Exchange of Correlated Binary Sources in Two-Way Relay Networks Using LDPC Codes

Ahmad Salim, *Member, IEEE*, and Tolga M. Duman, *Fellow, IEEE*

Abstract—We consider the problem of exchanging messages in two-way relay (TWR) systems when the sources are correlated binary sequences. In a TWR system, two users communicate simultaneously in both directions to exchange their messages with the help of a relay. Harnessing the fact that the users have access to their own non-compressed messages as side information, each user can compress its message according to the Slepian-Wolf coding strategy by using low-density parity-check codes, particularly, the syndrome approach. Through numerical examples, we show that the proposed scheme offers significant improvements in compression rates compared to the existing solutions in the literature.

Index Terms—Two-way relay, compression with side information, correlated sources, Slepian-Wolf coding, LDPC codes.

I. INTRODUCTION

MOST of the existing schemes for two-way relay (TWR) systems assume independent sources (see [1], [2], and the references therein). However, in many practical scenarios the users' messages are correlated, which, if properly harnessed, could allow for the use of distributed source coding techniques. As an example, consider a wireless sensor network in which the nodes wish to exchange their measurements. Such a setup may also model a cooperative file-sharing network in which users communicate through a relay.

A widely-adopted scheme in TWR systems is physical-layer network coding (PNC) [1] in which users exchange data by first simultaneously transmitting their messages to a relay. The relay then maps the superimposed signal to the estimate of exclusive-OR (XOR) of the users' bits, modulates the latter and broadcasts an amplified version of the modulated symbol. In the current literature, only a limited number of works considered exchange of correlated messages in TWR systems. For instance, [3] proposes Huffman-compressed PNC (HPNC) in which compression is performed at the relay by utilizing the sources' correlation structure. Specifically, the relay maps the received signals to the corresponding PNC-coded symbols and performs Huffman coding. Upon receiving the noise-corrupted Huffman coded packet, each user uncompresses it and retrieves

its partner's message via symbol-wise XOR operation between the non-compressed packet and its own message.

In this letter, to improve the temporal efficiency (defined as the number of exchanged bits per unit time), we propose a scheme that utilizes the correlation between the users' messages to perform compression via distributed source coding, thus performing compression at the users rather than the relay.

Based on Slepian-Wolf (SW) coding, distributed encoders can achieve the same compression rate achieved by a single encoder that has access to the outputs of the correlated sources. In our model, and considering detection at user B, the encoding (compression) at user A applies the syndrome approach based on low-density parity-check (LDPC) codes. User A compresses its message based on the fact that user B has knowledge of its own non-compressed message which is correlated with the message of user A. This formulation resembles the problem of compression of binary sources with side information [4], which we extend to the case of TWR systems with additive white Gaussian noise (AWGN) channels (instead of a perfect link). SW-based compression has been also adopted in a parallel work [5] to propose source compression with PNC (SCPNC). SCPNC uses a linear block code with a correlation-dependent correction capability that guarantees the ability to retrieve the partner's message. Here, instead of using a generic linear code, we employ an LDPC code and design its specific iterative decoder that can efficiently decode the partner's uncompressed message by jointly using the received symbols and the side information. We refer to the proposed scheme as LDPC-Compressed XOR Sum (LXS). Through numerical examples, we show that the proposed scheme outperforms existing solutions in the literature. Low error rates are obtained while compressing the users' messages at rates close to the SW coding bound.

Notation: Unless stated otherwise, bold-capital letters, bold-lower case letters, and lower-case letters denote matrices, vectors, and scalars, respectively. $H_b(p)$ is the binary entropy function, $H_b(p) = -p \log_2 p - (1-p) \log_2(1-p)$, $0 \le p \le 1$. The notation $L(x|y) = \log(\frac{\Pr(x=0|y)}{\Pr(x=1|y)})$ denotes the log-likelihood ratio (LLR) of x given the knowledge of y. The notations $\oplus$, $\mathbf{0}_M$ and $\mathbf{I}_M$ refer to XOR sum, length-M all-zero column vector and the $M \times M$ identity matrix, respectively.

II. SYSTEM MODEL

We consider a TWR system wherein two users exchange messages by first transmitting their compressed messages to a relay, which then processes and broadcasts its received signal.

The data vector representing the message of the ith user, $i \in \{A, B\}$, is denoted by $\boldsymbol{c}_i = [c_{i,1}, c_{i,2}, \ldots, c_{i,N}]^T$ where $c_{i,n}$, $n \in [1 : N]$, are independent and identically distributed (i.i.d.)
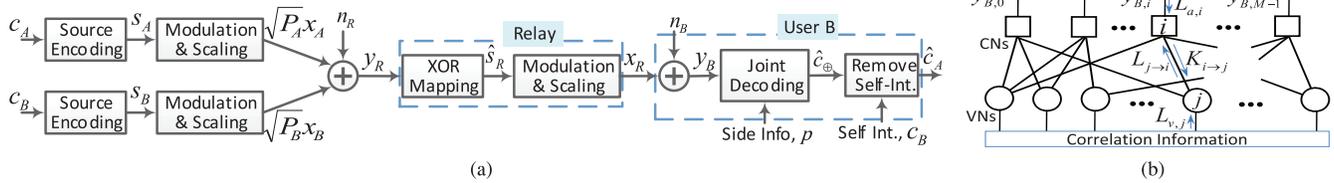
Fig. 1. (a) System model of the proposed LXS scheme based on XOR mapping at the relay. (b) Tanner graph of the decoder.

equiprobable binary random variables. We assume that $c_{A,n}$ and $c_{B,n}$ are correlated with $\Pr(c_{A,n} \neq c_{B,n}) = p$, and that $c_{A,n}$ and $c_{B,n'}$, $n \neq n'$, are independent. Fig. 1a depicts the system model of the two users' transmitters, the relay and the receiver of user B. The two blocks c_A and c_B are compressed to s_A and s_B, respectively, where $s_i = [s_{i,1}, s_{i,2}, \ldots, s_{i,M}]^T$ with $M \leq N$. The latter are then modulated using binary phase-shift keying (BPSK) modulation to obtain $x_i = [x_{i,1}, x_{i,2}, \ldots, x_{i,M}]^T$, $i \in \{A, B\}$. After that, the two users simultaneously transmit $\sqrt{P_A}x_A$ and $\sqrt{P_B}x_B$ where P_i, $i \in \{A, B\}$, is the transmission power at the ith user. The relay's received signal is given by $y_R = \sqrt{P_A}x_A + \sqrt{P_B}x_B + n_R$ where $n_R \sim \mathcal{N}(\mathbf{0}_M, \sigma_R^2 I_M)$ and σ_R^2 is the noise variance at the relay. We adopt a Gaussian TWR model to simplify the description of the decoder even though the model can be extended to account for channel fading and possible phase shifts in practical systems.

III. THE LDPC-COMPRESSED XOR SUM (LXS) SCHEME

To compress the messages, we apply the syndrome approach based on LDPC codes [4], in which each user selects an LDPC code of rate $R_{\text{LDPC}} = \frac{N-M}{N}$, and obtains the length-M compressed message characterized by the syndrome $s_i = H_i c_i$, $i \in \{A, B\}$, where H_i is the $M \times N$ parity-check matrix of the LDPC code of user i. We assume symmetry in terms of the selected LDPC codes, hence we write H instead of H_i.

Discarding noise, the proposed scheme can come very close to the SW coding bound from the perspective of each user [4]. With noise, however, the scheme is only approximate and its performance is not necessarily close to optimal. From the perspective of user i', the problem is simply to compress c_i in a way that efficiently harnesses its side information, i.e., $c_{i'}$, which is correlated with c_i. This formulation resembles the asymmetric case of SW coding wherein one of the sources is available losslessly at the decoder.

Let R_i denote the rate used to compress c_i. Since the other user has side information characterized by its own non-compressed message $c_{i'}$, $i' \neq i$, the decoder at user i' has access to $c_{i'}$ with a rate equal to its entropy (i.e., $NR_{i'} = NH(c_{i',n}) = N$ bits). Thus, according to the SW theorem, the theoretical limit for lossless compression of c_i is given by $NR_i \geq NH(c_{i,n}|c_{i',n}) = NH_b(p)$. Having $p = 0.5$ corresponds to the independent sources case, and hence the users cannot compress below their individual entropies, i.e., $NR_i \geq N$, while having $p = 0$ indicates full correlation, and hence the users need not send anything, i.e., $NR_i \geq 0$.

We perform XOR mapping at the relay (as in conventional PNC) in which y_R is mapped to the estimate of $s_\oplus$, which can be optimally performed by minimizing the probability of error. For the ith received symbol of y_R, this mapping is given by

$$\hat{s}_{R,i} = \begin{cases} 1, & -\gamma < y_{R,i} < \gamma \\ 0, & else \end{cases}, \quad i \in [1:M], \quad (1)$$

where γ is the optimal decision threshold derived as $\gamma = \frac{\sqrt{P_A}+\sqrt{P_B}}{2} + \frac{\sigma_R^2 \log 2}{\sqrt{P_A}+\sqrt{P_B}}$. The derivation follows from [6] by noting that P_A and P_B can be unequal in our case. The relay then performs BPSK modulation and broadcasts $x_R = \sqrt{P_R}(1 - 2\hat{s}_R)$ where $\hat{s}_R = [\hat{s}_{R,1}, \hat{s}_{R,2}, \ldots, \hat{s}_{R,M}]^T$.

Due to symmetry, we only describe the detection process at user B. The received M-sample block is given by $y_B = [y_{B,1}, y_{B,2}, \ldots, y_{B,M}]^T = x_R + n_B$ where $n_B \sim \mathcal{N}(\mathbf{0}_M, \sigma_B^2 I_M)$. A joint LDPC decoder that uses y_B and the side information p is then used to decode the partner's message. Since $H(c_{A,n}) = H(c_{B,n})$, the two users can compress their messages in a lossless manner down to the same compression rate, specifically, $NH(c_{A,n}|c_{B,n}) = NH(c_{B,n}|c_{A,n})$. Therefore, the same rates for the LDPC codes are adopted by the two users. To make the decoding of the LXS scheme simpler, we further assume that the two users use the same LDPC code, and since the code is linear under binary addition, $s_\oplus = s_A \oplus s_B$ is the syndrome of $c_\oplus = c_A \oplus c_B$. The objective of the decoder is thus to decode $c_\oplus$ which is then used to decode c_A using c_B. We adopt the following notation for the decoder:

$L_{j \to i}$: The LLR sent from the jth variable node (VN) to the ith check node (CN).

$K_{i \to j}$: The LLR sent from the ith CN to the jth VN.

$\mathcal{C}(j)$: The set containing indices of all CNs connected to the jth VN, i.e., $\mathcal{C}(j) = \{i | i \in [1:M], [H]_{ij} = 1\}$.

$\mathcal{V}(i)$: The set containing indices of all VNs connected to the ith CN, i.e., $\mathcal{V}(i) = \{j | j \in [1:N], [H]_{ij} = 1\}$.

The joint LDPC decoder is a variant of the conventional sum-product algorithm (SPA) with soft-decision decoding [7]. We characterize the correlation between c_A and c_B by a binary symmetric channel (BSC) with cross-over probability p. Other correlation models, e.g., described by a joint probability mass function (PMF), including higher order modulation schemes, can be addressed similarly, wherein, if the joint PMF is known, the LLRs can be readily calculated. The decoding process can be described as follows.

Initialization: The decoder's Tanner graph is shown in Fig. 1b. Decoding starts by calculating the LLRs associated with the virtual BSC at the VNs, which are calculated as

$$L_{v,j} = L(c_{\oplus,j}|c_{B,j}) = \log \frac{1-p}{p}, \quad j \in [1:N], \quad (2)$$

which, clearly, does not depend on the jth bit of c_B. Instead, it only depends on the correlation structure of the two sources, which, in our case of using a BSC model, is strictly described by p. Hence, the side information in Fig. 1a is denoted by p.

The LLR of the ith bit of $s_\oplus$, $s_{\oplus,i}$, at the ith CN corresponding to the (physical) binary-input AWGN channel is denoted by $L_{a,i} = L(s_{\oplus,i}|y_{B,i})$ where "a" refers to AWGN. We model $s_{\oplus,i}$ as $s_{\oplus,i} = \hat{s}_{R,i} \oplus z_i$, where the binary variable z_i is 0 if there is no decoding error at the relay, and 1 otherwise. Hence, $L_{a,i}$ can be calculated similar to the way it is done in single parity check codes that uses the conventional

"tanh rule" [7], specifically, using the LLRs $L(\hat{s}_{R,i}|y_{B,i}) = 2a_i$ and $L(z_i|y_{R,i}) = \log((1 - P_{E,\text{XS}})/(P_{E,\text{XS}}))$ as inputs where $a_i = \sqrt{P_R}y_{B,i}/\sigma_B^2$ and $P_{E,\text{XS}}$ is the average probability of bit error incurred while mapping $y_{R,i}$ to $\hat{s}_{R,i}$, $i \in [1 : M]$. Evaluation of $P_{E,\text{XS}}$ depends on the modulation scheme and the XOR mapping at the relay. For the two-user BPSK case, $P_{E,\text{XS}} = \frac{1}{2}Q(\frac{\sqrt{P_A} + \sqrt{P_B} - \gamma}{\sigma_R}) + Q(\frac{\gamma}{\sigma_R})$ where $Q(\cdot)$ is the Q-function [8, Appendix E]. $L_{a,i}$ simplifies to

$$L_{a,i} = \log\left(\frac{1 - (1 - \exp(-2a_i))P_{E,\text{XS}}}{\exp(-2a_i) - (\exp(-2a_i) - 1)P_{E,\text{XS}}}\right).$$

Iterations:
1) The LLRs sent from the jth VN to the ith CN are given by

$$L_{j \to i} = L_{v,j} + \sum_{i' \in C(j) - \{i\}} K_{i' \to j}, \qquad (3)$$

where $K_{i' \to j} \; \forall i', j$ are initialized to zero.
2) The LLRs sent from the ith CN to the jth VN are given by

$$K_{i \to j} = 2\tanh^{-1}\left(\tanh\left(\frac{1}{2}L_{a,i}\right)\prod_{j' \in \mathcal{V}(i) - \{j\}}\tanh\left(\frac{1}{2}L_{j' \to i}\right)\right).$$

Termination: When a stopping criterion is reached, the estimate of $c_{\oplus,j}$ is

$$\hat{c}_{\oplus,j} = \begin{cases} 0, & L_{v,j} + \sum_{i \in C(j)} K_{i \to j} \geq 0, \\ 1, & \text{else.} \end{cases} \qquad (4)$$

The receiver then removes the self interference (c_B) to detect its partner's non-compressed message as $\hat{c}_A = \hat{c}_{\oplus} \oplus c_B$.

Even though the LXS scheme assumes perfect time and carrier-phase synchronization, since the decoder performs belief propagation for decoding, the iterative decoder can be redesigned to efficiently estimate and compensate for time and frequency offset as in [1]. Furthermore, other non-idealities can be addressed by extending the corresponding results from conventional PNC. This includes more-than-a-symbol time misalignment [9], [10] and lack of CSI knowledge [11].

IV. NUMERICAL RESULTS

In this section, we evaluate the performance of the proposed scheme in relation to some recently proposed solutions. We use BPSK modulation and assume that $\text{SNR} = 1/\sigma^2$, $\sigma_B^2 = \sigma_R^2 = \sigma^2$ and the LDPC decoders terminate after 100 iterations.

First, we compare the lower bound of the compression rate of the Huffman-compressed PNC scheme in [3] to that of the LXS scheme as a function of the correlation level characterized by p. The lossless compression rate in case of HPNC is bounded as $C_{r,\text{HPNC}} \geq (1 + H_b(p))/2$ [3], while in LXS it is bounded as $C_r \geq H_b(p)$. Notably, since $0 \leq H_b(p) \leq 1$, LXS can provide significantly lower compression rates. For instance, for $p = 0.1$, the compression rates are bounded by about 0.74 and 0.47, for HPNC and SW coding, respectively.

In Fig. 2, we evaluate the LXS scheme at different SNRs as a function of $H_b(p)$. We consider a rate-1/2 irregular LDPC code with lengths 1k, 10k and 20k, randomly generated using the degree distribution in [12, Example 2], which is optimized for BSCs. As shown in Fig. 2, as the code
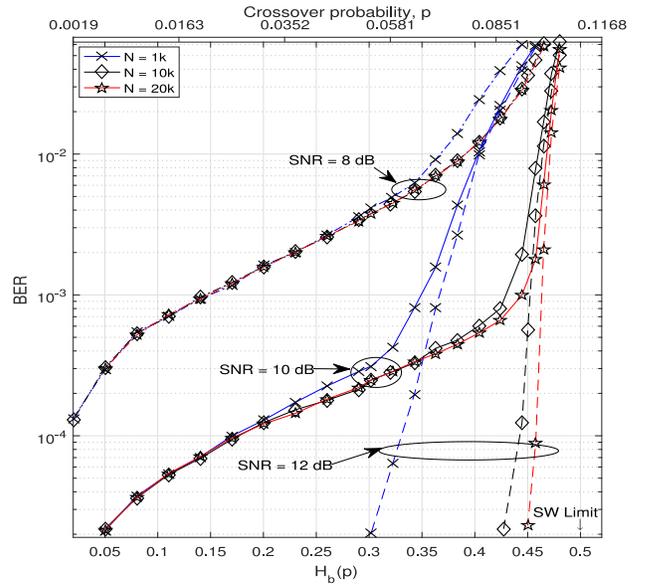

Fig. 2. Performance of the LXS scheme with rate-1/2 LDPC codes for SNRs of 8 dB (dash-dotted), 10 dB (solid) and 12 dB (dashed).
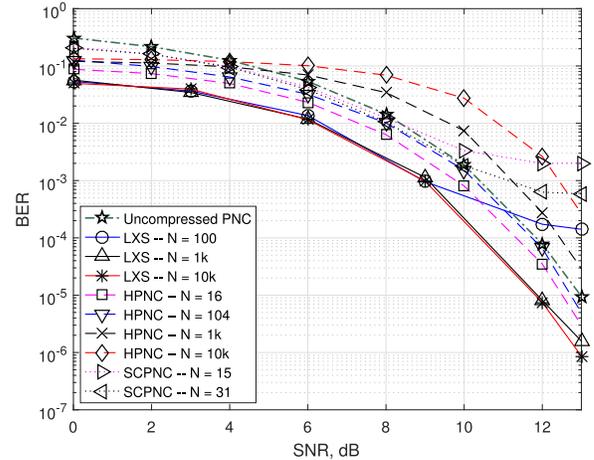

Fig. 3. BER performance of the LXS and the HPNC schemes. Curves for uncompressed PNC, LXS, HPNC, and SCPNC are represented by dash-dotted, solid, dashed, and dotted lines, respectively.

length increases, the performance improves. In this comparison with $C_{r,\text{LXS}} = M/N = 1 - R_{\text{LDPC}}$ fixed, the noiseless SW limit for compression is $H_b(p) = 1/2$ bit, and, as the code length and SNR increase, the gap between this limit and the LDPC code threshold gradually decreases. The SW limit is only approachable if both the code length and SNR tend to infinity.

To further show the advantages of LXS, we compare its performance in Fig. 3 to those of HPNC and SCPNC versus the SNR at the same correlation level ($p = 0.05$). For all schemes, the transmission of one frame involves N bits. For HPNC, we assume that the length of the users' transmitted blocks is $N_{\text{Huff}} = 8$ bits where one frame consists of $N/8$ blocks. At the relay, the corresponding PNC-coded symbols are first obtained, then conventional Huffman coding is performed. On the other hand, the frame in SCPNC and LXS is one block of N bits which is compressed to M bits.

For a fair comparison, the compression ratios $C_{r,\text{HPNC}} = (N_{\text{Huff}} + \overline{N}_{\text{Huff}})/(2N_{\text{Huff}})$ and $C_{r,\text{SCPNC}} = C_{r,\text{LXS}} = M/N$ for

HPNC, SCPNC and LXS, respectively, are set equal, where $\overline{N}_{\mathrm{Huff}}$ is the average length of Huffman-compressed blocks. Herein, we pick $p = 0.05$ resulting in $H_b(p) = 0.2864$, and with $N_{\mathrm{Huff}} = 8$, the resulting $C_{r,\mathrm{HPNC}}$ is about 0.65. To match the compression rates, LXS uses a randomly generated irregular LDPC code of rate $\frac{N-M}{N} = 1/3$ following the degree distributions in [13, Table II] with a maximal left degree of 50 while we use primitive binary BCH codes with approximately the same code rate. The selected BCH codes are the (31, 11) and the (15, 5) codes with error correction capabilities (ECCs) of 3 and 5, respectively. Fig. 3 shows that, unlike LXS, due to error propagation, the performance of HPNC degrades as the frame length increases. Clearly, the LXS scheme outperforms HPNC in the considered SNR range for $N = 1k$ and $N = 10k$. However, an error floor is observed when $N = 100$ since the employed ensemble is designed for long codes, and there are many short cycles resulting in an inferior iterative decoder performance. This error floor can be lowered by designing the code such that the occurrence of trapping sets is reduced [14].

In addition, LXS outperforms SCPNC as the latter is based on taking a hard decision on $s_\oplus$ prior to decoding (unlike LXS), and also because the selected "short-length" BCH codes for the latter have low ECCs unlike the LDPC codes. We avoid long block length BCH codes as they require huge syndrome decoding tables (with a brute force decoding approach), and even if bounded-distance decoding (whose decoding table lists only the error patterns guaranteed by the ECC) is used, it still requires huge memory. Moreover, the error floor in SCPNC is due to the fact that our correlation model does not guarantee a maximum difference between the users' messages (which is an assumption in SCPNC); but instead it describes their average bit difference (ABD) given by $2pN$. That also explains why the (31,11) code outperforms the (15,5) code as it is less probable to cause an uncorrectable error pattern due to the larger difference between its ECC and ABD (i.e., $5 - 3.1 = 1.9$) versus (3-1.5=1.5) for the latter.

We further plot the performance of uncompressed PNC in [6] which has a transmission rate of 1 bit/s while the other curves assume a compression rate of about 0.65. Hence, to maintain fairness, the SNR of the former is penalized. As shown in Fig. 3, the LXS scheme (at large block lengths) and also the HPNC scheme (at small block lengths) provide a better performance than conventional PNC due to the added coding advantage. However, at large block lengths, the HPNC falls behind the conventional PNC due to error propagation.

Finally, we remark that the irregular codes used in this letter (from [12] and [13]) are optimized for a different model. For large block length codes, techniques adopted from density evolution or EXIT chart analysis [7], that use random codes, can be used to design good LDPC codes for our model, but the recursions would have to be modified accordingly. Such techniques aim at minimizing the decoding threshold, possibly at the expense of a higher error floor. Unlike designs intended for channel coding, here we have two sources of a priori information, specifically, the "physical" AWGN channel and the "virtual" BSC that characterizes the correlation. For EXIT chart analysis, the extrinsic mutual information (for a given prior mutual information) is calculated for the VN and CN decoders. For the VNs, the input LLRs are from the BSC and CNs, whereas for CNS, they are from VNs and the AWGN channel. Interestingly, the "virtual" BSC supplies

the same a priori information to each VN which causes a specific mean shift (that depends on p) to the distribution of the output LLRs of the VN decoder. For finite block lengths, using random codes may not guarantee good performance, but there have been successful designs based on structured LDPC codes (e.g., quasi-cyclic LDPC codes [15]) and trellis-based codes [16].

V. Conclusion

We have proposed a novel solution to the problem of exchanging correlated messages in TWR systems. By using the syndrome approach coupled with LDPC codes, each user compresses its message assuming that the other user that will receive it has access to side information. Through numerical examples, we showed that the proposed scheme offers significant advantages in terms of reduced compression rates compared to other alternatives for the present setup.

References

[1] S. C. Liew, S. Zhang, and L. Lu, "Physical-layer network coding: Tutorial, survey, and beyond," *Phys. Commun.*, vol. 6, pp. 4–42, Mar. 2013.

[2] M. Hekrdla and J. Sykora, "Constellations maximizing minimal distance for physical-layer network coding multiway relaying," in *Proc. IEEE 81st Veh. Technol. Conf.*, Glasgow, U.K., May 2015, pp. 1–6.

[3] Q. Huo, K. Yang, L. Song, Y. Li, and B. Jiao, "Compressed relaying for two-way relay networks with correlated sources," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 30–33, Feb. 2015.

[4] A. D. Liveris, Z. Xiong, and C. N. Georghiades, "Compression of binary sources with side information at the decoder using LDPC codes," *IEEE Commun. Lett.*, vol. 6, no. 10, pp. 440–442, Oct. 2002.

[5] Q. Huo, L. Song, Y. Li, and B. Jiao, "Source and physical-layer network coding for correlated two-way relaying," *IET Commun.*, vol. 10, no. 5, pp. 502–507, Mar. 2016.

[6] S. Zhang, S. C. Liew, and P. P. Lam, "Hot topic: Physical-layer network coding," in *Proc. 12th Annu. Int. Conf. Mobile Comput. Netw.*, Los Angeles, CA, USA, 2006, pp. 358–365.

[7] W. Ryan and S. Lin, *Channel Codes: Classical and Modern*. Cambridge, U.K: Cambridge Univ. Press, 2009.

[8] A. Salim, "Transmission strategies for two-way relay channels," Ph.D. dissertation, School Elect. Comput. Energy Eng., Arizona State Univ., Tempe, AZ, USA, 2015.

[9] A. Salim and T. M. Duman, "An asynchronous two-way relay system with full delay diversity in time-varying multipath environments," in *Proc. Int. Conf. Comput. Netw. Commun.*, Garden Grove, CA, USA, Feb. 2015, pp. 900–904.

[10] A. Salim and T. M. Duman, "A delay-tolerant asynchronous two-way-relay system over doubly-selective fading channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3850–3865, Jul. 2015.

[11] A. Salim and T. M. Duman, "Differential modulation for asynchronous two-way relay systems over frequency-selective fading channels," *Wireless Commun. Mobile Comput.*, vol. 16, no. 16, pp. 2422–2435, 2016.

[12] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 619–637, Feb. 2001.

[13] J. Hou, P. H. Siegel, and L. B. Milstein, "Performance analysis and code optimization of low density parity-check codes on Rayleigh fading channels," *IEEE J. Sel. Areas Commun.*, vol. 19, no. 5, pp. 924–934, May 2001.

[14] T. Richardson, "Error floors of LDPC codes," in *Proc. Allerton Conf. Commun. Control Comput.*, vol. 41. 2003, pp. 1426–1435.

[15] C.-M. Huang, J.-F. Huang, and C.-C. Yang, "Construction of quasi-cyclic LDPC codes from quadratic congruences," *IEEE Commun. Lett.*, vol. 12, no. 4, pp. 313–315, Apr. 2008.

[16] A. Özcelikkale and T. M. Duman, "Short length trellis-based codes for Gaussian multiple-access channels," *IEEE Signal Process. Lett.*, vol. 21, no. 10, pp. 1177–1181, Oct. 2014.