Transactions Letters

Multiple-User Cooperative Communications Based on Linear Network Coding

Ming Xiao, *Member, IEEE,* and Mikael Skoglund, *Senior Member, IEEE*

***Abstract*—We propose a new scheme for cooperative wireless networking based on linear network codes. The network consists of multiple ($M \geq 2$) users having independent information to be transmitted to a common basestation (BS), assuming block-fading channels with independent fading for different codewords. The users collaborate in relaying messages. Because of potential transmission errors in links, resulting in erasures, the network topology is dynamic. To efficiently exploit the diversity available by cooperation and time-varying fading, we propose the use of diversity network codes (DNCs) over finite fields. These codes are designed such that the BS is able to rebuild the user information from a minimum possible set of coded blocks conveyed through the dynamic network. We show the existence of deterministic DNCs. We also show that the resulting diversity order using the proposed DNCs is $2M-1$, which is higher than schemes without network coding or with binary network coding. Numerical results from simulations also show substantial improvement by the proposed DNCs over the benchmark schemes. We also propose simplified versions of the DNCs, which have much lower design complexity and still achieve the diversity order $2M-1$.**

***Index Terms*—Linear network coding, cooperative communications, source-coding, outage probability, code construction, dynamic topology, field size.**

I. Introduction

As an efficient method to combat wireless fading, cooperative communications [1]–[3] has attracted substantial research efforts. In the scenarios we consider, two or more users sending messages to a common basestation (BS) form partners to help each other in the information transmission. In a classic two-user cooperative scenario [1]–[3], when a node (say user 1) communicates to the BS, the partner node (user 2) also receives the message because of the broadcasting property of the wireless medium. Then, the partner node can try to decode, and if the decoding is successful, it can forward the message of user 1 to the BS. A similar scheme works when user 2 transmits and user 1 relays. Therefore, information messages are transmitted to the BS through two independently fading paths: one direct path and one through a relay node.

Most of the early cooperative communication protocols keep information of different users separate in different orthogonal channels. As a new strategy for information transmission in networks, *network coding* [4], [5], allows messages from different sources (or to different sinks) to mix in the intermediate nodes. Performance gains in terms of network flow [4], robustness [5] or energy efficiency [6] are obtained. Network coding has also been applied to implement cooperative communication schemes [7]–[10]. Reference [7] considers a scheme for two-user cooperation, in which each user transmits the binary sum of its own source message and partner messages, resulting in spectrally efficient transmission. However, the approach in [7] is hard to generalize to multiple user networks (more than 2 users), since when decoding a partner message at a relaying node local source messages need to be used, and these may not be available in the case of multiple users. Reference [8] studies a scheme based on binary combination at the relaying nodes for ad-hoc wireless networks. In [9], an adaptive random sparse matrix coding approach is combined with network coding for multiple-user cooperative networks. In that scheme, a significant number of user nodes is needed to form random codes, limiting the application of the scheme. In [10], an approach that combines network coding and multi-user detection is proposed, resulting in improved BER performance. All approaches suggested in [7]–[10] only consider binary network coding, based on XOR operations, which may not be optimal in the sense of asymptotic performance for certain network settings.

For wireless cooperative networks, as we shall show, carefully designed network codes over finite fields can have solid performance improvement over previous schemes based on binary codes. Compared to routing, the advantage of network coding is the ability to achieve the min-cut capacity, i.e., to rebuild the source from the minimum possible set of coded blocks. One challenge, however, in network code design for wireless cooperative networks is the dynamic nature of the network topology due to the fact that transmission errors at the physical layer can result in erasures at the network layer. That is, from the point of view of network coding, individual links "disappear" at random, resulting in different topologies. At this background, our goal in this paper is to exploit the *min-cut* achieving capability of network coding in cooperative wireless networks. To accomplish this, the network codes need to work over sufficiently large fields and follow certain structures [4], [5].

We propose a new method for using network coding in M-user cooperative wireless networks with block fading channels. We design network codes over finite fields such that the BS is able to rebuild user information from a minimum possible set of different coded blocks. Compared to cooperative communications without network coding or with binary network coding,

Paper approved by F. Alajaji, the Editor for Source and Source/Channel Coding of the IEEE Communications Society. Manuscript received February 18, 2010; revised June 2, 2010.

Parts of this work were presented at the IEEE Information Theory Workshop, Volos, Greece, June, 2009.

The authors are with the Communication Theory Lab, School of Electrical Engineering and the ACCESS Linnaeus Center, Royal Institute of Technology, Sweden (e-mail: {ming.xiao, skoglund}@ee.kth.se).

This work has been supported in part by the Swedish Research Council (VR), VINNOVA, and by Wireless@KTH.

Digital Object Identifier 10.1109/TCOMM.2010.092810.100045

0090-6778/10$25.00 © 2010 IEEE

the proposed scheme can substantially improve performance, especially at medium-to-high signal-to-noise ratios (SNRs). The improvement is more pronounced in the case of more cooperating users.

The organization of the paper is as follows. In Section II, we study the two-user scenario, and in Section III, we investigate multiple ($M > 2$) users networks. We leave detailed proofs to an appendix.

II. Two-User Cooperative Networks

For simplicity, and the purpose of illustration, we start by investigating the two-user cooperative scenario.

A. System Description

The proposed system is illustrated in Fig. 1, in which we use network codes over finite fields, on top of channel coding, to encode relayed and local messages. The network coding scheme is time-invariant in each relay node (deterministic codes). In the first time slot[1], the two source nodes use proper channel coding to transmit their own messages I_1 and I_2 (systematic blocks) respectively in different orthogonal channels. In the second time slot, if both relay nodes successfully decode the channel codes, the transmitted messages for user 1 and user 2 are encoded using network coding as $I_1 + I_2$ and $I_1 + 2I_2$, respectively. Here, we consider network coding over GF(4), constructed based on the minimal polynomial $p(X) = X^2 + X + 1$. Hence, the four elements are the polynomials $0, 1, X$ and $X + 1$. For simplicity, we use integer notation for the field elements, i.e., $0, 1, 2$ and 3, respectively. We assume block fading channels, that is, the channels stay constant over the transmission of a codeword at the physical layer, but vary independently between successively transmitted blocks. We assume that the variation is independent and identically distributed (i.i.d.). Clearly, in total, the BS receives codewords carrying four different messages: I_1, I_2, $I_1 + I_2$ and $I_1 + 2I_2$, where each message has experienced independent fading. Any two of these four blocks can rebuild the two source blocks I_1 and I_2. If a relay node cannot decode correctly, it instead repeats its own message using the same channel code. Then the BS performs MRC (maximum ratio combination) of these codewords and decodes. Here we assume perfect error detection. Thus, for all channels, the outputs from channel decoders are either dropped or can be considered error-free.

B. Performance Analysis

To measure performance in the range of medium-to-high SNR, we study outage probabilities. In particular, we will be interested in the resulting diversity order D [2], [11],

$$D \triangleq \lim_{\text{SNR}\to\infty} \frac{-\log P}{\log \text{SNR}}, \tag{1}$$

where P is the relevant error probability under consideration (e.g., frame error probability or outage probability). In our setup, a received codeword is obtained as $Y_{i,j,k} = a_{i,j,k}X_{i,j,k} + n_{i,j,k}$, where $X_{i,j,k}$ and $Y_{i,j,k}$ are transmitted and received channel codewords, respectively; $n_{i,j,k}$ is additive white Gaussian noise with zero-mean and unit variance; $a_{i,j,k}$ denotes the fading channel gain. The index $i = 1, 2$ denotes the transmitting user 1 or 2, $j = 0, 1, 2$ denotes the receiving BS, user 1 and user 2, respectively, and k denotes the time slot. The $a_{i,j,k}$s are i.i.d. random variables for different i, j or k with a Rayleigh distribution and unit variance. We first consider reciprocal inter-user channels, i.e., $a_{i,j,k} = a_{j,i,k}$. Assuming i.i.d. Gaussian codewords ($X_{i,j,k}$s), the mutual information (MI) between $Y_{i,j,k}$ and $X_{i,j,k}$ is $\text{MI}_{i,j,k} = \frac{1}{2}\log(1 + |a_{i,j,k}|^2\text{SNR})$. Here we assume all channels have the same transmitting power, and all channel codewords have the same rate R. Hence, $X_{i,j,k}$ cannot be decoded correctly if $|a_{i,j,k}|^2 < g$, where $g = \frac{2^{2R}-1}{\text{SNR}}$. For Rayleigh fading, the corresponding outage probability of the link/transmission corresponding to $a_{i,j,k}$ is obtained as ([2], [11])

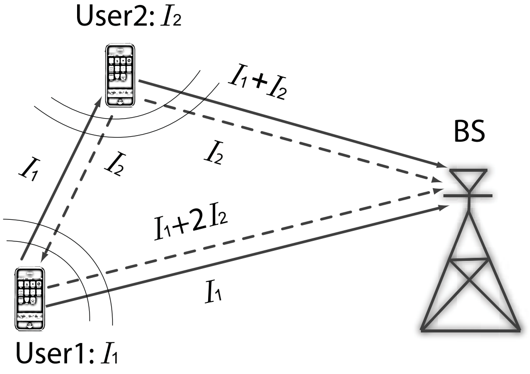

Fig. 1. Two-user cooperative networks with proposed designed network codes over finite fields. The information messages I_1 and I_2 of user 1 and 2, respectively, are realized over GF(4). Network coding is also in GF(4). All transmission blocks are subject to independent fading.

$$P_e = Pr\{|a_{i,j,k}|^2 < g\} = 1 - e^{-g} \approx \frac{2^{2R}-1}{\text{SNR}}. \tag{2}$$

The approximation holds for high SNRs. Without loss of generality, we analyze the overall outage probability for user 1. If there is no outage in the inter-user channel, there are 4 different network code blocks. An outage occurs only when the direct systematic codeword (I_1) cannot be decoded, and 2 (or 3) out of other 3 codewords (for I_2, $I_1 + I_2$ or $I_1 + 2I_2$) cannot be decoded at the BS. Since the $a_{i,j,k}$s are i.i.d, the overall outage probability is hence obtained as

$$P_0 = P_e(\binom{3}{2}P_e^2(1-P_e) + P_e^3) \approx 3P_e^3. \tag{3}$$

With probability P_e, the relaying node cannot decode the partner's codeword. In this case, the BS performs MRC and decodes. Thus, overall outage occurs when

$$\text{MI}_{\text{MRC}} = \frac{1}{2}\log(1 + (|a_{i,j,1}|^2 + |a_{i,j,2}|^2)\text{SNR}) < R. \tag{4}$$

Then, the outage probability is ([2]) $P_1 = 0.5g^2 \approx \frac{(2^{2R}-1)^2}{2\text{SNR}^2}$. Combining, we get the total outage probability

$$P_{o,1} = P_eP_1 + (1-P_e)P_0 \approx 3.5P_e^3. \tag{5}$$

Consequently, the diversity order is $D_{NC} = 3$. If the inter-user channels are not reciprocal, we only need to separately consider the outage probability of two inter-user channels. By a similar analysis, the outage probability for user 1 is $P_{o,2} \approx 4P_e^3$. Hence, the diversity order is still 3.

[1] We use "time slot" and "block" interchangeably to denote the the time-period corresponding to one transmitted codeword at the physical layer.

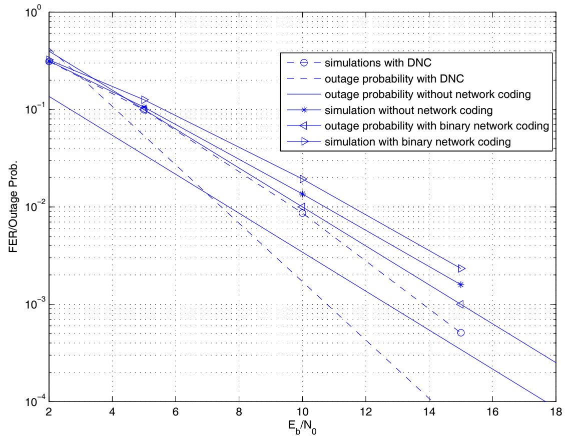

Fig. 2. Simulations and outage probabilities for Fig. 1 with reciprocal inter-user channels. The channel codes are regular LDPC codes with 200 information bits, 400 coded bits and each column of parity check matrix has three 1s.

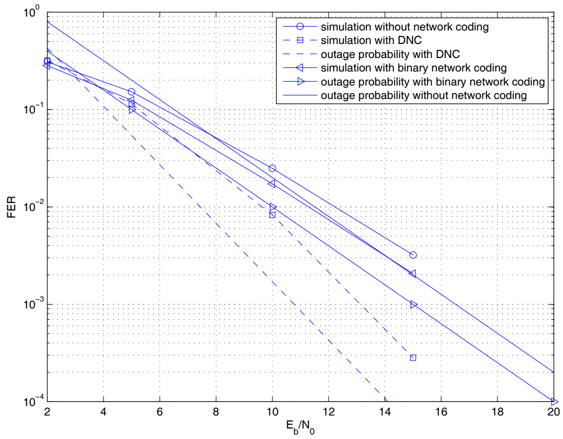

Fig. 3. Simulations and outage probabilities for non-reciprocal inter-user channels. The channel codes are regular LDPC codes with 500 information bits, 1000 coded bits.

An important comment in this paper, is that *it is necessary that the user messages can be reconstructed from any two out of four network codewords to achieve diversity order* 3. This requires carefully designed network codes over finite fields. We also note that we assume independent fading for successive codewords of the same channels. Our network codes are designed to exploit the diversity of both independent block fading and cooperation among users, that is, we utilize both time and space diversity. This cannot be fully accomplished by schemes based on binary network coding. To see this, note that if the second blocks of both users are both $I_1 \oplus I_2$ over GF(2) (as suggested e.g. in [7]–[10]), then the received blocks at the BS are I_1, I_2, $I_1 \oplus I_2$ and $I_1 \oplus I_2$. For user 1, outage hence occurs when two blocks cannot be decoded. These two blocks can be I_1 and I_2 (two $I_1 \oplus I_2$ cannot rebuild the source messages), resulting in a diversity order of 2. This conclusion holds also for previously proposed cooperative schemes not employing network coding, e.g., [1]–[2]. Thus, the approach based on non-binary network codes we propose can achieve a higher diversity order, and a resulting performance gain for medium-to-high SNRs. We also emphasize that the network codes in Fig. 1 can achieve the min-cut bound in the dynamic case (random erasures), since they rebuild the two messages from *any* two of the received codewords. Thus, we call such network codes *diversity network codes* (DNCs). A more general definition will be given later.

In Fig. 2, we show simulation results for networks without cooperative communication, cooperative communication without network coding, and cooperation based on the proposed DNCs. Here we use regular low-density parity-check (LDPC) codes as physical layer channel codes. In Fig. 2, we assume reciprocal inter-user channels. The codes have 200 input bits and 400 output coded bits. Each column of the parity check matrix has three 1s and the other elements are 0s. We use BPSK signals for transmission. In the same figure, we also show the outage probabilities. In Fig. 3, we show the simulations and outage probabilities for networks with non-reciprocal inter-user channels. The LDPC code have 500 input and 1000 output bits. From both figures, we can see the improvement by using DNCs in cooperative communications. The improvement is pronounced in the medium to high SNRs.

III. Multiple-User Networks

Here we generalize the proposed scheme to multi-user networks. We first state the general system description.

A. System Description

We assume $M (M \geq 2)$ users, each with a message to be transmitted to a common BS. Each user transmits the same amount of information in one transmission period, consisting of M consecutive blocks. As before, we assume i.i.d. block fading, with each channel being constant over the duration of a block. In the first time slot, all users transmit their own information (providing systematic blocks) in different orthogonal channels using physical layer channel coding. All users listen, and after the first time slot they all act to relay the messages they were able to decode after the first slot, and perform network coding on their own and all successfully received messages. The resulting network codewords are sent to the BS in the remaining slots 2 to M. In the case a relay node cannot decode from any of the $M-1$ partners, it repeats its own information $M-1$ times using the same channel codeword. Thus, each user transmits M times in M time slots. These M codewords are transmitted in independent block fading channels. We denote the source message of user z by I_z. For user j $(j = 1, 2, \cdots, M)$, the network codeword in the ith $(i = 2, 3, \cdots, M)$ time slot is then obtained as

$$C_{j,i} = \sum_{z=1}^{M} \alpha_{j,z,i} I_z, \tag{6}$$

where $\alpha_{j,z,i}$ is a coding coefficient in GF(Z). If node j cannot decode I_z for partner z, it uses an all-zero message to replace I_z (or equally, set the corresponding $\alpha_{j,z,i}$ to the zero element, for $i = 2, \ldots, M$). The BS first decodes $C_{j,i}$ for all time slots, by physical layer channel decoding and error detection, and then decodes I_j based on the structure of the network code. In the case of re-transmitted channel codewords, the BS first performs MRC and then decodes.

We note that since different users transmit in orthogonal channels, and each user needs M independent fading blocks there are in total M^2 channels. We have implicitly assumed that these are created by using orthogonal frequency slots for the M users, and different time slots for the in total M messages transmitted by one user. However, in practice, the M^2 orthogonal slots needed for the overall transmission can be allocated differently in time and frequency, achieving different trade-offs between the required bandwidth and delay.

B. Network Code Design

Let $\hat{D}_j$ $(j = 1, 2, \cdots, M)$ denote the set of nodes that can successfully decode the message I_j from node j, and can hence help to relay this message. The network codewords transmitted from users in $\hat{D}_j$ will all involve I_j according to (6). Also, let $D_j = \hat{D}_j \cup \{\text{user j}\}$. Since each user transmits M codewords, there are in total $M|D_j|$ codewords transmitted for users in D_j (where $|\cdot|$ denotes cardinality). The network codes we propose are then designed based on the following definition:

Definition 1. By a *diversity network code* (DNC) we mean any deterministic network code, used as described, such that the BS can recover I_j if it can successfully decode any subset of $|D_j|$ different channel codewords out of the total $M|D_j|$ codewords from users in D_j, for all possible D_j, and for any user j $(j = 1, 2, \cdots, M)$.

We refer to cooperative wireless networking based on DNCs as *coded cooperative networking*. Such schemes can always be constructed, as a consequence of the following proposition.

Proposition 1. M-user DNCs exist.

Proof: We omit a detailed proof, due to the similarities with the proof of Theorem 11 in [5] (linear robust network codes). One difference is that we regard an erasure of a channel codeword as a link failure, and the corresponding error patterns (the set of channels with erasures due to link failures) may change for each transmission period. Another difference is that we consider multiple source nodes. However, the considered networks are still acyclic and each user has the same transmission rate. Thus, the proof is essentially the same as that in [5]. ■

Clearly, the problem of constructing DNCs for coded cooperative networks with M users is equivalent to finding a code with an encoding matrix [5] being non-singular for all users, and for all error patterns. The encoding matrix T describes the linear relation between the source messages and network codewords. The first M columns of T form a diagonal $M \times M$ sub-matrix, corresponding to the directly transmitted blocks. The remaining $M-1$ columns and M rows correspond to the remaining $M-1$ codewords sent by each user, according to (7).

By arranging T as above, the variable $\alpha_{j,z,i}$ in (6) corresponds to $\alpha_{z,M+(M-1)(j-1)+i-1}$ in (7). In the case of no outages, neither between users nor between any of the users and the BS, the set of symbols received by the BS are obtained as the components of the vector

$$\sum_{z=1}^{M} I_z t_z, \tag{8}$$

where t_z denotes the zth row of T. However, since there may be outages, the effective T seen by the BS may change. If there is an inter-user channel outage in the link $z \to j$, we set the corresponding variables $\alpha_{j,z,i}, i = 2, \ldots, M$, to zero, and in the case of outage between a user and the BS, we erase the corresponding column in T. Then if we can show that the resulting matrix for any set of K or fewer outages is still full rank, the BS will be able to recover all user messages if there are K outages or fewer, providing a design criterion for constructing DNCs. This approach has high complexity, however, since we need to consider all possible error patterns. Before presenting a simplified approach, we analyze the outage probability for the proposed coded cooperative networks with M users.

C. Outage Probability and Diversity Order

We again use P_e to denote the outage probability of an individual channel. We assume that I_j can be successfully decoded by a set of users $\hat{D}_j$, and cannot be decoded by the other $M - |\hat{D}_j| - 1$ users. The probability is $P(\hat{D}_j) \approx P_e^{M-|\hat{D}_j|-1}$. We consider reciprocal inter-user channels, for simplicity (the results are similar for non-reciprocal inter-user channels). Then, user j can also decode messages from $\hat{D}_j$. Clearly, $\hat{D}_j$ is mainly decided by the quality of the inter-user channels and is random during each transmission period. Now we evaluate the outage probability for user j. We have the following theorem.

Theorem 1. The diversity order obtained by the proposed coded cooperative networking scheme based on DNCs is $2M - 1$.

Proof: The proof is given in Appendix IV-A. ■

We note that the diversity order $2M - 1$ is the highest possible in our scenario, since the error scenario that dominates the overall outage probability is when all inter-user links fail (exponent $M - 1$) and hence only time diversity directly to the BS is available (exponent M). In all other scenarios, cooperative gain is achieved. Conditioned that at least one inter-user link is not in outage, DNCs can build messages from the minimum possible number of coded blocks and thus achieve higher diversity orders than $2M - 1$, as we analyze in Appendix IV-A. We also note that from the perspective of a single user, an alternative approach to exploit temporal diversity is to perform interleaving and coding over consecutive fading blocks. However, to achieve the diversity order $2M - 1$, interleaving among $2M - 1$ blocks would be required [11]. By the proposed network coding scheme, we are able to achieve diversity order $2M - 1$ by encoding among only M consecutive blocks. Thus, the delay of our systems is substantially reduced relative to using interleaving, especially for a large M.

For the same setup as in our case, previous schemes with binary network coding or without network coding cannot achieve diversity order $2M-1$. In the case of binary network codes, the dominating error event occurs when the systematic blocks of all M users are in outage. Then, no network codewords can be decoded and no additional time diversity is available, limiting the diversity order to M (the exponent of this error scenario). For protocols without network coding, based on decode-and-forward relaying, each information message is involved in only M different transmissions, again

$$T = \begin{pmatrix} 1 & 0 & \cdot\cdot & 0 & \alpha_{1,1} & \cdot\cdot & \alpha_{1,M-1} & \cdot\cdot & \alpha_{1,M(M-1)} \\ 0 & 1 & \cdot\cdot & 0 & \alpha_{2,1} & \cdot\cdot & \alpha_{2,M-1} & \cdot\cdot & \alpha_{2,M(M-1)} \\ & & \cdot\cdot & & & & \cdots & & \\ 0 & 0 & \cdot\cdot & 1 & \alpha_{M,1} & \cdot\cdot & \alpha_{M,M-1} & \cdot\cdot & \alpha_{M,M(M-1)} \end{pmatrix}. \tag{7}$$

limiting the diversity order to M. Hence, the proposed scheme can substantially improve the outage performance over block fading channels compared with previously proposed protocols. However, we note that our scheme is designed for maximum diversity and there is no constraint on the loss of spectral efficiency. Hence, according to general diversity–multiplexing trade-off considerations, the scheme is operating at the extreme of diversity only, and its spectral efficiency is poor. Still, this is the case also for the benchmark schemes we have commented on.

D. Simplified Code Construction

It is clear that the complexity of designing a DNC based on the discussion above is high for large M, since we need to consider all possible error patterns. Therefore, we propose a simplified construction, which can greatly reduce the complexity, and still achieve the diversity order $2M-1$. Again, we arrange the encoding matrix of all users as T in (7). Then, we define a simplified DNC as follows.

Definition 2. We define a *simplified DNC* as a network code corresponding to an encoding matrix T as in (7), such that any M columns of T are linearly independent (that is, having rank M).

In the case of simplified DNCs, we do not need to set variables to zero, or remove columns of T, which greatly simplifies the code construction. If we regard T as a generator matrix for coding the M user messages, then the simplified DNC is a type of maximum distance separable (MDS) code [16, p. 319]). The difference between our construction and traditional MDS channel codes is that in our case the M messages stem from different users, and messages are encoded at the intermediate nodes (also some messages may not be available at a partner node, due to outage of inter-user channels). The following result shows that the diversity order of the resulting simplified construction does not decrease.

Theorem 2. Simplified DNCs can achieve the diversity order $2M-1$.

Proof: The proof is given in Appendix IV-B. ■

To design a simplified DNC, we just find the product of all sub-matrices formed by M columns of T, and use e.g. the greedy algorithm in [5] to specify all nonzero $\alpha_{i,j}$s. For instance, in the case of $M=3$, we obtain the encoding matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 2 & 3 & 4 & 7 \\ 0 & 1 & 0 & 1 & 2 & 3 & 13 & 11 & 5 \\ 0 & 0 & 1 & 5 & 4 & 1 & 1 & 15 & 14 \end{pmatrix}. \tag{9}$$

Here we again use integer notation for the field elements in GF(2^4) with minimal polynomial $p(x)=x^4+x+1$ (identifying the elements as the integers corresponding to the reversed natural binary representations, e.g., $1+x^2 \leftrightarrow 1010 \leftrightarrow 5$). It is easy to verify that every sub-matrix with 3 columns of (9) has full-rank.

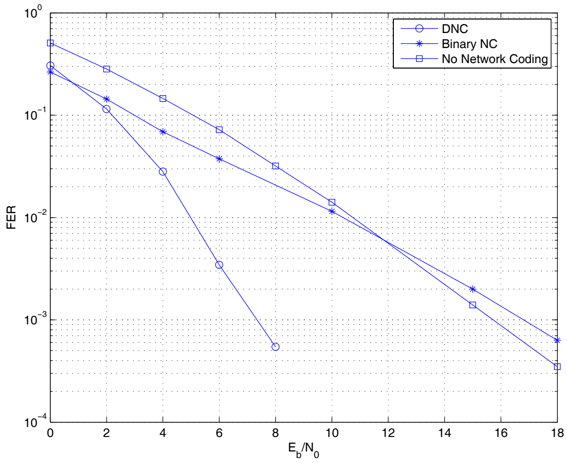

Fig. 4. FER simulations for a 3-user cooperative networks. The channel codes are regular LDPC codes with 200 information bits, 400 coded bits.

Above we assume that all channels have the same SNR. In a practical scenario where users are "close" and the BS is "far," it may be reasonable to assume that all the inter-user channels have better quality than the corresponding user–BS channels. Thus, inter-user channels can be practically regarded as error-free. Yet, our coding construction captures all inter-user outage scenarios, including non-outage as a special situation. Hence, we can still use DNCs or simplified DNCs, and all users can relay the messages of all partners using network coding. Then there are M^2 codewords received at the BS, and for any user outage occurs only when M^2-M+1 or more codewords are in outage. The diversity order is thus M^2-M+1 in this scenario.

In Fig. 4, we show FER simulations for a 3-user network with different cooperative protocols. For DNCs, we use the simplified codes with the transfer matrix in (9). For the simulations, LDPC cods with 200 input and 400 output bits are used. From the figure, we can clearly see the advantages of the proposed DNCs, which have a diversity order 5. For the scheme with binary network codes, all three users use identical codes, namely, $I_1 \oplus I_2 \oplus I_3$, for two relaying blocks. One can verify that the system with binary codes has a diversity order 2. Compared with the cooperative system without network coding, the system with binary network coding has worse performance in the high SNR region. Yet, at low SNRs, the system with binary network coding is better than that without coding, due to an achieved coding gain.

E. Alphabet Size

Here we investigate the alphabet size used for M-user DNCs, since the field size greatly impacts the complexity and delay of the resulting codes [4], [14], [15]. First, we state the result:

Proposition 2. In the considered scenario, $\binom{M^2-1}{M-1}$ is a sufficient alphabet size to achieve the diversity order $2M-1$ using simplified DNCs.

Proof: By Definition 2, simplified DNCs have rank M for any M columns in T, that is, any sub-matrix of M columns has full rank. Hence, a sufficient criterion to construct a valid encoding matrix T is that the determinant of the product of all possible $M \times M$ sub-matrices is non-zero. Clearly, T is an $M \times M^2$ matrix. Thus, in identifying sub-matrices, any variable is in at most $\binom{M^2-1}{M-1}$ different of these. Hence, in computing the overall determinant, any variable is multiplied with itself at most $\binom{M^2-1}{M-1}$ times. Then, according to, e.g., Lemma 2.17 in [12], the field size $\binom{M^2-1}{M-1}$ is sufficient. ■

With coding over a field of characteristic 2 (elements represented as binary polynomials), the minimum field size is hence obtained as 2^m where m is the lowest integer such that $2^m \geq \binom{M^2-1}{M-1}$. Note that Proposition 2 gives an upper bound for the required alphabet size, at which we can always find a coding scheme for the simplified DNCs. For a concrete coding scheme, the alphabet size may be smaller. For instance, as a specific construction for the non-systematic part of T, we can use a Cauchy matrix, and arrive at the following result.

Proposition 3. In the special case of using a Cauchy matrix for the non-systematic part of T, a sufficient alphabet size is $M + M(M-1)$ to achieve the diversity order $2M-1$, for simplified DNCs.

Proof: For Cauchy matrices, any square sub-matrix is non-singular over a finite field [16, p. 323]. Thus, Cauchy matrices can be used as the non-systematic part of T of the simplified DNCs. Since there are M rows and $M(M-1)$ columns for the non-systematic part of T, an alphabet size $M+M(M-1)$ is then sufficient to construct a Cauchy matrix. ■

It has been shown that random network codes [14] can achieve the min-cut with infinitely large alphabet sizes. In the scheme, one or more coding coefficients are randomly chosen. Thus, constructing the network code is greatly simplified. However, randomly generated coding coefficients are not guaranteed to be valid for finite alphabet sizes. Hence random network codes cannot guarantee the diversity order $2M-1$. For instance, in Fig. 1, two users may choose the same coding coefficients, and the resulting diversity order is 2, as that for binary network coding. However, at unbounded alphabet size, random codes are a suitable candidate for cooperative network coding.

IV. Conclusions

We have considered M-user cooperative transmission over block fading channels, to a common basestation. We propose a new method of using network coding for cooperative wireless networking over block fading channels. From the point of view of network coding, the network is dynamic, since random outages occur in the links between users and/or between users and the basestation. In this scenario, we consider coding over non-binary finite fields, and present a construction that allows the basestation to rebuild the source information from a minimum possible set of coded blocks. The proposed network codes then achieve the min-cut capacity. Hence, the proposed codes can efficiently exploit both the diversity available from cooperation among users and time-varying block fading.

In the case of two users we analyzed the resulting outage probabilities and presented simulations using specific physical layer channel codes. The numerical results demonstrate considerable improvements. Then, we generalize to M users, and investigate the existence of deterministic network codes in the general scenario. We show that the resulting diversity order of the proposed scheme is $2M-1$, which is higher than that obtained by previously reported protocols not using network coding or based on binary coding. We also propose a simplified code construction which has much lower design complexity and still can achieve the diversity order $2M-1$. Finally, we show that an alphabet size of $\binom{M^2-1}{M-1}$ is sufficient for the existence of simplified DNCs. One drawback of using network coding over non-binary fields may be higher complexity, since computations in large finite fields are more complex than over the binary field.

Acknowledgments

The authors wish to thank three anonymous reviewers for constructive comments that helped to improve the quality of the paper. Also, in particular, we would like to thank one of the reviewers for a suggestion that directly led to the formulation of Proposition 3.

Appendix

A. Proof of Theorem 1

Without loss of generality, we analyze the outage probability of user j. We first discuss the situation that $|\hat{D}_j| = 0$, which means no message from user j was decoded by partners. Since the inter-user channels are reciprocal, I_j cannot be decoded at any other user either. Hence, $M-1$ inter-user channels are in outage. The probability is $P(|\hat{D}_j| = 0) \approx P_e^{M-1}$. Then, user j repeats $M-1$ times the same channel codeword as the first time slot, and BS performs MRC and tries to decode for user j. Thus, the outage probability for user j is approximated as ([2], [11])

$$P_o(MR||\hat{D}_j| = 0) \approx \left(\frac{2^{MR}-1}{\text{SNR}}\right)^M \frac{1}{M!}. \tag{10}$$

If $|\hat{D}_j| > 0$, user k $(k \in \hat{D}_j)$ can successfully decode I_j. In time slot $i, (i = 2, 3, \cdots, M)$, the transmitted codeword of user k is produced from codewords including I_j as $C_{k,i} = \sum_{z=1}^{M} \alpha_{k,z,i} I_z$. Thus, there are $(M-1) \cdot |\hat{D}_j| + M$ codewords including I_j. In the worst case, all users in $\hat{D}_j$ only successfully decode I_j (or messages from users in $\hat{D}_j$). Letting $D_j = \hat{D}_j \cup \{\text{user i}\}$, there are in total $M|D_j|$ codewords received at the BS. Since any correctly received $|D_j|$ codewords can recover I_j from D_j, the outage probability is

$$P_{o,5} \approx P_e \binom{M|D_j|-1}{|D_j|} P_e^{M|D_j|-|D_j|}. \tag{11}$$

The first P_e in (13) corresponds to the outage probability of the direct transmission block from user j to the BS in the first time slot. If the messages of user k $(k \in \hat{D}_j)$ are also decoded by other users, the information messages of I_k have higher diversity. Then, the decoding error probability for I_k is lower. This will decrease the decoding error probability of I_j. Thus, the resulting outage probability of user j is lower than $P_{o,5}$, and we have

$$P_o(MR||\hat{D}_j|>0) \leq P_e \binom{M|D_j|-1}{|D_j|} P_e^{M|D_j|-|D_j|}. \quad (12)$$

Clearly, the probability of non-empty $\hat{D}_j$ is $P(|\hat{D}_j|>0) \approx P_e^{M-1-|\hat{D}_j|}$, since $M-1-|\hat{D}_j|$ users cannot decode I_j. Thus, the outage probability for user j is upper bounded by

$$\begin{aligned} P_{o,M} \quad &\leq \quad P(|\hat{D}_j|=0)P_o(MR||\hat{D}_j|=0) \\ &+ \quad P(|\hat{D}_j|>0)P_o(MR||\hat{D}_j|>0). \end{aligned} \quad (13)$$

The diversity order of the first term is $D_{M,1}=2M-1$, and that for the second term is $D_{M,2}=(M-2)|\hat{D}_j|+2M-1$. For $M>2$, $D_{M,2}$ is an increasing function of $|\hat{D}_j|$. If $|\hat{D}_j|=0$, $D_{M,2}$ reduces to $D_{M,1}$. Thus, $D_{M,2}>D_{M,1}$ for $|\hat{D}_j|>0$ (and $M>2$). Hence, the diversity order is $2M-1$. Q.E.D.

B. Proof of Theorem 2

Assume that an arbitrary user i can decode the messages of n_1 partners (denoted by S_1), and cannot decode those of the other $M-1-n_1$ partners. The resulting probability is $P_e^{M-1-n_1}$. Since each user transmits one systematic block and $M-1$ network codewords, we use $S_{i,c}$ to denote the set of these M blocks and the systematic blocks of S_1. There are $M+n_1$ blocks in $S_{i,c}$. Now we show that any n_1+1 blocks in $S_{i,c}$ can decode the n_1+1 messages (including I_i), in the case of simplified DNCs. We denote the coding coefficients of $S_{i,c}$ by

$$T_1 = \begin{pmatrix} 1 & 0 & \cdot\cdot & 0 & \alpha_{1,1} & \cdot\cdot & \alpha_{1,n_1+1} \\ 0 & 1 & \cdot\cdot & 0 & \alpha_{2,1} & \cdot\cdot & \alpha_{2,n_1+1} \\ & & \cdot\cdot & & & & \cdots \\ 0 & 0 & \cdot\cdot & 1 & \alpha_{n_1+1,1} & \cdot\cdot & \alpha_{n_1+1,n_1+1} \end{pmatrix}. \quad (14)$$

Thus, if any combination of n_1+1 columns in T_1 has a rank n_1+1, then any n_1+1 blocks in $S_{i,c}$ can decode the n_1+1 information messages. For this, we assume that the matrix A_1 formed by some n_1+1 columns of T_1 has a rank $R_1<n_1+1$. Then we construct a new matrix T_2 by

$$T_2 = \begin{pmatrix} 1 & 0 & \cdot\cdot & 0 & \underline{0} \\ & \cdot\cdot & & \cdots & \\ 0 & \cdot\cdot & \cdot\cdot & 1 & \underline{0} \\ \underline{0} & \cdot\cdot & \cdot\cdot & \underline{0} & A_1 \end{pmatrix}, \quad (15)$$

where $\underline{0}$ denotes all-zero vectors or matrices. We add $M-n_1-1$ 1s in the diagonal of T_2 ($M \times M$ matrix). Clearly, The rank of T_2 is $R_2=R_1+M-n_1-1<M$. We can rebuild M columns of coding coefficients of T by simple column transferring from T_1, since the upper-left $M-n_1-1$ columns and rows form a diagonal matrix. The resulting matrix is denoted by T_3. Then T_3 has a rank $R_2<M$. This is impossible, since any M columns of T have rank M. Thus, any n_1+1 columns of T_1 have a rank n_1+1, and any n_1+1 blocks in $S_{i,c}$ can decode the n_1+1 information messages. Thus, an outage occurs for these n_1+1 messages using $S_{i,c}$ only when M or more blocks cannot be decoded. The probability is $P_{o,6} \approx P_e^M$. Combining the probability of S_1 (occurring), the outage probability for I_i (and all information in S_1) transmitted by user i is thus $P_{o,7}=P_{o,6}P_e^{M-1-n_1}=P_e^{2M-1-n_1}$. Then, we assume n_2 partners can decode I_i and denote them as a set S_2. The other $M-1-n_2$ partners cannot decode. The probability is $P_{o,8} \approx P_e^{M-1-n_2}$. With the same analysis as user i, each of these partners (that can decode I_i) is outage in a probability of $P_{o,9}=P_e^{2M-1-n_3}$. Here n_3 is the number of messages that the partner can decode from its partner. Clearly, $P_e^M \leq P_{0,9} \leq P_e^{2M-1}$. For any two partners in S_2, there might be an overlap in the outage for systematic blocks. Yet, there are no more than $M-2$ overlapping outage blocks for any two partners. Thus, the probability ($P_{o,10}$) for all n_2 users in S_2 in outage is lower-bounded by $P_e^{(2M-1)n_2-(M-2)(n_2-1)}=P_e^{(M+1)n_2+M-2} \leq P_{o,10}$. Considering $P_{o,8}$, the probability for I_i transmitted by the partners in outage has probability $P_{o,11} \geq P_e^{2M+Mn_2-3}$. There might also be maximum $M-2$ overlapping outage blocks in S_1 and S_2. Combining $P_{o,7}$ and $P_{o,11}$, the overall outage probability for user i is $P_{o,12} \geq P_{o,7}P_{o,11}P_e^{-(M-2)}=P_e^{3M-2-n_1+Mn_2}$. For any $n_1(\leq M-1)$, n_2 and $M \geq 2$, $P_e^{2M-1} \leq P_{0,12}$. Thus, the simplified DNCs achieves diversity order $2M-1$. Q.E.D.

References

[1] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity—part I and part II," *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1927-1948, Nov. 2003.

[2] J. N. Laneman and G. W. Wornell, "Distributed space-time-coded protocols for exploiting cooperative diversity in wireless networks," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2415-2425, Oct. 2003.

[3] T. E. Hunter, S. Sanayei, and A. Nosratinia, "Outage analysis of coded cooperation," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 375-391, Feb. 2006.

[4] S. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, pp. 371-381, Feb. 2003.

[5] R. Koetter and M. Medard, "An algebraic approach to network coding," *IEEE/ACM Trans. Networking*, vol. 11, pp. 782-795, Oct. 2003.

[6] M. Xiao and T. Aulin, "Optimal decoding and performance analysis of a noisy channel network with network coding," *IEEE Trans. Commun.*, vol. 57, no. 5, pp. 1402-1412, May 2009.

[7] L. Xiao, T. Fuja, J. Kliewer, and D. Costello, "A network coding approach to cooperative diversity," *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3714-3722, Oct. 2007.

[8] S. Fu, K. Lu, Y. Qian, and M. Varanasi, "Cooperative network coding for wireless ad-hoc networks," in *Proc. IEEE Globecom*, pp. 812-816, Nov. 2007.

[9] X. Bao and J. Li, "Adaptive network coded cooperation (ANCC) for wireless relay networks: matching code-on-graph with network-on-graph," *IEEE Trans. Wireless Commun.*, vol. 7, no. 2, pp. 574-583, Feb. 2008.

[10] Z. Han, X. Zhang, and V. H. Poor, "High performance cooperative transmission protocols based on multiuser detection and network coding," *IEEE Trans. Wireless Commun.*, vol. 8, no. 5, pp. 2352-2361, May 2009.

[11] D. Tse and P. Viswanath *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[12] R. W. Yeung, S. Li, N. Cai, and Z. Zhang, *Network Coding Theory*. Hanover, MA: NOW publishers, Inc., 2006.

[13] S. Lin and D. Costello, *Error Control Coding*. Pearson Prentice Hall, 2004.

[14] T. Ho, M. Medard, R. Koetter, D. Karger, M. Effros, *et al.*, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, pp. 4413-4430, Oct. 2006.

[15] C. Fragouli and E. Soljanin, "Information flow decomposition for network coding," *IEEE Trans. Inf. Theory*, vol. 52, pp. 829-848, Mar. 2006.

[16] F. J. Macwilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*. New York: North-Holland, 1978.