Network Coding Design for Multi-Source Multi-Relay Cooperative Wireless Networks

Pratik Patil, M Wasif Khan
Department of Electrical and Electronics Engineering
Indian Institute of Technology Guwahati
Guwahati, India 781039
Email: {n.patil, m.khan}@iitg.ernet.in

Prof. R. Bhattacharjee, Prof. S. Bose
Department of Electrical and Electronics Engineering
Indian Institute of Technology Guwahati
Guwahati, India 781039
Email: {ratnajit, skbose}@iitg.ernet.in

***Abstract*—In this paper, we study the design of network codes for multi-source, multi-relay networks over frequency non-selective slow fading channels. Specifically, we consider a system with M sources each having independent information to be transmitted to a common destination with the help of N relays (called an $M-N-1$ system). A finite field (non-binary) based method is suggested to design binary network codes. For construction of the codes, we investigate full system diversity achieving criteria and constraints imposed by it in terms of linear independence of columns (or sets of columns) of generator matrix for codes over finite fields (including binary). First, we design such full diversity achieving codes over polynomial fields of the form GF(2^K) and then using a novel uplifting technique (matrix representation of finite fields), convert these back into frame based binary codes to reduce encoding complexity at relays (as only binary operations are used). Simulation results confirm the diversity claims of the proposed codes under perfect as well as realistic source-to-relay (S-R) channel links. We also apply belief propagation (BP) decoding on these codes. The codes are compared with that from existing algorithm and similar performance is observed with smaller frame size for the case considered.**

***Index Terms*—Network coding, multi-source multi-relay cooperative wireless networks, diversity order, binary network codes, finite field, belief propagation.**

I. Introduction

With more than five billion people using mobile phones [1] and with variety of several multimedia services, location based applications and high speed Internet access, data traffic in wireless networks is rising exponentially. Today's LTE networks deliver data download rates about ten times those of 3G [2]. In order to provide such high data rates, novel wireless technologies for reliable and efficient transmission are necessary. One of the biggest challenges with wireless networks is the unreliability and fading multi path effect (especially in urban environments). Spatial diversity has widely been accepted as one of the most effective technique to combat fading over wireless channels. Numerous practical schemes like spatial multiplexing and space-time coding are designed using multiple antennas on transmitter and/or receiver side (MIMO). But inherent limitation with MIMO is that achieving full diversity gain requires multiple antennas to be placed sufficiently apart. Thus MIMO techniques become inappropriate at user devices due to size, power and cost.

Cooperative communication is another innovative technique which takes advantage of broadcast nature of wireless channels and can achieve spatial diversity gain without deploying multiple antennas at the nodes. Relays can be used to realize cooperative multi-hop transmission. The basic idea of relaying has been introduced in [3]. The users also can themselves act as relay for the other user and thus avoiding the need for separate relays. The idea of user cooperation has been introduced by [4], [5] for up link transmission. It improves the capacity and lowers the outage probability for a given data rate. Later, [6] extended the concept of cooperation, by designing energy efficient multiple access protocols based on decode-and-forward (DF) and amplify-and-forward (AF) relaying modes.

One of the drawbacks of cooperation in wireless networks is the additional resources overhead. Network coding which was originally proposed for purely wired networks by Ahlswede and others. Because of its usefulness and potential to increase the capacity of cooperative systems [7] has recently gained interest for application in wireless networks. In this new method, the intermediate nodes can decode the data and then are allowed to process the data before transmitting to the base station or other node. Traditional role of relays (decode and forward) can thus be viewed as a special case of network coding, where processing is the just to reproduce the received signal. Authors in [8] have investigated the diversity gain using XOR based network coding for multiple access relay channel (MARC) and showed that network coding improves the bandwidth of MARC from 1/2 to 2/3, without affecting its diversity gain.

For multi-user, single relay, single destination ($M-1-1$ system), authors of [9] have proposed binary field network coding (BFNC) schemes where messages of all the users are XORed at the relay, while that of [10] have proposed Galois field network coding (GFNC) where messages are superimposed in Galois field. Complex field network coding (CFNC) has also been studied in the context of relaying networks [11]. However, the main drawback of the GFNC schemes is high decoding complexity and large field size (with increase in the number of the sources and relays) leading to high encoding complexity. CFNC schemes are also impacted negatively through low coding gain. This provides us the motivation to design good network codes for the $M-N-1$ system which can easily be encoded and have low decoding complexity. Authors of [13] have proposed vector-wise binary network coding schemes for achieving full diversity with modified BP decoder for large block lengths.

In this paper we study the design of such full diversity achieving network codes for the $M-N-1$ system with slow fading channels. We approach the design by first considering full diversity conditions and constraints on the generator matrix in both finite field (non-binary) and binary domain. We then form network codes in finite field domain (polynomial fields of the form GF(2^K)). Issues of minimum field size (frame size) are discussed. Secondly using a novel uplifting technique, we convert these codes back into binary codes to ease encoding. The codes formed this way are simulated and are shown to achieve full system diversity as claimed. Also belief propagation (BP decoding) is observed to be applicable to these codes and thus reduced decoding complexity can be achieved for large block lengths. Simulation results are compared with the codes formed from existing method and codes designed by our method provide similar performance (with possibility of reduced frame length).

II. System Model

Consider relay communication with M sources, N half-duplexing relays and Q destinations ($M-N-Q$ system). For unidirectional communication, transmission to a single destination is independent of the transmission to others. So without loss of generality, we can assume a generic multi-source multi-relay network with M sources, N relays and a single destination ($M-N-1$) system as an independent subsystem as shown in figure 1. Transmitting nodes access channel using Time Division Multiple Access (TDMA) scheme, where each transmission takes place in a different time-slot, and multiple-access interference can be neglected. We assume direct links between sources and destination exist, and that relays assist deliver the information frame to final destination with better reliability. The protocol is composed of two main phases: a) Broadcasting phase and b) Relaying phase. During first phase, ith source S_i transmits the information frame intended to the destination in time-slot T_i (i=1 to M). These M frames are overheard by N relays which store them in their buffers for further processing. This phase takes M time slots. During second phase, jth relay R_j forwards a linear combination of received frames to the destination in time-slot T_{M+j} (j=1 to N).

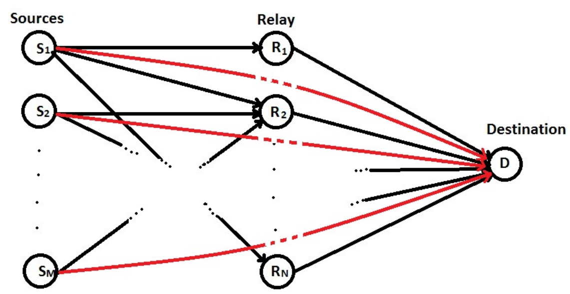

Fig. 1. $M-N-1$ System Model

There are two ways in which relays can process the received source signals: a) Decode and Forward (DecF) and b) Demodulate and Forward (DemF). In DecF, relays decode the source frames, check for errors and ask for retransmission in case of error. So relays only transmit a combination of error free source frames. While in DemF, relays just demodulate, combine and transmit without any error check. It is proved in [12] (section V) that as far as diversity gain is concerned, network codes can be designed by using the same optimization criteria as for networks with perfect source-relay (S-R) links. Thus, in our analysis, we have considered only the second case with perfect S-R links. According to the working operation of the protocol, we notice that broadcasting and relaying phases have a total duration of $M+N$ time-slots. Since M information frames are transmitted by sources in $(M+N)$ time slots, the protocol offers a fixed rate of $R = M/(M+N)$.

For analytical tractability and simplicity, we retain following reasonable assumptions: a) Uncoded transmissions without any channel coding b) Only BPSK modulation c) Symbol-by-Symbol transmission. Also, the channel is assumed to be frequency non-selective slow faded channel with block length, $l_{block} = (M+N)K$ where K is the frame length.

A. Broadcasting and Relaying Phase

1) Broadcasting: First the generic sources S_i ($1 \leq i \leq M$) broadcast, in time slot T_i, a BPSK modulated signal, x_{S_i}, with average energy E_S, i.e., $x_{S_i} = \sqrt{E_S}(-1)^{b_{S_i}}$, where $b_{S_i} \in (0,1)$ is the corresponding bit transmitted by source S_i. Then, signals received at relays R_j ($1 \leq j \leq N$) and destination D are

$$y_{S_i,R_j} = h_{S_i,R_j} x_{S_i} + n_{S_i,R_j} \quad (1)$$

$$y_{S_i,D} = h_{S_i,D} x_{S_i} + n_{S_i,D} \quad (2)$$

where, $h_{X,Y}$ is the fading coefficient from node X to node Y with $|h_{X,Y}|$ a Raleigh random variable with zero mean and variance $\sigma^2_{X,Y}/2$. $\sigma_{X,Y}$ is given by $\sigma^2_{X,Y} = d^{-\alpha}_{X,Y}$, where, d is relative distance d/d_0 (d_0-threshold distance) and α is path loss exponent of each wireless link. $n_{X,Y}$ is additive white Gaussian noise. The AWGN in different time slots is i.i.d with zero mean and variance $N_0/2$ per dimension.

2) Relaying: Upon reception of y_{S_i,R_j} and $y_{S_i,D}$ in time slot T_i, relay R_j ($\forall j$) and destination D, demodulate these according to the following equations:

$$\hat{b}_{S_i,R_j} = (1 - sign(y_{S_i,R_j}))/2 \quad (3)$$

$$\hat{b}_{S_i,D} = (1 - sign(y_{S_i,D}))/2 \quad (4)$$

Each relay now combines these bits according to some function (Network Coding) as

$$b_{R_j} = f_{R_j}(\hat{b}_{S_1,R_j}, \hat{b}_{S_2,R_j}, \cdots, \hat{b}_{S_M,R_j}) \quad (5)$$

Relay R_j broadcasts in time slot T_{M+j}, a BPSK modulated signal, x_{R_j} with average energy E_R, i.e., $x_{R_j} = \sqrt{E_R}(-1)^{b_{R_j}}$. Then, the signals received at destination D for j=1 to N are

$$y_{R_j,D} = h_{R_j,D} x_{R_j} + n_{R_j,D} \quad (6)$$

Total energy $E_T = ME_S + NE_R$. Since sources and relays don't know CSI, the fair allocation of energy to all sources and relays is assumed. Therefore, $E_S = E_R = E$ and $E_T = (M+N)E$.

III. Preliminaries

Mathematically, diversity order is defined as

$$d = \lim_{SNR \to +\infty} -\frac{\log(p_{sys})}{\log(SNR)} \tag{7}$$

where p_{sys} is system error probability and SNR is ratio of average signal power to noise power. To understand what it means for the system to have diversity order of d, we assume an erasure model. In the network coded system, assume channel fading to be of only two extreme types- a) very low resulting error free links (with probability of making an error in correctly decoding the symbol, $p_e \approx 0$), and b) deep fading (effectively culminating in $p_e \approx 1$ or erasure). This gives $p_e = P(Erasure) = p_E$ (say). Now if the system is able to correctly decode with u or less erasures, then for nonzero p_{sys}, there must be $u+1$ or more erasures. p_{sys} in this case thus can be written as (assuming the erasure probability to be same for all S-D and R-D links with perfect S-R links),

$$p_{sys} = \binom{n}{u+1} p_E^{u+1} + \binom{n}{u+2} p_E^{u+2} + \ldots + \binom{n}{n} p_E^{n} \tag{8}$$

$$p_{sys} = O(p_E^{u+1}) \tag{9}$$

From definition of diversity,

$$\begin{aligned} d &= \lim_{SNR \to +\infty} -\frac{\log(p_{sys})}{\log(SNR)} \\ &\approx u+1 \end{aligned} \tag{10}$$

In short, for the system to have diversity order d, it should be able to decode correctly with $d-1$ erasures at worst. Note that user diversity and system diversity are two different terms. The distinction between them is made clear in the following subsection.

A. User diversity and System diversity

1) *User diversity(d_u):* User diversity order for a user/source S_i being n implies the probability of error in discerning information from S_i i.e. p_{s_i} is of order O(p_E^n) or as explained in the last subsection, user S_i can be decoded correctly with arbitrary $n-1$ or less erasures. In short there are n independent paths available from S_i to destination D.
2) *System diversity(d_S):* System diversity can be defined as order in which probability of error in correctly finding all the bits transmitted for the system decreases with increase in SNR. Mathematically, it is equivalent to diversity order of the worst performing user.

$$d_S = \min_{i \le M}(d_{S_i}) \tag{11}$$

B. Maximum system diversity with/without NC

As for each source there are $N+1$ independent paths (1-$(S-D)$ and N-$(S-R-D)$), network coding can make use of all the paths available efficiently, and thus source message can still be decoded with N erasures. Hence,

$$d_{S_{max}} = N+1 \tag{12}$$

IV. Conditions for full system diversity

We investigate full diversity conditions for bitwise network coding (all NC operations are done on bit level), finite field network coding (field wise NC operations on symbols treated as elements of non-binary field of form $\mathbb{F}_{2^K}$) and frame based network coding (NC operations on frames of bits) in the following sections.

A. Bitwise network coding

The jth relay will forward b_{R_j} which can be expressed as a linear combination of source bits b_{S_i} as follows:

$$\begin{aligned} b_{R_j} &= b_{S_1} g_{1_j} \oplus b_{S_2} g_{2_j} \oplus \ldots b_{S_M} g_{M_j} \\ &= (\textstyle\sum b_{S_i} g_{i_j}) \quad mod \quad 2 \end{aligned}$$

where g_{i_j} is either 0 or 1 or in matrix form, we have

$$\begin{aligned} &\begin{bmatrix} b_{S_1} \cdots b_{S_M} & b_{R_1} \cdots b_{R_N} \end{bmatrix} \\ &= \begin{bmatrix} b_{S_1} \cdots b_{S_M} \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & g_{11} & \cdots & g_{1N} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_{M1} & \cdots & g_{MN} \end{bmatrix} \end{aligned} \tag{13}$$

(call the above matrix on right G) In order to achieve full system diversity $(N+1)$, destination must be able to decode all source bits from any arbitrary N erasures. This leaves destination with $(N+M)-N = M$ frames. Let $\overline{B}$ be received vector such that, $\begin{bmatrix} \tilde{b}_1 \cdots \tilde{b}_M \end{bmatrix} = \begin{bmatrix} b_{S_1} \cdots b_{S_N} \end{bmatrix} G_1$ where G_1 contains the corresponding columns from G. Thus, for full diversity G_1 must be invertible. As erasures are arbitrary, the condition on G is that matrix formed from any M columns of G must be full rank.

1) $M-1-1$ system: For full diversity, we must be able to work with single erasure. Let, there be an erasure in S_i then ith row of G will be $\begin{bmatrix} 0 & \cdots & 0 & g_{i1} \end{bmatrix}$. According to the full diversity condition, this row should be non-zero $\implies g_i \neq 0$ or $g_i = 1$. But as erasure is arbitrary $\implies g_i = 1 \quad (\forall i) \implies R = S_1 \oplus S_2 \ldots \oplus S_N$
2) $M-2-1$ system: We must be able to work with double erasures. Let erasures be of S_i & R_j. Similar to the argument in $M-1-1$ case $g_{ij'} = 1$ for $j' \neq j$ but as i & j are arbitrary, $g_{ij} = 1 \; \forall i$ & $\forall j$ Let the two erasures be S_1 & $S_2 \implies G_1^T = \begin{bmatrix} 0 & 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & \ldots & 1 \\ 1 & 1 & 1 & 1 & \ldots & 1 \\ 1 & 1 & 1 & 1 & \ldots & 1 \end{bmatrix}$ which is non-invertible $\implies M-2-1$ system can't achieve full diversity. In fact similar argument can be used to prove that $M-N-1$ where $N \geq 1$ can't achieve full diversity for bitwise network coding.

B. Finite field network coding with non-binary symbols

Arguments above hinge on the fact that there is only one option for non-zero coefficient which is 1. Whole argument breaks down when we have other non-zero coefficients, say $\alpha \neq 1$. As underlying modulation is BPSK, we work with binary symbols. So we merge K bits and map it to a GF(2^K) symbol (symbol $\alpha \in \{0, \omega^1, \omega^2, \ldots, \omega^{q-1}\}$ where, $q = 2^K$ and ω is a primitive element of GF(2^K)). We then have $2^K - 1$ non-zero symbols. Now for full system diversity, as in last section, necessary and sufficient condition is to construct generator matrix G such that all the matrices formed from arbitrary M columns of G are full rank over $\mathbb{F}_{2^K}$ (equivalently, all sets of M columns from G must be independent over $\mathbb{F}_2^K$).

1) $2-N-1$ system: Full diversity requires every two columns of NC matrix to be independent of each other. For $M = 2$, $G = \begin{bmatrix} 1 & 0 & 1 & 1\cdots 1 \\ 0 & 1 & \alpha_1 & \alpha_2 \cdots \alpha_N \end{bmatrix}$. It is possible to construct required G (such that $\alpha_i \neq \alpha_j$ for $i \neq j$) as long as $N \leq q$ (this guarantees any 2×2 matrix formed out of 2 columns to be a non-singular matrix). Hence, for full diversity $N \leq N_{max} = q-1 = 2^K - 1$ for $M = 2 \implies K \geq \log(N+1)$

2) $M-2-1$ system: We have the following theorem.

   Theorem. *For $N = 2$, full diversity can't be achieved if $M \geq q$.*

   Proof: With single relay, full diversity matrix looks like $G^T = \begin{bmatrix} & & I_M & & \\ 1 & 1 & 1 & \ldots & 1 \end{bmatrix}$. Let's add one more relay (column) to the code. Now with 2 erasures, (columns j_1 and j_2)

$$G^T = \begin{bmatrix} 1 & 0 & \ldots & 0 & \ldots & 0 & \ldots & 1 \\ 0 & 1 & \ldots & 0 & \ldots & 0 & \ldots & 1 \\ \vdots & \vdots & \ddots & 0 & \vdots & 0 & \vdots & 1 \\ 1 & 1 & \ldots & 1 & \ldots & 1 & \ldots & 1 \\ g_1 & g_2 & \ldots & g_{j_1} & \ldots & g_{j_2} & \ldots & g_{j_M} \end{bmatrix}$$

   For independence $\begin{bmatrix} 1 & 1 \\ g_{j_1} & g_{j_2} \end{bmatrix}$ should be invertible $\implies g_{j_1} \neq g_{j_2} \;\forall\; j_1, \; j_2 \implies$ all coefficients in last row should be different which is not possible if $M > q - 1 = \#$ non-zero coefficients. ■

C. Frame based binary network coding

Here we work with frames of K bits. With source frames as input and received frames as output, NC can be seen as a function from $M \times K \to (M+N) \times K$. Considering only linear relations such function can be expressed by a generator matrix $G = \begin{bmatrix} I_{Ml\times Ml} & A_{Ml\times Nl} \end{bmatrix}_{Nl\times(M+N)l}$ (as first M received frames are source frames, first Ml set of the function forms an identity matrix). Let the received frame vector at destination $B_{received} = \begin{bmatrix} \hat{b_1} & \hat{b_2} & \cdots & \hat{b_{(M+N)}} \end{bmatrix} = \begin{bmatrix} \hat{b_{S_1}} & \hat{b_{S_2}} & \cdots & \hat{b_{S_M}} & \hat{b_{R_1}} & \hat{b_{R_2}} & \cdots & \hat{b_{R_N}} \end{bmatrix}$ where $b_x = \begin{bmatrix} b_x(1) & b_x(2) & \cdots & b_x(K) \end{bmatrix}$ is a frame of K bits for any index x. As stated earlier, diversity d means decoder is able to decode in case of $d-1$ erasures (i.e. with the help of $M+N-d+1 = T$ frames). Let $\begin{bmatrix} \hat{b_{i_1}} & \hat{b_{i_2}} & \cdots & \hat{b_{(i_T)}} \end{bmatrix}$ be the frame received for any arbitrary index i_k ($k \leq T$).

$$\begin{aligned} \begin{bmatrix} \hat{b_{i_1}} & \hat{b_{i_2}} & \cdots & \hat{b_{i_T}} \end{bmatrix} &= \begin{bmatrix} \hat{b_{S_1}} & \hat{b_{S_2}} & \cdots & \hat{b_{S_M}} \end{bmatrix} \times G'_{MK\times TK} \\ &= \begin{bmatrix} \hat{b_{S_1}} & \hat{b_{S_2}} & \cdots & \hat{b_{S_M}} \end{bmatrix} \\ &\quad \times \begin{bmatrix} C_{i_1} & C_{i_2} & \cdots & C_{i_T} \end{bmatrix} \end{aligned}$$

where C_{i_T} is the i_Tth column of G. According to the erasure model, this should form a set of consistent solvable equations. For this, we must have at least MK independent columns among TK columns of G'.

$$\begin{aligned} \tilde{B} &= B_S \times \begin{bmatrix} C_{j_1} & C_{j_2} & \cdots & C_{j_{MK}} \end{bmatrix} \\ &= B_S G'' \implies B_S = \tilde{B} G''^{-1} \end{aligned}$$

Thus, for full diversity, $T = M+N-(N+1)+1 = M$ and G' is a $MK \times MK$ matrix and such G' should be invertible (MK independent columns).

V. Construction of Full-diversity Network Codes

A. Construction of finite-field based non-binary codes

As explained in section IV-B, for full diversity we need to construct generator matrix G such that all the matrices formed from arbitrary M columns of G are invertible over $\mathbb{F}_2^K$ (or equivalently, all sets of M columns from G must be independent over $\mathbb{F}_2^K$). Currently, there is no algorithm to find such set 'systematically' but for sufficiently large K, construction of such G is fairly easy. Finding lower bound on frame size, K which guarantees such G is an interesting open problem.

One noteworthy point is that finding such G is equivalent to finding a parity check matrix H of $(M+N, N, N+1)$ code over $\mathbb{F}_2^K$. If such code exists, then NC matrix G can be easily found by converting H to systematic form.

$$H \xrightarrow[Elimination]{Gauss-Jordan} \begin{bmatrix} I & B \end{bmatrix} = G \tag{14}$$

B. Translation of finite field based non-binary network codes to binary network codes

We apply a novel uplifting technique to convert back finite field codes into binary codes using concepts of matrix representation of finite fields [14]. Binary codes reduce encoding complexity as only binary operations are used at relays. Also iterative decoding can be effectively applied to such codes to reduce decoding complexity at the destination. Overall system mapping can be shown as follows:

$$\underset{MK}{b} \to \underset{M}{\alpha} \xrightarrow[Operation]{GFNC} \underset{M+N}{\alpha'} \to \underset{(M+N)K}{b'}$$

where b, b' are binary vectors and α, α' are vectors with elements from finite field. Thus we first reduce frame of MK bits into M size finite field vector, apply NC to make it $M+N$ size vector and then convert it back to binary vector of size $(M+N)K$ bits as per following theorem.

Theorem. *Let $\mathbb{F}_{2^K}[x] = \mathbb{F}_2^K[x] = a_0 + a_1 x + \cdots + a_{K-1}x^{K-1}/m(x)$ where $a_i \in \mathbb{F}_2$ and $m(x)$ is K-order primitive polynomial in $\mathbb{F}_2$ with primitive element w. The linear relation $R(w) = S_1(w) + w^K S_2(w)$ in $\mathbb{F}$ is equivalent to $\overline{R} = \overline{S_1} + \overline{S_2}\,\overline{A}^k$ where $\overline{R}, \overline{S_1}$ and $\overline{S_2}$ are binary vectors and $\overline{A}$ is a binary matrix. (All operations are carried modulo 2)*

Proof: If ω is a root of polynomial $m(x)$, then ω can serve as primitive element of $\mathbb{F}$ and $\mathbb{F}_{2^K} = \{0, \omega, \omega^2, \cdots, \omega^{2^K-1} (= 1)\}$ The mapping we consider is $\omega^j = \alpha = \sum_{i=0}^{K-1} a_i \omega^i = p(\omega)$ Let $m(x) = (\sum_{i=0}^{K-1} b_i x^i) + x^K$ with $b_i \in \{0,1\}$, and

$$p(\omega) = \sum_{i=0}^{K-1} a_i \omega^i$$

$$m(w) = 0 \implies \omega^K = \sum_{i=0}^{K-1} b_i \omega^i$$

$$\omega p(\omega) = \sum_{i=0}^{K-1} a_i{}^{(1)} \omega^i \tag{15}$$

$$= \sum_{i=0}^{K-1} a_i \omega^{i+1} = (\sum_{i=0}^{K-2} a_i \omega^{i+1}) + a_{K-1} (\sum_{i=0}^{K-1} b_i \omega^i)$$

$$= a_{K-1} b_0 + (a_0 + a_{K-1} b_1)\omega + \cdots + (a_{K-2} + a_{K-1} b_{K-1})\omega^{K-1} \tag{16}$$

Comparing (15) and (16),

$$\begin{bmatrix} a_0^{(1)} & a_1^{(1)} & \cdots & a_{K-1}^{(1)} \end{bmatrix}$$
$$= \begin{bmatrix} a_{K-1} b_0 & a_0 + a_{K-1} b_1 & \cdots & a_{K-2} + a_{K-1} b_{K-1} \end{bmatrix}$$
$$= \begin{bmatrix} a_0 & a_1 & \cdots & a_{K-1} \end{bmatrix} \times \begin{bmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ b_0 & b_1 & \cdots & b_{K-1} \end{bmatrix}$$

We can easily show that $\overline{a}^{(K)} = \overline{a}\overline{A}^K$. Also as polynomials add in fields, $r(\omega) = p(\omega) + q(\omega) \implies \overline{r} = \overline{a} + \overline{e}$. Hence, $R(\omega) = S_1(\omega) + \omega^K S_2(\omega) \implies \overline{R} = \overline{S_1} + \overline{S_2 A}^K$ or simply, $R(\omega) = \sum_{i=1}^{M} S_i(\omega)\omega^{k_i} \implies \overline{R} = \sum_{i=1}^{M} \overline{S_1} A^{k_i} =$

$$\begin{bmatrix} \overline{S_1} & \overline{S_2} & \cdots & \overline{S_M} \end{bmatrix} \begin{bmatrix} A^{k_1} \\ A^{k_2} \\ \vdots \\ A^{k_M} \end{bmatrix} \qquad \blacksquare$$

VI. Example of code construction for $2-3-1$ system

As shown already, there does not exist any bitwise binary network code for $N > 1$ that achieves full diversity. Now with the frame based approach as given above, we show by example how to construct full-diversity achieving binary network code for $2-3-1$ system. We start with minimum frame size i.e. K=2. $\mathbb{F}_4$=$(a_0 + a_1 x)$ mod $(1 + x + x^2)$ where $a_0, a_1 \in \mathbb{F}_2$. For $1 + \omega + \omega^2 = 0$, it can be shown that $\mathbb{F}_4 = \{0, \omega, \omega^2, \omega^3 = 1\}$. A network coding matrix satisfying full diversity in $\mathbb{F}_4$ is G_W=$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & \omega & \omega^2 \end{bmatrix}$. Translating G_W into a binary matrix G_B using theorem given above, we get A=$\begin{bmatrix} 0 & 1 \\ b_0 & b_1 \end{bmatrix}$=$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ $\implies$ G_B=

$$\begin{bmatrix} I & 0 & I & I & I \\ 0 & I & I & A & A^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Performance of this code is reported in the section below. $G_W = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & w & w^2 \end{bmatrix}$

VII. Simulation Results

We simulate our codes for $2-2-1$ and $2-3-1$ systems and compare them with direct transmissions and existing frame-based network codes formed from algorithm given in [13]. Maximal likelihood (ML) decoding is used at the destination unless mentioned otherwise. Fig 2 shows performance of proposed network code (NC) with generator matrix as constructed from section VI compared with direct transmission for $2-3-1$ case. As diversity order of direct transmission is 1, diversity order for NC is calculated by computing ratio of slope of $log(p_E)$ vs. $log(E_T/N_0)$) for NC to that of direct plot. It comes out to be approximately 4.0898 which is close to theoretical value 4. This confirms our full diversity claim. We compare performance of code

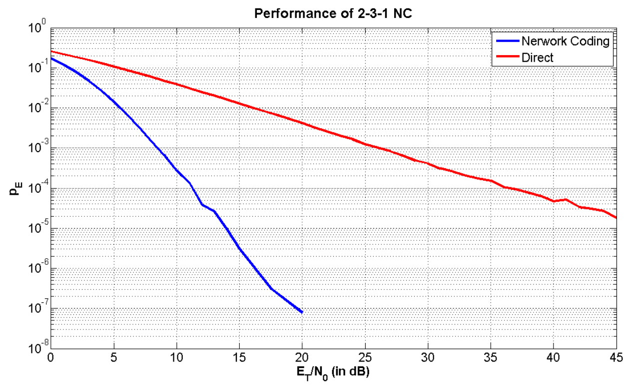

Fig. 2. BER plot for $2-3-1$ system

generated by proposed method for $2-2-1$ system with that generated by existing method in [13] (Fig 3). We observe that performance of the two codes is similar with lesser frame size for our code ($K = 2$ for our proposed code while existing code uses $K = 3$). We also apply iterative

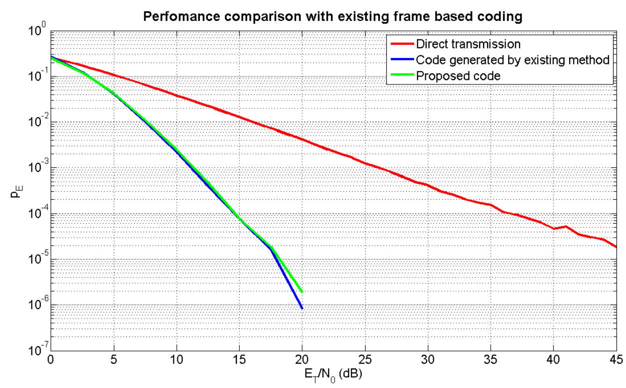

Fig. 3. Comparison with existing frame based coding for $2-3-1$ system

decoding (belief propagation) to binary code for $2-3-1$ system. Such decoding is effective in reducing decoding complexity for large frame sizes when M and N are large (given the generator matrix is sparse enough). Fig 4 shows performance of belief propagation along with that of ML decoding. BP works almost similar to ML decoding though for such short frame sizes ML runs faster.

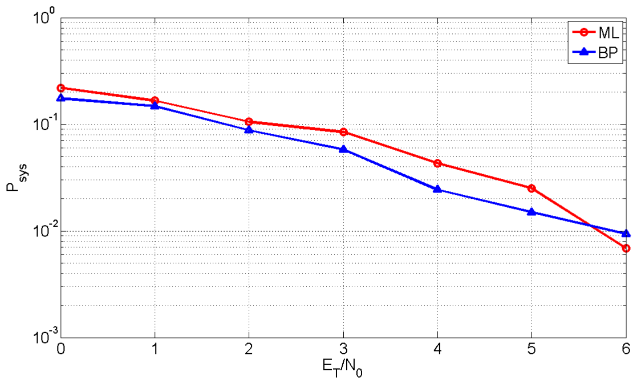

Fig. 4. Comparison of belief propagation decoding with maximal likelihood decoding for $2-3-1$ system

VIII. Conclusion

In this paper, we have considered network coding design for multi-source multi-relay wireless networks under slow fading channels. We investigated full diversity achieving constraints (imposed on the generator matrix) for both binary and finite field (non-binary) network codes. To design such codes, we suggested a finite field based method to first construct finite field codes and then to covert them back to binary codes using a novel uplifting technique to ease encoding and decoding. Our simulation results confirm the diversity claims and proposed codes perform similar to the existing codes (with lesser frame size). We also applied belief propagation (BP) decoding and results show performance similar maximal likelihood decoding (ML). There are several interesting future directions such as finding bounds on frame size K, finding an explicit algorithm to construct required finite field codes and error analysis of these codes.

References

[1] http://reviews.cnet.com/8301-13970_7-10454065-78.html

[2] http://spectrum.ieee.org/telecom/wireless/fantastic-4g

[3] E. C. V. der Meulen, "Three Terminal Communication Channels," *Advanced Applied Probability*, vol. 3, pp. 120–154, 1971

[4] A. Sendonaris, E. Erkip, and B. Aazhang, "Increasing Uplink Capacity via User Cooperation Diversity," in *Proceedings of IEEE International Symposium on Information Theory (ISIT 1998)*, Cambridge, MA , USA, August 1998, p. 156.

[5] A. Sendonaris, E. Erkip, and B. Aazhang, "User Cooperation Diversity Part I and Part II," *IEEE Transactions on Communications*, vol. 51, no. 11, pp. 1927–48, Nov 2003.

[6] J. N. Laneman and G. W. Wornell, "Energy Efficient Antenna Sharing and Relaying for Wireless Networks," in *Proceedings of IEEE Wireless Communications and Networking Conference*, WCNC. 2000, pp. 7–12.

[7] R. Ahlswede, N. Cai, S. Li, and R. W. Yeung, "Network Information Flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, July 2000.

[8] Y. Chen, S. Kishore, and J. Li, "Wireless Diversity through Network Coding," in *Proceedings of IEEE Wireless Communications and Networking Conference*, 2006., pp. 1681–1686.

[9] M. Xiao and T. Aulin, "Optimal decoding and performance analysis of a noisy channel network with network coding," *IEEE Trans. on Commun.*, vol. 57, pp. 1402-1412, May 2009.

[10] M. Xiao and M. Skoglund, "Design of network codes for multiple-user multiple-relay wireless networks," *IEEE International Symposium on Information Theory (ISIT)*, pp. 2562-2566, Jun. 2009.

[11] T. Wang and G. B. Giannakis, "Complex Field Network Coding for Multiuser Cooperative Communications," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 3, pp. 561-571, Apr. 2008.

[12] Marco Di Renzo, Michela Iezzi, and Fabio Graziosi, "Diversity and Coding Gain of Multi-Source Multi-Relay Cooperative Wireless Networks with Binary Network Coding," in *arXiv*

[13] Jun Li, Jinhong Yuan, Robert Malaney and Ming Xiao, "Binary Field Network Coding Design for Multi-Source Multi-Relay Networks" in *Proceedings of IEEE International Conference of Communication (ICC), 2011*

[14] W.P. Wardlaw, "Matrix representation of finite fields," *Math. Mag.*, 67 (1994), pp. 289293.