The benefits of Conditional Random Linear Network Coding over GF(q^m)

Aicha Guefrachi, Sonia Zaibi, Ammar Bouallègue
Ecole Nationale d'Ingénieurs de Tunis (ENIT), Sys'Com Laboratory
Tunis,Tunisia

***Abstract*— Network coding is a novel coding technique for which each received packet is a linear combination of multiple previously received packets. The main problem introduced by this approach is error propagation where a corrupt packet may infect other packets when combined with them. In this paper, we propose a new implementation of a subspace code for non-coherent networks said kk-code (Kötter-Kschichang code) to solve this problem when Random Linear Network Coding (RLNC) and conditional RLNC are applied over F_q. In the first case, the coefficients of combination at each intermediate node are chosen randomly in GF(q^m). In the second case, if all random coefficients are nulls, they have to be regenerated until at least one of them is not null. Performance in the case of transmission over a q-ary Gilbert-Elliot channel is evaluated. Simulation results show that RLNC verify the theoretical results of Medard and Kötter but the proposed conditional RLNC leads to significant performance gain in comparison with the RLNC.**

Keywords- Constant-dimension codes; kk-code; Random linear network coding (RLNC), Subspace codes

I. INTRODUCTION

The network coding concept was first introduced for satellite communication networks in [12] and then developed in [9] where the term network coding was invented and its benefits was demonstrated. Instead of the simple store and forward communication technique, intermediate node is allowed to combine received packets into one packet and then to send it to the multiple destination which increase the throughput and save bandwidth and energy. This concept is illustrated by a simple example depicted in Fig. 1. We have two source nodes A and B that produce two packets a and b, respectively. Node A wants to send packet a to B and node B wants to send packet b to A through an intermediate relay node R. Fig. 1(a) shows a traditional approach in which the relay node first receives a and b then broadcast them respectively to both A and B. In this case, four transmissions are required. Fig. 1(b) shows the network coding approach in which the relay node first obtains the two packets a and b then generates a combination packet a ⊕ (⊕ denotes the modulo addition) that will be broadcasted to A and B. This scheme requires only three transmissions and the downlink bandwidth can be reduced by 50% [13].

Simply XORing received packets cannot achieves the benefits of network coding because real networks can be

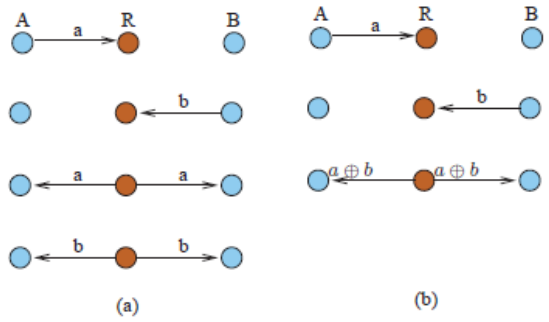

Figure 1. Wireless communication network. (a) traditional approach. (b) networkcoding approach.

extremely complex. In this context, two coding approaches were applied: Linear Network Coding (LNC) [11], [14] said deterministic LNC (DLNC) and random linear network coding [15] (RLNC). The deterministic case is a centralized approach where all coding operations at nodes are defined linear combinations of packets over a finite field which is too rigid and requires knowledge of network. For the random case, where the output packets of network nodes are a result of random linear mappings of inputs over some field, Medard and Kötter [15] show that the capacity is achieved with high probability if the field has sufficiently large size. This approach is decentralized, robust to packets loss and topology changes. Thus, RLNC is the considerable class of network coding.

The network coding approach is not always optimal. Thus, an erroneous packet may corrupt other free error packets when linearly combined at the intermediate nodes and then leading to error propagation. This phenomenon is well shown in Fig. 2.

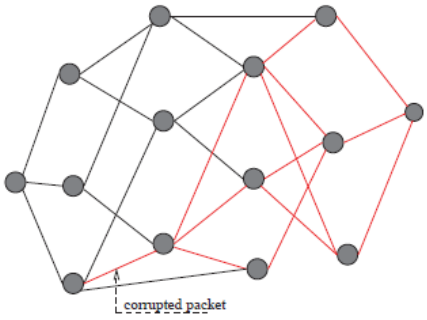

Figure 2. Figure 2. The phenomenon of error propagation induced by network coding. A produced error at a link is propagated to the next links after packets mixing.

New coding schemes are needed to solve this error correction problem for coherent and non-coherent networks. The schemes of the first type depend on the network topology or the coding operations performed at network nodes [4]. The second type [10], [3] assume that the source and sinks have no knowledge of such channel transfer characteristics.

Recently, a subspace code for an error control in non-coherent network has been introduced in [10] where the information message is coded in the choice of a vector space as a codeword at the source. This choice is ensured by transmission of a set of packets that span the codeword subspace. In this work, we implement such code when RLNC and conditional RLNC are they have to be regenerated until at least one of them is not null.

The paper is organized as follows. After briefly reviewing the basic notions in Section II, we present the coding-decoding scheme of kk-code in Section III. In Section IV, we give a short description of our simulator that implements network coding in mesh network and a kk-coder/decoder. In Section V, we give an example illustrating the transmission over such network. In Section VI, the simulation results on the PER (Packet Error Rate) performances will be illustrated and compared when RLNC and conditional RLNC are applied. In Section VII, we conclude this paper.

II. PRELIMINARIES

Let $q \geq 2$ be a power of a prime and $F_q = GF(q)$ a finite field of order q. We note $F = F_q^m$ the extension filed which may be considered as m-vector space over F_q.

A. Linearized Polynomials

For a fixed q, we will let [i] to denote q^i. Linearized polynomials over F_q^m are polynomials of the form given by (1).

$$P(x) = \sum_{i=0}^{d} a_i x^{q^i} = \sum_{i=0}^{d} a_i x^{[i]}. \quad (1)$$

with coefficients $a_i \in F$, i = 0,..., d.

Given any two linearized polynomials a(x) and b(x), there exist a unique linearized polynomials q(x) and r(x) such that $a(x)=q(x)\otimes b(x)+r(x)$, where r(x)=0 or deg(r(x)) < deg(b(x)).

Let $f(x,y)=f_x(x)+f_y(y)$ be a bivariate linearized polynomial, which means that both $f_x(x)$ and $f_y(y)$ are linearized polynomials. Let the degree of $f_x(x)$ and $f_y(y)$ be $q^{d}_{x(f)}$ and $q^{d}_{y(f)}$,respectively. The (1,k-1)-weighted degree of

f(x, y) is defined as

$$\deg_{1,k-1} = \max\{d_{x(f)}, k-1+d_{y(f)}\} \quad (2)$$

B. Ambient space

Let $A=\{a_1,...,a_l\} \subset \mathbb{F}$ the set of linearly independent elements in F. These elements span an *l*-dimensional vector space $\langle A\rangle \subseteq F$ over F_q, $l \leq m$. We will define as ambient space the direct sum $W=\langle A\rangle \oplus \mathbb{F} = \{(\alpha,\beta): \alpha \in \langle A\rangle, \beta \in \mathbb{F}\}$ which is a vector space of dimension *l+m* over F_q. P(W, |A|) denote the set of all |A|-dimensional subspaces of W.

III. CODING-DECODING SCHEME

The communication system model considered in this paper is presented in Fig. 3 and consists of a kk-encoder, a communication network where network coding is applied, and a kk-decoder. We suppose a source generating a block of message symbols $u= (u_0, u_1... u_{k-1})$ from the finite field F.

A. Code Constructions

Let $A=\{a_1, ..., a_l\}$ a set of linearly independent elements. In the first step, we define a linearized polynomial with coefficients corresponding to u

$$f(x) = \sum_{i=0}^{k-1} u_i x^{[i]}.$$

In the second step, we calculate $\beta=\{\beta_i=f(a_i), i=1, ... , l\}$. Each pair (a_i, β_i), i =1… l, is a vector in W. Since A is a linearly independent set, so is $(a_1, \beta_1)\ldots (a_l, \beta_l)$; hence this set spans an l-dimensional subspace V of W which represents the codeword.

B. Decoding procedure

Let V the codeword transmitted over a network where network coding is allowed. We assume that the received word U is an (l-ρ+t)-dimensional subspace of W where t and ρ are respectively the number of errors and erasures. We are able to recover V from U if $\rho+t<D/2=l-k+1$ where D is the minimum distance of constructed code given by theorem 1 of [10]. Decoding steps are:

1) Find a basis (xi, yi) ∈ W, i=1... r, for U.
Use Interpolate to find a bivariate linearized polynomial $Q(x,y)=Q_x(x)+Q_y(y)$ of minimal (1,k-1)-weighted degree that vanishes on the vector space U.

2) Use RDiv for $-Q_x(x)(x)$ and $Q_y(x)$ to find a linearized polynomial f(x) with the property that $-Q_x(x) = Q_y(x)\otimes f(x)$. If no such polynomial can be found declare "failure".

Figure 3. Block diagram of the studied transmission system.

IV. SIMULATOR FEATURES

In our work, data processed must be in finite field. For this reason, we first developed a C library that handles operations on numbers, vectors, matrix, and polynomials over GF(q^m). In the forthcoming we will describe the features of our implementation of network coding and kk-coder/decoder.

1) Network architecture: a network is defined by a set of nodes as the source, destination and intermediate nodes. The connections between the various nodes are described by a binary matrix:

- 1 if there is a link
- 0 otherwise

The links of the network can be Gaussian, Rayleigh or Gilbert Elliot channels. Each channel has its own characteristics.

2) Transmitted data: as described previously source node generates the message to be send. By applying the KK-coding algorithm that we have implemented in C, we get the codeword to be transmitted over the network. The encoder parameters are:

- q: the field characteristic,
- m: the field dimension,
- poly: the primitive polynomial,
- k: the number of symbols to be sent by the source,
- l = |A|.

The codeword is a subspace generated by the row vectors. We are going to send only generator vectors which we note as packets.

3) Linear Network Coding: the source will send a packet on every output link. The transmission will be a symbol by symbol in a series of round as in [1]. During each round, a number of transmission steps will be achieved. Each intermediate node of network generate random coefficients in GF(q) and forward packet that is linear combination of packets inside local buffers using generated coefficients. Thus, coefficients and packets used to construct a forwarded packets are unknown a priori. The transmission is stopped upon reaching the destination. As mentioned in the introduction, when conditionnal RLNC is appling, if all random coefficients are nulls, they have to be regenerated until at least one of them is not null.

4) Received data: after all sent packets reached the destination, the kk-decoding algorithm is applied to extract information within the limits of its correction capability.

V. ILLUSTRATIVE EXAMPLE

We illustrate the given coding-decoding procedure by an example of sending two symbols over $F = F_5^4$.

Let q=5, m=4, k=2 and l=4. The field F is generated by $g(x)=2+2x+x^2+x^4$ (662). Let $u=(3,10) \in F^2$ a block of message symbols, consisting of k=2 symbols over F or, equivalently, m×k = 8 symbols over F_5.

A. Coding steps

1) Let $f(x)=3x^{[0]}+10x^{[1]}$, be the linearized polynomial with coefficients corresponding to u.

2) Let $A=\{1, \alpha, \alpha^2, \alpha^3\}=\{1, 5, 25, 125\}$ be a set of linearly independent elements in the vector space F.

3) $\beta=\{3+2\alpha,4+2\alpha+3\alpha^2+\alpha^3,2+4\alpha+\alpha^3,4+3\alpha^2+2\alpha^3\}=\{13, 214, 149, 329\}$.

The linear space $V = < \begin{pmatrix} 1 & 13 \\ 5 & 214 \\ 25 & 149 \\ 125 & 329 \end{pmatrix} >$

We expand them over the F_5 starting from the least significant symbol. Hence the sent subspace codeword is given by

$$V = < \begin{pmatrix} 1 & 0 & 0 & 0 & 3 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 4 & 2 & 3 & 1 \\ 0 & 0 & 1 & 0 & 2 & 4 & 0 & 4 \\ 0 & 0 & 0 & 1 & 4 & 0 & 3 & 2 \end{pmatrix} >$$

B. Transmission steps

The codeword V is a subspace generated by the 4 row vectors. We are going to send only generator vectors which we note as packets. Thus, the source will send a packet on every output link over the network given by Fig. 4.

We have 4 packets: $\{p_{1,2}=[1\ 0\ 0\ 0\ 3\ 2\ 0\ 0]$, $p_{1,3}=[0\ 1\ 0\ 0\ 4\ 2\ 3\ 1]$, $p_{1,4}=[0\ 0\ 1\ 0\ 2\ 4\ 0\ 4]$, $p_{1,5}=[0\ 0\ 0\ 1\ 4\ 0\ 3\ 2]\}$. We explain now the transmission steps of these packets in order to reach the destination.

- round 1: The source 1 sends $p_{1,2}$ to node 2, $p_{1,3}$ to node 3, $p_{1,4}$ to node 4 and $p_{1,5}$ to node 5.
- round 2: Every node generate random coefficients in GF(5) (in this case the coefficient is 3 for all nodes) and send the linear combination of received packets. Node 2 send $p_2=3\times p_{1,2}$ to nodes 6 and 7, node 3 send $p_3=3\times p_2$ to nodes 6 and 8 but an error was produced in the link (3,8) then the received packet by node 8 is $p_3=[0\ 3\ 0\ 0\ 0\ 3\ 2\ 1]$, node 4 send $p_4=3\times p_3$ to node 9 and node 5 send $p_5=3\times p_4$ to node 8.
- round 3: Nodes 6, 7, 8 and 9 generate respectively random coefficients in GF(5), (4 4), (3), (2 4) and (2) then the packets send by each node are respectively $p_6=4\times p_2+4\times p_3=[2\ 2\ 0\ 0\ 4\ 3\ 1\ 2]$ to nodes 10 and 11, $p_7=3\times p_2=[4\ 0\ 0\ 0\ 2\ 3\ 0\ 0]$ to nodes 10 and 13, $p_8=2\times p_3+4\times p_5=[0\ 1\ 0\ 2\ 3\ 1\ 0\ 1]$ to nodes 11 and 13 and $p_9=2\times p_4=[0\ 0\ 1\ 0\ 2\ 4\ 0\ 4]$ to node 12.

- round 4: Nodes 10, 11, 12 and 13 generate respectively coefficients in GF(5), (2 3), (3 1) (4) and (2 3) then the packets send by each node to the destination are respectively $p_{10}=2\times p_6+3\times p_7$=[1 4 0 0 4 0 2 4], $p_{11}=3\times p_6+ p_8$=[1 2 0 2 0 0 3 2], $p_{12}=4\times p_9$=[0 0 4 0 3 1 0 1] and $p_{13}=2\times p_7+3\times p_8$=[3 3 0 1 3 4 0 3].

The received packets form the following matrix

$$M = \begin{pmatrix} 1 & 4 & 0 & 0 & 4 & 0 & 2 & 4 \\ 1 & 2 & 0 & 2 & 0 & 0 & 3 & 2 \\ 0 & 0 & 4 & 0 & 3 & 1 & 0 & 1 \\ 3 & 3 & 0 & 1 & 3 & 4 & 0 & 3 \end{pmatrix}$$

C. Decoding Steps

1) Let U=< M >. The basis of U is {(1 4 0 0 4 0 2 4),(1 2 0 2 0 0 3 2),(0 0 4 0 3 1 0 1),(3 3 0 1 3 4 0 3)}.

2) The input of Interpolation are X=[21, 261, 100, 143] and Y=[554, 325, 133, 398]. The outputs are $Q(x,y)=270X^{[0]}+451X^{[1]}+372X^{[2]}+515Y^{[0]}+139Y^{[1]}$.

3) RDiv outputs are $q(x)=f(x)=3X^{[0]}+10X^{[1]}$ and r(x)=0. Finally, the decoded message is $\hat{u} = u = (3, 10)$.

VI. PERFORMANCE EVALUATION

The goal of this sections is to deriving the condition under which network coding improves the system performance.

A. Network Architecture

The network we consider for our simulation is as shown in Fig. 4. Every node is allowed to use network coding. We consider that each link is a q-ary Gilbert Elliot channel given by Fig. 5 where

- *Pgb*: probability to pass from ”Good” to ”Bad” state,
- *Pbg*: probability to pass from”Bad” to”Good” state.
- *Pe*(*G*), the error probability in the ”Good” state,
- *Pe*(*B*), the error probability in the ”Bad” state.

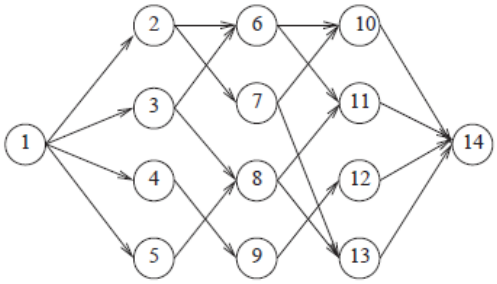

Figure 4. The network used in our simulation. Every node is allowed to use network coding.

We present the simulation results of the coder structure for two network coding approaches: RLNC and the proposed conditional RLNC in terms of the PER (Packet Error Rate) in the case of transmission over the q-ary Gilbert Elliot channel. Results are compared for different field characteristic q as given by Tab. I.

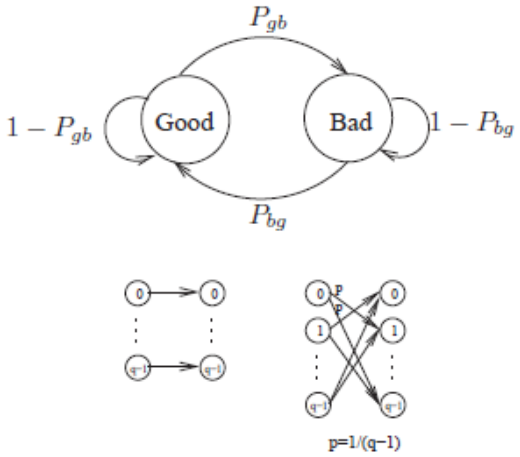

Figure 5. q-ary Gilbert-Elliot channel model used in our simulations.

We suppose that Pe(G)=0 and Pe(B)=1 as in [7], [2]. We note the transmitted symbol s_t and the received one sr. Under such conditions, in the ”Good” state $s_r=s_t$ and in the ”Bad” state $s_r \in \{0, 1\ldots q-1\} \setminus s_t$. In other words, in ”Good” state, every symbol is left untouched with probability 1 and in ”Bad” state every symbol is distorted to each of the q-1 possible different symbols with equal probability p=1/q-1.

B. Simulation Results

TABLE I. THE GALOIS FIELDS CHARACTERISTICS AND THEIR PRIMITIVE POLYNOMIALS

q	Primitive polynomial
2	25
3	86
5	662
7	2476

The investigated scheme considers the transmission of source-symbol sequences of k = 2 symbols and the obtained results are depicted in Fig. 6. We have plotted the PER as a function of BER (Bit Error Rate) per link for different field

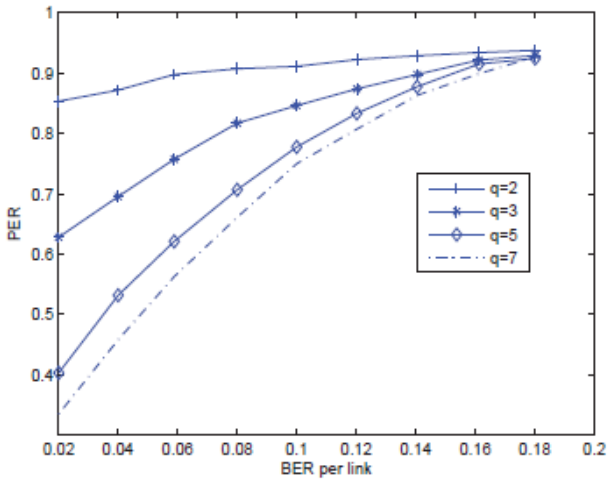

Figure 6. Packet error rate as a function of the BER per link of network 4 when RLNC is applied, m = 4, k = 2 and l = 4.

characteristic q when RLNC is applied at intermediate nodes. Each node generates random coefficients in Fq and sends a linear combination of received packets. We note that the PER introduced by the network decreases as a function of q then a significant gain is obtained for q = 7. In fact, if q increases then the probability of having independent vectors increases and thus reduces the PER. These results confirm the theoretical result made in [15] where the authors gave a lower bound for the probability that a random network code is valid. According to theorem 2 of [15], this probability is at least $(1-d/q)^{\eta}$, where d is the number of receivers and η the number of links (For our network d=1 and η=21).

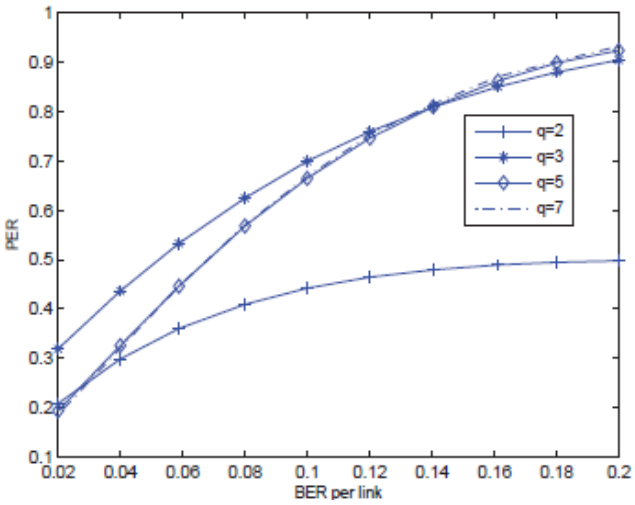

Figure 7. Packet error rate as a function of the BER per link of network 4 when conditional RLNC is applied, *m* = 4, *k* = 2 and *l* = 4.

In the second experiment, we propose to investigate the effect of the conditional RLNC. As mentioned in the introduction, if all random coefficients are nulls, they have to be regenerated until at least one of them is not null. We present, in Fig. 7, simulation results obtained for different values of *q*. We can see that with *q* = 2 we have, for a BER=0.1, an improvement of about 48%. Increasing *q* to 7 results in a small additional gain of PER. We observe an improvement in the performance for the minimum value of *q* which is contradictory to the results already proved theoretically. In fact, if *q* decreases, the probability of having null vectors increases. Then applying the condition at intermediate node decreases the number of dependent packets and thus the number of erasures. In spite of this result don't prove the theoretical results of [15], it gives a significant gain for the different fields.

This results are justified also in the case of transmission aver an AWGN channel with BPSK modulation under such conditions. The simulation results are given by Fig. 8 and Fig. 9.

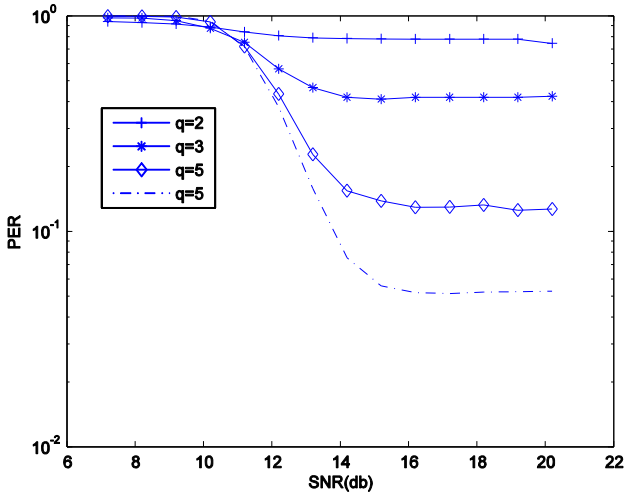

Figure 8. PER versus SNR in the case of transmission over an AWGN channel with BPSK modulation for network when RLNC is applied, *m* = 4, *k* = 2 and *l* = 4.

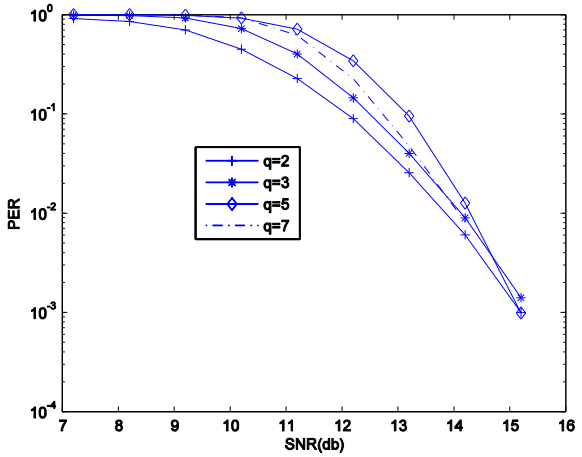

Figure 9. PER versus SNR in the case of transmission over an AWGN channel with BPSK modulation for network when Conditional RLNC is applied, $m = 4$, $k = 2$ and $l = 4$.

VII. CONCLUSION

In this paper, we have evaluated the performance of kk-code in the context of non-coherent network coding for different field characteristic q. On one hand, we have shown that, when simply applying RLNC at intermediate nodes, simulation results prove the theoretical result of Medard and Kötter in [15] and the simulation result of [2]. On the other hand, as packets are lost at intermediate nodes when generated coefficients at these nodes are all nulls, every node has to regenerate their coefficients until at least one of them not null. In this case, an additional gain of 48% has been demonstrated for $q = 2$. This network coding approach that we have called conditional RLNC improves the performance in terms of PER compared to RLNC but gives results that are contradictory to those already proved theoretically.

REFERENCES

[1] A. Al Hamra, C. Barakat, T. Turletti, "Network coding for wireless mesh networks: a case study", Conference Publications, 9 pp.-114, 2006.

[2] A. Guefrachi, S. Zaibi, A. Bouall`egue, "Performance evaluation of constant dimension subspace code for error and erasures correcting in linear network coding", IJARCSEE, VOL 1, NO 9, pp.117-123, 2012.

[3] D. Silva, FR. Kschischang, and R. K¨otter, "A Rank-Metric Approach to Error Control in Random Network Coding", IEEE Trans. Info. Theory, vol. 54, no. 9, pp. 3951-3967, September 2008.

[4] J. Zhang, K. B. Letaief and P. Fan, "Distributed Product Coding Approach For Robust Network Coding", Comm. ICC '08. IEEE International Conference on . 10.1109/ICC.2008.40, pp. 176-180,2008.

[5] N.Cai and R.Yeung, "Network coding and error correction", Proc. 2002 IEEE Inform. Theory Workshop, Bangalore, India, Oct.20-25, pp. 119-122, 2002.

[6] Ning Chen, Zhiyuan Yan, Maximilien Gadouleau, Ying Wang and Bruce W. Suter "Rank Metric Decoder Architectures for Random Linear Network Coding with Error Control", IEEE Trans. vol. 20, no. 2, pp. 296-309, Feb. 2012.

[7] Pau Bernat and Guri Hundertmark, "Bit Error Combating Network Coding Techniques", June 2010.

[8] Raymond W. Yeung, Shuo-Yen Robert Li, Ning Cai, Zhen Zhang, "Network Coding Theory", Foundation and Trends in Communications and Info. Theory, vol 2, no. 4 and 5, pp. 241-381, 2005.

[9] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow", IEEE Info. Theory, vol. 46, no. 4, pp. 1024- 1016, 2000.

[10] R. Koetter and F.R. Kschischang, "Coding for Errors and Erasures in Random Network Coding", IEEE Trans. Info. Theory, vol. 54, no. 8, 3579 - 3591, 2008.

[11] R.Koetter and M.Médard, "An algebraic approach to network coding", IEEE/ACM Trans. Netw., vol. 11, no. 5, pp. 782-795, Oct. 2003.

[12] R.W. Yeung and Z. Zhang, "Distributed source coding for satellite communications", IEEE Trans. Inform. Theory, IT- 45: 1111-1120, 1999.

[13] RW. Yeung, SYR. Li, N. Cai, and Z. Zhang, "Network Coding Theory", now Publishers, 2005.

[14] SYR. Li, RW. Yeung, and N. Cai, "Linear network coding", IEEE Trans. Info. Theory, vol. 49, no. 2, 371-381, 2003.

[15] T.Ho, M. Medard, R. K¨otter, D.R. Karger, M. Effros, J. Shi, and B. Leong, "A Random Linear Network Coding Approach to Multicast", IEEE Trans. on Info. Theory, vol. 52, no. 10, 4413- 4430, 2006.