基于网络编码的协作恢复机制线性可解性研究

殷俊[1,2]，沙雪琪[2]，王磊[1,2]，张登银[1,2]，杨余旺[3]
（1. 南京邮电大学江苏省宽带无线通信重点实验室，江苏 南京 210003；2. 南京邮电大学物联网学院，江苏 南京 210003；
3. 南京理工大学计算机科学与工程学院，江苏 南京 210004）

摘 要：针对基于网络编码的协作恢复（CR）机制线性可解性未知问题，建立了 CR 机制网络编码包的线性可解性的量化分析模型，给出了在任意阶伽罗华编码有限域下接收方解码出所有源数据包的概率上下界，并提出了一种改进 Gauss-Jordan 的线性可解性在线判定算法。数值实验结果验证了所提上下界的紧密性和改进 Gauss-Jordan 算法解码的低等待时延特性，节点部署实验显示改进 Gauss-Jordan 算法较传统 Gauss 算法解码复杂度降低 35%。

关键词：协作恢复；网络编码；线性可解性；改进 Gauss-Jordan 算法
中图分类号：TN92
文献标识码：A
DOI: 10.11959/j.issn.1000−436x.2021050

Research on linear solvability of network coding based cooperative recovery scheme

YIN Jun[1,2], SHA Xueqi[2], WANG Lei[1,2], ZHANG Dengyin[1,2], YANG Yuwang[3]
1. Jiangsu Key Laboratory of Broadband Wireless Communication, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
2. School of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
3. School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210004, China

Abstract: The linear solvability of network coding based cooperative recovery/repair (CR) scheme was studied. Specifically, the solvability analysis model for network coding based CR scheme was established, the upper and lower bounds of the probability for any receiver to decode all original information under arbitrary order of Galois coding field were proposed and proved, and an on-line solvability judgement algorithm was designed by improvement of Gauss-Jordan algorithm. Numerical results validate the compactness of the proposed upper and lower bounds as well as the short-time decoding waiting delay of the improved Gauss-Jordan algorithm. Node deployment experiments show that the decoding complexity of the improved Gauss Jordan algorithm is reduced by 35% compared with the traditional Gauss algorithm.
Keywords: cooperative recovery/repair, network coding, linear solvability, improved Gauss-Jordan algorithm

1 引言

无线广播/多播是一种经典且高效的信息分发方式。但由于无线电波传播特性，信源传输到不同接收端的数据包具有独立删除特征，如何保证多接收方可靠接收是现代广播/多播系统设计的难点[1-2]。注意到，无线通信节点的一个典型发展趋势是多接口化，如各类智能终端、车联网车辆[3]均配置了远程通信接口和短程通信接口，基于此研究人员提出了协作恢复（CR, cooperative recovery/repair）机制。CR 通

收稿日期：2020−11−19；**修回日期**：2021−02−07
通信作者：王磊，leiwang@njupt.edu.cn
基金项目：国家自然科学基金资助项目（No.61971235, No.61801236）；国家基础科研计划基金资助项目（No.JCKY201760xxx003, No.JCKY201860xxx001）；南邮科研基金资助项目（No.NY217148, No.NY219111）；苏州创新计划基金资助项目（No.SYG201826）
Foundation Items: The National Natural Science Foundation of China (No.61971235, No.61801236), Basic Research Foundation of China (No.JCKY201760xxx003, No.JCKY201860xxx001), Nanjing University of Posts and Telecommunications Science Foundation (No.NY217148, No.NY219111), Research Program of Suzhou (No.SYG201826)

过利用相邻节点间的短程通信来恢复彼此在远程广播通信中丢失的数据包。大量实践结果表明，CR 可有效地提高多播吞吐量，增强网络可靠性[4-5]。CR 在车联网中的一种典型应用场景如图 1 所示，路侧单元（RSU, road side unit）需要通过广播方式向覆盖范围内的车辆广播信息。由于车辆通常会快速驶离 RSU 的通信覆盖范围，因此无法持续依赖 RSU 进行出错数据包的修复。考虑到不同车辆在 RSU 广播阶段接收正确或出错的数据包各异，使用 CR 机制的车辆在移出 RSU 覆盖范围后依然可以依靠短距离通信接口互相修复彼此在 RSU 广播过程中丢失的数据包。

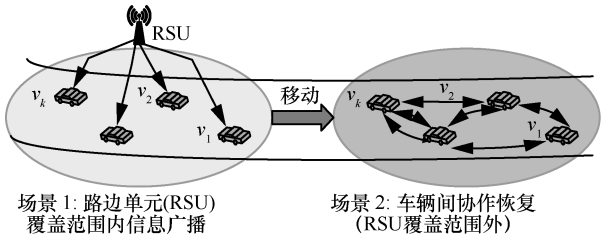


图 1　CR 在车联网中的一种典型应用场景

与传统的自动重传请求（ARQ, automatic repeat request）、信源重传等可靠传输方案相比，CR 具有较明显的优势。首先，CR 降低了源节点的重传负担。其次，邻居节点之间在交互阶段使用短距离通信接口，信道质量较广播源与节点间的长程信道更高，使 CR 交互过程的丢包率远小于源节点传输过程。需要指出的是，邻居节点间可以采用 ad-hoc 模式进行分布式管理，因此 CR 的交互过程整体控制负担较小。大量研究表明，在 CR 基础上引入网络编码可以进一步提高节点协作效率[6-14]。网络编码由 Ahlswede 等[15]提出，其核心思想是允许中间节点对接收到的信息进行再编码，打破了传统网络中间节点仅对信息进行存储转发的限制，可以有效提升通信网络的吞吐量和可靠性。

Park 等[6]最早提出将随机线性网络编码（RLNC, random linear network coding）[16]应用于 CR 过程，协作节点需要将接收到的数据包进行随机线性组合生成多个线性无关的编码包，信宿节点收到这些编码包后进行解码，得到原始数据包。但由于 RLNC 在解码时需要信宿节点必须接收到足够多的编码包，因此信宿节点等待解码的时延较大。近年来，随着直连通信（D2D, device to device）的理念提出，基于网络编码的 CR 机制往往与 D2D 相结合[7]。Yan 等[8]提出基于机会网络编码（ONC, opportunistic network coding）的 CR 机制，数据包的编码组合仅依赖每个协作节点当前接收或丢失的状态。与 RLNC 相比，ONC 更加灵活，节点待解码的时延更小。综合来看，当前本领域的研究主要集中在以下 2 个方面。

1) 寻找更优的机会网络编码码字构造方法。其中典型的有立即可解网络编码（IDNC, instantly decodable network coding）[9-11]。由于 IDNC 的编解码复杂度较低，解码过程具有及时性，因此适用于时延敏感型的近邻视频交互、实时对战游戏等应用场景。

2) 寻找更合理的节点协作传输策略，降低 CR 过程开销。与传统的一对多网络传输过程不同，CR 在网络重传阶段的信源转变为某一个或多个网络内节点，所以协作过程的另一个重要研究内容是结合具体编码和底层传输协议寻找协作节点的内容传输策略[10-14]。文献[10]提出在 D2D 网络中采用集中化方式选择 IDNC 的编码包，降低单次重传的解码时延增量。在此基础上，文献[11]提出一种构造终端节点间协作传输的矛盾图算法，通过搜索极大独立集选择并行协作重传终端，降低节点间协作重传开销。文献[12]引出了节点协作过程的公平性问题。针对此问题，文献[13]将 CR 过程抽象为广播和协作传输 2 个阶段，并设计了一种分布式的调度算法，提高了协作传输阶段的信息恢复效率。出于同样的思想，文献[14]基于时分多址接入（TDMA, time division multiple access）协议提出了一种面向车联网的分布式 CR 重传实施方法。

然而，上述 2 类研究在分析和讨论节点解码时的线性可解性上均直接采用经典 RLNC 方法的结论[16]。经典 RLNC 线性可解性理论认为当编码有限域足够大时，只要某个目的节点成功接收到的编码包个数和源数据包个数相等就能以极高的概率解码[17]。例如，对于有限域 GF(2^{16})，当源数据包个数为 5 时，接收到 5 个随机线性编码数据包的目的节点解码概率超过 96%。而本质上 CR 编码过程是一种机会的网络编码，与 RLNC 的编解码过程不可等价，直接利用 RLNC 结论假设 CR 协作恢复阶段目的节点收到与源数据包相同数量的编码包即可解码显然是不合理的。本文针对基于网络编码的 CR 机制应用中线性可解性这一关键、基础问题展开研究，主要贡献如下。

1) 建立了基于网络编码的CR机制线性可解性分析模型；给出了不同包删除率、编码伽罗华域阶、协作节点数等多种参数综合影响下，基于网络编码的 CR 机制网络内任意节点解码出所有源数据包的概率上下界。数值实验验证了该理论上、下界的准确性和紧密性。

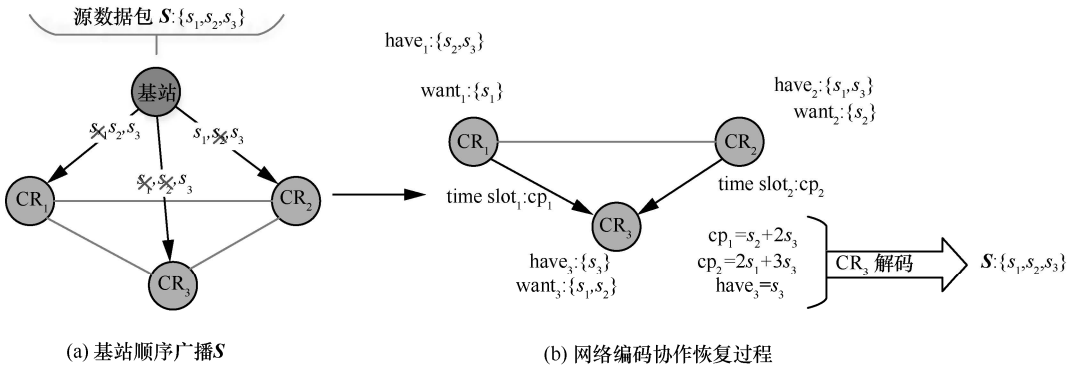
2) 提出了一种 CR 线性可解性在线判定算法。协作簇内节点可根据该算法在协作恢复过程进行编码包部分解码，不需要等待协作阶段结束。理论分析和实验表明，该算法降低了传统高斯方法的解码等待时延和存储开销。

2 系统模型

由于应用场景差异，不同研究中基于网络编码的 CR 系统模型会有细微区别，本文考虑如图 1 所示的典型应用场景下的两阶段 CR 模型[12-13]。远程基站需要向其覆盖范围内的所有移动节点广播源信息 $\boldsymbol{S}$（不失一般性，假设 $\boldsymbol{S}$ 包含 N 个数据包并记 $\boldsymbol{S}=\{s_1,s_2,\cdots,s_N\}$）。采用 CR 机制，$\boldsymbol{S}$ 的交付过程将被分为 2 个阶段。第一阶段，基站顺序广播 $\boldsymbol{S}$。由于广播信道的删除特性，网络内节点可能无法全部正确接收 N 个数据包。为了恢复丢失的包，相邻的节点根据地理位置或者移动特征，预先形成了若干个协作簇。第二阶段，网络编码协作恢复过程。协作簇内节点间可以通过短距离无线通信接口交换网络编码包，从而恢复彼此在第一阶段接收过程中丢失的包。假设某协作簇包含 M 个协作中继节点，并记为 $\{\mathrm{CR}_1,\mathrm{CR}_2,\cdots,\mathrm{CR}_M\}$，簇内的任意节点 CR_i 进行网络编码协作恢复的过程。若 CR_i 第一阶段成功接收了 k 个源数据包 $\boldsymbol{s}^i=\{s'_1,s'_2,\cdots,s'_k\}$，首先，$\mathrm{CR}_i$ 在有限域上随机生成前 k 个元素非零编码向量 $\boldsymbol{a}=\{a_1,a_2,\cdots,a_k\}$；然后，进行线性编码 $\mathbf{cp}_i=\boldsymbol{a}\boldsymbol{s}^i$ 产生编码结果 $\mathbf{cp}_i$；最后，将编码结果 $\mathbf{cp}_i$ 和编码向量 $\boldsymbol{a}$ 打包成一个编码包传递给簇内的邻居节点。

通过如图 2 所示的基于网络编码的 CR 系统模型详细展示上述过程。远程基站需要尽最大可能向覆盖范围内节点交付信息 $\boldsymbol{S}=\{s_1,s_2,s_3\}$。经过第一阶段基站广播传输后，网络内节点 CR_1、CR_2 和 CR_3 分别接收到了部分数据包（如图 2(a)所示，其中画×的数据包表示对应节点未能成功接收该数据包）。第二阶段，3 个节点形成一个协作簇，簇内采用网络编码进行丢失信息修复。CR_1 节点根据第一轮接收到的源数据包 $\mathrm{have}_1=\{s_2,s_3\}$，从有限域里随机生成一个编码系数向量（假设为(1,2)），根据编码向量对源数据包进行线性组合，生成一个编码包 $\mathrm{cp}_1=s_2+2s_3$，并占用一个时间片传输给了邻居节点。类似地，节点 CR_2 编码并传输了 $\mathrm{cp}_2=2s_1+3s_3$。对于节点 CR_3，由于它侦听到了 2 个编码数据包，结合在第一阶段节点收到的源数据包（也可视作以编码向量为单位向量的编码包），CR_3 节点共接收到 3 个线性无关数据包，因此可以通过高斯消去解码出源数据包 $S=\{s_1,s_2,s_3\}$，完成 CR 修复过程。

通过图 2 的例子可以发现，如果节点间协作传输 MAC 协议采用 CSMA/CA 或 TDMA 协议，簇内节点在协作恢复过程同一时间片只有一个节点处于发送状态，簇内其他节点均处于接收状态可监听到该数据包（存在一定的删除率）。例如在图 2 中，对于含有 M（M=3）个节点的协作簇，在整个第二阶段共需要消耗 M 个时间片，任意节点均消耗一个时间片进行编码传输，消耗 $M-1$ 个时间片进行接收。由于采用网络编码的 CR 机制工作时簇内节



(a) 基站顺序广播$\boldsymbol{S}$ (b) 网络编码协作恢复过程

图 2 基于网络编码的 CR 系统模型

点间直接交互编码数据包而不是源数据包，而编码数据包是多个源数据包信息的混合，每个簇内节点只要在两阶段时间片内接收到 N 个线性无关编码包即可解码出所有源数据。因此，基于网络编码的 CR 传输过程可自组织，减少了传统 CR 过程中修复过程的时延，也避免了借助额外的控制机制所带来的资源开销。本文推导经过一轮这样的 CR 传输后，簇内任意节点能够成功解码出 N 个源数据包的概率，这也是基于网络编码的 CR 机制里一个待解决的基础问题。

注意到，解码过程不仅受到协作恢复的节点数量、具体网络编码有限域影响，还在很大程度上受到数据包在两阶段物理信道上传输时的删除率影响。本文采用基于文献[13, 18]的具体物理信道模型建模数据包删除率：假设两阶段传输信道均为加性白高斯噪声（AWGN, additive white Gaussian noise）信道，并且各信道间独立。本文信道模型只是 CR 传输领域若干模型中的一种典型模型[13, 18]，而基于网络编码的 CR 过程线性可解性不仅受物理信道参数影响，还受到编码有限域、协作节点数等参数影响。为了保证本文结论可适应其他信道模型，后文所提出的线性可解性及其结论仅依赖于信道上传输的数据包删除率，独立于具体底层所使用的物理信道。因此，应用了其他信道模型的 CR 机制容易在本文信道模型建模思路上修改使用。在基站广播阶段，簇内任意节点 CR_i 收到的信号为

$$r_{\mathrm{base},i}=\sqrt{P_{\mathrm{base}}}h_{\mathrm{base},i}s+n_{\mathrm{base},i} \tag{1}$$

其中，P_{base} 表示基站传输功率；$h_{\mathrm{base},i}$ 表示基站和节点 CR_i 间的信道增益，是一个均值为 0、方差为 $\sigma^2_{\mathrm{base},i}/2$ 的循环对称复高斯变量；s 是基站广播的信号；$n_{\mathrm{base},i}$ 是均值为 0、方差为 $N_0/2$ 的复 AWGN 噪声。同理，在协作传输阶段，任意节点 CR_i 接收到来自节点 CR_j 的信号为

$$r_{i,j}=\sqrt{P_j}h_{j,i}\mathrm{cp}_j+n_{j,i} \tag{2}$$

其中，P_j 表示基站传输功率；$h_{j,i}$ 表示两节点间的信道增益循环对称复高斯变量，其均值为 0、方差为 $\sigma^2_{j,i}/2$；cp_j 表示发送的信号；$n_{j,i}$ 表示 AWGN 噪声。对于瑞利衰落信道，本文将两阶段传输的信道增益分别定义为 $\sigma^2_{\mathrm{base},i}=d^{-\mu}_{\mathrm{base},i}$ 和 $\sigma^2_{j,i}=d^{-\mu}_{j,i}$，其中，$d_{\mathrm{base},i}$ 和 $d_{j,i}$ 分别表示 CR_i 和基站与 CR_i 和 CR_j 的距离；u 为路径损耗指数，取值范围一般为(2,6)[19]。记广播和协作传播阶段的 CR_i 接收信道信噪比分别为 $\mathrm{snr}_{\mathrm{base},i}=|h_{\mathrm{base},i}|^2P_{\mathrm{base}}/N_0$ 和 $\mathrm{snr}_{j,i}=|h_{j,i}|^2P_j/N_0$，则根据文献[18]可得，两阶段信道删除率分别为

$$e_{\mathrm{sr}}=\Pr\{\log(1+\mathrm{snr}_{\mathrm{base},i})<E_{\mathrm{threshold}}\} \tag{3}$$

$$e_{\mathrm{rd}}=\Pr\{\log(1+\mathrm{snr}_{j,i})<E_{\mathrm{threshold}}\} \tag{4}$$

其中，e_{sr} 表示第一阶段广播信道的删除率，e_{rd} 表示第二阶段协作交互信道的删除率；$E_{\mathrm{threshold}}$ 表示预设的频谱效率门限值。据此，可以建模 CR 过程，记 M 为协作簇的节点个数，F_q 为阶为 q 的网络编码运算有限域，模型详细参数如表 1 所示。不失一般性，从 M 个协作节点中任选一个节点 CR_i 为目标节点，下面将分析经过一次完整的两阶段 CR 数据传输过程之后，节点 CR_i 能够成功解码出全部 N 个源数据包的概率。

表 1　　模型参数及其含义

参数	含义
M	协作簇内节点数量
$\boldsymbol{s}_N$	源数据包集合向量，数据包数量为 N
F_q	阶为 q 的编码伽罗华有限域 GF(q)
e_{sr}	广播阶段信道删除率
e_{rd}	协作阶段信道删除率
$\mathrm{Pr}_{\mathrm{suc}}$	一次完整 CR 过程节点解码出所有源数据包概率
$\boldsymbol{C}$	编码系数矩阵，也称为传输矩阵
$\mathrm{snr}_{i,j}$	节点间协作传输信道信噪比
$\mathrm{snr}_{\mathrm{base},i}$	基站与节点间广播信道信噪比
$E_{\mathrm{threshold}}$	频谱效率门限
$h_{i,j}$	节点间协作传输信道增益
$h_{\mathrm{base},i}$	基站与节点间广播信道增益
$n_{i,j}$	节点间协作传输信道噪声
$n_{\mathrm{base},i}$	基站与节点间广播信道噪声
u	路径损耗指数
P_{base}	基站广播信号功率
P_i	节点间协作传输信号功率

3　基于网络编码的 CR 线性可解性分析

根据第 2 节的系统模型可知，对于包含 M 个节点 $\{\mathrm{CR}_1,\mathrm{CR}_2,\cdots,\mathrm{CR}_M\}$ 的协作簇，簇内任意节点 CR_i 在整个 CR 传输过程中可以接收的（编码）数据包有 2 个来源：第一阶段广播信道上基站发送的 N 个源数据包和第二阶段交互信道上簇内其他邻

居节点发送的 $M-1$ 个编码数据包。假设节点 CR_i 在广播阶段成功接收了 $k(0\leqslant k\leqslant N)$ 个数据包，其概率为 $\Pr_{\mathrm{suc\_brod}}(k)$，由于信道传输过程独立，因此由二项分布得

$$\Pr_{\mathrm{suc\_brod}}(k)=\binom{N}{k}\left(1-e_{\mathrm{sr}}\right)^{k} e_{\mathrm{sr}}{}^{N-k} \tag{5}$$

其中，e_{sr} 表示广播信道的删除率。由全概率公式可得，经过一轮完整的 CR 数据传输过程之后 CR_i 成功解码出所有 N 个源数据包的概率 $\Pr_{\mathrm{suc}}$ 为

$$\Pr_{\mathrm{suc}}=\sum_{k=0}^{N}\Pr_{\mathrm{suc\_broad}}(k)\Pr_{\mathrm{suc\_coop}}^{k}(N)=\sum_{k=0}^{N}\Pr_{\mathrm{suc\_broad}}(k)(1-\Pr_{\mathrm{fail\_coop}}^{k}(N)) \tag{6}$$

其中，$\Pr_{\mathrm{suc\_coop}}^{k}(N)$ 和 $\Pr_{\mathrm{fail\_coop}}^{k}(N)$ 分别表示 CR_i 节点第一阶段接收到 k 个数据包后通过 CR 机制在协作阶段成功和未能解码出其余的 $N-k$ 个数据包的概率。因此，由式(5)和式(6)可得，CR 线性可解性分析的关键在于如何评估概率 $\Pr_{\mathrm{suc\_coop}}^{k}(N)$ 或 $\Pr_{\mathrm{fail\_coop}}^{k}(N)$。下面，本文将通过对 CR_i 在两阶段的传输过程所获得的（编码）数据包系数矩阵分析 $\Pr_{\mathrm{fail\_coop}}^{k}(N)$。

记向量 $\boldsymbol{S}_N\in F_q^{N\times 1}$ 表示 N 个源数据包，F_q 表示编码有限域，矩阵 $\boldsymbol{C}\in F_q^{(k+M-1)\times N}$ 表示节点 CR_i 在两阶段接收到的数据包编码系数矩阵。需要指出的是，$\boldsymbol{C}$ 在一些文献中也被称为传输矩阵[8]，且可被分片表示为 $\boldsymbol{C}=[\boldsymbol{C}_{k\times N}\ \boldsymbol{C}_{(M-1)\times N}]^{\mathrm{T}}$。广播阶段接收的 k 个源数据包未经过编码，因此 $\boldsymbol{C}_{k\times N}$ 各行是互异的单位向量；协作阶段若节点 CR_i 未接收到节点 CR_j 的编码包，则在 $\boldsymbol{C}_{(M-1)\times N}$ 对应 CR_j 的编码行元素均为 0。则 CR_i 在两阶段接收到的编码数据包向量 $\mathbf{CP}$ 为

$$\mathbf{CP}=\boldsymbol{C}\boldsymbol{S}_N=\begin{pmatrix}\boldsymbol{C}_{k\times N}\\ \boldsymbol{C}_{(M-1)\times N}\end{pmatrix}\boldsymbol{S}_N=\begin{pmatrix}\boldsymbol{E}_{k\times k} & \mathbf{0}\\ \boldsymbol{C}'_{(M-1)\times k} & \boldsymbol{C}'_{(M-1)\times(N-k)}\end{pmatrix}\boldsymbol{Q}_{N\times N}\boldsymbol{S}_N \tag{7}$$

其中，$\boldsymbol{E}_{k\times k}$ 是 k 阶单位阵；$\boldsymbol{Q}_{N\times N}$ 是 N 阶初等列变换阵，可交换矩阵 $(\boldsymbol{E}_{k\times k}\ \mathbf{0})$ 列次序使 $(\boldsymbol{E}_{k\times k}\ \mathbf{0})\boldsymbol{Q}_{N\times N}=\boldsymbol{C}_{k\times N}$。

示例 1 如图 2 所示的 CR 过程，节点 CR_3 在两阶段接收的编码包 $\mathbf{CP}=[s_3\ \ s_2+2s_3\ \ 2s_1+3s_3]^{\mathrm{T}}$ 及其传输矩阵按式(7)分解过程

$$\boldsymbol{CP}=\underbrace{\begin{pmatrix}0&0&1\\0&1&2\\2&0&3\end{pmatrix}}_{\boldsymbol{C}}\underbrace{\begin{pmatrix}s_1\\s_2\\s_3\end{pmatrix}}_{\boldsymbol{S}_N}=\underbrace{\left(\begin{array}{c:cc}1&0&0\\ \hdashline 2&1&0\\3&0&2\end{array}\right)}_{\boldsymbol{C}'_{(M-1)\times(N-k)}}\underbrace{\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}}_{\boldsymbol{Q}_{N\times N}}\underbrace{\begin{pmatrix}s_1\\s_2\\s_3\end{pmatrix}}_{\boldsymbol{S}_N}$$

因此，CR_i 在接收到 $\mathbf{CP}$ 后是否能够成功解码出所有源数据包 $\boldsymbol{S}_N$ 问题等价于式(7)的线性方程组是否有唯一解，因此从列秩考虑解码失败的概率为

$$\Pr_{\mathrm{fail\_coop}}^{k}(N)=\Pr(\mathrm{rank}(\boldsymbol{C})<N))=\Pr(\mathrm{rank}(\boldsymbol{C}'_{(M-1)\times(N-k)})<N-k) \tag{8}$$

式(8)成立是因为只有传输矩阵 $\boldsymbol{C}$ 的秩为 N 时，方程组才可由 $\mathbf{CP}$ 解码出 $\boldsymbol{S}_N$。考虑到 $\mathrm{rank}(Q_{N\times N})=N$，且 $\mathrm{rank}(\boldsymbol{E}_{k\times k})=k$，有 $\mathrm{rank}(\boldsymbol{C})=k+\mathrm{rank}(\boldsymbol{C}'_{(M-1)\times(N-k)})$。因此，$\mathrm{CR}_i$ 成功解码的概率可以通过判断 $\boldsymbol{C}'_{(M-1)\times(N-k)}$ 是否列满秩来判定。为了简便，下文将 $\boldsymbol{C}'_{(M-1)\times(N-k)}$ 简记为 $\boldsymbol{C}'$。事实上，$\boldsymbol{Q}_{N\times N}$ 仅交换了 $\boldsymbol{C}$ 的列次序，使矩阵 $\boldsymbol{C}'$ 各列对应的是 CR_i 第一阶段未成功接收的 $N-k$ 个数据包，并未改变 $\boldsymbol{C}'$ 元素值，而 $\boldsymbol{C}'$ 元素值在 $\boldsymbol{F}_q/0$ 上随机分布，由两阶段传输过程共同决定。记 ε_l 表示簇内除 CR_i 外第 $l(1\leqslant l\leqslant M-1)$ 个节点传输到 CR_i 节点的编码包删除率，显然 $\Pr\{\varepsilon_l\}=e_{\mathrm{rd}}$，$\Pr\{\overline{\varepsilon_l}\}=1-e_{\mathrm{rd}}$。如果哑变量 θ 来自 F_q，则 $\boldsymbol{C}'$ 中第 l 行上任意元素 $c_{lj}(1\leqslant j\leqslant N-k)$ 的取值概率为

$$\Pr\{c_{lj}=0\mid\varepsilon_l\}=1$$

$$\Pr\{c_{lj}=\theta\mid\overline{\varepsilon_l}\}=\begin{cases}e_{\mathrm{sr}},\ \theta=0\\ \dfrac{1-e_{\mathrm{sr}}}{q-1},\ \theta\neq 0\end{cases} \tag{9}$$

这是由于对于 CR_i 节点而言，若在交互的过程中来自第 l 个节点的编码包发生删除，则矩阵 $\boldsymbol{C}'$ 的第 l 行所有元素 $c_{lj}(1\leqslant j\leqslant N-k)$ 一定全为 0；反之，则 c_{lj} 由第 l 个节点在广播过程是否接收到源数据包 s_j 来确定元素是否为 0。若 2 个阶段均未发生删除，则 c_{lj} 值可以为 q 阶有限域 $\boldsymbol{F}_q$ 中任意一个非零元。因此，c_{lj} 取到某一确定的非零元的概率为 $1/(q-1)$。

综上，CR 可解性分析思路是由式(9)的 CR 过程编码矩阵 $\boldsymbol{C}'$ 元素取值概率，然后根据式(8)分析 $\boldsymbol{C}'$ 的秩，从而求解 CR_i 协作阶段不能成功解码出剩余 $N-k$ 个数据包的概率 $\Pr_{\mathrm{fail\_coop}}^{k}(N)$ 的上下界，进

而根据式(6)得到 CR_i 解码出所有 N 个源数据包 $\mathrm{Pr}_{\mathrm{suc}}$ 的上界 $P_{\max}$ 和下界 $P_{\min}$。

4　基于网络编码的 CR 线性可解性上界

与第 3 节分析的场景一致，本文依旧假设簇内任意节点 CR_i 在广播阶段仅收到 N 个源数据包里的 $k(0\leqslant k\leqslant N)$ 个。根据 CR 传输过程容易发现，若簇内所有节点均未能在广播阶段成功接收某一个源数据包，则通过基于网络编码的 CR 过程也一定不能成功解码出这一源数据包。例如，在图 2 所示例子中，若节点 CR_2 广播阶段未能接收到源数据包 s_1，则簇内任意节点无法通过协作过程解码恢复出 s_1。因此，根据二项分布容易得到簇内任意节点 CR_i 解码失败概率 $\mathrm{Pr}_{\mathrm{fail\_coop}}^{k}(N)$ 的一个简单下界为

$$\mathrm{Pr}_{\mathrm{fail\_coop}}^{k}(N)\geqslant \sum_{i=1}^{N-k}\binom{N-k}{i}\left(e_{\mathrm{sr}}{}^{M-1}\right)^{i}\left(\left(1-e_{\mathrm{sr}}\right)^{M-1}\right)^{(N-k)-i} \tag{10}$$

容易发现，式(10)给出的下界仅考虑了广播阶段数据包删除率，忽略了更关键的交互阶段。因此，下面，本文将基于文献[20]的稀疏矩阵线性可解性判定思想，给出 $\mathrm{Pr}_{\mathrm{fail\_coop}}^{k}(N)$ 的另一个下界。

定理 1　在基于网络编码的 CR 机制中，对于包含 M 个节点的协作簇，若簇内任意节点 CR_i 在广播阶段仅收到 N 个源数据包里的 $k(0\leqslant k\leqslant N)$ 个，则 CR_i 在协作阶段不能够完全解码出其余 $N-k$ 个源数据包的概率 $\mathrm{Pr}_{\mathrm{fail\_coop}}^{k}(N)$ 的一个下界可以表示为

$$\mathrm{Pr}_{\mathrm{fail\_coop}}^{k}(N)\geqslant 1-\prod_{j=1}^{N-k}(1-\eta^{(M-1)-j+1}) \tag{11}$$

其中，$\eta=\min(e_{\mathrm{rd}}+(1-e_{\mathrm{rd}})e_{\mathrm{sr}},(1-e_{\mathrm{sr}})(1-e_{\mathrm{rd}})/(q-1))$。

证明　详见附录 1。

因此，综合式(10)和定理 1，即可得到的一个较紧密下界为

$$P_{\mathrm{fail\_min}}\left(N-k\right)=\max\left(\sum_{i=1}^{N-k}\binom{N-k}{i}\left(e_{\mathrm{sr}}^{M-1}\right)^{i}\cdot\left(\left(1-\delta_1\right)^{M-1}\right)^{(N-k)-i},1-\prod_{j=1}^{N-k}(1-\eta^{(M-1)-j+1})\right) \tag{12}$$

其中，$\eta=\min(e_{\mathrm{rd}}+(1-e_{\mathrm{rd}})e_{\mathrm{sr}},(1-e_{\mathrm{sr}})(1-e_{\mathrm{rd}})/(q-1)$。由簇内任意节点 CR_i 在广播阶段仅收到 N 个源数据包里的 k 个，且 $0\leqslant k\leqslant N$，因此将式(12)代入式(6)，即可得到 CR_i 经过一次完整的数据传输过程之后成功解码出 N 个数据包的概率 $\mathrm{Pr}_{\mathrm{suc}}$ 的一个较紧密上界 $P_{\max}$ 为

$$P_{\max}=\sum_{k=0}^{N}\binom{N}{k}\left(1-e_{\mathrm{sr}}\right)^{k}e_{\mathrm{sr}}^{N-k}\left(1-P_{\mathrm{fail\_min}}\left(N-k\right)\right) \tag{13}$$

5　基于网络编码的 CR 线性可解性下界

与上界分析的模型一致，本节分析 CR 线性可解性的下界。

定理 2　在基于网络编码的 CR 机制中，对于包含 M 个节点的协作簇，若簇内任意节点 CR_i 在广播阶段仅收到 N 个源数据包里的 $k(0\leqslant k\leqslant N)$ 个，则 CR_i 在协作阶段不能够完全解码出其余 $N-k$ 个源数据包的概率 $\mathrm{Pr}_{\mathrm{fail\_coop}}^{k}(N)$ 的一个上界为

$$\mathrm{Pr}_{\mathrm{fail\_coop}}^{k}(N)\leqslant\frac{1}{q-1}\sum_{i=1}^{N-k}\binom{N-k}{i}(q-1)^{i}\left(e_{\mathrm{rd}}+\left(1-e_{\mathrm{rd}}\right)\cdot\left(q^{-1}+\left(1-q^{-1}\right)\left(\frac{qe_{\mathrm{sr}}-1}{q-1}\right)^{i}\right)\right)^{M-1}$$

其中，e_{sr} 和 e_{rd} 分别是两阶段的数据包删除率，q 是编码有限域阶。

证明　详见附录 2。

实验表明，定理 2 所得到的上界在编码有限域阶 q 的值较小时紧密；而当 q 较大时，其值趋近于 1，失去指导价值，需要进一步优化。注意到，由定理 1 的证明过程，解码失败概率的上界还可以表示为

$$\mathrm{Pr}_{\mathrm{fail\_coop}}^{k}(N)\leqslant 1-\prod_{i=1}^{N-k}(1-\varphi^{(M-1)-i+1}) \tag{14}$$

其中，$\varphi=\max(e_{\mathrm{rd}}+(1-e_{\mathrm{rd}})e_{\mathrm{sr}},(1-e_{\mathrm{sr}})(1-e_{\mathrm{rd}})/(q-1))$。证明过程与定理 1 相同，此处不再赘述。

因此，综合式(14)和定理 2，即可得到 $\mathrm{Pr}_{\mathrm{fail\_coop}}^{k}(N)$ 的一个较紧密上界为

$$P_{\mathrm{fail\_max}}\left(N-k\right)=\min\left(\frac{1}{q-1}\sum_{i=1}^{N-k}\binom{N-k}{i}(q-1)^{i}\left(e_{\mathrm{rd}}+\left(1-e_{\mathrm{rd}}\right)\cdot\left(q^{-1}+\left(1-q^{-1}\right)\left(\frac{qe_{\mathrm{sr}}-1}{q-1}\right)^{i}\right)\right)^{M-1},1-\prod_{i=1}^{N-k}\left(1-\varphi^{(M-1)-i+1}\right)\right)$$

其中，$\varphi=\max(e_{\mathrm{rd}}+(1-e_{\mathrm{rd}})e_{\mathrm{sr}},(1-e_{\mathrm{sr}})(1-e_{\mathrm{rd}})/(q-1))$。将上式代入式(6)，即可得到簇内任意节点 CR_i 经过一次完整的数据传输过程之后成功解码出 N 个数据包的概率 $\mathrm{Pr}_{\mathrm{suc}}$ 的一个较紧密下界 $P_{\min}$ 为

$$P_{\min}=\sum_{k=0}^{N}\binom{N}{k}(1-e_{\mathrm{sr}})^{k}e_{\mathrm{sr}}^{N-k}\left(1-P_{\mathrm{fail\_max}}(N-k)\right) \quad (15)$$

6 基于网络编码的 CR 线性可解性在线判定算法设计

在已有基于网络编码的 CR 研究中，簇内节点对编码数据包的解码发生在整个 CR 协作恢复阶段完成之后，采用 Gauss 消去法对其所有接收到的编码包进行统一解码。若能解码出所有源数据包，则说明线性可解，反之则不可解。因此，传统研究中每个簇内节点在整个协作阶段均需要侦听所有编码包，然后在协作阶段完成后统一解码，因此解码的等待时延较高，节点持续侦听引起的能耗也较高，并且节点还需要预留足够的存储空间以缓存待解码数据包。针对该问题，本文提出一种在线判定算法——改进 Gauss-Jordan 法，工作流程如图 3 所示，每个簇内节点能够在 CR 协作恢复过程中就根据自身接收到的编码包进行部分解码，不需要等待协作阶段完成再进行，不仅降低了传统高斯方法的解码等待时延，也避免了需预设编码包缓存空间所引起的存储开销。

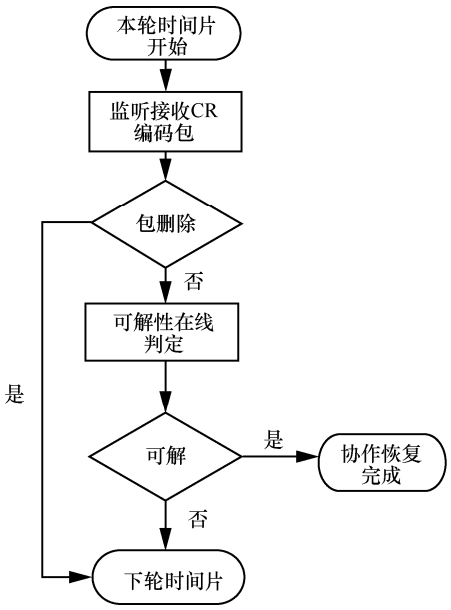


图 3 改进 Gauss-Jordan 法的工作流程

簇内任意节点 CR_i 采用改进 Gauss-Jordan 法的解码过程描述如算法 1 所示，注意，可解性在线判定过程也是逐步解码的过程。对于图 2 所示例子，采用所提算法的节点 CR_3 在两阶段 CR 过程在线解码过程如表 2 所示，该过程共消耗了 5 个时间片，3 个为广播阶段接收源数据包，2 个为协作修复阶段接收编码包。

表 2 改进 Gauss-Jordan 算法解码过程

时间片	事件	解码矩阵 $\boldsymbol{C}$	码字阵 **CP**
1	Receive(s_1) (失败)	NULL	NULL
2	Receive(s_2) (失败)	NULL	NULL
3	Receive(s_3)	$\begin{bmatrix}0&0&1\end{bmatrix}$	$\begin{bmatrix}s_3\end{bmatrix}$
4	Receive($\mathbf{cp}_1$)	$\begin{bmatrix}0&1&0\\0&0&1\end{bmatrix}$	$\begin{bmatrix}s_2\\s_3\end{bmatrix}$
5	Receive($\mathbf{cp}_2$)	$\begin{bmatrix}2&0&0\\0&1&0\\0&0&1\end{bmatrix}$	$\begin{bmatrix}2s_1\\s_2\\s_3\end{bmatrix}$
5	rank=3 (解码完成)	$\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$	$\begin{bmatrix}s_1\\s_2\\s_3\end{bmatrix}$

算法 1 改进 Gauss-Jordan 算法的 CR 协作过程可解性判定与渐进解码算法

1) 初始化//初始化广播阶段完成后 CR_i 的状态，**CP** 记录了广播阶段成功接收到的数据包，解码矩阵 $\boldsymbol{C}$ 的各行初始化为各包的编码系数向量，因此若广播阶段成功接收 N 个源包中的 k 个，则 $\boldsymbol{C}$ 的秩也为 k

2) while rank < N//需要编码协作恢复

3) $t\leftarrow t+1$//接收编码包需消耗一个时间片

4) if($t==N+M$) break//时间片用完，协作恢复阶段结束，未成功解码

5) else

6) Receive(state, $\boldsymbol{c}_t$, $\mathbf{cp}_t$)//从邻居节点接收编码数据包 $\mathbf{cp}_t$ 及其编码系数 s_t

7) if(state == FALSE) continue//丢包

8) else

9) for j=1:1:Row($\boldsymbol{C}$) //对码字和编码系数同时进行 Gauss-Jordan 消元

10) $\boldsymbol{c}_t\leftarrow\boldsymbol{c}_t-\dfrac{c_k}{C_{jk}}\boldsymbol{C}_j$ // C_{jk} 是 $\boldsymbol{C}$ 的第 j 行向量 $\boldsymbol{C}_j$ 中第一个非 0 元系数

11) $\mathbf{cp}_t\leftarrow\mathbf{cp}_t-\dfrac{c_k}{C_{jk}}\mathbf{CP}_j$

12) end for

13)　if ($\boldsymbol{c}_t \neq \mathbf{0}$)

14)　rank ← rank+1

15)　将 $\boldsymbol{c}_t$ 和 $\mathbf{cp}_t$ 分别插入 $\boldsymbol{C}$ 和 $\mathbf{CP}$ 的第 l 行使 $\boldsymbol{C}$ 阶梯化//l 为 $\boldsymbol{c}_t$ 第一个非 0 元出现的序号

16)　end if

17)　end if

18)　end if

19)　if (rank == N) break//协作修复成功，自下而上从增广矩阵 $[\boldsymbol{C}\ \mathbf{CP}]$ 中逐个解方程组得解 $\boldsymbol{x}_N, \boldsymbol{x}_{N-1}, \cdots, \boldsymbol{x}_1$，解 $\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_N$ 即为 N 个源数据包。节点此时可进入休眠，不需要侦听其余编码包

20)　end if

21) end while

7　改进 Gauss-Jordan 算法与传统 Gauss 方法性能对比分析

7.1　解码时延对比分析

1) 传统 Gauss 方法

在传统 Gauss 方法解码过程中，协作簇内任意节点 CR_i 在第二阶段完成后才尝试进行高斯消去解码，因此解码出源数据包的时延 T_{Gaussian} 就是两阶段 CR 传输过程所消耗的时间，即广播阶段基站发送 N 个源数据包的发送（传输）时延 T_{broad} 和协作恢复阶段的编码数据包排队待解码的时延 T_{coop}。为了简化分析过程，解码时延分析未考虑无线信号的传播时延和解码过程的运算处理时延。若协作簇包含 M 个节点，并且为了分析方便，将两阶段信道传输一个数据包或编码包的时延均记为一个时间片，则 Gauss 方法 CR_i 解码成功的时延恒定，值为 $T_{\text{Gaussian}}=T_{\text{broad}}+T_{\text{coop}}=N+M$，单位为时间片。

2) 改进 Gauss-Jordan 算法

与传统 Gauss 方法相比，簇内任意节点 CR_i 采用改进 Gauss-Jordan 算法的时延 $T_{\text{Gauss-Jordan}}$ 也包括两部分：广播阶段消耗的时间片 T_{broad}（$T_{\text{broad}}=N$）和协作阶段在线解码时延 T'_{coop}。由于 CR_i 在协作修复阶段采用所提出的改进 Gauss-Jordan 算法可在线判断可解性，随着接收编码包累积的过程，一旦发现解码矩阵 $\mathbf{CP}$ 线性可解即停止侦听并完成解码。因此，CR_i 协作阶段解码时延 T'_{coop} 是随着编码包接收过程直到解码矩阵 $\mathbf{CP}$ 满秩的平均时间。为了量化分析 T'_{coop}，本文将节点采用改进 Gauss-Jordan 算法的解码过程建模为一种齐次吸收马尔可夫过程（AMP, absorbing Markov process）。

定义 1　在 CR 协作恢复阶段，当且仅当 $\mathrm{rank}(\mathbf{CP})=r$，$k \leqslant r \leqslant N$，簇内任意节点的解码状态对应 AMP 的状态 s_r。

改进 Gauss-Jordan 算法的解码 AMP 模型如图 4 所示。为了合理估算簇内任意节点的平均解码时延，AMP 的初始状态设置为广播阶段完成后簇内任意节点成功接收到的数据包个数期望。因此，s_k 为节点协作阶段解码矩阵 $\mathbf{CP}$ 秩的初始值，且 $k=\lceil Ne_{\text{sr}} \rceil$，其中 $\lceil * \rceil$ 为取整运算。AMP 的吸收态为 $\mathbf{CP}$ 满秩状态 s_N，因此此状态下转移概率 $p_{N,N}$=1。为了求解 AMP 的状态转移矩阵以分析平均时延，本文接下来给出一些基础的定理。

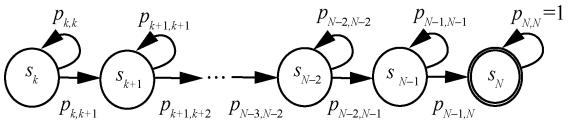


图 4　改进 Gauss-Jordan 算法的解码 AMP 模型

引理 1[20]　对于一个 $n \times n$ 矩阵 $\boldsymbol{M}$，若其矩阵元素均从有限域 GF(q) 上随机选取，且选取值为 0 的概率为 1−p，选取 GF(q) 上任意非 0 元的概率为 $p/(q-1)$，则矩阵 $\boldsymbol{M}$ 非奇异的概率至少为 $\prod_{i=1}^{n}(1-\pi^i)$，其中 $\pi=\max\{p/(q-1), 1-p\}$。

证明　见参考文献[20]“Theorem 6.3”。

推论 1　在 CR 协作恢复阶段采用改进 Gauss-Jordan 算法解码，协作簇内任意节点的解码矩阵记为 $\mathbf{CP}$，若某时间片编码矩阵 $\mathbf{CP}$ 秩为 t，则后续时间片该节点若成功接收一个新的编码包，更新解码矩阵为 $\mathbf{CP}'$ 后，解码矩阵 $\mathbf{CP}'$ 秩增为 t+1 的概率为

$$p(t,N) \geqslant 1-\left[\max\left(e_{\text{sr}}, \frac{1-e_{\text{sr}}}{q-1}\right)\right]^{N-t}$$

其中，e_{sr} 是 CR 广播阶段数据包平均删除率。

证明　详见附录 3。

由于寻找 $p(t,N)$ 的精确解一直是数论领域的一个待解难题，尚未寻找到其解析解[21]，在下文 AMP 的状态转移概率分析中，本文采用推论 1 的结论来近似 $p(t,N)$，即

$$p(t,N) \approx 1-\left[\max\left(e_{\text{sr}}, \frac{1-e_{\text{sr}}}{q-1}\right)\right]^{N-t}$$

基于此，本文分析协作恢复阶段任意节点解码过程 AMP 的任意两状态间的转移概率。

引理 2 在 CR 协作恢复阶段采用 Gauss-Jordan 算法解码，若协作阶段编码包删除率为 e_{rd}，则间隔一个时间片簇内任意节点的马尔可夫过程由当前状态 s_i 转移至状态 s_j 的概率 $p_{i,j}$ 为

$$p_{i,j}=\begin{cases}p(i,N)(1-e_{\mathrm{rd}}), j=i+1\\ 1-p(i,N)(1-e_{\mathrm{rd}}), j=i\\ 0,\text{其他}\end{cases}$$

证明 详见附录 4。

引理 2 给出了 AMP 任意两状态转移概率，将它作为矩阵元素容易得到 AMP 的一步状态转移概率矩阵 $\boldsymbol{P}$，按标准型[22]分块排列后形如

$$\boldsymbol{P}=\begin{pmatrix}1 & 0\\ \boldsymbol{S} & \boldsymbol{Q}\end{pmatrix} \tag{16}$$

其中，$\boldsymbol{P}$ 的第一行和第一列对应 AMP 吸收态 s_n，其余行列按次序分别对应瞬时态 $s_k,\cdots,s_{n-1}$，$(n-k)\times(n-k)$ 矩阵 $\boldsymbol{Q}$ 为所有瞬时态间的一步转移概率矩阵。接下来，本文将根据 $\boldsymbol{P}$ 和吸收马尔可夫链性质估算出改进 Gauss-Jordan 算法 AMP 从初始态 s_k 转移至吸收态 s_n 的平均步数，而 AMP 每移动一步均消耗一个时间片，即可得到改进 Gauss-Jordan 算法的平均解码时延。

定理 3 M 个节点在 CR 协作阶段采用改进 Gauss-Jordan 算法恢复 N 个源数据包，其在线解码过程平均时延 $T'_{\mathrm{coop}}=\min\left(\sum_{i=1}^{N-1}T_{1,i},M\right)$，$\boldsymbol{T}=(\boldsymbol{I}-\boldsymbol{Q})^{-1}$，其中 $\boldsymbol{I}$ 为单位阵，$\boldsymbol{Q}$ 为所有瞬时态间的一步转移概率矩阵。

证明 详见附录 5。

由于改进 Gauss-Jordan 算法总时延 $T_{\text{Gauss-Jordan}}$ 包括固定的广播阶段时延 T_{broad}（T_{broad}=N）和协作阶段在线解码时延 T'_{coop} 两部分，由定理 3 得

$$T_{\text{Gauss-Jordan}}=T_{\mathrm{broad}}+T'_{\mathrm{coop}}=N+\min\left(\sum_{i=1}^{N-1}T_{1,i},M\right) \tag{17}$$

因此，在解码时延方面改进 Gauss-Jordan 算法明显优于传统高斯方法（$T_{\text{Gaussian}}=N+M$），且只有在最坏情况即解码失败时才会等于传统高斯方法。

7.2 算法复杂度对比分析

采用传统 Gauss 方法解码时，解码过程发生在两阶段 CR 传输过程结束后，在解码时需将两阶段接收到的所有编码包联立方程组求解。由伯努利过程性质知，具有 M 个节点的协作簇，任意节点在广播阶段平均收到 N 个源数据包中的 Ne_{sr} 个，在协作恢复阶段平均收到 $(M-1)e_{\mathrm{rd}}$ 个编码包，因此基于高斯消去的 Gauss 方法的解码时间复杂度为 $O((e_{\mathrm{sr}}N+e_{\mathrm{rd}}(M-1))^3)$。

本文所提出的改进 Gauss-Jordan 算法在协作恢复阶段，每个时间片成功接收到新的编码包后会执行一次消元处理，这样的消元处理共有（$N-e_{\mathrm{sr}}N$）次。由算法 1 知，协作阶段若第 i 次收到编码数据包，则第 i 次消元运算规模为 $(e_{\mathrm{sr}}N+i)^2$ 次，因此改进 Gauss-Jordan 算法的总时间复杂度为 $O\left(\sum_{i=e_{\mathrm{sr}}N+1}^{N}i^2\right)$，即 $O\left(\frac{N(N+1)(2N+1)-e_{\mathrm{sr}}N(e_{\mathrm{sr}}N+1)(2e_{\mathrm{sr}}N+1)}{6}\right)$。与 Gauss 方法对比，2 种解码方法均为多项式复杂度，但改进 Gauss-Jordan 算法复杂度较小，且问题规模不受协作簇节点数影响，更适应于大范围的部署应用。

8 数值结果

本节通过数值模拟与实际部署相结合的思路来检验上文给出的结论和算法。仿真过程采用控制变量法，控制编码有限域阶数、协作节点数、源数据包数、两阶段信道删除率等多种变量参数，检验 CR 过程结果并与上文结论进行对比。例如，对于解码成功率检测实验，通过实验协作网络内任意目标节点解码出所有源节点数据包的概率，再与式(13)给出的理论上界 $P_{\max}$ 和式(15)给出的理论下界 $P_{\min}$ 进行对比验证。为了降低误差，每组实验均运行了 10^6 次。可解性理论上下界验证实验参数设置如表 3 所示。

表 3 可解性理论上下界验证实验参数设置

参数	含义	取值范围
M/个	协作簇内节点数量	10～25
N/个	源数据包数量	5～15
q	编码有限域 F_q /GF(q)的阶	2～2^{16}
e_{sr}	广播阶段数据包删除率	0.1～0.9
e_{rd}	协作阶段数据包删除率	0.1～0.9

首先，实验编码有限域阶对目标节点线性可解性的影响。固定源数据包数 $N=10$，协作节点数 $M=15$，节点广播信道删除率 $e_{\mathrm{sr}}=0.5$ 和协作信道

删除率均为 $e_{\mathrm{rd}}=0.5$，当编码有限域 F_q 阶 q 变化范围为 2～2^{16} 时，簇内节点经过 CR 过程解码成功率如图 5 所示。

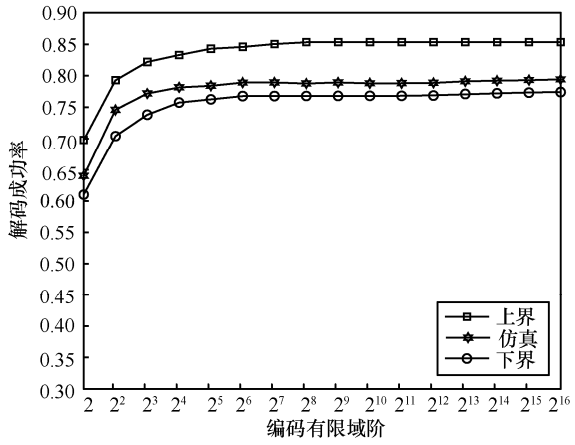


图 5　编码有限域阶对解码成功率的影响

从图 5 可以发现，在不同编码有限域阶下，所提出的理论上下界均有效，并且当编码有限域阶小于 2^4 时，随着有限域阶的增加，节点解码成功率迅速上升，这一趋势在编码阶处于 2^4～2^8 时会变缓，而当编码阶大于 2^8 时，编码有限域选择不再对线性可解性和理论上下界产生明显影响(编码有限域阶从 2^8 增加到 2^{16},但解码成功率仅从 0.788 增加到 0.794)。这说明编码有限域阶选取过小会造成 CR 机制可解性差，而当有限域阶超过一定值时就不再成为可解性的主要约束因素,因此设计具体 CR 机制需要在考虑编解码效率基础上合理地选择编码有限域。

在此基础上，进一步实验所提出的改进 Gauss-Jordan 算法在不同编码有限域下的渐进解码算法解码时延，实验时维持源数据包数、协作节点数、广播信道删除率均与图 5 所示实验一致，实验结果如图 6 所示。结果显示，在同一个编码有限域下，随着协作阶段数据包删除率增加，解码时延明显递增，最终趋近于传统 Gauss 方法解码时延。这是由于随着协作删除率增加，节点的线性可解性下降直至解码失败。横向对比不同域在某一个协作信道删除率下的解码时延可以发现，编码有限域阶越小，解码时延越大，但当编码有限域阶大于 2^8 时，编码有限域阶对解码时延影响变弱，如图 6 中 2^8 和 2^{16} 这 2 种编码有限域，虽然编码有限域阶扩大了一倍，但平均解码时延仅降低了 0.1，该现象说明合理提高编码有限域阶能够增加 CR 机制的协作过程解码成功率，降低解码时延，但当编码有限域阶超过一定阈值时，则提升效果有限。

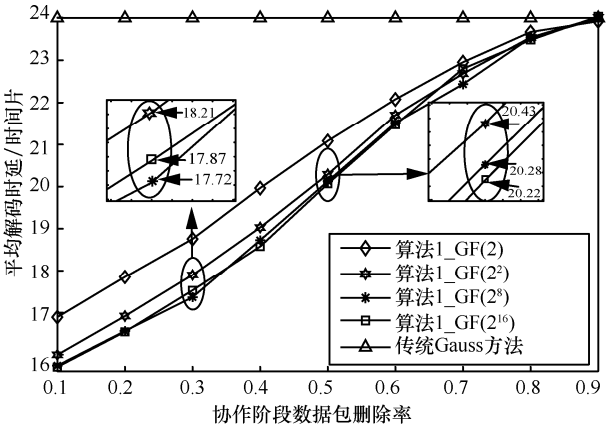


图 6　改进 Gauss-Jordan 算法与传统 Gauss 方法解码时延比较

由 7.2 节算法复杂性分析可知，2 种解码算法的复杂性主要受到源数据包数 N、协作节点数 M 和节点广播信道删除率 e_{sr} 决定，而网络编码运算是基于有限域的运算,在实际节点上的运行复杂度还受到具体有限域运算实现方法影响。为了对比 2 种解码算法的计算复杂度,基于一维查找表和二维查找表 2 种有限域实施方法[23]分别实现了 2 种解码算法，并部署在 Freescale MC13213 节点上(MC13213 是 Freescale 生产的一种基于经典 HCS08 系列微程序控制器的 RF 片上系统（SiP），在 WPAN、ZigBee 等各类无线组网应用领域得到广泛使用)。实验时关闭了节点天线，并通过随机函数来模拟 CR 过程中是否成功接收到编码数据包（对天线的收发处理需要处理器的介入，而解码算法复杂度本身与天线编码包接收过程独立。因此，不关闭天线会造成算法复杂度测试结果不准确)，具体实验参数设置如表 4 所示。在节点上共执行了 4 组对比实验，每次实验均编码 32 KB 的随机数据，每组实验重复 10^6 次，实验结果如图 7 所示。

表 4　改进 Gauss-Jordan 算法复杂度实验参数设置

参数	值	参数	值
微处理器	MC9S08GB60	闪存/KB	512
RAM/KB	4	工作电压/V	3.4
有限域阶	2^4,2^8	时钟频率/MHz	40
e_{sr}	0.5	源数据包数	32
数据包载荷/ksymbol	1	实验重复次数	10^6

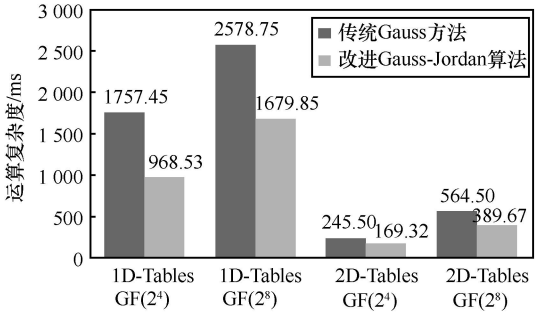


图 7　改进 Gauss-Jordan 算法与传统 Gauss 方法运算复杂度比较

实验结果表明，在 2 种有限域实现方法上本文所提出的改进 Gauss-Jordan 算法均较传统 Gauss 方法复杂度低约 35%，这是因为改进算法的消元迭代次数较少。同时也能发现，有限域阶对 2 种解码算法的复杂度影响较明显，这是因为有限域阶对有限域运算方法的 RAM 存储需求差异显著。对于一维查表法，在 2^4 阶有限域上共需要设置 96 B 的指数表和对数表，而 2^8 域则需要 4 160 B；同样，对于二维查表法，在 2^4 阶域上共需要设置 528 B 的指数表和乘、除法表，而 2^8 域需要超过 128 KB 闪存空间。相较于有限域的一维查表实现法，2 种解码算法在二维查表法下运算效率提升显著，但二维表法的 RAM 存储需求较高，尤其是对于需要高阶有限域的 CR 协作过程，本质上来说，有限域的二维查表实现就是一种以存储空间来换取运算效率的方法。

接下来，本文仿真实验广播阶段数据包删除率对目标节点线性可解性的影响。设置广播信道的删除率 e_{sr} 变化范围为 0.1～0.9、编码有限域固定为 GF(2^4)、交互阶段数据包的删除率固定为 $e_{rd}=0.4$，当源数据包个数 $N=10$、协作节点数 $M=15$ 时，实验结果如图 8 所示。从实验网络内节点解码成功率对比上，仿真结果曲线落在下界曲线和上界曲线之间，并且更逼近下界。例如在编码有限域为 GF(2^4) 的情况下，理论下界与实际结果误差区间仅为 0.83%。统计发现，上界平均误差区间为 19.46%，在首尾端较紧密。这是由于随着广播信道删除率增加，当 e_{sr} 超过 0.35 时协作节点的编码向量稀疏度会急速增大，引起由定理 1 作用的理论上界松弛度扩大，这一过程会持续到 e_{sr}=0.7 时，此时理论上界会切换到由式(10)所形成的约束，紧密度会得到提高。

最后，分析源数据包数和协作簇内节点数对线性可解性上下界影响。固定广播信道删除率固定为 e_{sr}=0.7，协作信道删除率固定为 e_{rd}=0.4，编码有限域为 GF(2^4)，分别考察源数据包数 N 为 5～15、协作簇内节点数 M 为 10～25 时的解码成功率，实验结果分别如图 9 和图 10 所示。实验发现，本文所提出的改进 Gauss-Jordan 算法的上下界在不同源数据包数、协作簇内节点数下均能够较精确地估算解码成功率，并且当 CR 机制各性能参数固定时，源数据包数和协作节点数对线性解码率影响较大，说明传输策略和节点协作簇建立策略是 CR 机制的重要内容。同时实验也验证了一个直观结论，即在相同的信道条件下，中继节点数越大，节点的解码成功率越大；源数据包数越小，节点的解码成功率越大。

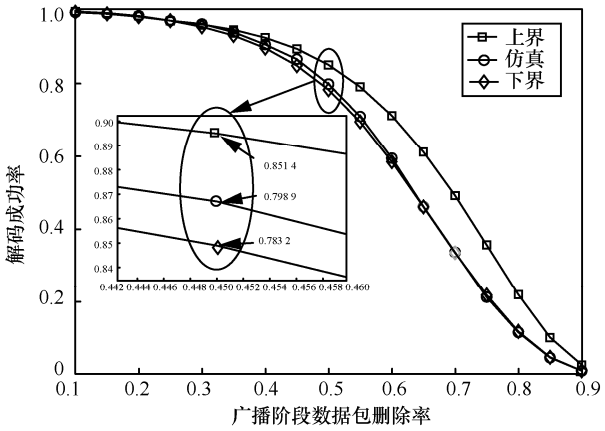


图 8　广播阶段数据包删除率对目标节点线性可解性的影响

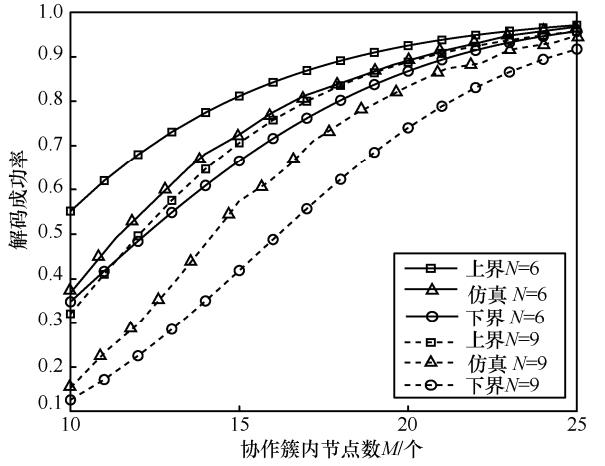


图 9　协作节点数对线性可解性的影响

9　结束语

线性可解性是基于网络编码的 CR 机制应用中的关键基础问题，本文建立了 CR 可解性的量化分析模型，并给出了紧密的理论上下界。在此基础上

设计了一种在线判定算法，降低了节点可解性识别的等待时延。下一步的工作可分成两个方向：一方面继续探索线性可解性精确解，鉴于该问题求解难度和稀疏随机矩阵的线性可解性探索等效，是数论领域待解难题，一个可行的解决思路是利用蒙特卡洛方法使用计算机实验出一个精确解再寻求理论验证；另一方向是基于本文所提出的理论上下界和渐进解码算法，设计流式协作恢复机制，实现广播和恢复两阶段的流水线联动，完成数据包的数据的在线编码传输功能，进一步在提高网络传输可靠性的同时降低 CR 恢复时延。

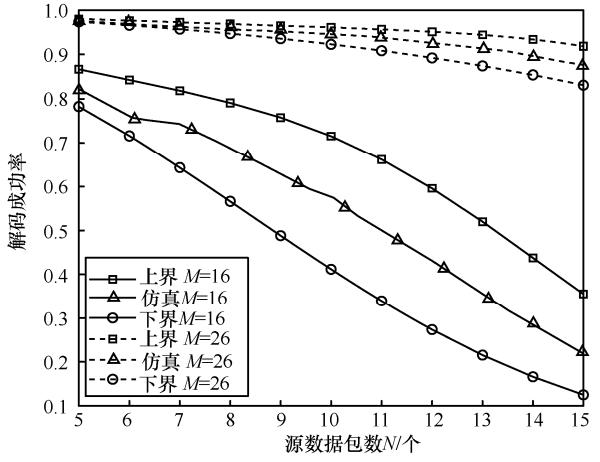


图 10　源数据包数对线性可解性的影响

附录 1　定理 1 的证明

证明　根据式(8)知 $\Pr^{k}_{\text{fail\_coop}}(N)=\Pr(\text{rank}(\boldsymbol{C}')<N-k)$，因此可以通过判断 $(M-1)\times(N-k)$ 矩阵 $\boldsymbol{C}'$ 所有列向量是否均线性无关来估算 $\Pr^{k}_{\text{fail\_coop}}(N)$ 界。若假设 $\boldsymbol{C}'$ 的前 $j(j=1,2,\cdots,N-k-1)$ 个列向量 $\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_j$ 已被证明线性独立，则当且仅当 $\boldsymbol{c}_{j+1}$ 不在这些向量所张成的线性子空间 $\boldsymbol{V}_j$ 中时，第 j+1 个列向量 $\boldsymbol{c}_{j+1}$ 与这些向量线性无关。记其概率为 p_{j+1}，则根据增量思想 $\boldsymbol{C}'$ 的所有 $N-k$ 个列向量均线性无关的概率可表示为 $\Pr(\text{rank}(\boldsymbol{C}')=N-k)=\prod_{j=0}^{N-k-1}p_{j+1}$，因此问题关键在于求解 p_{j+1}。

考虑 $\boldsymbol{C}'$ 中前 j 个列向量 $\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_j$ 形成的矩阵，由于这 j 个列向量线性无关，因此可以通过矩阵的初等列变换，类似高斯消去，形成存在 $j\times j$ 单位阵的变换阵。不失一般性，本文假设 $\boldsymbol{C}'$ 前 j 行形成了新阵的单位阵。因为初等列变换不改变空间的基，所以新阵的列向量张成的线性子空间与原空间 $\boldsymbol{V}_j$ 相同。由于新阵的列向量构成了子空间 $\boldsymbol{V}_j$ 的一组基，因此容易发现属于子空间的所有向量前 j 个系数可以任意取值，而其余 $(M-1)-j$ 个系数取值由前 j 个系数唯一确立。又由式(9)知 $\boldsymbol{C}'$ 里任意元素取域 F_q 中 0 元的概率为 $e_{\text{rd}}+(1-e_{\text{rd}})e_{\text{sr}}$，且任意一个非 0 元概率为 $(1-e_{\text{sr}})(1-e_{\text{rd}})/(q-1)$，因此向量 $\boldsymbol{c}_{j+1}$ 落在 $\boldsymbol{V}_j$ 里的概率 p_{j+1} 至多为 $1-\eta^{(M-1)-j}$，从而 $\Pr^{k}_{\text{fail\_coop}}(N)=\Pr(\neg\text{rank}(\boldsymbol{C}')=N-k)\geqslant 1-\prod_{j=0}^{N-k-1}(1-\eta^{(M-1)-j})$，定理 1 得证。

附录 2　定理 2 的证明

证明　由式(8)可知

$$\Pr^{k}_{\text{fail\_coop}}(N)=\Pr\{\text{rank}(\boldsymbol{C}')<N-k\}=$$
$$\Pr\{\exists\boldsymbol{v}\in F_q^{N-k}\text{and }\boldsymbol{v}\neq\boldsymbol{0}^{\mathrm{T}}\text{ subject to }\boldsymbol{C}'\boldsymbol{v}=\boldsymbol{0}^{\mathrm{T}}\}\leqslant$$
$$\sum_{l=1}^{N-k}\Pr\{\boldsymbol{C}'\boldsymbol{x}=\boldsymbol{0}^{\mathrm{T}}\,|\,\|\boldsymbol{x}\|_0=l,\boldsymbol{x}\in\{F_q^{N-k}\}\}=$$
$$\frac{1}{q-1}\sum_{l=1}^{N-k}\binom{N-k}{l}(q-1)^l\Pr\{\boldsymbol{C}'\boldsymbol{x}=\boldsymbol{0}^{\mathrm{T}}\,|\,\|\boldsymbol{x}\|_0=l\}\tag{18}$$

其中，$\|\boldsymbol{x}\|_0$ 表示向量 $\boldsymbol{x}$ 的 L_0 范数。式(18)乘以 $1/(q-1)$ 是因为若存在一个非零向量 $\boldsymbol{x}$ 使 $\boldsymbol{C}'\boldsymbol{x}=\boldsymbol{0}^{\mathrm{T}}$，则 F_q 域内任意非 0 元 α 均满足 $\boldsymbol{C}'(\alpha\boldsymbol{x})=\boldsymbol{0}^{\mathrm{T}}$ 成立；而在 q 阶有限域 F_q 中，非 0 元 α 恰有 $q-1$ 个。因此，定理 2 的证明转化为如何确立 $\Pr\{\boldsymbol{C}'\boldsymbol{x}=\boldsymbol{0}^{\mathrm{T}}\,|\,\|\boldsymbol{x}\|_0=l\}$，记其值为 P_l。若 $\boldsymbol{C}'$ 按行分片的 $M-1$ 个行向量为 $\boldsymbol{C}'=[\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_{M-1}]^{\mathrm{T}}$，$\boldsymbol{C}'$ 的第 i 行向量 $\boldsymbol{c}_i$ 为 $\boldsymbol{c}_i=[c_{i1},\cdots,c_{i(N-k)}]\,(1\leqslant i\leqslant M-1)$，$\|\boldsymbol{x}\|_0=l$ 的向量为 $\boldsymbol{x}=[x_1,\cdots,x_{N-k}]^{\mathrm{T}}$，不失一般性，假设其前 l 个元素非 0（即 $\boldsymbol{x}=\{x_1,x_2,\cdots,x_l,0,\cdots,0\}^{\mathrm{T}}$），则寻找满足 $\boldsymbol{C}'\boldsymbol{x}=\boldsymbol{0}^{\mathrm{T}}$ 的 $(N-k)\times1$ 维向量 $\boldsymbol{x}$ 等价于寻找 $\boldsymbol{C}'$ 的 $M-1$ 个满足 $\boldsymbol{c}_i\boldsymbol{x}=0$ 的 $1\times(N-k)$ 维行向量 $\boldsymbol{c}_i$。若设 $S_k=\Pr\{\boldsymbol{c}_i\boldsymbol{x}=0\}=\Pr\left\{\sum_{j=1}^{l}c_{ij}x_j=0\right\}$，则由于 $\boldsymbol{C}'$ 各行独立，因此 $P_k=\prod_{i=1}^{M-1}\Pr\{\boldsymbol{c}_i\boldsymbol{x}=0\}=(S_l)^{M-1}$。由式(9)可知 $\Pr\{c_{ij}=0\,|\,\varepsilon_i\}=1$，所以 $\Pr\{\boldsymbol{c}_i\boldsymbol{x}=0\,|\,\varepsilon_i\}=1$，因此

$$S_k=\Pr\{\boldsymbol{c}_i\boldsymbol{x}=0\}=\Pr\{\varepsilon_i\}\Pr\{\boldsymbol{c}_i\boldsymbol{x}=0\,|\,\varepsilon_i\}+$$
$$\Pr\{\overline{\varepsilon_i}\}\Pr\{\boldsymbol{c}_i\boldsymbol{x}=0\,|\,\overline{\varepsilon_i}\}=e_{\text{rd}}+(1-e_{\text{rd}})\Pr\left\{\sum_{j=1}^{l}c_{ij}x_j=0\,|\,\overline{\varepsilon_i}\right\}\tag{19}$$

若令 $f_l=\Pr\left\{\sum_{j=1}^{l}c_{ij}x_j=0\,|\,\overline{\varepsilon_i}\right\}$，则有 $f_{l+1}=\Pr\left\{\sum_{j=1}^{l+1}c_{ij}x_j=0\,|\,\overline{\varepsilon_i}\right\}$，且

$$f_{l+1}=\Pr\left\{\sum_{j=1}^{l}c_{ij}x_j=0\,|\,\overline{\varepsilon_i}\right\}\Pr\{c_{i(l+1)}x_{l+1}=0\}+$$
$$\Pr\left\{\sum_{j=1}^{l}c_{ij}x_j=\theta\,|\,\overline{\varepsilon_i}\right\}\Pr\{c_{i(l+1)}x_{l+1}=-\theta\}=$$
$$f_le_{\text{sr}}+\frac{(1-f_l)(1-e_{\text{sr}})}{(q-1)}\tag{20}$$

其中，$\theta \neq 0$ $(\theta \in F_q)$。从式(20)可以整理得

$$(f_{l+1}-q^{-1})=\left(\frac{e_{\mathrm{sr}}q-1}{q-1}\right)(f_l-q^{-1}) \tag{21}$$

又由式(9)得 $f_1=\Pr\left\{c_{i1}x_1 \mid \overline{\varepsilon_i}\right\}=e_{\mathrm{sr}}$，因此从式(21)的通项公式整理得

$$f_l=q^{-1}+\left(1-q^{-1}\right)\left(\frac{qe_{\mathrm{sr}}-1}{q-1}\right)^l \tag{22}$$

从而，将式(22)结论代入式(19)即可得 $S_l=e_{\mathrm{rd}}+\left(1-e_{\mathrm{rd}}\right)\left(q^{-1}+\left(1-q^{-1}\right)\left(\frac{qe_{\mathrm{sr}}-1}{q-1}\right)^l\right)$。又因为 $P_l=\left(S_l\right)^{M-1}$，所以

$$P_l=\left(e_{\mathrm{rd}}+\left(1-e_{\mathrm{rd}}\right)\left(q^{-1}+\left(1-q^{-1}\right)\left(\frac{qe_{\mathrm{sr}}-1}{q-1}\right)^l\right)\right)^{M-1} \tag{23}$$

将式(23)代入式(18)，定理 2 即可得证。

附录 3 推论 1 的证明

证明 由式(9)知，在协作恢复阶段，任意簇内节点成功接收到的编码包编码系数是一个 $1\times N$ 维的稀疏向量，该向量的稀疏度即为广播阶段数据包删除率 e_{sr}。当簇内节点成功接收到一个新编码包后，解码矩阵秩由 t 增加为 t+1，这一过程等价于新接收的编码包编码系数向量 $\boldsymbol{c}$ 与由原秩为 t 解码阵 **CP** 的行向量所组成的向量组线性无关。根据算法 1 可知，秩为 t 的解码阵 **CP** 共含 t 行向量且呈行阶梯型分布，因此当 $\boldsymbol{c}$ 与 **CP** 阶梯对应的前 t 个元素值确立后，稀疏随机向量 $\boldsymbol{c}$ 与 **CP** 是否线性相关取决于剩余的 $N-t$ 个元素，且线性相关时的解取值唯一，代入引理 1，推论 1 即可得证。

附录 4 引理 2 的证明

证明 若簇内任意节点 CR_i 在当前时间片末（假设为 t）的解码矩阵秩为 i（此时对应图 4 所示的解码过程吸收马尔可夫链应处于 s_i 状态），则在第 t+1 时间片末 CR_i 的解码矩阵秩只可能出现 2 种情况。

情况 1 秩增 1 变为 i+1。这种情况发生的条件是 CR_i 在 t+1 时间片成功接收到一个编码包，并且该编码包的编码系数向量与原解码矩阵线性无关，此时 AMP 由 s_i 转移至状态 s_{i+1}，因此这种情况的转移概率 $p_{i,i+1}=(1-e_{\mathrm{rd}})p(i,N)$。

情况 2 秩维持 i 不变。这种情况发生有 2 种可能，一种是 CR_i 在 t+1 时间片未能成功侦听到一个编码包，即发生了删除；另一种是成功接收到编码包但是编码系数与已有编码矩阵线性相关，因此这种情况的转移概率 $p_{i,i}=e_{\mathrm{rd}}+(1-e_{\mathrm{rd}})\left(1-p(i,N)\right)=1-(1-e_{\mathrm{rd}})p(i,N)$，引理 2 得证。

附录 5 定理 3 的证明

证明 由 M 个节点组成的 CR 协作簇采用改进 Gauss-Jordan 算法恢复 N 个源数据包，其成功解码过程包括 2 种情况。

情况 1 由于 CR 协作恢复阶段总时长只有 M 个时间片，改进 Gauss-Jordan 算法需在此时间片内判定解码矩阵是否可解，超过 M 则终止算法，因此解码时延 $T'_{\mathrm{coop}} \leqslant M$。

情况 2 对任意吸收马尔可夫链 AMP 从瞬时态 s_i 出发至吸收态时经过瞬态 s_j 的平均次数 Y_{ij} 为

$$Y_{ij}=\mathrm{E}\left(Y_{ij} \mid X_0=s_i\right)=\sum_{n=0}^{\infty}P\left\{X_n=s_j \mid X_0=s_i\right\} \tag{24}$$

若记任意 AMP 瞬时状态转移矩阵为 $\boldsymbol{Q}$，由式(24)得 Y_{ij} 是联合矩阵 $\boldsymbol{I}+\boldsymbol{Q}+\boldsymbol{Q}^2+\boldsymbol{Q}^3+\cdots$ 的(i,j)元素，又

$$(\boldsymbol{I}+\boldsymbol{Q}+\boldsymbol{Q}^2+\boldsymbol{Q}^3+\cdots)(\boldsymbol{I}-\boldsymbol{Q})=\boldsymbol{I}-\lim_{n\to\infty}\boldsymbol{Q}^n \tag{25}$$

根据瞬时态转移特性知，当 $n\to\infty$ 时任意 AMP 的 n 步转移概率阵极限 $\lim_{n\to\infty}\boldsymbol{Q}^n=\boldsymbol{0}$，因此 $\boldsymbol{I}+\boldsymbol{Q}+\boldsymbol{Q}^2+\boldsymbol{Q}^3+\cdots=(\boldsymbol{I}-\boldsymbol{Q})^{-1}$，即 Y_{ij} 是 $(\boldsymbol{I}-\boldsymbol{Q})^{-1}$ 的(i,j)元素，若记 $\boldsymbol{T}=(\boldsymbol{I}-\boldsymbol{Q})^{-1}$，则 $Y_{ij}=T_{ij}$。

记 S_i 表示任意 AMP 从瞬时态 s_i 到达吸收态的平均步数，S_{ij} 表示到达吸收态前经过瞬时态 s_j 的次数，则

$$S_i=\mathrm{E}\left(\sum_{j\neq N}S_{ij} \mid X_0=s_i\right)=\sum_{j\neq N}Y_{ij} \tag{26}$$

在 CR 协作恢复阶段采用改进 Gauss-Jordan 算法成功解码的平均在线解码时延 T'_{coop} 等于对应 AMP 转移至吸收态 s_n 的平均步数。由定义 1 知，所求 AMP 初始状态 s_k 对应 $\boldsymbol{T}$ 第一行，根据式(26)得 $T'_{\mathrm{coop}}=\sum_{i=1}^{N-1}T_{1,i}$。

综合情况 1 和情况 2 得 $T'_{\mathrm{coop}}=\min\left(\sum_{i=1}^{N-1}T_{1,i},M\right)$，定理 3 得证。

参考文献：

[1] GUO W, FUENTES M, CHRISTODOULOU L, et al. Roads to multimedia broadcast multicast services in 5G new radio[C]//International Symposium on Broadband Multimedia Systems and Broadcasting, Piscataway: IEEE Press, 2018: 1-5.

[2] DRESSLER F, KLINGLER F, SOMMER C, et al. Not all VANET broadcasts are the same: context-aware class based broadcast[J]. IEEE/ACM Transactions on Networking, 2018, 26(1): 17-30.

[3] KARIMI P, SHERMAN M, BRONZINO F, et al. Evaluating 5G multihoming services in the MobilityFirst future Internet architecture[C]//2017 IEEE 85th Vehicular Technology Conference. Piscata-

way: IEEE Press, 2017: 1-5.

[4] QIU C X, SHEN H Y, SOLTANI S, et al. CEDAR: a low-latency and distributed strategy for packet recovery in wireless networks[J]. IEEE/ACM Transactions on Networking, 2015, 23(5): 1514-1527.

[5] BENRHAIEM W, HAFID A, SAHU P K. Reliable emergency message dissemination scheme for urban vehicular networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 21(3): 1154-1166.

[6] PARK J S, GERLA M, LUN D S, et al. Codecast: a network-coding-based ad hoc multicast protocol[J]. IEEE Wireless Communications, 2006, 13(5): 76-81.

[7] DATSIKA E, ANTONOPOULOS A, ZORBA N, et al. Cross-network performance analysis of network coding aided cooperative outband D2D communications[J]. IEEE Transactions on Wireless Communications, 2017, 16(5): 3176-3188.

[8] YAN Y, ZHANG B X, LI C. Opportunistic network coding based cooperative retransmissions in D2D communications[J]. Computer Networks, 2017, 113: 72-83.

[9] GOU L, ZHANG G X, BIAN Z G, et al. Minimizing completion time for relay-assisted multicast with instantly decodable network coding[J]. IEEE Communications Letters, 2016, 20(3): 434-437.

[10] ABOUTORAB N, SADEGHI P, TAJBAKHSH S E. Instantly decodable network coding for delay reduction in cooperative data exchange systems[C]//2013 IEEE International Symposium on Information Theory. Piscataway: IEEE Press, 2013: 3095-3099.

[11] 王练, 王萌, 任治豪, 等. D2D 网络中基于立即可解网络编码的时延最小化重传方案[J].电子与信息学报, 2018, 40(7): 1691-1698.
WANG L, WANG M, REN Z H, et al. Delay minimization retransmission scheme based on instantly decodable network coding for D2D communications[J]. Journal of Electronics & Information Technology, 2018, 40(7):1691-1698.

[12] FAN Y F, JIANG Y X, ZHU H J, et al. PIE: cooperative peer-to-peer information exchange in network coding enabled wireless networks[J]. IEEE Transactions on Wireless Communications, 2010, 9(3): 945-950.

[13] XU X L, KUMAR M P, GUAN Y L, et al. Two-phase cooperative broadcasting based on batched network code[J]. IEEE Transactions on Communications, 2016, 64(2): 706-714.

[14] 欧莽, 汪继文. VANETs 中基于分布式 TDMA 的协作网络编码方法[J]. 华南理工大学学报(自然科学版), 2020, 48(1): 104-113.
OU M, WANG J W. Cooperative network coding in VANETs based on distributed TDMA[J]. Journal of South China University of Technology (Natural Science Edition), 2020, 48(1): 104-113.

[15] AHLSWEDE R, CAI N, LI S Y R, et al. Network information flow[J]. IEEE Transactions on Information Theory, 2000, 46(4): 1204-1216.

[16] HO T, MEDARD M, KOETTER R, et al. A random linear network coding approach to multicast[J]. IEEE Transactions on Information Theory, 2006, 52(10): 4413-4430.

[17] TRULLOLS-CRUCES O, BARCELO-ORDINAS J M, FIORE M. Exact decoding probability under random linear network coding[J]. IEEE Communications Letters, 2011, 15(1): 67-69.

[18] LANEMAN J N, WORNELL G W. Distributed space-time-coded protocols for exploiting cooperative diversity in wireless networks[J]. IEEE Transactions on Information Theory, 2003, 49(10): 2415-2425.

[19] TSE D, VISWANATH P. Fundamentals of wireless communication[M]. Cambridge: Cambridge University Press, 2005.

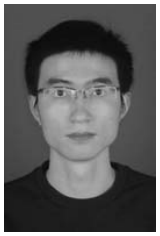
[20] BLÖMER J, KARP R, WELZL E. The rank of sparse random matrices over finite fields[J]. Random Structures & Algorithms, 1997, 10(4): 407-419.

[21] LI X L, MOW W H, TSANG F L. Rank distribution analysis for sparse random linear network coding[C]//2011 International Symposium on Networking Coding. Piscataway: IEEE Press, 2011: 1-6.

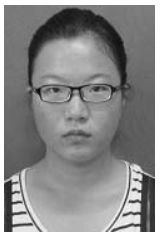
[22] MARRIOT P. Finite Markov chains[R]. Waterloo: University of Waterloo, 2015,

[23] 王磊. 网络编码理论与实践[M]. 上海: 上海交通大学出版社, 2017.
WANG L. Network coding theory and applications[M]. ShangHai: ShangHai Jiao Tong University Press, 2017.

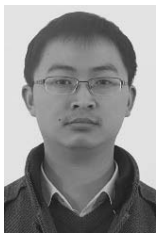
[作者简介]



殷俊（1989− ），男，安徽巢湖人，博士，南京邮电大学讲师，主要研究方向为网络编码及其应用。



沙雪琪（2000− ），女，江苏徐州人，南京邮电大学硕士生，主要研究方向为协作通信。



王磊（1986− ），男，安徽马鞍山人，博士，南京邮电大学副教授，主要研究方向为网络编码及其应用。

张登银（1964− ），男，江苏靖江人，博士，南京邮电大学研究员，主要研究方向为现代通信网络、信号与信息处理技术等。

杨余旺（1966− ），男，安徽桐城人，博士，南京理工大学教授，主要研究方向为网络编码、工业物联网等。