0.0019	0.000008
BLER_m	0.0084	0	0.0024	0.0009	0.0071	0.00005

Table 2: Performance comparison under different n and Δ for Type-II code.

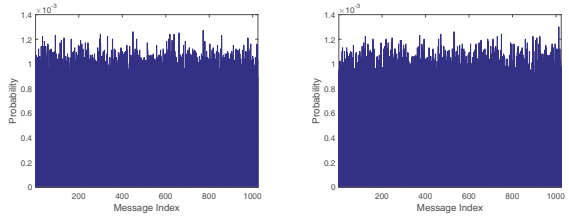
main channel case, the equivocation $\mathcal{E}$ increases as Δ increases. The block error rate BLER_m and the bit error rate BER_m of the main channel are shown in Table 2. It is easy to see that both BER_m and BLER_m are very close to 0. That means the system can achieve nearly *perfect secrecy* and reliability by introducing the transmission rate tradeoff.

Compared to the noiseless scenario, Type-II wiretap code can be used for a noisy main channel, so it can work well for long-range communications. However, when the main channel is noisy, a much larger Δ has to be used to realize nearly *perfect secrecy*, *i.e.*, a larger capacity difference between C_m and C_e is required and C_e cannot be very large.



(a) Prototype (b) Device deployment

Figure 13: Prototype and deployment of devices



(a) $\Delta = 0.23$ (b) no tradeoff

Figure 14: Message distribution with and without using Δ when $n = 240$.

n	C_e^{max}	Δ	$\mathcal{E}$	BER_e
240	0.3562	0.23	9.9928	0.4998
	0.5862	0	9.9926	0.4984
120	0.3562	0.23	9.9926	0.4986
	0.5862	0	9.9932	0.4938

Table 3: Performance for the worst channel case.

6. SYSTEM IMPLEMENTATION AND EXPERIMENTAL RESULTS

In this section, we finally implement the wiretap channel and use real-world experiments to evaluate the system performance. As shown in Fig. 13 (a), we build a communication prototype consisting of three USRP N210 devices with WBX daughter boards operating in the 850MHz as Alice, Bob and Eve, respectively. Alice and Bob are deployed and tested in the green area, Eve is deployed and tested in the red area. Note that, in the blue area, the eavesdropper's channel may be too *good* that it is not suitable for generating enough capacity difference to implement the wiretap channel (in the worst channel case).

In our experiment, we evaluate the performance of the worst channel case and the case where instantaneous channel capacity feedback is available to deal with the variation of channel states. Similar to the simulation study, we limit the message to be $10bits$, and transmit 100000 codewords. Finally, we calculate the equivocation and the bit error rate at the eavesdropper, and the bit error rate and the block error rate at the receiver.

6.1 Performance Evaluation of the Worst Cha -nnel Case

For the worst channel case, the maximum capacity of the eavesdropper's channel is obtained by experiments over a long period of time, but the real-time capacity of the eavesdropper's channel is not available. Through experiments, we find that the main channel is almost error-free if the receiver is close to the sender, say they are within one room.

We first evaluate the system performance when the main channel is noiseless and Type-I wiretap code is adopted for message encoding. In the experiments, it is required that

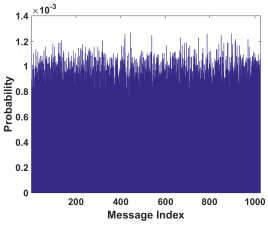


Figure 15: Message distribution when $n = 120$.

n	C_e^{max}	C_m^{min}	Δ	$\mathcal{E}$	BER_e	BER_m	BLER_m
240	0.5051	0.8777	0.1667	9.9929	0.4996	2.8E-5	1.2E-4
120	0.5051	0.8777	0.1667	9.9928	0.4993	7.8E-5	5.1E-4

Table 4: Performance for the worst channel case.

n	Δ	$\mathcal{E}$	BER_e	n	Δ	$\mathcal{E}$	BER_e
120	0.3	9.9925	04954	60	0.3	9.9926	0.4975
	0	9.9923	0.4931		0	9.9933	0.4867

Table 5: Performance for the feedback scheme.

Eve is within "restricted zones" such that the eavesdropper's channel capacity is always below the specific C_e^{max}. Fig. 14 shows the distribution of the received messages for the worst channel case with and without transmission rate tradeoff Δ when $n = 240$, respectively. Table 3 shows $\mathcal{E}$ and BER_e for $n = 120$ and 240. The results indicate that the system performance is almost the same for the worst channel cases with and without introducing Δ. This is because the worst channel case inherently has overestimated the capacity of the eavesdropper's channel, and additional tradeoffs may not be needed to guarantee nearly *perfect secrecy*. Due to this reason, the system can achieve nearly perfect secure communications for the worst channel case without using our proposed tradeoff approach.

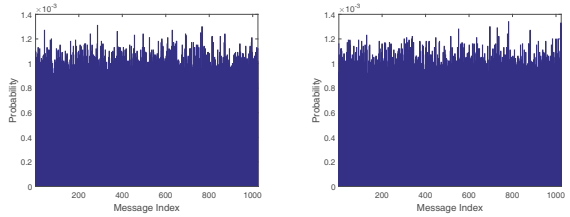
We then evaluate the system performance when the main channel is noisy and Type-II wiretap code is adopted for message encoding. In the experiments, it is required that the receiver is located in the area with C_m always larger than the specific C_m^{min} while the eavesdropper is located in the "restricted zones" with C_e always smaller than the specific C_e^{max}. Fig. 15 shows the distribution of the received messages, and the bit error rate and the block error rate are shown in Table 4. It can be seen that the system also achieves nearly *perfect secrecy* and high reliability.

In summary, the advantage of communicating message under the worst case channel is that we do not need to know the real-time channel state information for obtaining secrecy and reliability, but it faces a limitation that the eavesdropper should be restricted to be certain areas.

6.2 Performance Evaluation of the Dynamic Feedback Case

In this application scenario, we deploy additional USRP N210 nodes on the floor to help estimate and transmit the instantaneous capacities of the main channel and the eavesdropper's channel. As shown in Fig. 4, the capacity only changes slightly between two frames. Thus, in our implementation a training sequence is transmitted to help estimate the channel capacities, based on which we can dynamically adjust the coding design.

We first evaluate the system performance when then main channel is noiseless and Type-I wiretap code is adopted for message encoding. In order to guarantee secrecy, we set



(a) $\Delta = 0.3$ (b) no tradeoff

Figure 16: Message distribution with and without using Δ when $n = 120$.

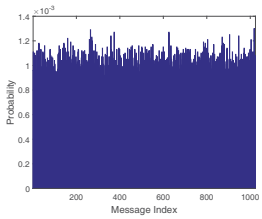


Figure 17: Message distribution when $n = 120$.

n	Δ	$\mathcal{E}$	BER_e	BER_m	BLER_m
120	0.3333	9.9931	0.4993	0.000035	0.00013
60	0.3333	9.9924	0.4991	0.000109	0.00047

Table 6: Performance for the feedback scheme.

the transmission rate tradeoff $\Delta = 0.3$. Fig. 16 shows the distribution of the received messages at the eavesdropper, and Table 5 reports the corresponding bit error rate and block error rate. Similar conclusions can be drawn as those of the worst channel case.

We then evaluate the system performance when the main channel is noisy and Type-II wiretap code is adopted for message encoding. Fig. 17 shows the distribution of the received messages, and Table 6 reports the results under our pre-defined evaluation metrics. Not surprisingly, nearly *perfect secrecy* can also be guaranteed. With dynamic capacity feedbacks, the eavesdropper does not have to be constrained in "restricted zones", but additional nodes need to be deployed to help to estimate the channel capacities.

7. CONCLUSIONS

This paper investigated the design and implementation of a secret message communication system under the classic wireless wiretap channel model. This is the first work to provide practical solutions with a comprehensive performance evaluation to our best knowledge. We tackled many challenges in the protocol design and implementation, and believe that the results and findings in this work can be viewed as the first step towards bridging the gap between the theoretical wiretap channel and its practice. Our immediate future work is to jointly consider the power allocation in optimizing the system performance in terms of secrecy rate and also explore the practicality of other advanced wiretap coding technqiues in the system implementation.

8. ACKNOWLEDGMENTS

We thank Ness Shroff for the inspiring discussions on the subject and the anonymous reviewers for their valuable feedbacks. Qian's research is supported in part by National Natural Science Foundation of China under Grant No. 61373167, National Basic Research Program of China (973 Program) under Grant No. 2014CB340600, and National High Technology Research and Development Program of China under Grant No. 2015AA016004. Kui's research is supported in part by US National Science Foundation under grants CNS-1421903, CNS-1318948 and CNS-1262275. Zhibo is the corresponding author, and his research is supported in part by National Natural Science Foundation of China under Grant No. 61502352, and Natural Science Foundation of Hubei Province under Grant No. 2015CFB203.

9. REFERENCES

[1] Bergmans, P. Random coding theorem for broadcast channels with degraded components. *IEEE Transactions on Information Theory 19*, 2 (1973), 197–207.

[2] Bloch, M., and Barros, J. *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[3] Chou, T.-H., Draper, S. C., and Sayeed, A. M. Key generation using external source excitation: Capacity, reliability, and secrecy exponent. *IEEE Transactions on Information Theory 58*, 4 (2012), 2455–2474.

[4] Cover, T. M. Comments on broadcast channels. *IEEE Transactions on information theory 44*, 6 (1998), 2524–2530.

[5] Gallager, R. G. Low-density parity-check codes. *IEEE Transactions on Information Theory 8*, 1 (1962), 21–28.

[6] Gungor, O., Tan, J., Koksal, C. E., El-Gamal, H., and Shroff, N. B. Secrecy outage capacity of fading channels. *IEEE Transactions on Information Theory 59*, 9 (2013), 5379–5397.

[7] Kanukurthi, B., and Reyzin, L. Key agreement from close secrets over unsecured channels. In *Proc. of EUROCRYPT'09* (2009), pp. 206–223.

[8] Khalil, K., Koyluoglu, O. O., Gamal, H. E., and Youssef, M. Opportunistic secrecy with a strict delay constraint. *IEEE Transactions on Communications 61*, 11 (2013), 4700–4709.

[9] Leung-Yan-Cheong, S., and Hellman, M. E. The gaussian wire-tap channel. *IEEE Transactions on Information Theory 24*, 4 (1978), 451–456.

[10] Ling, C., Luzzi, L., Belfiore, J., and Stehlé, D. Semantically secure lattice codes for the gaussian wiretap channel. *IEEE Transactions on Information Theory 60*, 10 (2012), 6399–6416.

[11] Mahdavifar, H., and Vardy, A. Achieving the secrecy capacity of wiretap channels using polar codes. *IEEE Transactions on Information Theory 57*, 10 (2011), 6428–6443.

[12] Mao, Z., Koksal, C. E., and Shroff, N. B. Achieving full secrecy rate with low packet delays: An optimal control approach. *IEEE Journal on Selected Areas in Communications 31*, 9 (2013), 1944–1956.

[13] Mathur, S., Trappe, W., Mandayam, N., Ye, C., and Reznik, A. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In *Proc. of MobiCom'08* (2008), ACM, pp. 128–139.

[14] Meister, B., and Oettli, W. On the capacity of a discrete, constant channel. *Information and Control 11*, 3 (1967), 341–351.

[15] Pan, B., Kemao, Q., Huang, L., and Asundi, A. Phase error analysis and compensation for nonsinusoidal waveforms in phase-shifting digital fringe projection profilometry. *Optics Letters 34*, 4 (2009), 416–418.

[16] Patwari, N., Croft, J., Jana, S., and Kasera, S. K. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. *IEEE Transactions on Mobile Computing 9*, 1 (2010), 17–30.

[17] Seidel, S. Y., and Rappaport, T. S. 914 mhz path loss prediction models for indoor wireless communications in multifloored buildings. *IEEE Transactions on Antennas and Propagation 40*, 2 (1992), 207–217.

[18] Sharon, E., Litsyn, S., and Goldberger, J. An efficient message-passing schedule for ldpc decoding. In *Proc. of IEEE Convention of Electrical and Electronics Engineers* (2004), IEEE, pp. 223–226.

[19] Thangaraj, A., Dihidar, S., Calderbank, A. R., McLaughlin, S. W., and Merolla, J.-M. Applications of ldpc codes to the wiretap channel. *IEEE Transactions on Information Theory 53*, 8 (2007), 2933–2945.

[20] Wyner, A. D. The wire-tap channel. *The Bell System Technical Journal 54*, 8 (1975), 1355–1387.