Build-in Wiretap Channel I with Feedback and LDPC Codes

Hong Wen, Guang Gong, and Pin-Han Ho

Abstract: **A wiretap channel I is one of the channel models that was proved to achieve unconditional security. However, it has been an open problem in realizing such a channel model in a practical network environment. The paper is committed to solve the open problem by introducing a novel approach for building wiretap channel I in which the eavesdropper sees a binary symmetric channel (BSC) with error probability p while the main channel is error free. By taking advantage of the feedback and low density parity check (LDPC) codes, our scheme adds randomness to the feedback signals from the destination for keeping an eavesdropper ignorant; on the other hand, redundancy is added and encoded by the LDPC codes such that a legitimate receiver can correctly receive and decode the signals. With the proposed approach, unconditionally-secure communication can be achieved through interactive communications, in which the legitimate partner can realize the secret information transmission without a pre-shared secret key even if the eavesdropper has better channel from the beginning.**

Index Terms: **Low-density parity-check (LDPC) codes, security, wiretap channel.**

I. INTRODUCTION

Due to broadcasting in nature, wireless networks are open to malicious intrusion from any outsider. This makes the issues of security a critical concern in the design and operation of a wireless network. The conventional security solutions have been extensively reported by way of context-based encryption and decryption; however, these solutions generally require a strict key distribution, renewal, and revocation process for initiating highly secure communications. This becomes particularly difficult in a dynamic wireless network environment such as a vehicular ad hoc network (VANET), where a key exchange mechanism between two nodes may need to be performed very frequently in order to resist various possible attacks. Therefore, using physical layer security techniques to complement the deficiency of conventional context-based security mechanism has been an interesting proposal that gradually attracts attentions from the research community.

Using physical-layer security techniques, which are based on the Shannon perfect secrecy model [1], is taken as an effective approach in resolving the boundary, efficiency and link reliability issues. A physical-layer transmission with built-in security refers to as a transmission with a guaranteed property of the low-probability-of-interception (LPI) in the aspects of modulation, signal, and channel, without resorting to source data encryption and a shared secret key. An alternative notion of communication with perfect secrecy was introduced by Wyner [2] and later by Csiszar and Korner [3], who developed the concept of wiretap channel for wired links. With a wiretap channel, the eavesdropper is assumed to receive messages transmitted by the sender over the channel that is noisier than the legitimate receiver's channel. Under this condition, it is possible to establish a perfectly secure source-destination link without relying on a shared secret key. From practical perspectives, however, it is generally hard to guarantee that the adversary's channel is noisier than the one taken by the legitimate partner. Therefore, it is generally not practical for achieving strictly positive secrecy capacity in a classical wiretap channel. Another important factors is that a practical and implementable wiretap code has never been available. These practical limitations have diminished the impact of these works, where an open problem of building a wiretap channel in a practical wireless network environment has been left there unsolved.

This fact has motivated the studies on the generalizations of Wyner's model in the past. In [4]–[6], the authors took advantage of a multiple antennas system for achieving perfect secrecy. In [7], the authors exploited user cooperation in facilitating secure the transmission of confidential messages. Tekin [8] *et al*. considered a multiple-access two-way wiretap channel. Lai [9] *et al*. proposed a feedback approach to build the wiretap channel. Among all the previously reported studies,several authors have suggested using the low density parity check (LDPC) codes [10], [11] as secret codes in supporting the wiretap channel.

In this paper, we present a novel approach in building the wiretap channel I [2] by using feedback and LDPC codes, such that an eavesdropper sees a binary symmetric channel (BSC) with error probability p while the main channel could be as error-free as possible. Our model is characterized by the most general situation where an eavesdropper can access to the signals through both the main and feedback channels. For this purpose, we firstly exercise Maurer's idea [7] and build an unconditionally-secure model through interactive communications such that the eavesdropper's channel is noisier than that of the legitimate partner. Then, we utilize the threshold property of LDPC codes [12] to correct the error of the main channel while the error of eavesdropper's channel remains. In this way, a practically realizable wiretap channel model I can be achieved, in which the main channel can be as error-free as possible while

Manuscript received April 09, 2009.

This work is supported by NSERC Discovery Grant and NSERC SPG Grant. The first author wishes to thank UESTC and 863 high technology plan (2007AA01Z299) for their support the research.

H. Wen was with the Dept. of Electrical Computer Engineering, University of Waterloo, Canada and now is working with UESTC, China. This work was done when she was with the University of Waterloo. email: h5wen@engmail.uwaterloo.ca.

G. Gong and P.-H. Ho are working with the Dept. of Electrical Computer Engineering, University of Waterloo, Canada, email: {ggong, p4ho}@uwaterloo.ca.

the eavesdropper's channel is kept noisy.

II. TWO-WAY COMMUNICATION FOR BUILDING WIRETAP CHANNELS

Wyner [2] introduced the wiretap channel in which the transmitter sends a confidential message to a legitimate receiver via the main channel in the presence of an eavesdropper, who listens to the message through its own channel. Wyner proved that the transmitter could send information to the legitimate receiver in virtually perfect secrecy without sharing a secret key with the legitimate receiver if the eavesdropper's channel is a degraded version of the main channel. However, the assumption that the adversary only receives a degraded signal from the legitimate receiver is generally unrealistic. This became a major problem in taking advantage of the advances in the wiretap channel model theory.

The above mentioned problem can be treated by two-way communications, in which feedback signals from the destination play the role of private keys that initiate secure communications. An example is shown as follows. Alice intends to send a sequence $\boldsymbol{M} = \{m_0, m_1, \cdots, m_{n-1}\}$ to Bob. To initiate a secure communication, firstly Bob sends a random sequence $\boldsymbol{Q} = \{q_0, q_1, \cdots, q_{n-1}\}$ to Alice, i.e., $Pr(q_i = 0) = Pr(q_i = 1) = 0.5$. Let $\boldsymbol{E} = \{e_0, e_1, \cdots, e_{n-1}\}$ and $\boldsymbol{EA} = \{ea_0, ea_1, \cdots, ea_{n-1}\}$ denote the error vectors of the Alice's and the eavesdropper's channel, respectively. The received signals of Alice and the eavesdropper is

$$\boldsymbol{T} = \boldsymbol{E} + \boldsymbol{Q} \tag{1a}$$

and

$$\boldsymbol{TE} = \boldsymbol{EA} + \boldsymbol{Q} \tag{1b}$$

respectively, where $\boldsymbol{T} = \{t_0, t_1, \cdots, t_{n-1}\}, t_i = q_i \oplus e_i$ and $\boldsymbol{TE} = \{te_0, te_1, \cdots, te_{n-1}\}, te_i = q_i \oplus ea_i$. Then, Alice uses the received signal $\boldsymbol{T}$ to calculate

$$\boldsymbol{U} = \boldsymbol{T} + \boldsymbol{M} \tag{2}$$

where $\boldsymbol{U} = \{u_0, u_1, \cdots, u_{n-1}\}, u_i = t_i \oplus m_i$. Alice encodes $\boldsymbol{U}$ such that

$$\boldsymbol{W} = \phi(\boldsymbol{U}) \tag{3}$$

where ϕ is the encoder function. Alice sends $\boldsymbol{W}$ over the channel. Bob and the eavesdropper receive the noise version of $\boldsymbol{W}$ as $\boldsymbol{W}'$ and decode $\boldsymbol{W}'$ as

$$\hat{\boldsymbol{U}} = \psi(\boldsymbol{W}') \tag{4}$$

where ψ is the decoder function. We assume the decoding error probability $Pr(\hat{\boldsymbol{U}} \neq \boldsymbol{U}) \rightarrow 0$. Bob and the eavesdropper received $\boldsymbol{U}$ with almost error free. Bob knows the random sequence $\boldsymbol{Q}$, so he can add wise $\boldsymbol{Q}$ to $\boldsymbol{U}$ as

$$\boldsymbol{Y} = \boldsymbol{U} \oplus \boldsymbol{Q} = \boldsymbol{M} \oplus \boldsymbol{E} \tag{5}$$

where $\boldsymbol{Y} = \{y_0, y_1, \cdots, y_{n-1}\}$. The eavesdropper only knows $\boldsymbol{TE}$ that is the noise version of $\boldsymbol{Q}$ and he only can add wise (1b) to $\boldsymbol{U}$ as:

$$\boldsymbol{Z} = \boldsymbol{U} \oplus \boldsymbol{TE} = \boldsymbol{M} \oplus \boldsymbol{E} \oplus \boldsymbol{EA} \tag{6}$$

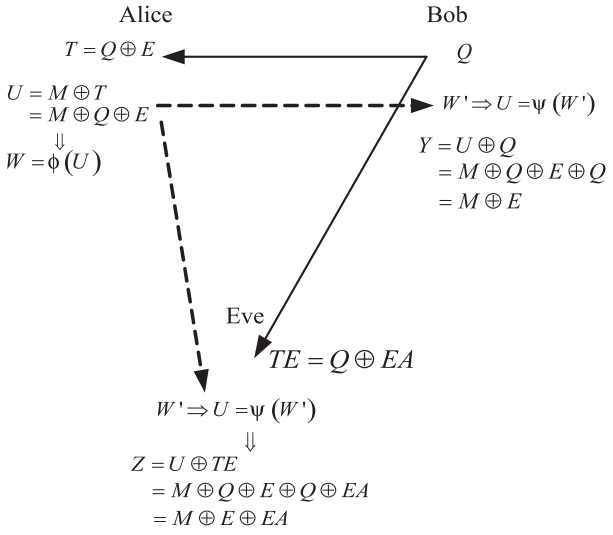


Fig. 1. Two way communication.

where $\boldsymbol{Z} = \{z_0, z_1, \cdots, z_{n-1}\}$. By comparing (5) with (6), $\boldsymbol{EA}$ becomes extra noise. Therefore, after the two-way communication in Fig. 1, the direction of the main channel is inverted when the eavesdropper has a better channel at the beginning.

Lemma 1: After a round-trip two-way communication, the error probability of the main channel is α, and the error probability of the eavesdropper's channel is $\alpha + \beta - 2\alpha\beta$.

Proof: Since

$$Pr(y_i \neq m_i) = Pr(e_i = 1),$$

and

$$\begin{aligned} Pr(z_i \neq m_i) =& Pr(e_i = 1) \cdot Pr(ea_i = 0) \\ &+ Pr(e_i = 0) \cdot Pr(ea_i = 1). \end{aligned}$$

Thus, $Pr(z_i \neq m_i) = \alpha + \beta - 2\alpha\beta$.

Because $\alpha \leq 0.5$ and $\beta \leq 0.5$, so we have $\alpha \leq \alpha + \beta - 2\alpha\beta$, the equality holds for $\alpha = 0.5$ or $\beta = 0.5$. □

III. MULTIPLE ROUNDS OF TWO-WAY COMMUNICATION FOR BUILDING WIRE TAP CHANNEL I

In [13], the secrecy capacity C_s is defined as the maximum rate at which a transmitter can reliably send information to an intended receiver such that the rate at which the attacker receives this information is arbitrarily small. If the intended receiver's channel and eavesdropper's channel have different bit error probabilities (BER) δ and ϵ, respectively, the secret capacity C_s is [7]:

$$C_s = \begin{cases} h(\delta) - h(\varepsilon), & \text{if } \delta > \varepsilon, \\ 0, & \text{otherwise} \end{cases} \tag{7}$$

where h denotes the binary entropy function.

A straightforward attack to the wiretap channel is to reduce the secrecy capacity, or equivalently, to ensure $\delta \leq \epsilon$. When β

is very small, from (7) we know that the secrecy capacity C_s is very small, and the secret level of the system is very weak. Nonetheless, it is clear that after a round-trip two-way communication, only the main channel quality is improved while the attacker's channel will still be as noisy as it was. Thus, there could be a method for changing the situation by continuing performing the two-way communication or parallel channel feedbacks round by round, where the advantage of the main channel will be increased accordingly. A wiretap channel can thus be built when the legitimate user's channel is better than that of the attacker by some extent.

Based on the above observations, our scheme for building wiretap channel I is presented as following. To transmit k-bit messages $\boldsymbol{M}$, we first select a (n, k) linear binary code $\boldsymbol{C}$ such that

$$\boldsymbol{C} = \chi(\boldsymbol{M}) \tag{8}$$

where χ is the encoder function which maps the k bits message $\boldsymbol{M}$ into a n bits codeword $\boldsymbol{C}$. Let us randomly choose $\boldsymbol{C}_0, \boldsymbol{C}_1, \boldsymbol{C}_1, \cdots, \boldsymbol{C}_{t-2}$, where $\boldsymbol{C}_i = (c_i^0, c_i^1, \cdots, c_i^{n-1},), 0 \le i < t-2$. Then, the vector can be calculated as:

$$\boldsymbol{C}_{t-1} = \boldsymbol{C}_0 \oplus \boldsymbol{C}_2 \oplus \cdots \oplus \boldsymbol{C}_{t-2} \oplus \boldsymbol{C}. \tag{9}$$

Firstly, Bob sends t random sequences $\boldsymbol{Q}_i = (q_i^0, q_i^1, \cdots, q_i^{n-1})$, $i = 0, 1, 2, \cdots, t-1$ to Alice by the t independent parallel channels or a channel in t different time slots. Let $\boldsymbol{E}_i = (e_i^0, e_i^1, \cdots, e_i^{n-1})$ and $\boldsymbol{EA}_i = (ea_i^0, ea_i^1, \cdots, ea_i^{n-1})$ denote the error vectors of the Alice's and the eavesdropper's channel correspond to the transmitted the random sequence $\boldsymbol{Q}_i$, respectively. The received signals of Alice and the eavesdropper are $\boldsymbol{T}_i$ and $\boldsymbol{TE}_i$, respectively. Then, Alice uses the received signal to calculate $\boldsymbol{U}_i = \boldsymbol{C}_i \oplus \boldsymbol{T}_i$ according to (2) and encode $\boldsymbol{U}_i$ to get $\boldsymbol{W}_i$ according to (3). Alice sends $\boldsymbol{W}_i$ over the channel. Alice and the eavesdropper receive the noise version of $\boldsymbol{W}_i$ as $\boldsymbol{W}_i'$ and decode $\boldsymbol{W}_i'$ according to (4). From (5) and (6), Bob and the eavesdropper can get $\boldsymbol{Y}_i = \boldsymbol{C}_i \oplus \boldsymbol{E}_i$ and $\boldsymbol{Z}_i = \boldsymbol{C}_i \oplus \boldsymbol{E}_i \oplus \boldsymbol{EA}_i$. By considering the discrete memoryless channel (DMC), we assume that the t words $\boldsymbol{C}_0, \boldsymbol{C}_1, \boldsymbol{C}_2, \cdots, \boldsymbol{C}_{t-1}$ and the t random sequences $\boldsymbol{Q}_0, \boldsymbol{Q}_1, \boldsymbol{Q}_2, \cdots, \boldsymbol{Q}_{t-1}$ are transmitted using the t independent parallel channels or a channel in t different time slots where the transmitted signals are independent each other. Our scheme is illustrated in Fig. 2.

We sum the $\boldsymbol{Y}_i, i = 0, 1, 2, \cdots, t-1$ and $\boldsymbol{Z}_i, i = 0, 1, 2, \cdots, t-1$, respectively as

$$\boldsymbol{Y} = \sum_{i=0}^{t-1} \boldsymbol{Y}_i = \sum_{i=0}^{t-1} \boldsymbol{C}_i \oplus \sum_{i=0}^{t-1} \boldsymbol{E}_i \tag{10a}$$

and

$$\boldsymbol{Z} = \sum_{i=0}^{t-1} \boldsymbol{Z}_i = \sum_{i=0}^{t-1} \boldsymbol{C}_i \oplus \sum_{i=0}^{t-1} \boldsymbol{E}_i \oplus \sum_{i=0}^{t-1} \boldsymbol{EA}_i. \tag{10b}$$

According to (9), (10a), and (10b) become:

$$\boldsymbol{Y} = \boldsymbol{C} \oplus \sum_{i=0}^{t-1} \boldsymbol{E}_i \tag{11a}$$

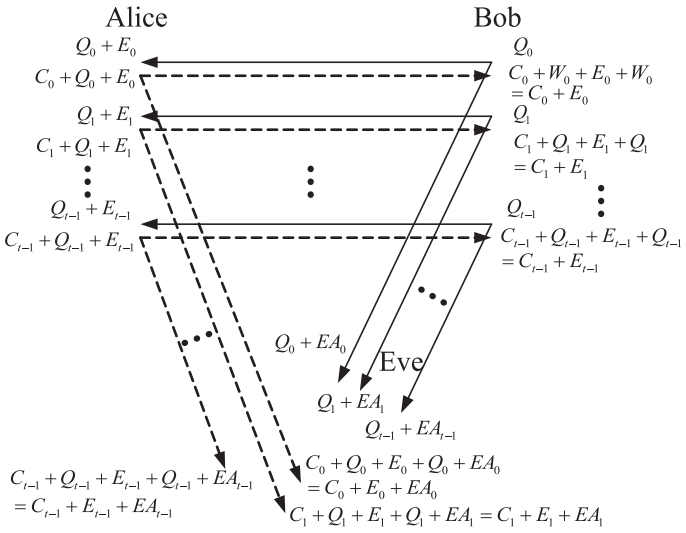


Fig. 2. Interactive communication.

and

$$\boldsymbol{Z} = \boldsymbol{C} \oplus \sum_{i=0}^{t-1} \boldsymbol{E}_i \oplus \sum_{i=0}^{t-1} \boldsymbol{EA}_i. \tag{11b}$$

The term $\sum_{i=0}^{t-1} \boldsymbol{EA}_i$ in (11b) becomes an extra error. Therefore, it is clear that the correct information $\boldsymbol{M}$ can be extracted from $\boldsymbol{Y}$ while keeping the extra error remaining in $\boldsymbol{Z}$ when decoding. Eventually, by employing the powerful LDPC codes as the encoding function in (8), we can get the wiretap channel model I [2] in which the main channel can be as error-free as possible while the eavesdropper's channel is noisy.

Lemma 2: Let the error probability of $\boldsymbol{E}_i$ be denoted as $Pr(e_j^i = 1) = \alpha_i$ and the error probability of $\boldsymbol{EA}_i$ be denoted as $Pr(ea_j^i = 1) = \beta_i$. The error probability of $\boldsymbol{Y}$ in (11a) and $\boldsymbol{Z}$ in (11b) are:

$$P(\boldsymbol{Y}) = \sum_{i=0}^{t-1} \alpha_i - 2 \sum_{\substack{i_1, i_2 = 0 \\ i_1 > i_2}}^{t-1} \alpha_{i_1} \alpha_{i_2} + 4 \sum_{\substack{i_1, i_2, i_3 = 0 \\ i_1 > i_2 > i_3}}^{t-1} \alpha_{i_1} \alpha_{i_2} \alpha_{i_3} + \cdots + (-1)^t 2^t \sum_{\substack{i_1, i_2, \cdots, i_t = 0 \\ i_1 > i_2 > \cdots > i_t}}^{t-1} \alpha_{i_1} \alpha_{i_2} \cdots \alpha_{i_t} \tag{12a}$$

and

$$P(\boldsymbol{Z}) = P(\boldsymbol{Y}) + P(\boldsymbol{ZEA}) - 2P(\boldsymbol{Y})P(\boldsymbol{ZEA}) \tag{12b}$$

where

$$P(\boldsymbol{ZEA}) = \sum_{i=0}^{t-1} \beta_i - 2 \sum_{\substack{i_1, i_2 = 0 \\ i_1 > i_2}}^{t-1} \beta_{i_1} \beta_{i_2} + 4 \sum_{\substack{i_1, i_2, i_3 = 0 \\ i_1 > i_2 > i_3}}^{t-1} \beta_{i_1} \beta_{i_2} \beta_{i_3} + \cdots + (-1)^t 2^t \sum_{\substack{i_1, i_2, \cdots, i_t = 0 \\ i_1 > i_2 > \cdots > i_t}}^{t-1} \beta_{i_1} \beta_{i_2} \cdots \beta_{i_t}.$$

The proof is derived from *lemma* 1 directly.

IV. PERFORMANCE WITH LDPC CODES

Turbo codes [14] and LDPC codes [15], [16] have already been proved in their excellent performance for error correction; thus both of them are good candidates for our scheme. This paper focuses on LDPC codes although we believe that turbo-codes or any other strong channel codes would yield similar results. But the long codeword length is necessary such that the exhaustive attacking complexity can be as high as possible.

A. The Threshold Property of LDPC Codes

LDPC code has been shown to provide excellent decoding performance that can approach the Shannon limit in some cases. The LDPC code exhibits a threshold phenomenon under a certain decoding method, which determines the asymptotic behavior of an ensemble of code. For a code chosen randomly from the ensemble, a large probability of successful decoding can be achieved if the transmission takes place below this threshold; on the other hand, the error probability will stay above a fixed constant if the transmission takes place above this threshold. Such threshold property of the LDPC code can be manipulated for the purpose of correcting the error of the main channel without correcting the error of eavesdropper's channel. Thus, in the following discussions, the LDPC codes serve as the encoding function as defined in (8). Further, because the BSC channel is considered, bit-flip (BF) iterative decoding method is employed [15].

Firstly, the upper bound of threshold that can achieve a correct decoding result is obtained as follows. By considering the regular LDPC codes, we define an n by $n-k$ parity-check matrix for (n, d_l, d_r) LDPC codes such that n columns of the matrix have d_l ones in each column, d_r ones in each row, and zeros elsewhere. Let p_0 denote the crossover probability of the BSC. It was shown in [12] that the expected number of errors in the ith iteration is given by the recursion:

$$a_i = p_0 - p_0 f^+(a_{i-1}) + (1-p_0) f^-(a_{i-1}) \tag{13}$$

where $f^+(x) = \lambda(\frac{1+\rho(1-2x)}{2})$, $f^-(x) = \lambda(\frac{1-\rho(1-2x)}{2})$ and the degree distribution pair $(\lambda(x), \rho(x))$ are function of the form: $\lambda(x) = \sum_{j=2}^{\infty} \lambda_j x^{j-1}$, $\rho(x) = \sum_{j=2}^{\infty} \rho_j x^{j-1}$, where λ_j and ρ_j denote the fraction of ones in the parity-check matrix of the code which are in columns (rows) of weight j.

Definition 1: The threshold P_{up}^* is the supremum of all p_0 in $[0, \frac{1}{2}]$ such that a_i as defined in (13) converges to zero as i tends to infinity.

Lemma 3 ([12])**:** Let τ denote the smallest positive real root of the polynomial $p(x) = xf^+(x) + (x-1)f^-(x)$ and $\lambda_2\rho'(1) < 1$ hold. Then,

$$P_{up}^* \le \min\left\{\frac{1-\lambda_2\rho'(1)}{\lambda'(1)\rho'(1) - \lambda_2\rho'(1)}\right\} \tag{14}$$

where $\lambda'(x)$ and $\rho'(x)$ denote derivatives of $\lambda(x)$ and $\rho(x)$, respectively.

After determined the upper threshold, we consider the lower threshold below which the decoder can not correctly recover the information encoded by the LPDC codes. The lower threshold is mainly determined by the Shannon limit for the BSC, and is described as follows.

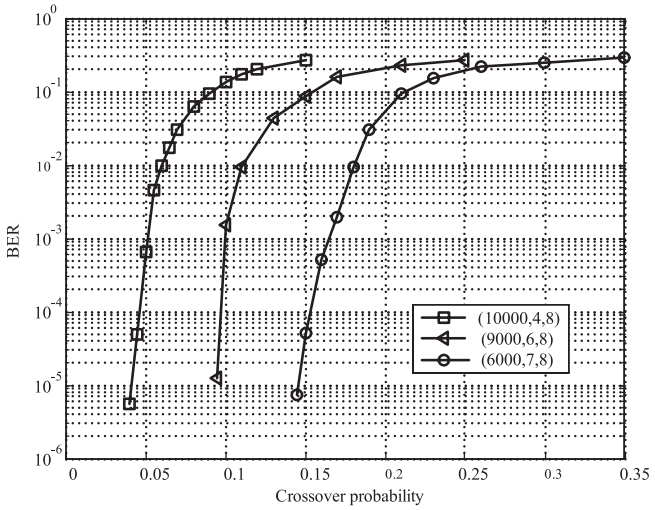


Fig. 3. The BER performances of LDPC codes.

Definition 2: The threshold p_{ep}^* is the infimum of all p_0 in $[0, \frac{1}{2}]$ such that the average error probability of the codeword is greater than a constant number $ep \le 0.5$ as the number of iterative decoding tends to infinity.

Therefore, it is desired that $P(\boldsymbol{Y}) < p_{up}^*$ and $P(\boldsymbol{Z}) > p_{ep}^*$ after several rounds of interactive transmissions. Thus, as the number of rounds is sufficient, the main channel could be as error-free as possible while the eavesdropper still remains an error probability of no smaller than ep that cannot be eliminated in the LDPC codes decoding process.

Table I includes the thresholds of some regular LDPC code ensembles. We let $ep = 0.2$ in Table I.

B. Some Performance Results

We use the random LDPC codes $(10000, 4, 8)$, $(9000, 6, 8)$, and $(6000, 7, 8)$ as the encoder function in (8). The BF decoding bit error rate (BER) of these codes is shown in Fig. 3. To make the channel of legitimate receiver better than that of the attacker by some extent, we launch two scenarios with a single round (i.e., $t = 1$) and two rounds (i.e., $t = 2$) of two-way communications. The maximum number of iterations in decoding is 200. The BER after LDPC codes decoding process are given in Table II and III, respectively, where P_{ir} and P_{Eve} denote the BER of the intended receiver and the eavesdropper after decoding. From the results, it is clearly demonstrated that the positive secret capacity can be achieved by interactive communications even when the eavesdropper has better channel at the beginning. Because the encoder function ϕ in (3) and the decoder function ψ in (4) do not affect to our results, it is reasonably assumable that there exists an error correcting codes such that $Pr(\hat{U}_i \ne U_i) \to 0$.

V. CONCLUSIONS

In this paper, a novel approach for building wiretap channel I was introduced. By adding randomness in the feedback from the destination and redundancy at the source through LDPC codes, a legitimate receiver can correctly receive and decode the sig-

Table 1. The thresholds of some regular LDPC code ensembles.

d_l	d_r	Rate	p^*_{up}	$p^*_{0.2}$	d_l	d_r	Rate	p^*_{up}	$p^*_{0.2}$
3	6	0.5	0.04	0.145	3	4	0.25	0.107	0.228
4	8	0.5	0.048	0.145	4	5	0.2	0.123	0.255
3	5	0.4	0.061	0.178	5	6	0.167	0.142	0.279
4	6	0.333	0.067	0.205	7	8	0.125	0.175	0.306

Table 2. The performance properties with $t = 1$.

Crossover probability	$\alpha = 0.04$ $\beta = 0.04$	$\alpha = 0.08$ $\beta = 0.04$	$\alpha = 0.08$ $\beta = 0.08$	$\alpha = 0.15$ $\beta = 0.075$	$\alpha = 0.15$ $\beta = 0.15$
LDPC code	(10000,4,8)	(9000,6,8)	(9000,6,8)	(6000,7,8)	(6000,7,8)
BER after interaction	$P(\boldsymbol{Y}) = 0.04$ $P(\boldsymbol{Z}) = 0.0768$	$P(\boldsymbol{Y}) = 0.08$ $P(\boldsymbol{Z}) = 0.1136$	$P(\boldsymbol{Y}) = 0.08$ $P(\boldsymbol{Z}) = 0.1472$	$P(\boldsymbol{Y}) = 0.15$ $P(\boldsymbol{Z}) = 0.2138$	$P(\boldsymbol{Y}) = 0.15$ $P(\boldsymbol{Z}) = 0.255$
BER after decoding	$P_{ir} < 10^{-5}$ $P_{Eve} = 0.05$	$P_{ir} < 1.25 \times 10^{-5}$ $P_{Eve} = 0.011$	$P_{ir} = 1.25 \times 10^{-5}$ $P_{Eve} = 0.075$	$P_{ir} = 5.2 \times 10^{-5}$ $P_{Eve} = 0.095$	$P_{ir} = 5.2 \times 10^{-5}$ $P_{Eve} = 0.2$
C_s in (7)	0.2862	0.0871	0.3841	0.4521	0.7211

Table 3. The performance properties with $t = 2$.

Crossover probability	$\alpha_1 = \alpha_2 = 0.02$ $\beta_1 = \beta_2 = 0.02$	$\alpha_1 = \alpha_2 = 0.04$ $\beta_1 = \beta_2 = 0.02$	$\alpha_1 = \alpha_2 = 0.04$ $\beta_1 = \beta_2 = 0.04$	$\alpha_1 = \alpha_2 = 0.08$ $\beta_1 = \beta_2 = 0.04$	$\alpha_1 = \alpha_2 = 0.08$ $\beta_1 = \beta_2 = 0.08$
LDPC code	(10000,4,8)	(9000,6,8)	(9000,6,8)	(6000,7,8)	(6000,7,8)
BER after interaction	$P(\boldsymbol{Y}) = 0.0392$ $P(\boldsymbol{Z}) = 0.0753$	$P(\boldsymbol{Y}) = 0.0768$ $P(\boldsymbol{Z}) = 0.11$	$P(\boldsymbol{Y}) = 0.0768$ $P(\boldsymbol{Z}) = 0.1418$	$P(\boldsymbol{Y}) = 0.1472$ $P(\boldsymbol{Z}) = 0.201$	$P(\boldsymbol{Y}) = 0.1472$ $P(\boldsymbol{Z}) = 0.251$
BER after decoding	$P_{ir} < 10^{-5}$ $P_{Eve} = 0.048$	$P_{ir} < 1.25 \times 10^{-5}$ $P_{Eve} = 0.0093$	$P_{ir} < 1.25 \times 10^{-5}$ $P_{Eve} = 0.071$	$P_{ir} = 1.5 \times 10^{-5}$ $P_{Eve} = 0.055$	$P_{ir} = 1.5 \times 10^{-5}$ $P_{Eve} = 0.205$
C_s in (7)	0.2777	0.0759	0.3694	0.3070	0.7316

nals while an eavesdropper's channel is kept error-prone. With such a mechanism, a wiretap channel I can be created by interactive communications, where an unconditionally-secure communication model can be achieved without a pre-shared secret key even if the eavesdropper has a better channel at the beginning. Under the proposed approach for wiretap channel I, the secret strength of the formed wiretap channel strongly depends on the secret capacity, which is in turn determined by the number of interactive communication rounds (parameter t). It is notable that our scheme is completely realizable in a practical wireless network environment, and our method cannot only be applied to BSC channels, but also continuous ones such as AWGN channel and Rayleigh channel. Another important feature is that our design includes the employment of three different LDPC codes, where the rate compatible (RC) LDPC codes [20] was observed the best choice since its coding rate can be easily adapted to the varying channel quality. To explore better efficiency, our future research efforts will focus on designing a more suitable RC LDPC codes.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 29, pp. 656–715, 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, May 1978.

[4] A. O. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[5] X. Li and J. Hwu, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *J. Commun.*, vol. 2, no. 3, pp. 24–32, May 2007.

[6] H. Kim and J. D. Villasenor, "Secure MIMO communcications in a system with equal numbers of transmit and receive antennas," *IEEE Commun. Lett.*, vol. 12, no. 5, pp. 386–388, May 2008.

[7] M. Yuksel and E. Erkip, "The relay channel with a wire-tapper," in *Proc. 41st Annual. CISS*, Mar. 2007.

[8] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.

[9] L. Lai, H. El Gamal and H. V. Poor, *The Wiretap Channel with Feedback: Encryption over the Channel*, [Online]. Available: http://www.ece.osu.edu/helgamal/publications.html

[10] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. McLaughlin, and J. M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[11] M. Nloch, J. Barros and M. R. D. Rodrigues, "Wireless information theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[12] L. Bazzi, T. J. Richardson, and R. L. Urbanke, "Exact thresholds and optimal codes for the binary-symmetric channel and gallager's decoding algorithm A," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2010–2021, Sept. 2004.

[13] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, pp. 733–742, Mar. 1993.

[14] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error correcting coding and decoding: Turbo codes," in *Proc. IEEE ICC*, (Geneva, Switzerland), 1993, pp. 1064–1070.

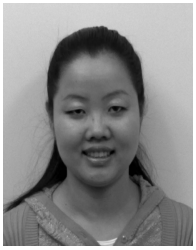
[15] R. G. Gallager, *Low Density Parity Check Codes*. Cambridge, MA: MIT Press, 1963.

[16] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inf. Theory*, vol. 45, pp. 399–431, Mar. 1999.

[17] S. Wolf, "Theoretically and computationally secure key agreement in cryptography", Ph.D. Dissertation, 1999.

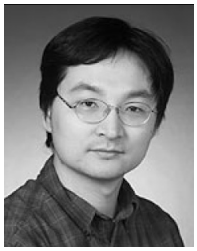
[18] I. Csiszar and P. Narayan, "Common randomness in information theory

and cryptography, part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, pp. 1121–1132, July 1993.
[19] J. Muramatsu, "Secret key agreement from correlated source outputs using low density parity check matrices," *IEICE Trans. Fund. Elec. Comm. Comp.*, vol. E89-A, no. 7, pp. 2036–2046, July 2006.
[20] B. Marco, C. iovanni, and C. Franco, "Variable rate LDPC codes for wireless applications," in *Proc. SoftCOM*, 2006, pp. 301–305.



Hong Wen was born in Chengdu, China. She received the B.Sc. and the M.Sc. degrees in Electrical Engineering from Sichuan Union University of Sichuan, China, in 1991 and 1997, respectively. From July 1994 to September 1994, she worked at Chengdu Engine Co. Ltd, China. From July 1997 to September 2001, she worked at the Chengdu University of Sichuan, China. Then, she went to purchase her Ph.D. degree in Communication and Computer Engineering Dept. of Southwest Jiaotong University. She got her Ph.D. degree in 2004. Then, she worked as Associate Professor at National Key Laboratory of Science and Technology on Communications of UESTC, China. From January 2008 to August 2009, she was research visitor and Postdoctoral Fellowship in Electrical Engineering Department at University of Waterloo. Her major interests are wireless communication system security and channel coding.

Guang Gong received a B.S. degree in Mathematics in 1981, an M.S. degree in Applied Mathematics in 1985, and a Ph.D. degree in Electrical Engineering in 1990, from Universities in China. She received a Postdoctoral Fellowship from the Fondazione Ugo Bordoni, in Rome, Italy, and spent the following year there. After returning from Italy, she was promoted to an Associate Professor at the University of Electrical Science and Technology of China. During 1995–1998, she worked with several internationally recognized, outstanding coding experts and cryptographers, including Dr. Solomon W. Golomb, at the University of Southern California Gong joined the University of Waterloo, Canada in 1998, as an Associate Professor in the Dept. of Electrical and Computer Engineering in September 2000. She has been a full Professor since 2004. Her research interests are in the areas of sequence design, cryptography, and communications security. She has authored or co-authored more than 200 technical papers and one book, co-authored with Dr. Golomb, entitled as Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar, published by Cambridge Press in 2005. She serves (served) as Associate Editors for several journals including Associate Editor for Sequences for IEEE Transactions on Information Theory, and served on a number of technical program committees and conferences. She has received several awards including the Best Paper Award from the Chinese Institute of Electronics in 1984, Outstanding Doctorate Faculty Award of Sichuan Province, China, in 1991, the Premier's Research Excellence Award, Ontario, Canada, in 2001, and NSERC Discovery Accelerator Supplement Award, 2009, Canada.



Pin Han Ho received his B.Sc. and M.Sc. degrees from the Electrical Engineering department in National Taiwan University in 1993 and 1995, respectively, and Ph.D. degree from Queen's University at Kingston at 2002. He is now an Associate Professor in the department of Electrical and Computer Engineering, University of Waterloo, Canada. He is the author/co-author of more than 150 refereed technical papers, several book chapters, and the co-author of a book on optical networking and survivability. His current research interests cover a wide range of topics in broadband wired and wireless communication networks, including survivable network design, wireless Metropolitan Area Networks such as IEEE 802.16 networks, Fiber-Wireless (FIWI) network integration, and network security. He is the recipient of Distinguished Research Excellent Award in the ECE department of University of Waterloo, Early Researcher Award (Premier Research Excellence Award) in 2005, the Best Paper Award in SPECTS'02, ICC'05 Optical Networking Symposium, and ICC'07 Security and Wireless Communications symposium, and the Outstanding Paper Award in HPSR'02.