WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. 2013; **13**:577–592
Published online 30 March 2011 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/wcm.1122

RESEARCH ARTICLE

Random network coding-based optimal scheme for perfect wireless packet retransmission problems

Zhenguo Gao[1,2,3]*, Weidong Xiang[3], Yunlong Zhao[2], Jing Zhao[2], Shaobin Cai[2], Wu Pan[3], Hua Jiang[3] and Huiqiang Wang[2]

[1] College of Automation, Harbin Engineering University, Harbin 150001, China
[2] College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China
[3] Department of Electrical and Computer Engineering, University of Michigan, Dearborn, MI 48141, U.S.A.

ABSTRACT

Solving wireless packet retransmission problems (WPRTPs) using network coding (NC) approach is increasingly attracting research efforts. However, existing researches are almost all focused on solutions in Galois field GF(2), and consequently, the solutions found by these schemes are usually less optimal. In this paper, we focus on optimal NC-based scheme for perfect WPRTPs (P-WPRTPs) where, with respect to each receiver, a packet is either requested by or already known to it. The number of retransmitted packets in optimal NC-based solutions to P-WPRTPs is firstly analyzed and proved. Then, random network coding-based optimal scheme (RNCOPT) is proposed for P-WRPTPs. RNCOPT is optimal in the sense that it guarantees to obtain a valid solution with minimum number of packet retransmissions. Furthermore, in RNCOPT, each coding vector is generated using a publicly known pseudorandom function with a randomly selected seed. The seed, instead of the coding vector, is used as decoding information to be retransmitted together with the coded packet. Thus, packet overhead of RNCOPT is reduced further. Extensive simulations show that RNCOPT distinctively outperforms some previous typical schemes for P-WPRTPs in saving the number of retransmitted packets. Copyright © 2011 John Wiley & Sons, Ltd.

KEYWORDS
perfect wireless packet retransmission problem; random network coding; optimal scheme

***Correspondence**
Zhenguo Gao, College of Automation, Harbin Engineering University, Harbin 150001, China.
E-mail: gag@hrbeu.edu.cn

1. INTRODUCTION

Because of erroneous wireless links, packet retransmission is necessary in wireless networks. One typical problem related to packet retransmission in wireless broadcast/multicast applications, named as wireless packet retransmission problem (WPRTP) in this paper, has attracted some research efforts in recent years [1–6]. A typical scenario for WPRTPs is as follows [1]. One sender and several receivers in a wireless network form a local system where all the receivers are in the radio range of the sender. The sender has a set of packets that need to be transmitted to the receivers, whereas each receiver has already obtained a subset of the packets through other ways, such as previous communications. Thus, each receiver individually requests the sender to retransmit a subset of the packets. The set of the packets requested by a receiver is called as its *Want* set, whereas the set of the packets already known to it is called as its *Has* set. Hence, the sender has to retransmit some packets. In order to reduce communication overhead, the number of the packets retransmitted by the sender should be minimized. Thus, a WPRTP emerges: how to perform packet retransmissions so as to minimize the total number of retransmitted packets.

The newly invented network coding (NC) [7] technology provides an interesting approach to many network problems. The term NC was first coined in 2000 by Ahlswede *et al.* [7]. Its core notation is to allow and encourage mixing of packets at intermediate nodes. Previous studies [8,9] have showed that NC can increase network throughput, enhance robustness, improve fairness, and reduce complexity of techniques in wireless networks by exploiting the intrinsic characteristics of wireless networks, such as data redundancy, broadcast nature of wireless transmissions, and spatial diversity. NC has been adopted in many research topics in wireless networks, such as multicast [10], unicast [11], and fault tolerance [12]. The invention of random network coding (RNC) [13] makes it more suitable for distributed applications.

Network coding also provides a promising approach to WPRTPs. By using NC, the sender can combine original packets into several coded packets and then transmit these coded packets instead of the original packets. If properly designed, each receiver could obtain all the packets in its *Want* set by decoding from the received coded packets. If the number of the coded packets transmitted by the sender is smaller than that of the original packets requested by the receivers, overhead in the metric of packet transmissions could be reduced.

Because of its theoretical significance and applications in wireless *ad hoc* networks, although named variously in the literature (such as the index coding problem [4] and the local mixing problem [6]), WPRTP has attracted a significant attention from the research community. Most existing works, such as [1,4–6], focused on theoretical perspectives of the problem, whereas some works [1–3] proposed some NC-based schemes for WPRTPs. Several other works, such as [14,15], although not focusing on WPRTPs exclusively, proposed some schemes that can be used to solve WPRTPs. However, these NC-based schemes search for NC solutions only on Galois field GF(2). Because finding optimal NC-based solutions to WPRTPs on GF(2) is an NP (Non-deterministic Polynomial time)-complete problem [1], the solutions found by these schemes are usually less optimal. Fortunately, for a subset of WPRTPs named as perfect WPRTPs (P-WPRTPs) where, for each receiver, a packet must be either in its *Want* set or in its *Has* set, we found that the minimum number of retransmitted packets in valid NC-based solutions on larger Galois fields can be determined easily.

In this paper, we focus on P-WPRTPs and try to analyze the number of retransmitted packets in optimal NC-based solutions to P-WPRTPs (in this paper, we only consider linear NC). Although the set of P-WPRTPs is only a subset of WPRTPs, an optimal NC-based solution to a P-WPRTP can be used as a first-attempt solution to the related WPRTPs.

The rest of the paper is organized as follows. Section 2 gives a review on related work. Section 3 provides the preliminaries of this work including the definitions related to WPRTPs and the operating processes of the sender and the receivers in general NC-based schemes to WPRTPs. Section 4 proposes and proves a theorem about the number of retransmitted packets in optimal NC-based solutions to P-WPRTPs, then mathematically analyzes the relative superiority of optimal NC-based solutions over traditional non-NC-based solutions in the metric of the number of retransmitted packets. In Section 5, an optimal scheme named random network coding-based optimal scheme (RNCOPT) is proposed for P-WPRTPs. In RNCOPT, each coding vector is generated using a publicly known pseudorandom function with a randomly selected seed. The seed, instead of the coding vector, is used as decoding information to be retransmitted together with the coded packet. Section 6 verifies the theoretical results and compares the performance of RNCOPT with some typical schemes for P-WPRTPs through simulations using MATLAB (a numerical computing environment developed by The MathWorks, Inc., Natick, Massachusetts, USA). Section 7 concludes the paper.

2. RELATED WORK

Mathematical background of NC is the Galois field theory. All calculations in NC are performed on a selected Galois field. In computer science, a Galois field is usually notated as GF(2^d) where d is an integer and $d \geq 1$.

Although named variously in the literature (such as the index coding problem [4] and the local mixing problem [6]), WPRTP has attracted a significant attention from the research community because of its theoretical significance and applications in wireless *ad hoc* networks. Most existing works, such as [1,4–6], focused on theoretical perspectives of the problem, whereas some works [1–3] proposed some NC-based schemes for WPRTPs. Several other works, such as [14,15], although not focusing on WPRTPs exclusively, proposed some schemes that can be used to solve WPRTPs.

In [5], Bar-Yossef *et al.* studied WPRTPs from a graph-theoretical perspective. They showed that a WPRTP is equivalent to finding the *minrank* of a corresponding graph. However, the latter is an intractable problem [4]. In [6], Wu *et al.* studied the information-theoretical aspects of the problem with the goal of characterizing the admissible rate region. In [1], El Rouayheb *et al.* proved that finding optimal NC-based solutions for WPRTPs is an NP-complete problem on GF(2). They then, in [4], analyzed the relation between WPRTPs and the more general NC problem, as well as the problem of finding a linear representation of a matroid. They showed that any instance of the NC problem and the matroid representation problem can be efficiently reduced to a WPRTP instance, and consequently, many important properties of the two problems carry over to WPRTPs.

In recent years, some works [1–3] began to focus on NC-based schemes for WPRTPs. However, these schemes search for solutions only on GF(2), where the coding and decoding calculations are both bitwise XOR operations.

El Rouayheb *et al.* [1] proposed a heuristic scheme for WPRTPs on GF(2). In their scheme, a WPRTP is firstly transformed to a new WPRTP where the size of the *Want* set of each receiver is just one. The transformation is performed by substituting a receiver that wants multiple packets with a set of new receivers such that (i) the *Has* set of each new receiver is equal to that of the original receiver, (ii) the *Want* set of each receiver contains just one packet in the *Want* set of the original receiver, and (iii) the union of all the *Want* sets of the new receivers equals to the *Want* set of the original receiver. Then an undirected graph $G(V, E)$ is constructed according to the new WPRTP such that (i) for each receiver, there is a corresponding vertex in

DOI: 10.1002/wcm

$G(V, E)$ and (ii) an edge exists between a pair of vertexes in $G(V, E)$ if and only one of the following two conditions hold for the two receivers corresponding to the two vertexes: (a) the two receivers have identical *Want* set, and (b) the *Want* set of each of the two receivers is a subset of the *Has* set of the other. At last, a heuristic algorithm is used to find a solution to the graph coloring problem of the complimentary graph of $G(V, E)$, and the solution is transformed to a final solution as follows: the *Want* sets of all the receivers that correspond to the set of vertexes with the same color are combined into one coded packet, and all such coded packets corresponding to the node sets with different colors in the complimentary graph make up a solution to the original WPRTP. In the following text, this scheme is designated as ColorNC. As the authors have mentioned, solutions found by ColorNC are usually suboptimal.

Xu *et al.* [2] also adopted graph theory to search for solutions for P-WPRTPs by transforming P-WPRTPs to clique partition problems of the corresponding graphs. Hence, this scheme is designated as CliqueNC in the following text. In CliqueNC, the graph $G(V, E)$ of a WPRTP is constructed according to the following two steps: (i) create a node in $G(V, E)$ for each packet, and (ii) for any pair of packets, create an edge in $G(V, E)$ if and only if no receiver whose *Want* set includes both packets. The edge creation criterion in CliqueNC assures that, if a pair of nodes in $G(V, E)$ is connected by an edge (denotes the two packets corresponding to the two nodes as p_1 and p_2, respectively), the sender can broadcast a coded packet $p_1 \oplus p_2$ (here, $\oplus$ represents bitwise XOR). When receiving the coded packet, all the corresponding receivers could obtain either p_1 or p_2 by decoding. Based on this property, a clique in $G(V, E)$ is transformed into a coded packet, and the set of all the coded packets transformed from the cliques in $G(V, E)$ makes up a valid solution to the corresponding P-WPRTP. Thus, the number of coded packets in a CliqueNC solution is equal to the number of cliques $G(V, E)$.

Nguyen *et al.* [3] proposed two NC-based packet retransmission schemes for P-WPRTPs in reliable wireless broadcast applications. The two NC-based schemes are named Scheme C (time-based retransmission) and Scheme D (improved time-based retransmission), respectively. In the two schemes, the sender does not retransmit the lost packet immediately when it receives a negative acknowledgment (NAK). Instead, the sender maintains a list of lost packets and their corresponding receivers for which their packets are lost. The sender waits until n packets have been transmitted before any retransmission takes place. Then, the sender changes to packet retransmission phase. In this phase, the sender forms a coded packet by XORing a maximum set of the lost packets from different receivers with the condition that each receiver has at most one *Wanted* packet in the packet set, and then, the XORed packet is broadcasted to the receivers. In Scheme C, the sender will keep retransmitting the XORed packet until all the receivers have received the XORed packet correctly. Obviously, Scheme C is suboptimal because the sender has to retransmit the same XORed packet regardless of the cases that some receivers may have already received it. Hence, Scheme D is proposed where the sender dynamically determines the set of the packets to be XORed on the fly and retransmits the new XORed packet. It is easy to notice that the basic idea of the two schemes is essentially the same to that of CliqueNC.

Besides those works focused on schemes for WPRTPs, some works [14,15] not focusing on WPRTPs exclusively also proposed some schemes that can be used to solve WPRTPs.

In [14], a new architecture for wireless mesh networks named as COPE (Coding Opportunistically) was proposed where routers can mix packets from different flows by using NC. The core problem of packet mixing is to determine the set of packets to be XORed so as to maximize the number of next-hop nodes that can recover a *Wanted* packet from the XORed packet. Obviously, this problem is indeed a WPRTP. The basic rule governing packet mixing in COPE, which can be used to solve WPRTPs, is as follows: the routers can XOR n packets together only if each next-hop node has all the other $n - 1$ packets. It is easy to notice that the rule in COPE is basically the same as that in CliqueNC.

Noticing some cases where NC opportunities are neglected by COPE, Dong *et al.* [15] proposed a robust coding technique named loop coding, where the corresponding coding graph contains some loops. Loop coding enhances robusticity at the expense of efficiency by XORing only two packets into one coded packet. Hence, with respect to WPRTPs, the loop coding is less efficient than COPE.

3. OPERATIONS OF NETWORK CODING-BASED SCHEMES FOR WIRELESS PACKET RETRANSMISSION PROBLEMS

3.1. Preliminaries

Definition 1. *Wireless packet retransmission problem (WPRTP). WPRTP can be described as a four-element tuple:*

$$\text{WPRTP} = \{P, R, \{H_i\}, \{W_i\}\}$$

where (i) $P = \{p_i | i \in \{1, 2, \ldots, |P|\}\}$ *represents the set of the packets considered in the problem;* (ii) $R = \{r_i | i \in \{1, 2, \ldots, |R|\}$ *represents the set of the receivers;* (iii) H_i *is the Has set of receiver* r_i*, that is, the set of the packets already known to receiver* r_i*, and thus,* $\{H_i\}$ *represents the set of the Has sets of all the receivers; and* (iv) W_i *is the Want set of receiver* r_i*, that is, the set of the packets requested by receiver* r_i*, and thus,* $\{W_i\}$ *represents the set of the Want sets of all the receivers.*

Definition 2. *Valid solutions to a WPRTP. A solution to a WPRTP is valid if all the receivers can obtain all the* *packets in their Want sets by decoding after receiving all the retransmitted packets in the solution.*

Definition 3. *Optimal solutions to a WPRTP. An optimal solution to a WPRTP is a valid solution with minimum number of retransmitted packets.*

Definition 4. *Perfect WPRTPs (P-WPRTPs). A WPRTP is a P-WPRTP if for $\forall r_i \in R$, $P = H_i \cup W_i$.*

Definition 5. *Imperfect WPRTPs (IP-WPRTPs). A WPRTP is an IP-WPRTP if $P \supset H_i \cup W_i$ holds for at least one receiver.*

This paper is focused on P-WPRTPs. Additionally, we assumed that $P = H_i \cup W_i$ for all $i \in \{1, 2, \ldots, |R|\}$. Otherwise, we can set $P = \bigcup_{r_i \in R} W_i$ and let $H_i = P - W_i$ for all $i \in \{1, 2, \ldots, |R|\}$. Obviously, an optimal/valid solution to the reduced P-WPRTP must also be an optimal/valid solution to the old P-WPRTP. In the following text, WPRTP refers to P-WPRTP unless explicitly specified.

3.2. Coding and decoding calculations in network coding

Calculations in NC are all performed on a selected GF(2^d). In NC, a packet of length L is considered as a list of symbols (or called as elements) on GF(2^d), and the size of the list is $\lceil L/d \rceil$. Here, $\lceil x \rceil$ means the least integer not less than x. Several bits will be appended to the packet if L is not exactly dividable by d. Coding calculation is performed following Equation (1) on GF(2^d) (in this paper, we only consider linear NC).

$$\boldsymbol{P}_\mathrm{Y} = \boldsymbol{M} \cdot \boldsymbol{P}_\mathrm{X} \tag{1}$$

where

$$\boldsymbol{P}_\mathrm{Y} = \begin{bmatrix} p_{\mathrm{Y},1} \\ p_{\mathrm{Y},2} \\ \vdots \\ p_{\mathrm{Y},k} \end{bmatrix} = \begin{bmatrix} y_{1,1} & y_{1,2} & \cdots & y_{1,\lceil L/d \rceil} \\ y_{2,1} & y_{2,2} & \cdots & y_{2,\lceil L/d \rceil} \\ \vdots & \vdots & \ddots & \vdots \\ y_{k,1} & y_{k,2} & \cdots & y_{k,\lceil L/d \rceil} \end{bmatrix},$$

$$\boldsymbol{M} = \begin{bmatrix} m_{1,1} & m_{1,2} & \cdots & m_{1,n} \\ m_{2,1} & m_{2,2} & \cdots & m_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{k,1} & m_{k,2} & \cdots & m_{k,n} \end{bmatrix},$$

$$\boldsymbol{P}_\mathrm{X} = \begin{bmatrix} p_{\mathrm{X},1} \\ p_{\mathrm{X},2} \\ \vdots \\ p_{\mathrm{X},n} \end{bmatrix} = \begin{bmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,\lceil L/d \rceil} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,\lceil L/d \rceil} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n,1} & x_{n,2} & \cdots & x_{n,\lceil L/d \rceil} \end{bmatrix}$$

In Equation (1), k coded packets $p_{\mathrm{Y},i}$ $(i = \{1, 2, ..., k\})$ are created from n original packets $p_{\mathrm{X},i}$ $(i = \{1, 2, ..., n\})$ using NC coefficient matrix $\boldsymbol{M}$ (called as coding matrix).

When transmitting packets using NC, the coded packet and some auxiliary information for decoding such as the coding vector used in creating the coded packet should also be enclosed in an assembled packet, and then, the assembled packet is broadcasted to the receivers. After receiving enough assembled packets, the receivers can construct an equation system similar to Equation (1). In decoding, some elimination methods (such as the Gauss elimination method [9]) can be performed on Equation (1) to obtain all the original packets.

Although coding and decoding calculations are performed on GF(2^d) symbols, we will say that coding calculations are performed on packets for simplicity because all the symbols in a packet are treated using the same coding matrix.

3.3. Operation processes of general network coding-based schemes for wireless packet retransmission problems

Network coding-based schemes for WPRTPs adopt similar operation processes. Major differences between different schemes lie in the parameters of their solutions, such as the number of coded packets, coding matrix, and the decoding information to be transmitted. Coding and decoding processes of general NC-based schemes for WPRTPs are as follows.

3.3.1. General operation process of the sender

Suppose that a solution to a WPRTP has been determined by an NC-based scheme, and the basic parameters of the solution are as follows: (i) the number of coded packets to be retransmitted is k and (ii) the coding matrix is M. Using this solution, the sender will retransmit packets. The general operation process of the sender is as follows (suppose that $|P| = n$):

(1) Calculate the vector of k coded packets $\boldsymbol{P}_\mathrm{Y} = [p_{\mathrm{Y},1}, p_{\mathrm{Y},2}, \ldots, p_{\mathrm{Y},k}]^\mathrm{T}$ by using $\boldsymbol{P}_\mathrm{Y} = \boldsymbol{M}_{k \times n} \times \boldsymbol{P}_\mathrm{X}$; here, $\boldsymbol{P}_\mathrm{X} = [p_{\mathrm{X},1}, p_{\mathrm{X},2}, \ldots, p_{\mathrm{X},n}]^\mathrm{T} = [p_1, p_2, \ldots, p_n]^\mathrm{T}$.

(2) Construct k assembled packets $p_{Z,i} = \{D_i, p_{\mathrm{Y},i}\}$, $i \in \{1, 2, \ldots, k\}$. Here, D_i represents auxiliary information for decoding, such as the coding vector used in creating $p_{\mathrm{Y},i}$. Actual information in D_i depends on the scheme used to solve the WPRTP.

(3) Broadcast all the assembled packets $p_{Z,i}$, $i \in \{1, 2, \ldots, k\}$.

3.3.2. General operation process of the receivers

When receiving assembled packets retransmitted by the sender, all the receivers perform the same process to obtain the packets in their *Want* sets. The general operation process of receiver r_i is as follows:

(1) For each packet $p_{i,j}$ in H_i, determine its order $x(i, j)$ in P and create a row vector v_j of length

n according to Equation (2), that is, the $x(i, j)$-th element of v_j is 1, and the other elements are all 0.

$$v_{j,\,t} = \begin{cases} 1 & t = x(i,\ j) \\ 0 & t \in \{1, ..., n\} \text{ and } t \neq x(i,\ j) \end{cases} \tag{2}$$

(2) Assemble all row vectors $v_i (i = \{1, 2, \ldots, |n_i|\})$ created in step (1) into a matrix $\boldsymbol{V}_{n_i \times n}$ with size $n_i \times n$, as shown in Equation (3); here $n_i = |H_i|$.

$$\boldsymbol{V}_{n_i \times n} = \begin{bmatrix} v_1 \\ \vdots \\ v_{n_\mathrm{i}} \end{bmatrix} = \begin{bmatrix} v_{1,1} & \cdots & v_{1,j} & \cdots & v_{1,n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ v_{n_i,1} & \cdots & v_{n_i,j} & \cdots & v_{n_i,n} \end{bmatrix} \tag{3}$$

(3) Arrange all packets $p_{\mathrm{H},j}$ $(j \in \{1, 2, \ldots, n_i\})$ in H_i into a column vector $\boldsymbol{P}_\mathrm{H} = [p_{\mathrm{H},1}, p_{\mathrm{H},2}, \ldots, p_{\mathrm{H},n_i}]^\mathrm{T}$.

(4) Upon receiving assembled packets $p_{\mathrm{Z},i} = \{D_i, p_{\mathrm{Y},i}\}$ $(i = \{1, 2, \ldots, k\})$, extract decoding information from D_i, such as coding vector m_i $(i = \{1, 2, \ldots, k\})$, and assemble them into a matrix $\boldsymbol{M}_{k \times n}$ of size $k \times n$.

(5) Assemble $\boldsymbol{V}_{n_i \times n}$ and $\boldsymbol{M}_{k \times n}$ into a hybrid matrix $\boldsymbol{M}'_{(n_i+k) \times n}$ as shown in Equation (4). $M'_{(n_i+k) \times n}$ is called the decoding matrix.

$$\boldsymbol{M}'_{(n_i+k) \times n} = \begin{bmatrix} \boldsymbol{V}_{n_i \times n} \\ \boldsymbol{M}_{k \times n} \end{bmatrix} \tag{4}$$

(6) Extract all coded packets $p_{\mathrm{Y},i}$ $(i = \{1, 2, \ldots, k\})$ from assembled packets $p_{\mathrm{Z},i} (i = \{1, 2, \ldots, k\})$ and construct a column vector $\boldsymbol{P}_\mathrm{Y} = [p_{\mathrm{Y},1}, p_{\mathrm{Y},2}, \ldots, p_{\mathrm{Y},k}]^\mathrm{T}$.

(7) Assemble $\boldsymbol{P}_\mathrm{H}$ and $\boldsymbol{P}_\mathrm{Y}$ into a longer vector $[P_\mathrm{A}]_{(n_i+k) \times 1}$ according to Equation (5).

$$[P_\mathrm{A}]_{(n_i+k) \times 1} = \begin{bmatrix} [P_\mathrm{H}]_{n_i \times 1} \\ [P_\mathrm{Y}]_{k \times 1} \end{bmatrix} \tag{5}$$

(8) Create an equation system as shown in Equation (6) using $[\boldsymbol{P}_\mathrm{X}]_{n \times 1} = [p_1, p_2, \ldots, p_n]^\mathrm{T}$, $[P_\mathrm{A}]_{(n_i+k) \times 1}$, and $\boldsymbol{M}'_{(n_i+k) \times n}$.

$$\boldsymbol{M}'_{(n_i+k) \times n} \cdot [\boldsymbol{P}_\mathrm{X}]_{n \times 1} = [P_\mathrm{A}]_{(n_i+k) \times 1} \tag{6}$$

(9) Solve Equation (6) on GF(2^d). So long as $rank(\boldsymbol{M}'_{(n_i+k) \times n}) = n$, receiver r_i will surely be able to obtain all packets in W_i; here and in the following text, $rank(\cdot)$ represents a function that calculates the rank of the input matrix on the selected Galois field.

(10) End.

4. NUMBER OF CODED PACKETS IN OPTIMAL NETWORK CODING-BASED SOLUTIONS TO PERFECT WIRELESS PACKET RETRANSMISSION PROBLEMS

Although several coded packets can be assembled into one assembled packet, in this paper, we consistently assume that one assembled packet contains only one coded packet. Thus, the number of retransmitted assembled packets is equal to the number of the coded packets in a valid NC-based solution.

About the number of retransmitted packets in optimal NC-based solutions to P-WPRTPs, we have the following Theorem 1.

Theorem 1. *Given that the used Galois field is sufficiently large, the number of the retransmitted packets in optimal linear NC-based solutions to P-WPRTP(*$P, R, \{H_i\}, \{W_i\}$*) is* $\max_{r_i \in R} |W_i|$.

Proof. In the proof, WPRTP refers to P-WPRTP. Suppose that the number of retransmitted packets in an optimal NC-based solution to WPRTP $(P, R, \{H_i\}, \{W_i\})$ is k. We now prove that $k = \max_{r_i \in R} |W_i|$ in the following two steps: (i) to prove that $k \geq \max_{r_i \in R} |W_i|$ and (ii) to prove that $k \leq \max_{r_i \in R} |W_i|$. If both $k \geq \max_{r_i \in R} |W_i|$ and $k \leq \max_{r_i \in R} |W_i|$ are proved, then there must be $k = \max_{r_i \in R} |W_i|$.

(1) To prove that $k \geq \max_{r_i \in R} |W_i|$

We will prove it by showing that for any valid NC-based solution to the WPRTP, the number of retransmitted packets in the solution, which is denoted as k', must be not less than $\max_{r_i \in R} |W_i|$, that is, $k' \geq \max_{r_i \in R} |W_i|$. Once $k' \geq \max_{r_i \in R} |W_i|$ is proven, $k \geq \max_{r_i \in R} |W_i|$ can be obtained directly because the discussed solution can be any valid NC-based solution, including any optimal NC-based solution.

According to the decoding process of general NC-based schemes to WPRTPs described in Section 3.3.2, if the number of retransmitted packets is k', then according to Equation (4), the decoding matrix of receiver r_i will be $M'_{(k'+n_i) \times n}$. Because the solution is valid, there must be $rank(M'_{(k'+n_i) \times n}) \geq n$ (here and in the following text, $rank(\cdot)$ returns the rank of the input matrix on the selected Galois field). Hence, $k' + n_i \geq n$ must be true. Thus, Equation (7) must also be true.

$$k' \geq n - n_i \quad i = \{1, 2, \ldots, |R|\} \tag{7}$$

Because for P-WPRTPs, (i) $|H_i| = n_i$, (ii) $|H_i \cup W_i| = |P| = n$, and (iii) $|H_i \cap W_i| = |\varnothing| = 0$, there must be $|W_i| = n - n_i$. Hence, Equation (7) can be transformed to Equation (8).

$$k' \geq |W_i| \quad i = \{1, 2, \ldots, |R|\} \tag{8}$$

Because Equation (8) is valid for any receiver r_i, Equation (9) must follow

$$k' \geq \max_{r_i \in R} |W_i| \tag{9}$$

Because k' in Equation (9) denotes the number of retransmitted packets in any valid NC-based solutions to the WPRTP, Equation (9) must also be valid for all optimal valid NC-based solutions. Therefore, the number of retransmitted packets in optimal NC-based solutions to the WPRTP, which is denoted as k, must also follow Equation (9), that is, $k \geq \max_{r_i \in R} |W_i|$. Thus, the first step of the proof is completed.

(2) To prove that $k \leq \max_{r_i \in R} |W_i|$

Suppose that there is a valid solution to the WPRTP where the number of retransmitted packets equals k'. If $k' \leq \max_{r_i \in R} |W_i|$, the number of retransmitted packets in optimal NC-based solutions to the WPRTP, which is denoted as k, must follow $k \leq k' \leq \max_{r_i \in R} |W_i|$. Thus, the second step can be completed easily.

We now prove that $k \leq \max_{r_i \in R} |W_i|$ by constructing a valid NC-based solution with $k' = \max_{r_i \in R} |W_i|$.

Firstly, construct a coding matrix $\boldsymbol{M}_{k' \times n}$ as shown in Equation (10). Here, $k' = \max_{r_i \in R} |W_i|$. Obviously, the coding matrix is a Vandermonde matrix. We assumed that $x_t (t = \{1, 2, ..., n\})$ are all different.

$$\boldsymbol{M}_{k' \times n} = \begin{bmatrix} 1 & \cdots & 1 & \cdots & 1 \\ x_1 & \cdots & x_j & \cdots & x_n \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ x_1^{k'-2} & \cdots & x_j^{k'-2} & \cdots & x_n^{k'-2} \\ x_1^{k'-1} & \cdots & x_j^{k'-1} & \cdots & x_n^{k-1} \end{bmatrix} \tag{10}$$

After having received all the coded packets, receiver r_i constructs its decoding matrix $\boldsymbol{M}'_{(k'+n_i) \times n}$ following the general decoding process described in Section 3.3.2. Because of the special format of the submatrix $\boldsymbol{V}_{n_i \times n}$ shown in Section 3.3.2, $\boldsymbol{M}'_{(k'+n_i) \times n}$ must be able to be transformed to a matrix with the format shown in Equation (11).

$$\boldsymbol{M}'_{(k'+n_i) \times n} = \begin{bmatrix} \boldsymbol{M}_{k' \times (n-n_i)} & 0_{k' \times n_i} \\ 0_{n_i \times (n-n_i)} & \boldsymbol{E}_{n_i \times n_i} \end{bmatrix} \tag{11}$$

In Equation (11), the submatrix $\boldsymbol{M}_{k' \times (n-n_i)}$ has the format shown in Equation (12), and the submatrix $\boldsymbol{E}_{n_i \times n_i}$ is an identity matrix.

$$\boldsymbol{M}_{k' \times (n-n_i)} = \begin{bmatrix} 1 & \cdots & 1 \\ x_{z_1} & \cdots & x_{z_{n-n_i}} \\ \vdots & \ddots & \vdots \\ x_{z_1}^{k'-1} & \cdots & x_{z_{n-n_i}}^{k'-1} \end{bmatrix} \tag{12}$$

Subscripts $z_j (j = \{1, 2, ..., n - n_i\})$ of the elements in the submatrix $\boldsymbol{M}_{k' \times (n-n_i)}$ in Equation (12) is a permutation of the subscripts t of the $n - n_i$ elements in the coding matrix $\boldsymbol{M}_{k' \times n}$. Obviously, submatrix $\boldsymbol{M}_{k' \times (n-n_i)}$ is also a Vandermonde matrix. Considering that $k' = \max_{r_i \in R} |W_i| \geq |W_i| = (n - n_i)$, and removing the rows from the n_i-th row to the k'-th row in $\boldsymbol{M}_{k'} \times (n - n_i)$, a matrix $\boldsymbol{M}'_{n \times n}$ shown in Equation (13) is obtained.

$$\boldsymbol{M}'_{n \times n} = \begin{bmatrix} \boldsymbol{M}_{(n-n_i) \times (n-n_i)} & 0_{(n-n_i) \times n_i} \\ 0_{n_i \times (n-n_i)} & \boldsymbol{E}_{n_i \times n_i} \end{bmatrix} \tag{13}$$

According to the property of Vandermonde determinant [16] and with the assumption in the theorem that the selected Galois field is large enough, Equation (14) can be obtained where the last inequality results from the assumption that $x_t (t \in \{1, 2, ..., n\})$ in $\boldsymbol{M}_{k' \times n}$ are all different.

$$\begin{aligned} |\boldsymbol{M}'_{n \times n}| &= |E_{n_\mathrm{i} \times n_\mathrm{i}}||\boldsymbol{M}'_{(n-n_\mathrm{i}) \times (n-n_\mathrm{i})}| \\ &= \prod_{1 \leq j < k \leq (n-n_i)} (x_{Z_k} - x_{Z_j}) \neq 0 \end{aligned} \tag{14}$$

Hence, $rank(\boldsymbol{M}'_{n \times n}) = n$, which means that all original packets can be decoded out. The receiver r_i discussed here can be any receiver. Hence, each receiver can obtain all the packets in its *Want* set. Therefore, the solution with coding matrix $\boldsymbol{M}_{k' \times n}$ is a valid solution.

Because there is a valid solution $\boldsymbol{M}_{k' \times n}$ where the number of retransmitted packets equals $k' = \max_{r_i \in R} |W_i|$, the number of retransmitted packets in any optimal NC-based solution to the WPRTP, which is denoted as k, must be true for $k \leq k' \leq \max_{r_i \in R} |W_i|$. Thus, the second step of the proof is completed.

Based on the results of the two steps, (i) $k \geq \max_{r_i \in R} |W_i|$ and (ii) $k \leq \max_{r_i \in R} |W_i|$, we obtained the final result $k = \max_{r_i \in R} |W_i|$. Hence, the theorem follows. □

Given a P-WPRTP$\{P, R, \{H_i\}, \{W_i\}\}$, we denoted $|P| = n$, $|R| = r$ and the probability that a packet in P falls into W_i of any given receiver r_i equals p_{Level}. A tuple $(n, r, p_{\mathrm{Level}})$ is called a WPRTP profile. Given a WPRTP profile $(n, r, p_{\mathrm{Level}})$, we have the following theorems about the number of retransmitted packets in traditional non-NC-based solutions (not using NC) and optimal NC-based solutions, respectively.

Theorem 2. *The probability that x packets are to be retransmitted in traditional non-NC-based solutions to WPRTP*$\{P, R, \{H_i\}, \{W_i\}\}$*, denoted as* $p_{\mathrm{NoNC}}(n, r, p_{\mathrm{Level}}, x)$*, is given by Equation (15), and the expected number of retransmitted packets, denoted as* $N_{\mathrm{NoNC}}(n, r, p_{\mathrm{Level}})$*, is given by Equation (16).*

$$\begin{aligned} p_{\mathrm{NoNC}}(n, r, p_{\mathrm{Level}}, x) =& C_n^x (1 - p_{\mathrm{Level}})^{r \cdot (n-x)} \\ & \cdot (1 - (1 - p_{\mathrm{Level}})^r)^x \end{aligned} \tag{15}$$

$$N_{\text{NoNC}}(n, r, p_{\text{Level}}) = \sum_{i=1}^{n} \left(i \cdot \left(C_n^i (1 - p_{\text{Level}})^{r \cdot (n-i)} \cdot (1 - (1 - p_{\text{Level}})^r)^i \right) \right) \tag{16}$$

Proof. Because the probability that a packet falls into W_i of any given receiver r_i equals p_{Level}, the probability that the packet is not being requested by all the receivers, denoted as $p_1(n, r, p_{\text{Level}})$, is given by Equation (17).

$$p_1(n, r, p_{\text{Level}}) = (1 - p_{\text{Level}})^r \tag{17}$$

Then, the probability that the number of the packets that are requested by at least one receiver equals x, denoted as $p_{\text{NoNC}}(n, r, p_{\text{Level}}, x)$, is given by Equation (18).

$$p_{\text{NoNC}}(n, r, p_{\text{Level}}, x) = C_n^x \cdot p_1(n, r, p_{\text{Level}})^{(n-x)} \cdot (1 - p_1(n, r, p_{\text{Level}}))^x \tag{18}$$

In other words, when not using NC, the probability that x packets are to be retransmitted to solve the WPRTP equals $p_{\text{NoNC}}(n, r, p_{\text{Level}}, x)$.

Hence, the expected number of retransmitted packets to solve WPRTP$\{P, R, \{H_i\}, \{W_i\}\}$ without using NC, denoted as $N_{\text{NoNC}}(n, r, p_{\text{Level}})$, is given by Equation (19).

$$\begin{aligned} N_{\text{NoNC}}(n, r, p_{\text{Level}}) &= \sum_{i=0}^{n} (i \cdot p_{\text{NoNC}}(n, r, p_{\text{Level}}, i)) \\ &= \sum_{i=1}^{n} (i \cdot p_{\text{NoNC}}(n, r, p_{\text{Level}}, i)) \end{aligned} \tag{19}$$

Combining Equations (17), (18), and (19), the theorem follows. □

Theorem 3. *The probability that x packets are to be transmitted in an optimal NC-based solution to WPRTP$\{P, R, \{H_i\}, \{W_i\}\}$, denoted as $p_{\text{NCOPT}}(n, r, p_{\text{Level}}, x)$, is given by Equation (20), and the expected number of retransmitted packets, denoted as $N_{\text{NCOPT}}(n, r, p_{\text{Level}})$, is given by Equation (21).*

Proof. The probability that the number of the packets in the *Want* set of a receiver equals x, denoted as $p_2(n, r, p_{\text{Level}}, x)$, is given by Equation (22).

$$p_2(n, r, p_{\text{Level}}, x) = C_n^x \cdot (1 - p_{\text{Level}})^{(n-x)} \cdot p_{\text{Level}}^x \tag{22}$$

The probability that the number of the packets in the *Want* set of a receiver is not larger than x, denoted as $p_3(n, r, p_{\text{Level}}, x)$, is given by Equation (23).

$$p_3(n, r, p_{\text{Level}}, x) = \sum_{i=0}^{x} p_2(n, r, p_{\text{Level}}, i) \tag{23}$$

The probability that the numbers of the packets in the *Want* sets of all the receivers are all not larger than x, denoted as $p_4(n, r, p_{\text{Level}}, x)$, is given by Equation (24).

$$p_4(n, r, p_{\text{Level}}, x) = (p_3(n, r, p_{\text{Level}}, x))^r \tag{24}$$

The probability that the maximum number of the packets in the *Want* sets of all these r receivers equals x, denoted as $p_{\text{NCOPT}}(n, r, p_{\text{Level}}, x)$, is given by Equation (25).

$$p_{\text{NCOPT}}(n, r, p_{\text{Level}}, x) = \begin{cases} p_4(n, r, p_{\text{Level}}, x) - p_4(n, r, p_{\text{Level}}, x - 1) & x > 0 \\ p_4(n, r, p_{\text{Level}}, 0) & x = 0 \end{cases} \tag{25}$$

In other words, when using NC, the probability that x packets should be retransmitted to solve the WPRTP equals $p_{\text{NCOPT}}(n, r, p_{\text{Level}}, x)$.

Hence, the expected number of packet retransmissions in optimal NC-based solutions to WPRTP$\{P, R, \{H_i\}, \{W_i\}\}$, denoted as $N_{\text{NCOPT}}(n, r, p_{\text{Level}})$, is given by Equation (26).

$$\begin{aligned} N_{\text{NCOPT}}(n, r, p_{\text{Level}}) &= \sum_{i=0}^{n} (i \cdot p_{\text{NCOPT}}(n, r, p_{\text{Level}}, i)) \\ &= \sum_{i=1}^{n} (i \cdot p_{\text{NCOPT}}(n, r, p_{\text{Level}}, i)) \end{aligned} \tag{26}$$

Combining Equations (22), (23), (24), (25), and (26), the theorem follows. □

$$p_{\text{NCOPT}}(n, r, p_{\text{Level}}, x) = \begin{cases} \left(\sum\limits_{i=0}^{x} \left(C_n^i \cdot (1 - p_{\text{Level}})^{n-i} \cdot p_{\text{Level}}^i \right) \right)^r - \left(\sum\limits_{i=0}^{x-1} \left(C_n^i \cdot (1 - p_{\text{Level}})^{n-i} \cdot p_{\text{Level}}^i \right) \right)^r & x > 0 \\ (1 - p_{\text{Level}})^{n \cdot r} & x = 0 \end{cases} \tag{20}$$

$$N_{\text{NCOPT}}(n, r, p_{\text{Level}}) = \sum_{i=1}^{n} \left(i \cdot \left(\left(\sum_{i=0}^{x} \left(C_n^i \cdot (1 - p_{\text{Level}})^{n-i} \cdot p_{\text{Level}}^i \right) \right)^r - \left(\sum_{i=0}^{x-1} \left(C_n^i \cdot (1 - p_{\text{Level}})^{n-i} \cdot p_{\text{Level}}^i \right) \right)^r \right) \right) \tag{21}$$

5. RANDOM NETWORK CODING-BASED OPTIMAL SCHEME FOR PERFECT WIRELESS PACKET RETRANSMISSION PROBLEMS

We proposed an optimal NC-based scheme for P-WPRTPs based on RNC. The scheme is optimal in the sense that it guarantees to obtain a valid solution with minimum number of packet retransmissions. Hence, it is called as RNCOPT.

When transmitting packets using NC, the coding vector used to create a coded packet should also be enclosed in the assembled packet and transmitted to the receivers. When the number of original packets to be retransmitted is larger, more bits will be required to store the coding vector in the final assembled packet. To relieve this negative effect, RNCOPT uses the following approach. Each coding vector is created using a publicly known pseudorandom function triggered with a randomly selected seed. The seed instead of the coding vector is enclosed in the assembled packet as auxiliary decoding information. Simulation results showed that the coding matrix created in this way almost makes up all valid solutions in the simulated configurations.

5.1. Parameters of random network coding-based optimal scheme

Random network coding-based optimal scheme has two main parameters: code coefficient bit length q and random seed bit length s. The parameter q controls the range from which code coefficients are selected. To be exact, the coefficients in coding matrix are randomly selected from range $[1, 2^q - 1]$ and treated as elements in Galois field GF(2^d) where $d \geq q$. If $d > q$, we say that the code coefficients are selected from GF(2^q) when there is no confusion. In our simulations in Section 6, d is fixed to 8.

Obviously, random seed bit length s and code coefficient bit length q control the probability that a randomly generated coding matrix in RNCOPT makes up a valid solution. The parameter s restricts the range of the seeds. If s is too small, there will be more cases that some of the randomly selected seeds are the same; hence, a solution using these seeds in RNCOPT will definitely be an invalid solution. Additionally, even if all the selected seeds are different, if q is too small, a randomly generated coding matrix in RNCOPT may also be an invalid solution. Hence, in order to make sure that a randomly generated coding matrix makes up a valid solution, larger s and q are preferred. However, larger s results in longer assembled packets, and larger q leads to increased coding and decoding complexity. Hence, proper values for s and q are of great importance to RNCOPT.

Fortunately, because the seeds are integers, detecting the cases where several seeds are the same is easy, and thus, the negative effect of small s can be eliminated easily in RNCOPT by insuring that all the seeds are different. Additionally, the simulation results in Section 6 show that on the condition that the seeds in a solution are different, a randomly generated coding matrix will probably make up a valid solution to the simulated cases when $q \geq 4$. The simulated cases can cover most scenarios in reality. However, to be conservative, $s = 16$ and $q = 8$ are selected as the default values for s and q in RNCOPT.

Given random seed bit length s and the number of seeds k, the probability that all the k randomly selected seeds are different, denoted as p_{DifSeed}, is given by Equation (27). The values of p_{DifSeed} corresponding to different values of s and k are shown in Figure 1.

$$p_{\text{DifSeed}} = \prod_{i=0}^{k-1} \left(\frac{2^s - i}{2^s} \right) \tag{27}$$

5.2. Operation process of the sender in random network coding-based optimal scheme

Assembled packets in RNCOPT for P-WPRTPs must contain the following two fields: *CodingCoefSeed* and *CodedPacket*. The field *CodingCoefSeed* stores the random seed corresponding to the coded packet. The field *CodedPacket* stores the coded packet. Other auxiliary fields could be appended in assembled packets when necessary in piratical implementation.

In RNCOPT, the operation process of the receivers is the same to that of general NC-based schemes described in Section 3.3.2 except that the coding vector corresponding to each coded packet is reconstructed from the seed stored in the *CodingCoefSeed* field. Comparatively, more modifications are made to the sender's operation process. The operation process of the sender in RNCOPT is as follows:

(1) Let $k = \max_{r_i \in R} |W_i|, n = |P|$.
(2) Create coding matrix $\boldsymbol{M}_{k \times n} = \{m_{i,j}\}_{k \times n}$ with size $k \times n$. Each row vector $m_i = (m_{i,1}, m_{i,2}, \ldots, m_{i,n})$

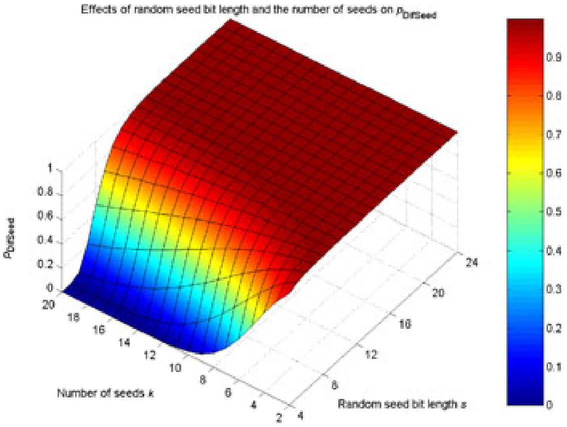


Figure 1. Effects of random seed bit length and the number of seeds on p_{DifSeed}.

is created using the publicly known pseudorandom function from a randomly selected seed $s_i \in [0, 2^s–1]$ that must be different to $s_j (j \in \{1, 2, \ldots, i-1\})$. The range of the random variables created by the random function equals [1, 2^q-1] and treated as elements on GF(2^d).

(3) Check whether $\boldsymbol{M}_{k\times n}$ makes up a valid solution by examining whether the corresponding decoding matrix $\boldsymbol{M}'_{(n_i+k)\times n}$ of each receiver is full rank. If it is true, then go to step (4); otherwise, go to step (2) to reconstruct a coding matrix. Please notice that the sender has enough information to determine the decoding matrix $\boldsymbol{M}'_{(n_i+k)\times n}$of each receiver.

(4) Construct a vector of original packets $\boldsymbol{P}_{\mathrm{X}} = [p_{\mathrm{X},1}, p_{\mathrm{X},2}, \ldots, p_{\mathrm{X},n}]^{\mathrm{T}} = [p_1, p_2, \ldots, p_n]^{\mathrm{T}}$.

(5) Calculate the vector of coded packets $\boldsymbol{P}_{\mathrm{Y}} = [p_{\mathrm{Y},1}, p_{\mathrm{Y},2}, \ldots, p_{\mathrm{Y},k}]^{\mathrm{T}}$ by using $\boldsymbol{P}_{\mathrm{Y}} = \boldsymbol{M}_{k\times n} \times \boldsymbol{P}_{\mathrm{X}}$.

(6) Construct k assembled packets $p_{Z,i} = \{s_i, p_{Y,i}\}$ $(i \in \{1, 2, \ldots, k\})$. Here, s_i represents the corresponding random seed used to create the coding vector for generating $p_{Y,i}$.

(7) Broadcast all assembled packets $p_{Z,i} (i \in \{1, 2, \ldots, k\})$.

5.3. Lengths of assembled packets

The lengths of assembled packets in several schemes for WPRTPs are analyzed in this section. Table I lists all the notations used in the analysis.

Calculations in NC are all performed in a certain Galois field GF(2^d). As a result obtained from the Galois field theory, coded symbols are also symbols in GF(2^d). Hence, the length of a coded symbol is the same as those of the original symbols. Because all packets are considered as a list of symbols, if the length of original packets is not exactly dividable by d, several bits will have to be appended to the packets. However, such cases could be made rare in practice. Hence, in our analysis, the length of a coded packet is assumed to be the same as those of the original packets. Therefore, the length of coded packets in the following analysis is also B.

With notations listed in Table I, the length of assembled packets in RNCOPT is given by Equation (28). The second approximation in Equation (28) results from the assumption that B can usually be divided exactly by d.

$$f_{\mathrm{RNCOPT}}(B, n, d, s) \approx k_{\mathrm{RNCOPT}} \cdot \left(s + d \cdot \left\lceil \frac{B}{d} \right\rceil\right) \approx k_{\mathrm{RNCOPT}} \cdot (s + B) \qquad (28)$$

In traditional scheme not using NC, which is denoted as NoNC in the following text, all packets in $\cup W_i$ should be retransmitted. Hence, the total bit length of all the packets in a solution found by NoNC is given by Equation (29).

$$f_{\mathrm{NoNC}}(B, n, d, s) = k_{\mathrm{NoNC}} \cdot B \qquad (29)$$

Although the format of the assembled packets in CliqueNC was not given in [2], we assume that, besides the field for storing the coded packet, it also contains a field for indicating which packets are selected to create the coded packet in the assembled packet. Here, we named the field *PacketBitFlag*. It can be assumed to be a vector of bits where each bit corresponds to one packet in P. If one bit is 1, the corresponding packet is selected. Otherwise, it is not selected. Thus, the total bit length of all the packets in a solution found by CliqueNC is given by Equation (30).

$$f_{\mathrm{CliqueNC}}(B, n, d, s) = k_{\mathrm{CliqueNC}}(n + B) \qquad (30)$$

We assumed that the format of the assembled packets in ColorNC is identical to that of the assembled packets in CliqueNC. Hence, the total bit length of all the packets in a solution found by ColorNC is given by Equation (31).

$$f_{\mathrm{ColorNC}}(B, n, d, s) = k_{\mathrm{ColorNC}}(n + B) \qquad (31)$$

Considering Equations (28) and (29), RNCOPT will outperform NoNC when Equation (32) follows.

$$\frac{k_{\mathrm{RNCOPT}}}{k_{\mathrm{NoNC}}} < \frac{B}{s + B} \qquad (32)$$

With Equations (28) and (30), RNCOPT will outperform CliqueNC when Equation (33) follows.

$$\frac{k_{\mathrm{RNCOPT}}}{k_{\mathrm{CliqueNC}}} < \frac{n + B}{s + B} \qquad (33)$$

Table I. Notations used in the analysis of the lengths of assembled packets in several schemes.

Notation	Meaning
B	Bit length of an original packet
n	The number of original packets in the target WPRTP
d	Bit length of the symbols in GF(2^d)
s	Random seed bit length
k_{NoNC}	The number of retransmitted packets in the solutions for WPRTPs found by NoNC
k_{RNCOPT}	The number of retransmitted packets in the solutions for WPRTPs found by RNCOPT
k_{ColorNC}	The number of retransmitted packets in the solutions for WPRTPs found by ColorNC
k_{CliqueNC}	The number of retransmitted packets in the solutions for WPRTPs found by CliqueNC

WPRTP, wireless packet retransmission problem; NoNC, traditional scheme not using NC; RNCOPT, random network coding-based optimal scheme.

Similarly, RNCOPT will outperform ColorNC when Equation (34) follows.

$$\frac{k_{\text{RNCOPT}}}{k_{\text{ColorNC}}} < \frac{n+B}{s+B} \tag{34}$$

Suppose that $B = 512$, $n = 5$, and $s = 16$, then according to Equation (32), RNCOPT will outperform NoNC if $k_{\text{RNCOPT}}/k_{\text{NoNC}} < 0.9697$, and RNCOPT will outperform CliqueNC and ColorNC if $k_{\text{RNCOPT}}/k_{\text{CliqueNC}} < 0.9792$ and $k_{\text{RNCOPT}}/k_{\text{ColorNC}} < 0.9792$ according to Equations (33) and (34), respectively. Simulation results in Section 6 show that these conditions are generally always satisfied.

5.4. Application discussion

Random network coding-based optimal scheme, as well as other schemes to WPRTPs, can be used as a substitute for the traditional automatic repeat-request schemes to build more reliable wireless links. RNCOPT can be implemented in real applications where packets are transmitted in batch mode, similar to the way described in [3].

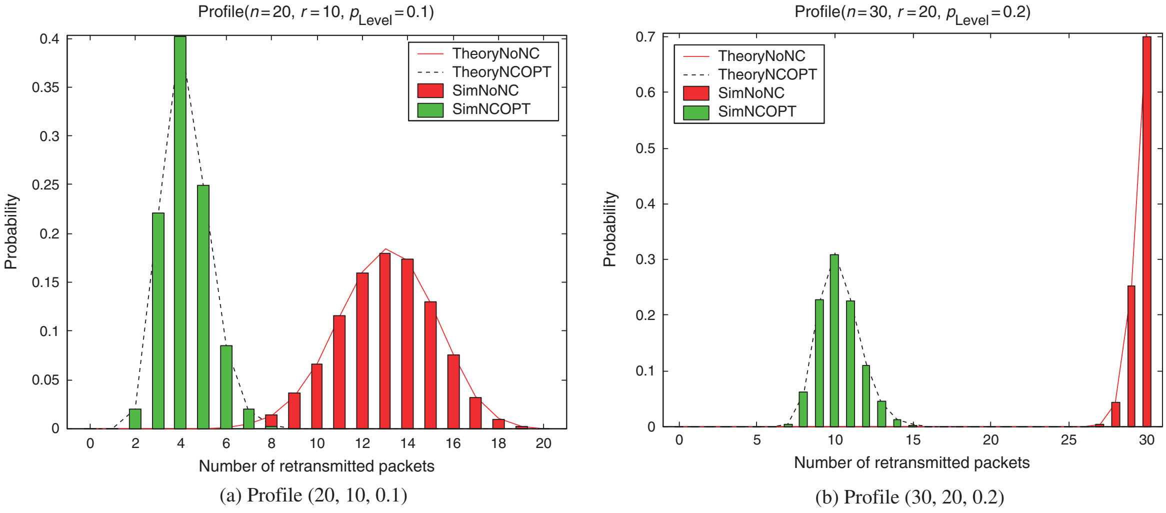
In batch mode packet transmission, a node does not retransmit a lost packet immediately when it receives a negative acknowledgment. Instead, the node maintains a list of lost packets and their corresponding receivers for which their packets are lost. The node waits until all the packets in the current batch have been transmitted. If all packets in the batch have been received correctly by all the receivers, the node then begins to transmit the next batch of packets immediately. Otherwise, it changes to packet retransmission phase. In this phase, the node retransmits some coded packets following RNCOPT; it then waits for responses from the receivers for a predefined long time. The response of a receiver indicates that the receiver has obtained all the packets in the batch. If the node failed to receive responses from all the receivers, it retransmits one coded packet created in the same way as used in RNCOPT and then waits for responses from the receivers for a predefined short time. The sender will continue this process (retransmitting one coded packet and then waiting for responses for a predefined short time) until responses from all the receivers are received. In that case, the packet retransmission phase terminates, and the node then begins to transmit the next batch of packets.

6. THEORETICAL RESULT VERIFICATION AND PERFORMANCE EVALUATION

6.1. Theoretical result verification

We verified Theorems 2 and 3 by using the Monte Carlo simulation. The verification process is as follows. For a WPRTP profile (n, r, p), generate 10 000 instances randomly, then take the statistics of the results, and then compare the statistical results with the theoretical values. Figures 2(a) and 2(b) show the results for profiles (20, 10, 0.1) and (30, 20, 0.2), respectively.

In Figures 2(a) and 2(b), the curves designated as TheoryNoNC and TheoryNCOPT represent the theoretical results obtained using Equations (15) and (20), respectively. Bar charts designated as SimNoNC and SimNCOPT represent the corresponding simulation results. The fine fitness between the simulation results and the theoretical values proves the correctness of Equation (15) in Theorem 2 and Equation (20) in Theorem 3. Consequently, Equation (16) in Theorem 2 and Equation (21) in Theorem 3 must also be correct. The correctness of Theorems 2 and 3 are also confirmed by the results in Section 6.



(a) Profile (20, 10, 0.1)

(b) Profile (30, 20, 0.2)

Figure 2. Verification of the theoretical results in Theorems 2 and 3.

6.2. Performance evaluation

Extensive simulations are performed using MATLAB to compare the performance of RNCOPT with other typical schemes for WPRTPs. The tested schemes include RNCOPT, ColorNC [1], CliqueNC [2], and NoNC (it represents a traditional non-NC-based scheme where all requested packets are retransmitted once). It can be found through simple analysis that the schemes proposed in [3,14] are substantially equivalent to CliqueNC [2], and the loop coding scheme proposed in [15] is basically inferior to CliqueNC in terms of the number of retransmitted packets. Hence, the schemes proposed in [3,14,15] are not included in the simulations.

In RNCOPT, coding matrix is generated repeatedly until a valid coding matrix is found. To reveal this effect, a dummy scheme designated as RNCOPT-DUP is included in our simulation. In RNCOPT-DUP, coding matrix recreation overhead is considered in the performance metrics used in the simulations.

6.2.1. Performance metrics

(1) Number of retransmitted packets

This metric represents the number of retransmitted packets in a solution to a WPRTP. Because the main objective of WPRTP is usually to find valid solutions with minimum number of retransmitted packets, this metric is used as the main metric for measuring the performance of the schemes. In the four NC-based schemes, RNCOPT, RNCOPT-DUP, CliqueNC, and ColorNC, this metric represents the number of assembled packets, whereas in NoNC, this metric represents $|\cup_{r_i \in R} W_i|$. The numbers of the retransmitted packets in RNCOPT and RNCOPT-DUP are considered differently. For example, if the number of retransmitted packets in optimal NC-based solutions to a WPRTP is 4 and the coding matrix generated in the first attempt is invalid whereas the coding matrix generated in the second attempt is valid, then the number of retransmitted packets in RNCOPT-DUP is calculated as $4 \times 2 = 8$; contrastively, it is 4 in RNCOPT.

In general, in an assembled packet, the length of the coded packet will be much longer than the bits for storing auxiliary decoding information. Hence, the number of retransmitted packets can partly reflect the differences between these schemes in the metric of the total bit length. If the total bit length of all retransmitted packets is preferred, the result as a product of the number of retransmitted packets and bit length of assembled packets can easily be obtained.

(2) Relative number of retransmitted packets

Relative number of retransmitted packets of *scheme1*/*scheme2* represents the ratio of the number of retransmitted packets in *scheme1* to that in *scheme2*. For example, relative number of retransmitted packets of RNCOPT/NoNC is the ratio of the number of retransmitted packets in RNCOPT to that in NoNC.

6.2.2. Simulation configuration

Basic simulation parameters of WPRTP $(P, R, \{H_i\}, \{W_i\})$ include packet number $|P|$, receiver number $|R|$, packet request level p_{Level}, code coefficient bit length q (which means code coefficients are selected from range [1, 2^q-1]), and random seed bit length s. The used Galois field is GF(2^d) with $d = 8$. A profile of $(|P|, |R|, p_{\text{Level}}, q, s)$ is called a simulation configuration.

In each simulation, a WPRTP is generated according to the current simulation configuration. Each WPRTP is represented as a two-dimensional matrix M_P of size $|R| \times |P|$. Each element $a_{i,j}$ in M_P has only two possible values: 0 and 1, which indicates whether packet p_j belongs to W_i. If $a_{i,j} = 0$, then $p_j \in W_i$; otherwise, $p_j \notin W_i$, that is, $p_j \in H_i$. Each element $a_{i,j}$ in M_P is generated as follows: (i) randomly select a variable x, which is evenly distributed in range [0, 1], and (ii) if $x < p_{\text{Level}}$, then $a_{i,j} = 0$; otherwise, $a_{i,j} = 1$. Larger p_{Level} leads to more packets being requested. It should be mentioned that here, p_{Level} is used only to control the diversity of the requested packets, and it does not reflect real packet error rate in transmissions.

For each simulation configuration, 300 WPRTPs are generated and treated with the selected schemes. Performance metrics are averaged over these scenarios, and their 95% confidence intervals are also calculated. In some figures in the following section, the curves designated as TheoryNoNC and TheoryNCOPT represent the results calculated using Equations (16) and (21), respectively. The confidence intervals are also shown in some figures in the following section.

For simplicity, in our simulations for ColorNC, solutions to WPRTPs are determined by using a greedy-based heuristic algorithm to solve the corresponding clique partition problems in the corresponding graphs instead of the graph coloring problems of the complementary graphs.

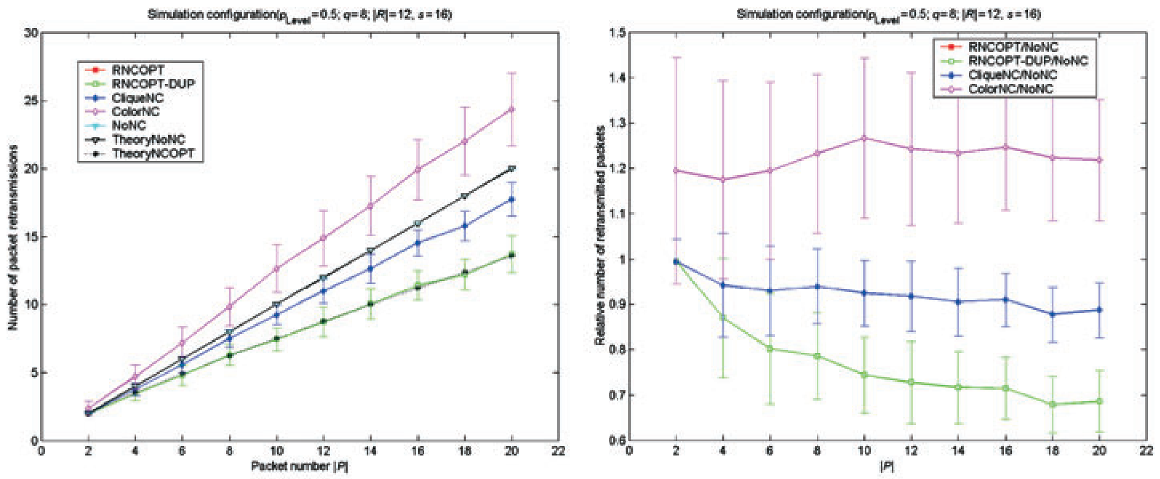
6.3. Simulation results

6.3.1. Effects of packet number and receiver number

A simulation set was performed to test the effects of packet number $|P|$ and receiver number $|R|$ on the schemes' performance. Simulation configurations were set as follows: packet request level $p_{\text{Level}} = 0.5$, code coefficient bit length $q = 8$, random seed bit length $s = 16$, packet number $|P|$ that increases from 2 to 20 with step size 2, and receiver number $|R|$ that also increases from 2 to 20 with step size 2. Results of these simulations are shown in Figures 3 and 4.

The two subfigures in Figure 3 show the variation of the two metrics when $|P|$ increases from 2 to 20 while $|R| = 12$. Results in Figure 3(a) show that when $|P| = 2$, these schemes show no distinctive performance differences. However, as $|P|$ increases, the numbers of retransmitted packets in the schemes as well as

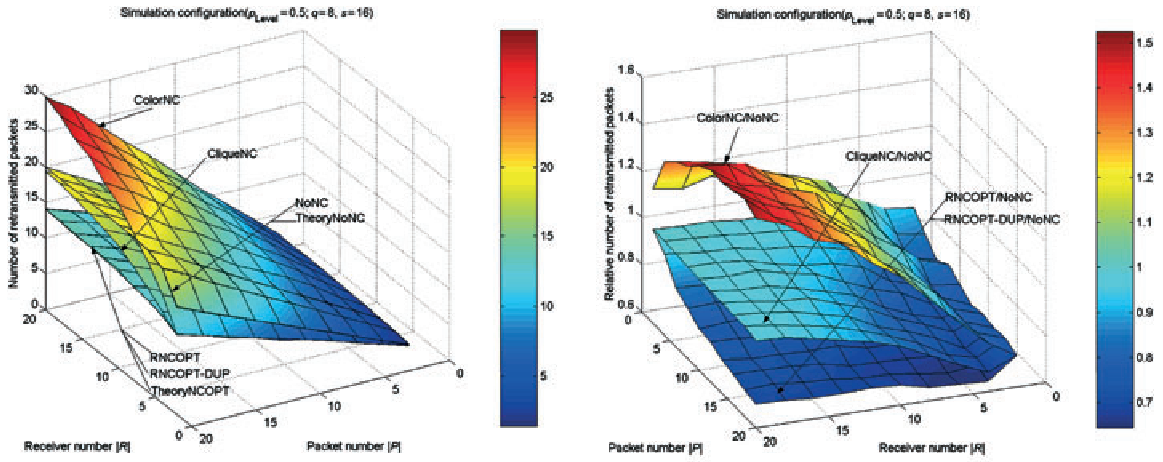
DOI: 10.1002/wcm



(a) Number of retransmitted packets

(b) Relative number of retransmitted packets

Figure 3. Effect of packet number on the schemes' performance when $|R| = 12$.



(a) Number of retransmitted packets

(b) Relative number of retransmitted packets

Figure 4. Effects of packet number and receiver number on the schemes' performance.

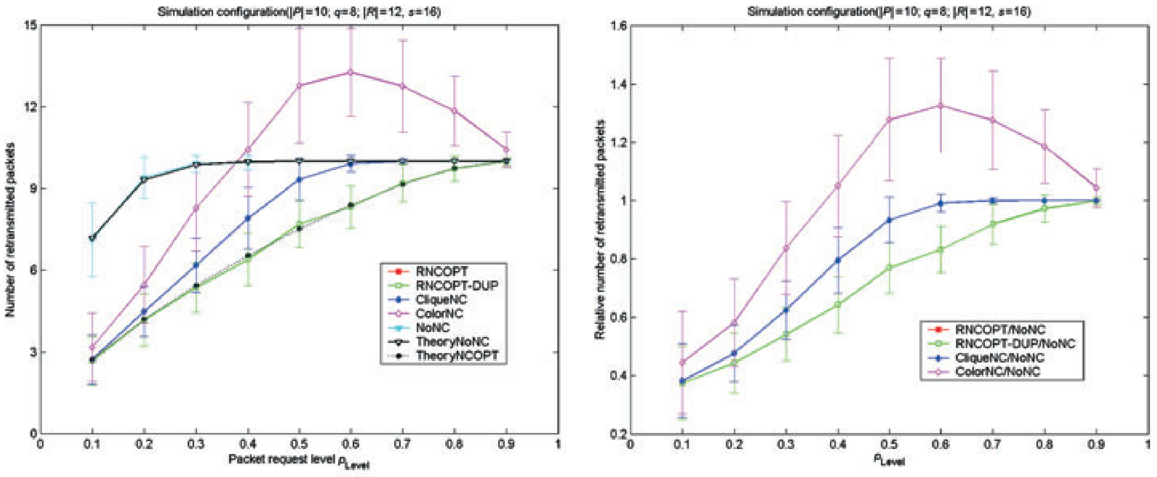
the differences among them increase linearly. The curve for RNCOPT-DUP overlays that of RNCOPT, and they perform best. Additionally, the two curves for RNCOPT and RNCOPT-DUP fit well with the theoretical results calculated using Equation (21), proving the correctness of Equation (21). Because of NC, CliqueNC outperforms NoNC. Performance differences between all the schemes in this metric are more evident in Figure 3 (b), where relative numbers of retransmitted packets in the tested schemes are shown. The larger the packet number $|P|$, the more the performance gains of RNCOPT, RNCOPT-DUP, and CliqueNC over NoNC. However, because of the considerably increased size of the new WPRTPs transformed from original WPRTPs and the inefficiency of the greedy-based heuristic algorithm used for solving clique partition problems, ColorNC performs even worse than NoNC.

The two subfigures in Figure 4 show the effects of $|P|$ and $|R|$ on the performance of all the schemes. As shown in Figure 4(a), when $|R|$ is small, RNCOPT obtains no distinct performance gain over CliqueNC. However, as $|R|$ increases, the numbers of retransmitted packets in CliqueNC and ColorNC increase quickly. When $|R| = 20$, CliqueNC approaches to NoNC, whereas ColorNC performs even worse than NoNC. Contrastively, $|R|$ has much slighter effect on RNCOPT, RNCOPT-DUP, and NoNC. Hence, performance gains of RNCOPT over CliqueNC and ColorNC increases as $|R|$ increases. When $|R| = 20$ and $|P| = 20$, performance gain of RNCOPT over NoNC is more than 30%.

6.3.2. Effects of packet request level and receiver number

Another simulation set was performed to test the effects of packet request level p_{Level} and receiver number $|R|$ on the schemes' performance. Simulation configurations were set as follows: code coefficient bit length $q = 8$, packet number $|P| = 10$, random seed bit length s=16, packet request level p_{Level} that increases from 0.1 to 0.9 with step size 0.1, and receiver number $|R|$ that increases from 2 to 20 with step size 2. The results are shown in Figures 5 and 6.

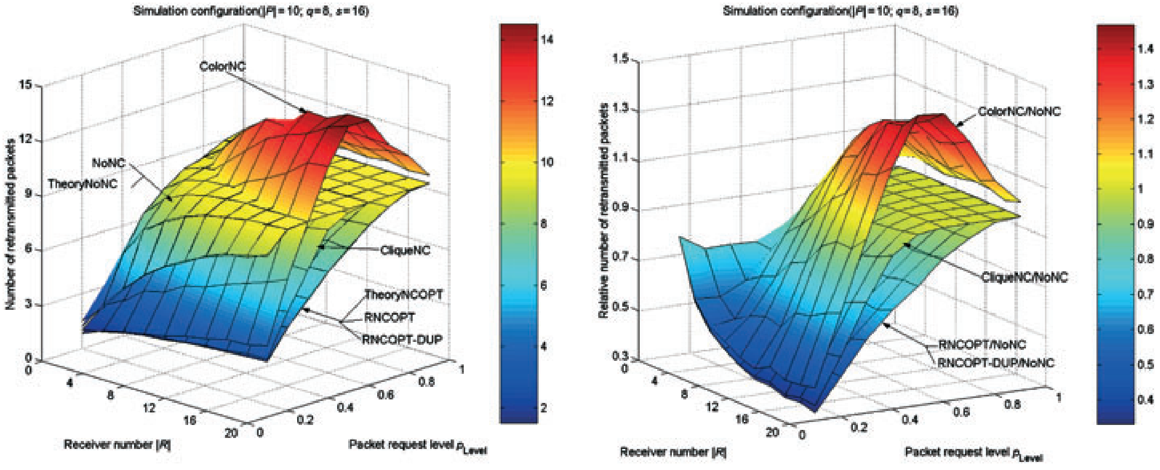
The subfigures in Figure 5 show the variation of the two metrics when p_{Level} increases from 0.1 to 0.9 with $|R| = 12$. Figure 5(a) shows that when $p_{\text{Level}} = 0.1$, all the numbers of retransmitted packets in NC-based schemes are about 3, whereas it is about 7 in NoNC. Thus, about 60% packet transmissions are saved by using NC. As p_{Level} increases from 0.1, the numbers of retransmitted packets in the schemes all increase quickly. However, the numbers of retransmitted packets in NoNC, ColorNC, and CliqueNC increase much more quickly than those in RNCOPT and RNCOPT-DUP. The number of retransmitted packets in NoNC reaches maximum at about $p_{\text{Level}} = 0.3$, whereas that of CliqueNC reaches maximum at about $p_{\text{Level}} = 0.6$. This metric of ColorNC also reaches its peak at $p_{\text{Level}} = 0.6$. However, the peak value of ColorNC is about 20% larger than that of CliqueNC. Contrastively, the number of retransmitted packets of RNCOPT and RNCOPT-DUP



(a) Number of retransmitted packets

(b) Relative number of retransmitted packets

Figure 5. Effect of packet request level on the schemes' performance when $|R| = 12$.

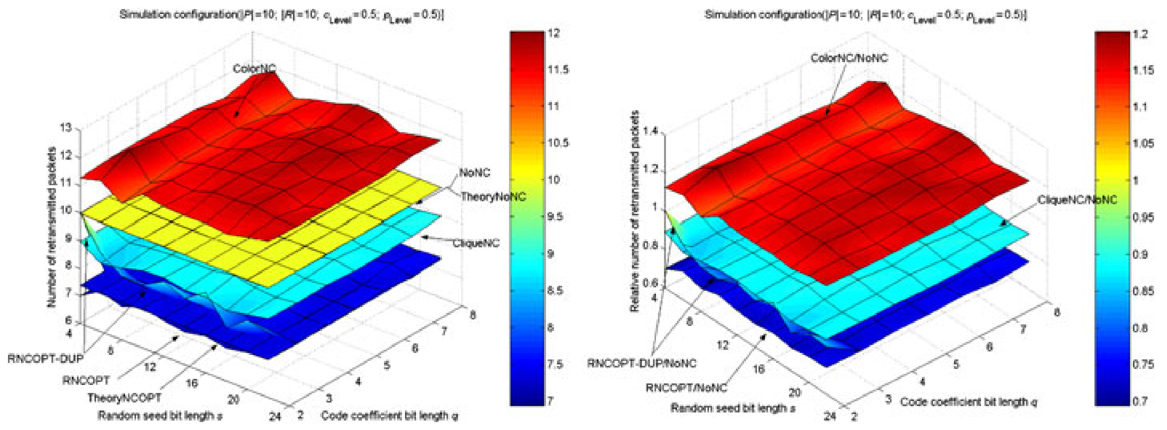


(a) Number of retransmitted packets

(b) Relative number of retransmitted packets

Figure 6. Effects of packet request level and receiver number on the schemes' performance.

DOI: 10.1002/wcm



(a) Number of retransmitted packets (b) Relative number of retransmitted packets

Figure 7. Effects of code coefficient bit length and random seed bit length on the schemes' performance.

approach to that of NoNC after $p_{\text{Level}} = 0.9$. The results in Figure 5 also confirm the correctness of the theoretical results in Equations (16) and (21).

The effects of packet request level p_{Level} and receiver number $|R|$ on the performance of the schemes are shown in a different perspective in Figure 6. Results in Figure 6(a) show that as $|R|$ increases, the numbers of retransmitted packets in these schemes all increase. However, this metric in ColorNC increases more quickly than those in the other schemes. ColorNC becomes even worse than NoNC. As p_{Level} increases, the numbers of retransmitted packets in the schemes all increase. However, this metric of ColorNC reaches maximum at about $p_{\text{Level}} = 0.6$ and then decreases gradually. The results in Figure 6(b) show that NC-based schemes are more preferable under cases with smaller p_{Level} and larger $|R|$. When $p_{\text{Level}} = 0.1$ and $|R| = 20$, the performance gain of RNCOPT over NoNC can be up to 60%.

6.3.3. Effects of code coefficient bit length and random seed bit length

Furthermore, another simulation set was performed to test the effects of code coefficient bit length q and random seed bit length s on the performance of the schemes. Simulation configurations were set as follows: packet number $|P| = 10$, receiver number $|R| = 10$, packet request level $p_{\text{Level}} = 0.5$, code coefficient bit length q that increases from 2 to 8 with step size 1, and random seed bit length s that increases from 6 to 24 with step size 2. Corresponding results are shown in Figure 7.

When $q \leq 3$, the large difference between the results of RNCOPT and RNCOPT-DUP in Figure 7 indicates that because of the higher probability that a randomly generated coding matrix does not make up a valid solution, more attempts are required to obtain a valid coding matrix. Fortunately, the results of RNCOPT-DUP fit well with those of RNCOPT when $q \geq 3$. The fine fitness indicates that a randomly generated coding matrix will probably make up a valid solution in scenarios similar to the simulated cases. To be conservative, $q = 8$ and $s = 16$ are used as the default values for q and s in RNCOPT. Because q and s are not used in all the other schemes, the two parameters have no effects on these schemes.

7. CONCLUSIONS

In this paper, optimal NC-based schemes for P-WPRTPs where, for one receiver, a packet is either requested by or already known to it are researched. Based on the analysis about the number of retransmitted packets in optimal NC-based solutions to P-WPRTPs, we proposed an optimal NC-based scheme for P-WPRTPs and named it as RNCOPT. RNCOPT is optimal in the sense that it guarantees to obtain a valid solution with minimum number of packet retransmissions. Furthermore, in RNCOPT, each coding vector is generated using a publicly known pseudorandom function with a randomly selected seed. It is the seed instead of the coding vector that is enclosed in the assembled packets to be retransmitted. Thus, packet overhead of RNCOPT is reduced further. Simulation results show that RNCOPT distinctively outperforms other typical schemes for P-WPRTPs.

RNCOPT is only optimal for P-WPRTPs. Although the set of P-WPRTPs is only a subset of WPRTPs, an optimal NC-based solution to a P-WPRTP can be used as a first-attempt solution to the related WPRTPs. We are working on efficient schemes for IP-WPRTPs where, for one receiver, a packet can be neither requested by nor already known to it.

ACKNOWLEDGEMENTS

We deeply appreciate the valuable comments and suggestions made by the anonymous reviewers that have helped us to significantly improve the quality of the manuscript. Thanks to Professor Hsiao-Chun Wu in Louisiana State University for his valuable suggestions. Thanks to Miss Boumediene Latifa for polishing the manuscript.

This work is jointly supported by the following: National Science Foundation of China (61073813, 60703090, 61003235, 61073182, 60873036, 60973027), National High Technology Research and Development Program of China (863) (2007AA01Z401), National Postdoctoral Scientific Research Program (20100470048), Young Teacher Supporting Project of Heilongjiang Province, Young Researcher Supporting Project of HRBEU (0811), Natural Science Foundation of Heilongjiang Province (F200902), and Fundamental Research Funds for the Central Universities (HEUCFT1007).

REFERENCES

1. El Rouayheb SY, Chaudhry MAR, Sprintson A. On the minimum number of transmissions in single-hop wireless coding networks. In *Proceedings of the IEEE Information Theory Workshop,* Lake Tahoe, CA. IEEE Information Society: Tahoe City, CA, 2007; 120–125.
2. Xu YL, Zhan C, Luo W, Li P. Network coding based reliable multicast for wireless ad hoc networks. *Journal of University of Science and Technology of China* 2008; **38**(7): 860–866.
3. Nguyen D, Tran T, Nguyen T, Bose B. Wireless broadcast using network coding. *IEEE Transactions on Vehicular Technology* 2009; **58**(2): 914–925.
4. El Rouayheb SY, Sprintson A, Georghiades CN. On the index coding problem and its relation to network coding and matroid theory. *IEEE Transactions on Information Theory* 2010; **56**(7): 3187–3195.
5. Bar-Yossef Z, Birk Y, Jayram TS, Kol T. Index coding with side information. In *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science,* Berkeley, CA. IEEE Computer Society: Washington, DC, 2006; 197–206.
6. Wu YN, Padhye J, Chandra R, Padmanabhan V, Chou PA. The local mixing problem. In *Proceedings of Information Theory and Applications Workshop,* San Diego. IEEE Press: La Jolla, CA, 2007.
7. Ahlswede R, Cai N, Li SYR, Yeung RW. Network information flow. *IEEE Transactions on Information Theory* 2000; **46**(4): 1204–1216.
8. Fragouli C, Katabi D, Markopoulou A, Médard M, Rahul H. Wireless network coding: opportunities & challenges. In *Proceedings of the IEEE Military Communications Conference,* Orlando, FL. IEEE Press: Piscataway, NJ, 2007; 1–8.
9. Fragouli C, Boudec JYL, Widmer J. Network coding: an instant primer. *ACM SIGCOMM Computer Communication Review* 2006; **36**(1): 63–68.
10. Wu YN, Kung SY. Reduced-complexity network coding for multicasting over ad hoc network. In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing,* Philadelphia, PA. IEEE Press: Piscataway, NJ, 2005; 18–23.
11. Sengupta S, Rayanchu S, Banerjee S. An analysis of wireless network coding for unicast sessions: the case for coding-aware routing. In *Proceedings of the 26th Annual IEEE Conference on Computer Communications,* Anchorage, AK. IEEE Communications Society: New York, NY, 2007; 1028–1036.
12. Zhang X, Wicker SB. Robustness vs efficiency in sensor networks. In *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks,* Kaohsiung. IEEE Press: Piscataway, NJ, 2005; 225–230.
13. Ho T, Médard M, Shi J, Effros M, Karger DR. On randomized network coding. In *Proceedings of the 41st Annual Allerton Conference on Communication, Control, and Computing,* Monticello, IL. IEEE Press: Piscataway, NJ, 2003.
14. Katti S, Rahul H, Hu WJ, Katabi D, Médard M, Crowcroft J. XORs in the air: practical wireless network coding. *ACM SIGCOMM Computer Communication Review* 2006; **36**(4): 243–254.
15. Dong QF, Wu JM, Hu WJ, Crowcroft J. Practical network coding in wireless networks. In *Proceedings of the 13th Annual International Conference on Mobile Computing and Networking,* Montréal, Quebec. ACM: New York, NY, 2007.
16. He MF, Bai TL, Ren LW. *Tutorial of Linear Algebra*. Press of Northeast Financial and Commercial University: Dalian, 2003.

AUTHORS' BIOGRAPHIES

Zhenguo Gao is a professor in Harbin Engineering University, Harbin, China. He is now a visiting professor in the University of Michigan, Dearborn. He has been working as a visiting professor in the University of Illinois at Urbana-Champaign in 2010. He received his BS and MS degree in Mechanical and Electrical Engineering from Harbin Institute of Technology, Harbin, China, in 1999 and 2001, respectively. Then he received his PhD degree in Computer Architecture from Harbin Institute of Technology, Harbin, China, in 2006. His research interests include wireless *ad hoc* network, cognitive radio network, network coding, and game theory applications in communication networks.

He is a senior member of China Computer Federation. He received National Science Foundation Career Award of

China in 2007 and Outstanding Junior Faculty Award of Harbin Engineering University in 2008. He is serving as a reviewer for project proposals to National Science Foundation of China, Ministry of Education of China, Science Foundation of HeiLongJiang Province, China. He is also serving as a reviewer for some journals including the IEEE Transactions on Mobile Computing, Wireless Networks and Mobile Computing, the Journal of Parallel and Distributed Computing, the Journal of Electronics (Chinese), and the Journal of Astronautics (Chinese), etc.

Weidong Xiang is now an Associate Professor in the University of Michigan-Dearborn. He received his MSEE and PhD degrees from Tsinghua University, Beijing, China, in 1996 and 1999, respectively. From 1999 to 2004, he worked as a postdoctoral fellow and then a research scientist at the Software Radio Laboratory at Georgia Institute of Technology, Atlanta. In September 2004, he joined the Electrical and Computer Engineering Department of the University of Michigan-Dearborn as an assistant professor. His research interests include orthogonal frequency-division multiplexing, multiple-input and multiple-output, cognitive radio, wireless access for vehicular environments, ultrawideband, and wireless networked control system.

Yunlong Zhao received his PhD degree in Computer Science from Harbin Institute of Technology in 2005. He is currently working as a visiting professor in University of Tokyo, Japan. He is an Associate Professor in the College of Computer Science and Technology of Harbin Engineering University. His primary research interests include *ad hoc* networks, *ad hoc* sensor network, underwater acoustic sensor network, and distributed computing.

Jing Zhao received her PhD degree in Computer Science from Harbin Institute of Technology in 2006. Now she is a Professor in the College of Computer Science and Technology in Harbin Engineering University. Her research interests include dependable systems, system reliability, and software lifetime prediction.

Shaobin Cai received his PhD degree in Computer Science from Harbin Institute of Technology in 2005 and worked as a post-doctor in UCLA in 2008 and 2009. His primary research interests include *ad hoc* networks, *ad hoc* sensor network, underwater acoustic sensor network, and distributed computing.

Wu Pan is a visiting scholar in the Department of Electrical and Computer Engineering, University of Michigan-Dearborn. He received his PhD degree from Tsinghua University, Beijing, China, in 2000. His interests include *ad hoc* networks, vehicular communications, and ultrawideband tracking system.

Hua Jiang is a visiting scholar in the Electrical and Computer Engineering Department of the University of Michigan-Dearborn. He was born in May 1962. He is the Dean of the Department of Communication Engineering, Beijing Electronic Science and Technology Institute. His research interests include information security, next generation network, communication engineering, and signal processing.

Huiqiang Wang is a Professor in the College of Computer Science and Technology of Harbin Engineering University, Harbin, China. He has been the Associate Research Director of the College of Computer Science and Technology of Harbin Engineering University. Now he is the Chief Engineer of the Ship-big Engineering and Researching Academe and the Superintendent of the Network Technology and Information Security Research Center. He is also a member of the three academic committees in China Computer Federation (Fault Tolerance, Open Systems and Distributed Systems, and Network and Digital Communication). He is now a Director of the Provincial Computer Federation of HeiLongJiang province as well as the Director of the Network Subcommittee. His primary research interests include computer networks, computer security, and distributed systems.