Exact Decoding Probability of Random Linear Network Coding for Tree Networks

Fang Li[1], Min Xie[1,2]
[1]State Key Laboratory of Integrated Services Networks (ISN), Xidian University
Xi′an, 710071, China
[e-mail: fangli@stu.xidian.edu.cn]
[2] School of Telecommunications Engineering, Xidian University
Xi′an, 710071, China
[e-mail: mxie@xidian.edu.cn]
*Corresponding author: Fang Li

Received September 15, 2014; revised December 12, 2014; accepted January 2, 2015; published February 28, 2015

Abstract

The hierarchical structure in networks is widely applied in many practical scenarios especially in some emergency cases. In this paper, we focus on a tree network with and without packet loss where one source sends data to n destinations, through m relay nodes employing random linear network coding (RLNC) over a Galois field in parallel transmission systems. We derive closed-form probability expressions of successful decoding at a destination node and at all destination nodes in this multicast scenario. For the convenience of computing, we also propose an upper bound for the failure probability. We then investigate the impact of the major parameters, i.e., the size of finite fields, the number of internal nodes, the number of sink nodes and the channel failure probability, on the decoding performance with simulation results. In addition, numerical results show that, under a fixed exact decoding probability, the required field size can be minimized. When failure decoding probabilities are given, the operation is simple and its complexity is low in a small finite field.

Keywords: Network coding, tree topology, random linear network coding, exact decoding probability

This work was partially supported by the National Natural Science Foundation of China (Grant No. 61271174 and No. 61301178). We express our thanks to the anonymous referees for their helpful comments and beneficial suggestions.

http://dx.doi.org/10.3837/tiis.2015.02.013 **ISSN : 1976-7277**

1. Introduction

Network coding (NC) has been shown to offer advantages in throughput, robustness, power consumption, and security in both wireline [1] and wireless networks [2], by allowing intermediate nodes to mix the information before forwarding it. Their work [1] was regarded as the commencement of research of NC. Li *et al.* [3] showed that linear network coding (LNC) can achieve the optimal throughput for a multicast transmission.

Later, Ho *et al*. [4] proposed that an effective, yet simple, approach is random linear network coding (RLNC). They also analyzed the performance by deriving upper bounds for the failure of this code. Furthermore, Huseyin *et al.* [5] defined two types of failure probabilities to characterize the performance analysis of RLNC and improved bounds in [4]. Their bounds are described by the number of internal nodes, instead of the number of channels or similar quantities.

Typically, the exact decoding probability under RLNC is derived in a fixed topology [6]- [8]. Trullols-Cruces *et al.* [6] computed the exact probability that a receiver obtains N linearly independent packets among $K \geq N$ received packets, when the senders use RLNC over a Galois field. This problem is equivalent to computing the probability that a $N \times K$ matrix has rank N , where each element is randomly selected from a Galois field with equal probability. Deriving the probability that this matrix has full rank in [7] can be viewed as a special case of Th. 1 in our work.

In this paper, we consider that the source sends information to all sinks at the theoretically maximum rate with RLNC for tree networks. From the network topological perspective, hierarchical structures can be reduced to tree-type networks. In addition, tree structured networks are scalable to expand coverage by increasing the depth of tree networks due to their flexibility and low delay, making it suitable for a variety of emergency applications. Such topology is widely used and is a basic building block of more complex multi-hop networks [9]-[13]. Because the topology of tree networks with packet loss is dynamic, RLNC allows higher data rates than routing and the operation is simple.

The main contributions of this paper are described as follows. Firstly, we derive the exact probability of RLNC over a Galois field for tree networks with and without packet loss. Secondly, for the convenience of computing, we propose upper bounds for the failure probability and improve the bound in [5] (Theorem 2) by replacing the number

$$\binom{m+\delta+1}{m}$$

by the number $m+1$ for tree networks to decrease the complexity. Here m is the number of internal nodes, δ is equal to $k-\omega$, k is the min-cut from s to all sinks $t \in T$, and ω is the number of symbols generated at the source. Finally, we illustrate that, the impact of major parameters, *i.e.*, the size of finite fields, the number of internal nodes, the number of sink nodes and the channel failure probability, on the decoding performance with simulation results. Numerical results also show that, under a fixed decoding probability, a required field size can be minimized.

The remainder of this paper is organized as follows. Section II introduces the definition of RLNC and presents the network model of tree networks. Section III derives closed-form probability expressions of the defined model, proves main results and

describes numerical results. Section IV provides concluding remarks.

2. Basic Definitions and the Network Model

We consider a multi-hop relay tree network composed of one source, m internal nodes and n sink nodes, *i.e.*, $T=\{t_1,\cdots,t_n\}$ in parallel transmission system as shown in **Fig. 1**. There are k multiple channels between two nodes. So, k is the min-cut from s to all sinks $t\in T$. Every channel can transmit one field symbol per unit time. Further, denote the channel leading from node i to node j by the direct edge $e=(i,j)$, where node i is called the tail of e and node j is called the head of e. For each node i, let $Out(i)$ be the set of edges leaving node i and let $In(i)$ be the set of edges entering node i.

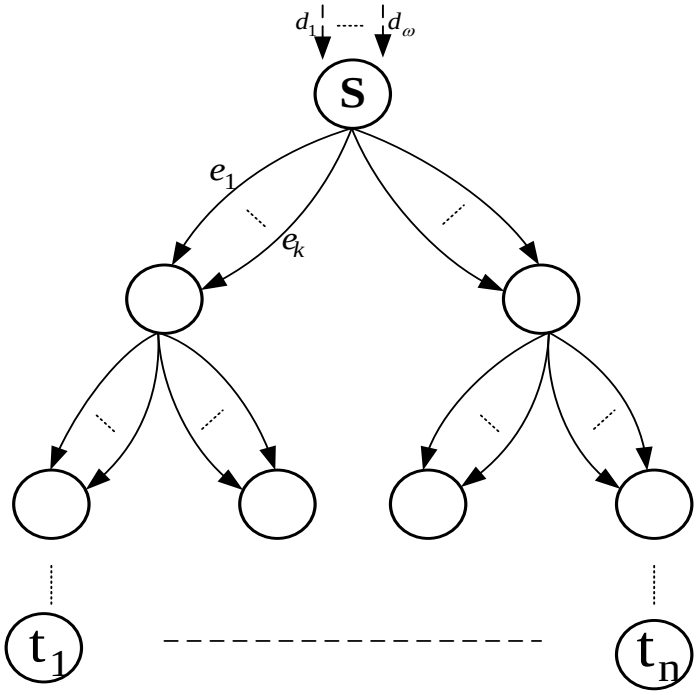


Fig. 1. Network model.

Source messages $\underline{X}=(x_1,\ldots,x_\omega)$ arranged in a row vector over a Galois field $\mathbf{F}_q$ of size q are transmitted to the source s through ω imaginary channels in $In(s)$. Note that all of the arithmetic operations are performed over this field. Each of the m relays encodes the received packets using RLNC, and it sends the resulting packet toward its child nodes. Even if nodes in **Fig. 1** join or leave, preexisting nodes do not need to change their coding operations to preserve the same guarantee of correctness. U_e is the message transmitted over the channel e. The coding process at each node i is represented as follows:

$$U_e=\sum_{d\in In(tail(e))}k_{de}U_d \tag{1}$$

where k_{de} is called local encoding kernel or coefficient. The coefficient used to encode the data packets is randomly extracted from a field $\mathbf{F}_q$, with equal probability.

As we know from [14], [15], the global kernel f_e for a channel e is a column vector such that

$$U_e = \underline{X} f_e \tag{2}$$

The global kernels can be determined by the local kernels inductively by the next formula

$$f_e = \sum_{d \in In(tail(e))} k_{de} f_d \tag{3}$$

Therefore, we denote by F_t the $\omega \times k$ matrix containing global kernels for channels in $In(t)$, *i.e.*,

$$F_t = (f_d : d \in In(t)) \tag{4}$$

where F_t is called the decoding matrix at sink t.

To simplify the discussion, we fix a sink node $t \in T$. Without loss of generality, let

$$s = i_0 \prec i_1 \prec, \ldots, \prec i_m \prec i_{m+1} = t$$

be an upstream to downstream order of nodes. The minimum cut capacity between the source node s and the sink node t is k, where $k > \omega$. Denote r_t be the number of internal nodes in disjoint paths $\mathrm{P}^{(t)}$ from s to t. Furthermore, since the Menger's Theorem, there exit k disjoint paths from s to t denoted by $\mathrm{P}^{(t)} = \{\mathrm{P}_j^{(t)} : 1 \le j \le k\}$. Let $E_{\mathrm{P}}^{(t)}$ be the set of all channels in these k paths. Let $\{e_{j,1}^{(t)}, e_{j,2}^{(t)}, \ldots, e_{j,r_t+1}^{(t)}\}$ be the sequence of channels in the path $\mathrm{P}_j^{(t)}$ satisfying

$$head\left(e_{j,i}^{(t)}\right) = tail\left(e_{j,i+1}^{(t)}\right) : 1 \le i \le r_t,\ tail\left(e_{j,1}^{(t)}\right) = s \text{ and } head\left(e_{j,r_t+1}^{(t)}\right) = t.$$

In the following we use the concept of cuts from s to t represented in [5]. Intuitively, the first cut is $CUT_0(t) = \{d_1, \cdots, d_\omega\}$ and the second cut is $CUT_1(t) = \{e_{i,1}^{(t)} : 1 \le i \le k\}$. At node i_1, the next cut is defined from $CUT_1(t)$ by replacing channels in $In(i_1) \cap CUT_1(t)$ by their respective next channels in the path. Subsequently, once $CUT_j(t)$ is defined, $CUT_{j+1}(t)$ is formed from [5] by the same method as above. By induction, all cuts $CUT_j(t)$ for $j = 0, \ldots, m+1$ can be defined. Furthermore, denote $CUT_j^{in}(t) = In(i_j) \cap CUT_j(t)$ and $CUT_j^{out}(t) = CUT_j(t) - CUT_j^{in}(t)$.

Before discussion, we immediately introduce the definition of successful decoding probabilities as follows. For convenience, let $\langle In(t) \rangle$ be the linear space spanned by the global encoding kernel in $\{f_e : e \in In(t)\}$.

Definition 1: The successful probability of random linear network coding at sink t is

$$\begin{aligned} P_r^{(t)} &= P_r\left(Rank(F_t) = \omega\right) \\ &= P_r\left(dim\left(\langle In(t) \rangle\right) = \omega\right) \end{aligned} \tag{5}$$

and the successful probability of random linear network coding at all sink nodes is

$$P_r = P_r\left(\forall t \in T : Rank\left(F_t\right) = \omega\right) \tag{6}$$

As shown in [3] and [5], we have the following result for the network. There exist network codes such that the messages can be decoded successfully at sink t, if and only if any one of the following statements is true:

1) $dim\left(\langle In(t)\rangle\right) = \omega$;

2) there exist ω linearly independent global encoding kernel vectors in $\{f_d : d \in In(t)\}$;

3) $Rank\left(F_t\right) = \omega$.

In addition, main notations used in section 3 are as follows:

$\mathbf{F}_q$: the finite field used.

q: the size of the finite field $\mathbf{F}_q$.

ω: the number of symbols generated at the source node.

δ: the number of redundancies, i.e., δ is equal to $k-\omega$.

m: the number of internal nodes.

n: the number of sink nodes.

k: the min-cut from s to all sinks $t \in T$.

r_t: the number of internal nodes in disjoint paths $\mathrm{P}^{(t)}$ from s to t.

r: the maximum number of r_t, *i.e.*, $max\{r_t : t \in T\}$.

3. Results

3.1 Exact Decoding Probabilities

We have known that the performance analysis of RLNC plays an important part in theory and application. In general, it is difficult to compute the exact decoding probability of RLNC for a general communication network because the topology of a general communication network is unfixed. In this section, we calculate the exact decoding probability of RLNC for tree networks. At first, we give the following theorem.

Theorem 1. Let L be an n-dimensional linear space over finite field $\mathbf{F}_q$, L_0 and L_1 be two subspaces of dimensional k_0 and k_1 in space L, respectively, and $\langle L_0 \cup L_1\rangle = L$. Let $l_1,\ldots,l_{n-k_0+m=r}(m \geq 1)$ be r uniformly distributed random vectors taking values in L. Then

$$p_r\left(\dim\left(\langle L_0 \cup \{l_1,\ldots,l_r\}\rangle = n\right)\right) = \prod_{i=r-n+k_0+1}^{r}\left(1-\frac{1}{q^i}\right) \tag{7}$$

Proof. To form the linear space L, we start with L_0, then add vectors in $l_1,\ldots,l_r$ to the subspace L_0 one by one. During the process of adding these vectors, if any vector l_i falls in the space

$$B_{i-1} = \langle L_0 \cup \{l_j : 1 \le j \le i-1\}\rangle,$$

a failure or a redundancy occurs, where $B_0 = L_0$. Under the condition that $l_i \notin B_{i-1}$ for $1 \le j \le i-1$, we have

$$dim(B_{i-1}) = dim(B_0) + i - 1 = k_0 + i - 1.$$

We prove this theorem by induction on $m = r - n + k_0$, the index of the number of redundancies in L_1.

For $m = 1$, we have $r = n - k_0 + 1$. Note that if a failure occurs firstly in the *j*th selection, there must not be any failure in the following sequence. If such failure occurs, with probability

$$\frac{q^{dim(\langle B_{j-1}\rangle)}}{q^{dim(L)}} = \frac{1}{q^{n-k_0-j+1}},$$

we will leave exactly $n - k_0$ linear independent vectors. In the derivation, we obtain the probability that $n - k_0$ linear independent vectors are picked, given $r = n - k_0 + 1$ selections, as

$$\begin{aligned} p_r &= \prod_{j=1}^{n-k_0} \frac{q^n - q^{k_0+j-1}}{q^n} \left(\sum_{r_1=k_0}^{n} \frac{q^i}{q^n} \right) \\ &= \prod_{j=2}^{n-k_0+1} \left(1 - \frac{1}{q^j} \right) \end{aligned} \tag{8}$$

By the above iterating method, we have proved it for $m = 1$ and obtain the probability for $m > 1$

$$\begin{aligned} p_r &= \prod_{j=1}^{n-k_0} \left(1 - \frac{1}{q^j} \right) \left(\sum_{r_1=k_0}^{n} \frac{q^{r_1}}{q^n} \cdots \sum_{r_m=r_{m-1}}^{n} \frac{q^{r_m}}{q^n} \right) \\ &= \prod_{j=m+1}^{n-k_0+m} \left(1 - \frac{1}{q^j} \right) \end{aligned} \tag{9}$$

From the above equation, we can get the formula

$$\prod_{j=1}^{m} \left(1 - \frac{1}{q^j} \right) \left(\sum_{r_1=k_0}^{n} \frac{q^{r_1}}{q^n} \cdots \sum_{r_m=r_{m-1}}^{n} \frac{q^{r_m}}{q^n} \right) = \prod_{j=n-k_0+1}^{n-k_0+m} \left(1 - \frac{1}{q^j} \right). \tag{10}$$

Assume that the result of the theorem is proved for $2, \cdots, m$, we now prove it for $m+1$, we have

$$
\begin{aligned}
p_r &= \prod_{j=1}^{n-k_0}\left(1-\frac{1}{q^j}\right)\left(\sum_{r_1=k_0}^{n}\frac{q^{r_1}}{q^n}\cdots\sum_{r_{m+1}=r_m}^{n}\frac{q^{r_{m+1}}}{q^n}\right)\\
&\overset{(a)}{=}\prod_{l=m+1}^{n-k_0}\left(1-\frac{1}{q^l}\right)\cdot\left[\sum_{r_1=k_0}^{n}\frac{q^{r_1}}{q^n}\prod_{j=n-r_1+1}^{n-r_1+m}\left(1-\frac{1}{q^j}\right)\right]\\
&=\prod_{l=m+1}^{n-k_0}\left(1-\frac{1}{q^l}\right)\prod_{i=n-k_0+1}^{km+k+m}\left(1-\frac{1}{q^i}\right)\prod_{j=km+k+m+2}^{n-k_0+m+1}\left(1-\frac{1}{q^j}\right)\left[1+\frac{1}{q^{m+1}}+\ldots+\frac{1}{q^{k(m+1)}}\right]\\
&=\prod_{i=m+2}^{n-k_0+m+1}\left(1-\frac{1}{q^i}\right)
\end{aligned}
\tag{11}
$$

where $k=\left\lfloor\frac{n-k_0}{m+1}\right\rfloor$ and Eq. (a) can be obtained from Eq. (10).

The theorem is proved. □

Remark 1. We can observe that $p_r\left(\dim\left(\langle L_0\cup\{l_1,\ldots,l_r\}\rangle=n\right)\right)$ is not related to the dimension of L_1 .We also notice that when $k_0=0$, we get the following corollary. This corollary can be directly proved by the method in combinatory in [16], too.

Corollary 2. Let L be an n - dimensional linear space over finite field $\mathbf{F}_q$. Let $l_1,\ldots,l_r$ be r uniformly distributed random vectors taking values in L . Then

$$
p_r\left(\dim\left(\langle\{l_1,\ldots,l_r\}\rangle=n\right)\right)=\prod_{i=r-n+1}^{r}\left(1-\frac{1}{q^i}\right) \tag{12}
$$

Applying this corollary and the definition of CUT_j , we compute exact decoding probability at a destination node and at all destination nodes in tree networks. In order to decode, a destination node has to collect as many linearly independent vectors as the number of packets that were originally mixed in, and then solve the resulting system of linear equations. The decoding probability thus depends on the coding design and the selected coefficients. The coefficients used to encode the data packets are extracted from a Galois field of size q.

Theorem 3. For tree networks as shown in **Fig. 1**, let the minimum cut capacity for sink node $t\in T$ be k and let the information rate be ω symbols per unit time. Local encoding coefficients are chosen independently and uniformly from the finite field $\mathbf{F}_q$.

(1) The failure decoding probability of RLNC at sink t satisfies:

$$
P_e^t=1-\left[\prod_{l=\delta+1}^{k}\left(1-\frac{1}{q^l}\right)\right]^{r_t+1} \tag{13}
$$

(2) The failure decoding probability of RLNC for tree networks satisfies:

$$
P_e=1-\left[\prod_{l=\delta+1}^{k}\left(1-\frac{1}{q^l}\right)\right]^{m+n} \tag{14}
$$

Proof. Given in Appendix A. □

In particular, we denote $r=max\{r_t:t\in T\}$. The following corollary can be obtained immediately.

Corollary 4: For tree networks as shown in **Fig. 1**, the failure decoding probability of RLNC at sink t satisfies:

$$P_e^t \le 1-\left[\prod_{l=\delta+1}^{k}\left(1-\frac{1}{q^l}\right)\right]^{r+1} \tag{15}$$

We have described that sometimes it is difficult to use predesigned LNC based on the network topology even if the topology is known. When nothing about the topology of tree networks except the number of internal numbers m are known, we analyze the performance of RLNC in the next corollary.

Corollary 5. For tree networks as shown in **Fig. 1**,

(1) the failure decoding probability of RLNC at sink t satisfies:

$$P_e^t < \frac{m+1}{(q-1)q^{\delta}} \tag{16}$$

(2) the failure decoding probability of RLNC for tree networks satisfies:

$$P_e < \frac{m+n}{(q-1)q^{\delta}} \tag{17}$$

We can notice that we improve the bound in [5] (theorem 2) by replacing the number

$$\binom{m+\delta+1}{m}$$

by the number $m+1$. As above mentioned, our analyses show that the failure probability is a function of m, δ and q.

In practice, due to various reasons, packet loss may occur. Unlike previous work, we consider that the relay nodes may not receive some packets due to link failures. This implies that a destination may be unable to successfully decode the received data packets due to both missing packets at the relays and linearly dependent coefficient vectors. In general, channel failure is a low probability event, that is, $0 \le p << 1/2$. In particular, when $p = 0$, the following theorem is equivalent to Theorem 3.

Theorem 6. For tree networks as shown in **Fig. 1** with channel failure probability p,

(1) the failure decoding probability of RLNC at sink t satisfies:

$$\overline{P_e^t} = 1-\left[\sum_{l=\omega}^{k}\binom{k}{l}(1-p)^l p^{k-l}\prod_{i=l-\omega+1}^{l}\left(1-\frac{1}{q^i}\right)\right]^{r_t+1} \tag{18}$$

(2) the failure decoding probability of RLNC for tree network satisfies:

$$\overline{P_e} = 1-\left[\sum_{l=\omega}^{k}\binom{k}{l}(1-p)^l p^{k-l}\prod_{i=l-\omega+1}^{l}\left(1-\frac{1}{q^i}\right)\right]^{m+n} \tag{19}$$

Proof. Given in Appendix B. □

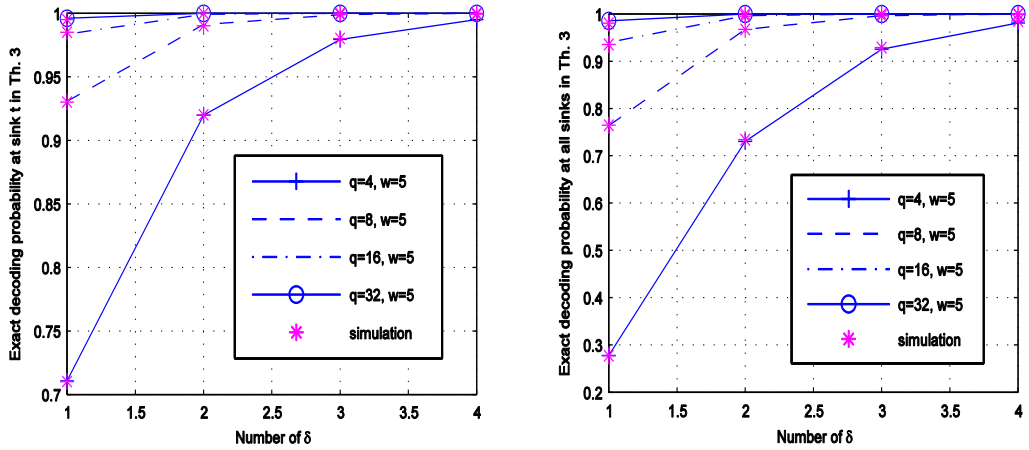
3.2 Numerical Results

We now show the impact of major parameters on the decoding performance. In the following, we fix the number of symbols generated at the source $\omega = 5$.

As discussed above, our analysis concerns the decoding probability at a (all) sink node(s) without packet loss, as a function of the size of finite field q, (the number of sink nodes n,) and the number of internal nodes m in Th. 3. Typically, the exact probability is limited to the linear independence of the random vectors employed for the encoding of received packets.

Firstly, by a comparison of **Fig. 2.(a)** and **Fig. 2.(b)**, we observe that the number of sink nodes n plays an important role in analysing the decoding performance. Under other

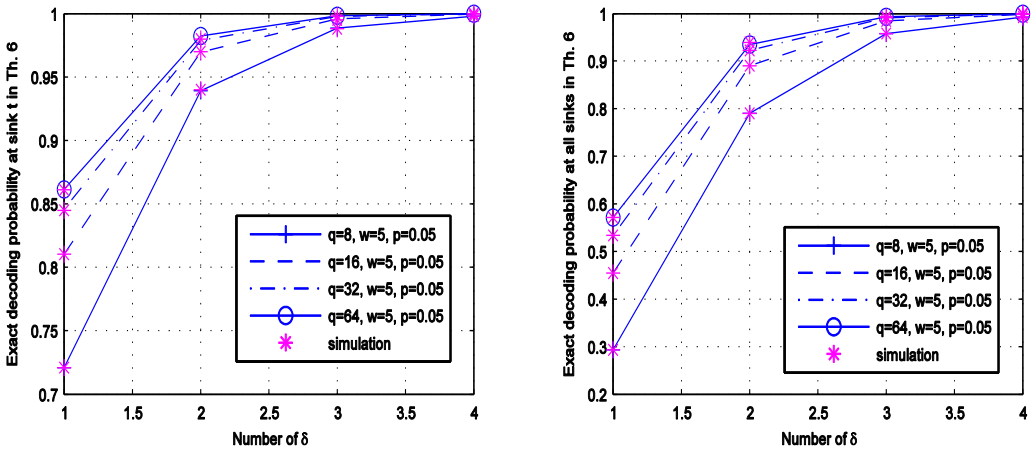
parameters are fixed, the smaller the number n is in a tree network, the better performance it has. Secondly, represented by different continuous and dashed lines, **Fig. 2** shows the exact decoding probability as a function of the size of finite field q, when δ is fixed. Clearly, as q increases, the performance improves greatly. We also observe that for $q=16$ both of two successful probabilities are larger than 0.9 even in the presence of a small number of redundancy. Finally, represented by each continuous or dashed line, **Fig. 2** shows the probability as a function of δ,when q is determined. Obviously, as δ increases to 2, the performance improves dramatically. We can obtain that δ has a significant impact on the decoding performance.



(a) (b)

Fig. 2. (a) shows the simulation results and the exact decoding probability at sink t obtained over 10^5 runs when $\omega=5$ and $r_t=3$.

(b) shows the simulation results and the exact decoding probability at all sinks obtained over 10^5 runs when $\omega=5$, $m=10$ and $n=5$.



(a) (b)

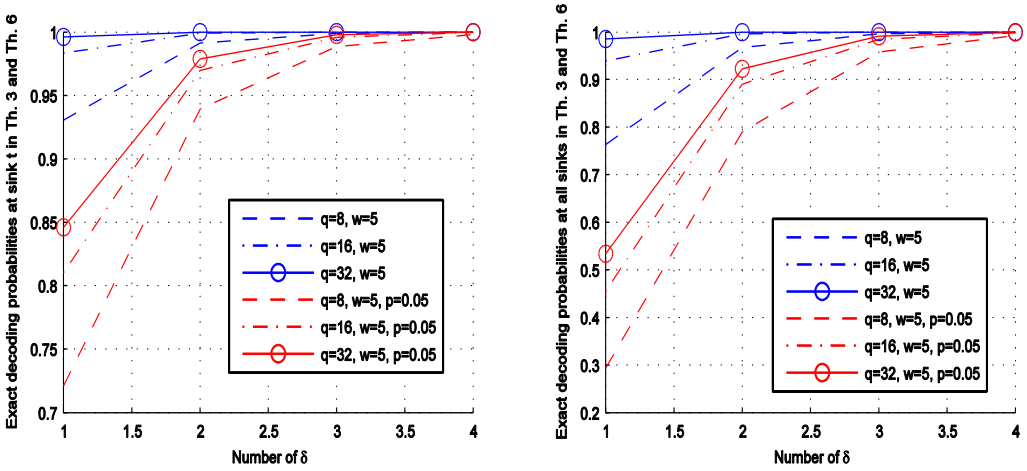
Fig. 3 (a) shows the simulation results and the exact decoding probability at sink t obtained over 10^5 runs when $\omega=5$, $p=0.1$ and $r_t=3$.

(b) shows the simulation and the exact decoding probability at all sinks obtained over

10^5 runs when $\omega = 5$, $p = 0.1$, $m = 10$ and $n = 5$.

The main difference between Th. 3 and Th. 6 is that packet loss may occur in the latter. We now show the impact of major parameters, i.e., the size of finite fields, the number of internal nodes m, the number of sink nodes n and the channel failure probability p, on the decoding performance at sink t and at all sinks with channel failure probability in Th. 6.

A comparison of **Fig. 3.(a)** and **Fig. 3.(b)** shows that the number of sink nodes n has a marked impact on the decoding performance, when other parameters are fixed. Clearly, as n increases, the decoding probability decreases greatly. Among different lines, we also show that the decoding probability is a function of the size of finite field q, when δ and p are fixed. As q increases, the performance improves greatly. Further, we observe that the decoding probability is a function of δ, when q and p are fixed in each line. We observe that for $\delta = 1$, very poor performance is obtained, indeed, the channel failure probability, which makes message decoding fail, has a dominant effect. Clearly, as δ increases to 2, the performance improves greatly and as δ increases to 3, both of two successful probabilities are larger than 0.95 even in the presence of a small number q. Differences between analytical and simulative results are in the order of 10^{-3} in **Fig. 2** and **Fig. 3**. This implies that simulation results match analytical results very well.



(a) (b)

Fig. 4. (a) shows a comparison of successful decoding probabilities with and without packet loss at sink t as δ varies.

(b) shows a comparison of successful decoding probabilities with and without packet loss at all sinks as δ varies.

We investigate the impact of the number of channel failure probability p on the decoding performance in **Fig. 4**. This figure shows the comparison of successful decoding probabilities with and without packet loss with $\omega = 5$, $r_t = 3$, $m = 10$, $n = 5$, $p = 0.05$, $q = 8, 16, 32$ and $\delta = 1, 2, 3, 4$. From the above figure, we can observe that our result in Th. 3 and Th. 6 represented by blue lines and red lines, respectively, and for $\delta = 1$ with channel failure probability $p = 0.05$, very poor performance is obtained. As δ increases

to 2, the performance improves greatly. However, as δ increases from 3 to 4, the performance improves slowly. The importance of q and p is confirmed by **Fig. 4**. Numerical results further showed that, as the field size increases, the decoding performance improves significantly.

4. Conclusion

In this paper, we mainly investigated RLNC for tree networks with and without packet loss by combining techniques from linear algebra, network flows and randomization. We derived closed-form decoding probability expressions of tree networks, as a function of the size of finite fields, the number of internal nodes, the number of sink nodes and the channel failure probability. For the purpose of simple computing , we also proposed a sharper bound on the required field size, when the failure probability is given.We investigated the impact of these major parameters on the decoding performance at one sink and at all sinks with simulation results. Furthermore, numerical results illustrated that the required field size can be minimized, when other parameters are fixed.

Appendix A

Proof of Theorem 3

We consider primarily the successful decoding probability P_r^t. By described above, computing the successful decoding probability is equivalent to the event "$\dim(\langle f_e \rangle) = \omega, e \in In(t)$". Further define $\omega \times k$ matrices $F_t^j = \left(f_e : e \in CUT_j(t) \right)$ for $j = 1, \ldots, m+1$.

Denote $F_t = \{ f_e : e \in In(t) \}$ be the decoding matrix at sink t. Intuitively, $F_t^{r_t+1} = F_t$. Denote the event "$Rank\left(F_t^j\right) = \omega$" by $\Gamma_j^{(t)}$. Because encoding at any sink is independent, the sink is successful as long as no failure has occurred up to this node. We obtain

$$\begin{aligned} P_r^{(t)} &= p_r\left(\Gamma_{m+1}^{(t)}\Gamma_m^{(t)}\cdots\Gamma_1^{(t)}\Gamma_0^{(t)}\right) \\ &= \prod_{j=0}^{m} p_r\left(\Gamma_{j+1}^{(t)} \mid \Gamma_j^{(t)}\right) p_r\left(\Gamma_0^{(t)}\right) \\ &\overset{(b)}{=} \prod_{j=0}^{r_t} p_r\left(\Gamma_{j+1}^{(t)} \mid \Gamma_j^{(t)}\right), \end{aligned}$$

where Eq. (b) can be obtained because

$$p_r\left(\Gamma_0^{(t)}\right) = p_r\left(Rank\left(In(s)\right) = \omega\right) \equiv 1.$$

We compute the $p_r\left(\Gamma_{j+1}^{(t)} \mid \Gamma_j^{(t)}\right)$ as follows. According to the definition of the $CUT_{j+1}(t)$, we choose the global decoding kernel of $e \in CUT_{j+1}(t)$, $CUT_j^{out}(t)$. To form the $CUT_{j+1}(t)$, we start with $CUT_j^{out}(t)$, then add channels in $Out(i_j) \cap \mathrm{P}^{(t)} = CUT_{j+1}(t) \cap Out(i_j)$ to the set $CUT_j^{out}(t)$. During the process of adding these vectors, we know that the vectors $f_{e_l} : e_l \in CUT_{j+1}(t) \cap Out(i_j)$ does not fall in the

space $\langle F_t^j \cup \{f_{e_1}, \cdots, f_{e_{l-1}}\}\rangle$ with probability $\prod_{l=\delta+1}^{k}\left(1-\frac{1}{q^l}\right)$ by applying Corollary 2 because $CUT_j^{out}(t)=\varnothing$ in the network model shown in **Fig. 1**. In the derivation, we get

$$P_r^t=\prod_{j=0}^{r_t}\prod_{l=\delta+1}^{k}\left(1-\frac{1}{q^l}\right)=\left[\prod_{l=\delta+1}^{k}\left(1-\frac{1}{q^l}\right)\right]^{r_t+1}.$$

When the event $\Gamma_k^{(t)}, \forall t\in T$ occurs at the same time, we can get the decoding probability with all sinks receiving all the source messages successfully

$$P_r=\left[\prod_{l=\delta+1}^{k}\left(1-\frac{1}{q^l}\right)\right]^{m+n},$$

where $\delta=k-\omega$, m and n are the number of internal nodes and sink nodes, respectively. The proof of the theorem is completed.

Appendix B

Proof of Theorem 6

At first, we consider the successful decoding probability $\overline{P_r^t}$. For each channel e_i, if e_i is not deleted from the network, we call "e_i is successful". We define $\overline{f_i}$ as the active global encoding kernel of e_i, where

$$\overline{f_{e_i}}=\begin{cases} f_{e_i}, & e_i \text{ is successful;}\\ \underline{0}, & \text{otherwise.}\end{cases}$$

Thus, computing the successful decoding probability is equivalent to the event $\dim\left(\langle \overline{f_e}\rangle\right)=\omega, e\in In(t)$. Further define $\omega\times k$ matrices $\overline{F_t^j}=\left(\overline{f_e}: e\in CUT_j(t)\right)$ for $j=1,\ldots,m+1$.

We use $\overline{\Gamma_t^j}$ to denote the event "$Rank\left(\overline{F_t^j}=\omega\right)$". Intuitively, $\overline{F_t^{r_t+1}}=\overline{F_t}$. Because encoding at any sink is independent, we have

$$\begin{aligned}\overline{P_r^t}&=\overline{p_r}(\overline{\Gamma_{m+1}^{(t)}}\,\overline{\Gamma_m^{(t)}}\cdots\overline{\Gamma_1^{(t)}}\,\overline{\Gamma_0^{(t)}})\\&=\prod_{j=0}^{m}\overline{p_r}(\overline{\Gamma_{j+1}^{(t)}}|\overline{\Gamma_j^{(t)}}\,\overline{p_r}\,\overline{\Gamma_0^{(t)}})\\&\overset{(c)}{=}\prod_{j=0}^{r_t}\overline{p_r}(\overline{\Gamma_{j+1}^{(t)}}|\overline{\Gamma_j^{(t)}})\end{aligned}\qquad(20)$$

where Eq. (c) can be obtained because the channel failure probability over imaginary incoming channels is p=0 and

$$p_r\left(\Gamma_0^{(t)}\right)=p_r\left(Rank\left(In(s)\right)=\omega\right)\equiv 1.$$

According to the definition of the $CUT_{j+1}(t)$, we choose the global coding kernel of $e\in CUT_{j+1}(t)$, $CUT_j^{out}(t)$. To form the $CUT_{j+1}(t)$, we start with $CUT_j^{out}(t)$, then add

channels in $CUT_{j+1}(t)\cap Out(i_j)$ to the set $CUT_j^{out}(t)$. Under the condition $CUT_j^{out}(t)=\varnothing$, we obtain have $CUT_{j+1}(t)=Out(i_j)\cap \mathrm{P}^{(t)}=CUT_{j+1}(t)\cap Out(i_j)$. Denote β_l^{j+1} be the event that "there are $l\left(\omega\le l\le k\right)$ successful channels in the process of adding channels to form $CUT_{j+1}(t)$" i.e., $CUT_{j+1}(t)=\{e_1,\cdots,e_l\}$.

We calculate

$$\overline{p_r}\left(\overline{\Gamma_{j+1}^{(t)}}|\overline{\Gamma_j^{(t)}}\right)=\sum_{l=\omega}^{k}p_r\left(\beta_l^{j+1}\right)p_r\left(\Gamma_{j+1}^{(t)}|\ \Gamma_j^{(t)},\beta_l^{j+1}\right) \tag{21}$$

in two steps as follows.

The probability that there are $l\left(\omega\le l\le k\right)$ successful channels is given by

$$p_r\left(\beta_l^{j+1}\right)=\binom{k}{l}p^{k-l}\left(1-p\right)^l \tag{22}$$

Then, for a fixed value of j, we can write the probability

$$p_r\left(\Gamma_{j+1}^{(t)}|\ \Gamma_j^{(t)},\beta_l^{j+1}\right)=\prod_{i=l-\omega+1}^{l}\left(1-\frac{1}{q^i}\right) \tag{23}$$

By replacing Eq. (24) and Eq. (25) in Eq. (23), we have

$$\overline{p_r}\left(\overline{\Gamma_{j+1}^{(t)}}|\overline{\Gamma_j^{(t)}}\right)=\sum_{l=\omega}^{k}\binom{k}{l}\left(1-p\right)^l p^{k-l}\prod_{i=l-\omega+1}^{l}\left(1-\frac{1}{q^i}\right) \tag{24}$$

In the derivation, we have

$$\begin{aligned}\overline{p_r^t}&=\prod_{j=0}^{r_t}\overline{p_r}\left(\overline{\Gamma_{j+1}^{(t)}}|\overline{\Gamma_j^{(t)}}\right)\\&=[\sum_{l=\omega}^{k}\binom{k}{l}\left(1-p\right)^l p^{k-l}\prod_{i=l-\omega+1}^{l}\left(1-\frac{1}{q^i}\right)]^{r_t+1}.\end{aligned}$$

When the event $\overline{\Gamma_j^{(t)}},\forall t\in T$ occurs at the same time, we can get the decoding probability with all sinks receiving all the source messages successfully

$$\overline{p_r}=[\sum_{l=\omega}^{k}\binom{k}{l}\left(1-p\right)^l p^{k-l}\prod_{i=l-\omega+1}^{l}\left(1-\frac{1}{q^i}\right)]^{m+n}.$$

The proof is completed.

References

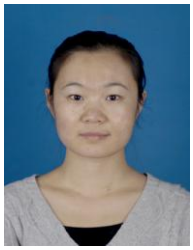
[1] L. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no.4, pp. 1204-1216, Jul. 2000. Article (CrossRef Link)

[2] Y Zou, J Zhu, B Zheng, "A fully distributed opportunistic network coding scheme for cellular relay networks," *Wireless Communications and Networking Conference (WCNC)*, pp. 2937-2942, 2013. Article (CrossRef Link)

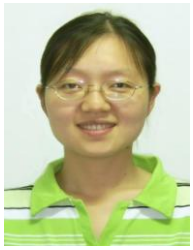
[3] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 371-381, Feb. 2003. Article (CrossRef Link)

[4] T. Ho, M. Médard, R. Koetter, D. Karger, M. Effros, J. Shi and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4 413-4430,

Oct. 2006. Article (CrossRef Link)
[5] H. Balli, X. Yan, and Z. Zhang, "On randomized linear network codes and their error correction capabilities," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3148-3160, Jul. 2009. Article (CrossRef Link)
[6] O. Trullols-Cruces, J.M. Barcelo-Ordinas, and M. Fiore, "Exact decoding probability under random linear network coding," *IEEE Commun. Lett.*, vol. 15, no. 1, pp. 67-69, Jan. 2011. Article (CrossRef Link)
[7] Xubo Zhao, "Notes on 'Exact Decoding Probability Under Random Linear Network Coding'," *IEEE Commun. Lett.*, vol. 16, No. 5, May 2012. Article (CrossRef Link)
[8] Carla-Fabiana Chiasserini, Emanuele Viterbo, and Claudio Casetti, "Decoding Probability in Random Linear Network Coding with Packet Losses," *IEEE Commun. Lett.*, vol. 17, No. 11, November 2013. Article (CrossRef Link)
[9] S. Bose, D. F. Gayme, S. Low and K. M. Chandy, "Optimal power flow over tree networks," in *Proc. of 49th Annu. Allerton Conf. Communication, Control, and Computing*, pp.1342-1348, 2011. Article (CrossRef Link)
[10] A. J. Bhavnagarwala, Ashok Kapoor, and J. D. Meindl, "Generic models for interconnect delay across arbitrary wire-tree networks," *Interconnect Technology Conference*, pp. 129-131, 2000. http://dx.doi.org/10.1109/IITC.2000.854302
[11] X. Ma, Q.-Y. Huang, X.-M. Shu, and Q.-Y. Lu, "Design and implementation of one redundancy function in wireless tree networks," in *Proc. of 2012 International Conference on MIC*, IEEE, 2012. Article (CrossRef Link)
[12] S.-H. Lee and S.-Y. Chung, "Capacity of a class of multicast tree networks," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3848-3857, 2013. Article (CrossRef Link)
[13] Kohavi, Zvi and Israel Berger, "Fault Diagnosis in Combinational Tree Networks," *IEEE Trans. Comp.*, pp.1161-1167, 1975. Article (CrossRef Link)
[14] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782-795, Oct. 2003. Article (CrossRef Link)
[15] N. Cai, *Network Coding Theory*, Now Publishers Inc, 2006.
[16] J.H. van Lint and R. M. Wilson, *A course in Combinatorics*, 2nd edition, Cambridge university press, 2001. Article (CrossRef Link)



Fang LI was born in 1986. She received the B.S. degree in information and computing science from Shangqiu Normal University, China in June 2009. She studied for M.S. degree in cryptography from Xidian University, China in September 2009. She is currently working towards her Ph.D. degree in cryptography at Xidian University, China. Her current research interest includes network coding and information theory.



Min XIE is now an associate professor at Xidian University. Her main research interest are stream ciphers, block ciphers, information theory, and network coding. She received her Ph.D degree in applied mathematics from Graduate from University of Chinese Academy of Sciences in 2003.