



国际信息工程先进技术译丛

网络编码基础与应用

Network Coding Fundamentals and Applications

Muriel Médard
(美) Alex Sprintson 等编著
郝建军 郭一珺 译

 机械工业出版社
CHINA MACHINE PRESS



014018736

TP393
1329

国际信息工程先进技术译丛

网络编码基础与应用

(美) Muriel Médard 等编著
Alex Sprintson

郝建军 郭一珩 译



机械工业出版社



北航

C1707238

TP393
1329

987810410

本书由 10 位作者撰写而成,集各家之所长于一体,从多个角度对网络编码技术进行了深入的讲解,包括对网络编码在无线网络、对等网络、数据压缩、LTE 网络、MANET、容错网络、保密与可靠通信网络、协同传输网络等场景中的研究与分析。

本书对于想要掌握该领域的基础知识并了解该技术的应用的网络专业人员来说是一个理想的选择。对于想要进行网络编码研究的研究生来说,本书也具有重要价值。本书可以作为重点在于网络编码或先进编码技术的课程的教科书或参考书。

Network Coding Fundamentals and Applications

Muriel Médard, Alex Sprintson

ISBN: 9780123809186

Copyright © 2012 by Elsevier. All rights reserved.

Authorized Simplified Chinese translation edition published by the Proprietor.

Copyright © 2013 by Elsevier (Singapore) Pte Ltd and China Machine Press.

All rights reserved.

Published in China by China Machine Press under special arrangement with Elsevier

(Singapore) Pte Ltd.

This edition is authorized for sale in China only, excluding Hong Kong SAR and Taiwan. Unauthorized export of this edition is a violation of the Copyright Act. Violation of this Law is subject to Civil and Criminal Penalties.

本书简体中文版由 Elsevier (Singapore) Pte Ltd. 授予机械工业出版社在中国大陆地区(不包括香港、澳门特别行政区以及台湾地区)出版与发行。未经许可之出口,视为违反著作权法,将受到法律之制裁。

本书封底贴有 Elsevier 防伪标签,无标签者不得销售。

本书版权登记号 01-2012-8721

图书在版编目(CIP)数据

网络编码基础与应用/(美)莫德尔等编著;郝建军,郭一珺译. —北京:机械工业出版社,2013.10

(国际信息工程先进技术译丛)

ISBN 978-7-111-44506-7

I. ①网… II. ①莫…②郝…③郭… III. ①计算机网络-编码程序-程序设计 IV. ①TP393

中国版本图书馆 CIP 数据核字(2013)第 251017 号

机械工业出版社(北京市百万庄大街 22 号 邮政编码 100037)

策划编辑:李馨馨 责任编辑:李馨馨 韩 静

版式设计:霍永明 责任校对:姜 婷

封面设计:赵颖喆 责任印制:张 楠

唐山丰电印务有限公司印刷

2014 年 1 月第 1 版第 1 次印刷

169mm×239mm·14 印张·308 千字

0001—3000 册

标准书号:ISBN 978-7-111-44506-7

定价:59.00 元

凡购本书,如有缺页、倒页、脱页,由本社发行部调换

电话服务

网络服务

社服务中心:(010)88361066 教材网:<http://www.cmpedu.com>

销售一部:(010)68326294 机工官网:<http://www.cmpbook.com>

销售二部:(010)88379649 机工官博:<http://weibo.com/cmp1952>

读者购书热线:(010)88379203 封面无防伪标均为盗版

前言

网络编码思想始创于千年更替之际,由 Ahlswede、蔡和杨在其开创性论文中提出后迅速吸引了世界各地的研究者和实践者。最近的研究工作阐明了网络编码的许多令人关注的问题、基本容量限制以及性能增益。对于一些重要的实际设定,研究者们设计了可达容量的网络编码,掌握了一些基本的网络编码问题的计算复杂度,并制定了有效的网络编码算法。此外,研究者们还揭示了网络编码和诸如网络、复杂理论、图论、拟阵论、编码理论以及信息论等一些其他领域之间的深刻联系。

尽管对网络编码的研究在理论方面已经取得了重大进展,但在实际应用方面才刚刚起步。虽然网络编码已经被成功地运用到了许多领域,例如最常见的内容分发系统,但对于无线网络、存储网络、容断网络等其他领域,网络编码在提升性能方面尚有许多潜力待开发。此外,网络编码技术在提高无线环境和有线环境中的安全性、鲁棒性、可管理性以及对于 QoS 的支持性方面也有着巨大的潜力。

本书提供了网络编码的入门教程以及在网络和分布式计算的不同领域中的各种实际应用的综合考察。我们的目标是发现网络编码应用的丰富性并寻找激动人心的新的研究机会。全书共分 10 章,每一章均由网络编码领域公认的专家撰写,并聚焦于一个特定的应用领域。本书力求表述清晰,且使用最少的数学符号,使每位熟悉基本网络概念的读者均可以理解本书。为了便于之后的阅读,每章中作者都给出了一个全面的文献综述,该综述参考了与该领域最相关的研究工作。

第 1 章以教程的形式介绍了网络编码的基本原理,并概述了网络信息流、线性网络编码、码构造的多项式时间算法、随机网络编码、编码优势、子空间传输以及非线性网络码。

第 2 章聚焦于在无线网络中实现网络编码的基本原则,讨论了机会监听和编码的原理,详细描述了转发架构和网络编码的性能增益,还阐述了模拟网络编码的基本原理。

第 3 章着重于内容分发和多媒体流,讨论了网络编码在对等网络中的应用,探讨了在运用网络编码的对等系统中的可能的设计空间,并展示了在该设定下使用编码技术的优势。

第 4 章讨论了网络编码在商业移动平台上的实现,描述了系统的基本构成和设计选择,并讨论了与在移动电话上实现网络编码算法相关的实际问题 and 性能问题。

第 5 章讨论了网络编码在 LTE 网络中的应用。作者重点介绍用于消失恢复的用户协同方案,并展示了利用网络编码技术带来的显著的性能增益。

第 6 章重点关注移动 Ad Hoc 网络,并描述了一个基于网络编码协议栈的完全实现的通信系统,考察了与在嵌入式系统上实现网络编码相关的一些实际实现问题,并给出

了现场测试的结果。

第7章聚焦于网络编码在提升网络安全方面的应用,考虑了只有窃听能力的被动攻击以及能够同时进行窃听和干扰的主动攻击,还讨论了攻击者计算能力有限的情况。

第8章讨论了网络编码、源编码和数据压缩之间的关系。

第9章重点讨论了当对无线网络的网络规模、编码窗口大小、网络信息流数量以及应用延迟约束进行一些缩放时,网络编码的性能变化,推导并分析了有助于量化网络编码在大型网络中的性能的标度律。

第10章聚焦于网络编码在延迟和容错网络中的应用,讨论了在设计这类网络时面临的独特的挑战,并证明了网络编码技术有助于解决这些挑战,讨论了传输和缓存管理、恢复方案以及在能量效率和提升延迟-传输权衡方面的编码效益。

目标读者

本书是为对网络编码的一般领域以及在通信网络的不同领域上的应用感兴趣的研究者和实践者们准备的。我们假定本书的读者只具备一般的网络技术背景,且之前没有接触过网络编码技术或网络编码应用。本书对于想要掌握该领域的基础知识并了解该技术的应用的网络专业人员来说是一个理想的选择。对于想要进行网络编码研究的研究生来说,本书也具有重要价值。本书可以作为重点在于网络编码或先进编码技术的课程的教科书或参考书。

Muriel Medard

美国马萨诸塞州,剑桥,麻省理工学院电子工程系

Alex Sprintson

美国,德克萨斯州,卡城,德州 A&M 大学。

致 谢

感谢所有作者在书写和校订各章节时所做的贡献、付出的热情和作出的承诺。显然，没有他们的慷慨付出，本书不可能得以完成。此外，还要感谢 Danilo Silva 对各章节的审阅；感谢来自学术出版社的 Tim Pitts、Naomi Robertson、Charlotte Kent 和 Lisa Jones 在本书编辑工作的各个方面所给予的支持、鼓励、理解和帮助。最后，感谢我们的配偶和家庭给予的鼓励和作出的牺牲，他们给了我们进行本项目的空闲时间，也带给了我们灵感。

2	致谢	1.2.1
3	致谢	1.2.2
4	致谢	1.3
5	致谢	1.3.1
6	致谢	1.3.2
7	致谢	1.3.3
8	致谢	1.3.4
9	致谢	1.4
10	致谢	1.4.1
11	致谢	1.4.2
12	致谢	1.5
13	致谢	1.6
14	致谢	1.6.1
15	致谢	1.6.2
16	致谢	1.7
17	致谢	1.8
18	致谢	1.9
19	致谢	1.10
20	致谢	1.10.1
21	致谢	1.10.2
22	致谢	1.10.3
23	致谢	1.10.4
24	致谢	1.10.5
25	致谢	1.10.6
26	致谢	1.10.7
27	致谢	1.10.8
28	致谢	1.10.9
29	致谢	1.10.10
30	致谢	1.10.11
31	致谢	1.10.12
32	致谢	1.10.13
33	致谢	1.10.14
34	致谢	1.10.15
35	致谢	1.10.16
36	致谢	1.10.17
37	致谢	1.10.18
38	致谢	1.10.19
39	致谢	1.10.20
40	致谢	1.10.21
41	致谢	1.10.22
42	致谢	1.10.23
43	致谢	1.10.24
44	致谢	1.10.25
45	致谢	1.10.26
46	致谢	1.10.27
47	致谢	1.10.28
48	致谢	1.10.29
49	致谢	1.10.30
50	致谢	1.10.31
51	致谢	1.10.32
52	致谢	1.10.33
53	致谢	1.10.34
54	致谢	1.10.35
55	致谢	1.10.36
56	致谢	1.10.37
57	致谢	1.10.38
58	致谢	1.10.39
59	致谢	1.10.40
60	致谢	1.10.41
61	致谢	1.10.42
62	致谢	1.10.43
63	致谢	1.10.44
64	致谢	1.10.45
65	致谢	1.10.46
66	致谢	1.10.47
67	致谢	1.10.48
68	致谢	1.10.49
69	致谢	1.10.50
70	致谢	1.10.51
71	致谢	1.10.52
72	致谢	1.10.53
73	致谢	1.10.54
74	致谢	1.10.55
75	致谢	1.10.56
76	致谢	1.10.57
77	致谢	1.10.58
78	致谢	1.10.59
79	致谢	1.10.60
80	致谢	1.10.61
81	致谢	1.10.62
82	致谢	1.10.63
83	致谢	1.10.64
84	致谢	1.10.65
85	致谢	1.10.66
86	致谢	1.10.67
87	致谢	1.10.68
88	致谢	1.10.69
89	致谢	1.10.70
90	致谢	1.10.71
91	致谢	1.10.72
92	致谢	1.10.73
93	致谢	1.10.74
94	致谢	1.10.75
95	致谢	1.10.76
96	致谢	1.10.77
97	致谢	1.10.78
98	致谢	1.10.79
99	致谢	1.10.80
100	致谢	1.10.81
101	致谢	1.10.82
102	致谢	1.10.83
103	致谢	1.10.84
104	致谢	1.10.85
105	致谢	1.10.86
106	致谢	1.10.87
107	致谢	1.10.88
108	致谢	1.10.89
109	致谢	1.10.90
110	致谢	1.10.91
111	致谢	1.10.92
112	致谢	1.10.93
113	致谢	1.10.94
114	致谢	1.10.95
115	致谢	1.10.96
116	致谢	1.10.97
117	致谢	1.10.98
118	致谢	1.10.99
119	致谢	1.10.100
120	致谢	1.10.101
121	致谢	1.10.102
122	致谢	1.10.103
123	致谢	1.10.104
124	致谢	1.10.105
125	致谢	1.10.106
126	致谢	1.10.107
127	致谢	1.10.108
128	致谢	1.10.109
129	致谢	1.10.110
130	致谢	1.10.111
131	致谢	1.10.112
132	致谢	1.10.113
133	致谢	1.10.114
134	致谢	1.10.115
135	致谢	1.10.116
136	致谢	1.10.117
137	致谢	1.10.118
138	致谢	1.10.119
139	致谢	1.10.120
140	致谢	1.10.121
141	致谢	1.10.122
142	致谢	1.10.123
143	致谢	1.10.124
144	致谢	1.10.125
145	致谢	1.10.126
146	致谢	1.10.127
147	致谢	1.10.128
148	致谢	1.10.129
149	致谢	1.10.130
150	致谢	1.10.131
151	致谢	1.10.132
152	致谢	1.10.133
153	致谢	1.10.134
154	致谢	1.10.135
155	致谢	1.10.136
156	致谢	1.10.137
157	致谢	1.10.138
158	致谢	1.10.139
159	致谢	1.10.140
160	致谢	1.10.141
161	致谢	1.10.142
162	致谢	1.10.143
163	致谢	1.10.144
164	致谢	1.10.145
165	致谢	1.10.146
166	致谢	1.10.147
167	致谢	1.10.148
168	致谢	1.10.149
169	致谢	1.10.150
170	致谢	1.10.151
171	致谢	1.10.152
172	致谢	1.10.153
173	致谢	1.10.154
174	致谢	1.10.155
175	致谢	1.10.156
176	致谢	1.10.157
177	致谢	1.10.158
178	致谢	1.10.159
179	致谢	1.10.160
180	致谢	1.10.161
181	致谢	1.10.162
182	致谢	1.10.163
183	致谢	1.10.164
184	致谢	1.10.165
185	致谢	1.10.166
186	致谢	1.10.167
187	致谢	1.10.168
188	致谢	1.10.169
189	致谢	1.10.170
190	致谢	1.10.171
191	致谢	1.10.172
192	致谢	1.10.173
193	致谢	1.10.174
194	致谢	1.10.175
195	致谢	1.10.176
196	致谢	1.10.177
197	致谢	1.10.178
198	致谢	1.10.179
199	致谢	1.10.180
200	致谢	1.10.181
201	致谢	1.10.182
202	致谢	1.10.183
203	致谢	1.10.184
204	致谢	1.10.185
205	致谢	1.10.186
206	致谢	1.10.187
207	致谢	1.10.188
208	致谢	1.10.189
209	致谢	1.10.190
210	致谢	1.10.191
211	致谢	1.10.192
212	致谢	1.10.193
213	致谢	1.10.194
214	致谢	1.10.195
215	致谢	1.10.196
216	致谢	1.10.197
217	致谢	1.10.198
218	致谢	1.10.199
219	致谢	1.10.200
220	致谢	1.10.201
221	致谢	1.10.202
222	致谢	1.10.203
223	致谢	1.10.204
224	致谢	1.10.205
225	致谢	1.10.206
226	致谢	1.10.207
227	致谢	1.10.208
228	致谢	1.10.209
229	致谢	1.10.210
230	致谢	1.10.211
231	致谢	1.10.212
232	致谢	1.10.213
233	致谢	1.10.214
234	致谢	1.10.215
235	致谢	1.10.216
236	致谢	1.10.217
237	致谢	1.10.218
238	致谢	1.10.219
239	致谢	1.10.220
240	致谢	1.10.221
241	致谢	1.10.222
242	致谢	1.10.223
243	致谢	1.10.224
244	致谢	1.10.225
245	致谢	1.10.226
246	致谢	1.10.227
247	致谢	1.10.228
248	致谢	1.10.229
249	致谢	1.10.230
250	致谢	1.10.231
251	致谢	1.10.232
252	致谢	1.10.233
253	致谢	1.10.234
254	致谢	1.10.235
255	致谢	1.10.236
256	致谢	1.10.237
257	致谢	1.10.238
258	致谢	1.10.239
259	致谢	1.10.240
260	致谢	1.10.241
261	致谢	1.10.242
262	致谢	1.10.243
263	致谢	1.10.244
264	致谢	1.10.245
265	致谢	1.10.246
266	致谢	1.10.247
267	致谢	1.10.248
268	致谢	1.10.249
269	致谢	1.10.250
270	致谢	1.10.251
271	致谢	1.10.252
272	致谢	1.10.253
273	致谢	1.10.254
274	致谢	1.10.255
275	致谢	1.10.256
276	致谢	1.10.257
277	致谢	1.10.258
278	致谢	1.10.259
279	致谢	1.10.260
280	致谢	1.10.261
281	致谢	1.10.262
282	致谢	1.10.263
283	致谢	1.10.264
284	致谢	1.10.265
285	致谢	1.10.266
286	致谢	1.10.267
287	致谢	1.10.268
288	致谢	1.10.269
289	致谢	1.10.270
290	致谢	1.10.271
291	致谢	1.10.272
292	致谢	1.10.273
293	致谢	1.10.274
294	致谢	1.10.275
295	致谢	1.10.276
296	致谢	1.10.277
297	致谢	1.10.278
298	致谢	1.10.279
299	致谢	1.10.280
300	致谢	1.10.281
301	致谢	1.10.282
302	致谢	1.10.283
303	致谢	1.10.284
304	致谢	1.10.285
305	致谢	1.10.286
306	致谢	1.10.287
307	致谢	1.10.288
308	致谢	1.10.289
309	致谢	1.10.290
310	致谢	1.10.291
311	致谢	1.10.292
312	致谢	1.10.293
313	致谢	1.10.294
314	致谢	1.10.295
315	致谢	1.10.296
316	致谢	1.10.297
317	致谢	1.10.298
318	致谢	1.10.299
319	致谢	1.10.300
320	致谢	1.10.301
321	致谢	1.10.302
322	致谢	1.10.303
323	致谢	1.10.304
324	致谢	1.10.305
325	致谢	1.10.306
326	致谢	1.10.307
327	致谢	1.10.308
328	致谢	1.10.309
329	致谢	1.10.310
330	致谢	1.10.311
331	致谢	1.10.312
332	致谢	1.10.313
333	致谢	1.10.314
334	致谢	1.10.315
335	致谢	1.10.316
336	致谢	1.10.317
337	致谢	1.10.318
338	致谢	1.10.319
339	致谢	1.10.320
340	致谢	1.10.321
341	致谢	1.10.322
342	致谢	1.10.323
343	致谢	1.10.324
344	致谢	1.10.325
345	致谢	1.10.326
346	致谢	1.10.327
347	致谢	1.10.328
348	致谢	1.10.329
349	致谢	1.10.330
350	致谢	1.10.331
351	致谢	1.10.332
352	致谢	1.10.333
353	致谢	1.10.334
354	致谢	1.10.335
355	致谢	1.10.336
356	致谢	1.10.337
357	致谢	1.10.338
358	致谢	1.10.339
359	致谢	1.10.340
360	致谢	1.10.341
361	致谢	1.10.342
362	致谢	1.10.343
363	致谢	1.10.344
364	致谢	1.10.345
365	致谢	1.10.346
366	致谢	1.10.347
367	致谢	1.10.348
368	致谢	1.10.349
369	致谢	1.10.350
370	致谢	1.10.351
371	致谢	1.10.352
372	致谢	1.10.353
373	致谢	1.10.354
374	致谢	1.10.355
375	致谢	1.10.356
376	致谢	1.10.357
377	致谢	1.10.358
378	致谢	1.10.359
379	致谢	1.10.360
380	致谢	1.10.361
381	致谢	1.10.362
382	致谢	1.10.363
383	致谢	1.10.364
384	致谢	1.10.365
385	致谢	1.10.366
386	致谢	1.10.367
387	致谢	1.10.368
388	致谢	1.10.369
389	致谢	1.10.370
390	致谢	1.10.371
391	致谢	1.10.372
392	致谢	1.10.373
393	致谢	1.10.374
394	致谢	1.10.375
395	致谢	1.10.376
396	致谢	1.10.377
397	致谢	1.10.378
398	致谢	1.10.379
399	致谢	1.10.380
400	致谢	1.10.381
401	致谢	1.10.382
402	致谢	1.10.383
403	致谢	1.10.384

目 录

前言	1
致谢	1
第1章 网络编码入门	1
1.1 蝶形网络	1
1.2 图和网络	3
1.2.1 组合包网络	3
1.2.2 网络信息流	5
1.3 单源多播问题	6
1.3.1 多播容量	6
1.3.2 线性网络编码	7
1.3.3 实现多播容量的线性网络编码	9
1.4 多播网络中的码字构造	10
1.4.1 线性信息流算法	10
1.4.2 随机构造	13
1.5 编码和路由	14
1.6 非相干网络编码	15
1.6.1 携带数据包报头的传输	15
1.6.2 子空间传输	16
1.7 关于字母表和非线性	17
1.8 结论	19
1.9 致谢	19
1.10 附录	19
1.10.1 有限域	19
1.10.2 多项式的零点和非零点	21
1.10.3 $\det(\mathbf{G}_i)$ 的次数	23
参考文献	24
第2章 无线系统中的网络编码	26
2.1 引言	26
2.2 网络编码背景：业内视点	27
2.3 网络编码在无线网络中的应用	29

2.3.1 COPE: 提高吞吐量的网络编码	29
2.3.1.1 COPE 协议	30
2.3.1.2 性能结果	32
2.3.2 MORE: 提高可靠性的网络编码	33
2.3.2.1 示例 1: 盲区	33
2.3.2.2 示例 2: 多播	34
2.3.2.3 MORE 协议	34
2.3.2.4 实证结果	35
2.3.3 模拟网络编码: 利用无线干扰	36
2.4 结论	39
参考文献	39
第 3 章 利用网络编码实现 P2P 网络的内容分发和多媒体流	42
3.1 运用网络编码的内容分发	42
3.1.1 怎样在 P2P 内容分发中使用网络编码?	42
3.1.2 为什么网络编码有助于 P2P 内容分发?	43
3.1.3 利用网络编码的 P2P 内容分发的理论结果	44
3.1.4 网络编码实现 P2P 内容分发的实际应用	47
3.2 运用网络编码的 P2P 多媒体流	48
3.2.1 网络编码怎样应用于 P2P 多媒体流?	48
3.2.1.1 随机网状结构中的随机 push	49
3.2.1.2 下游对等体的及时反馈	50
3.2.1.3 同步播放和初始缓冲延迟	51
3.2.2 为什么网络编码对多媒体流有帮助?	51
3.2.3 基于网络编码的 P2P 多媒体流的理论结果	52
3.2.4 基于网络编码的 P2P 多媒体流中的实际问题	55
3.3 总结	56
参考文献	56
第 4 章 真实世界中的网络编码	59
4.1 引言: 并非火箭科学	59
4.2 移动电话上的网络编码	59
4.3 系统组成与设计选择	64
4.4 实际问题	66
4.5 二进制确定性方法	67
4.6 随机线性网络编码	68
4.7 通过优化提升随机线性网络编码	69
4.8 通过设计提升随机线性网络编码	71

4.9 采用了网络编码的移动电话应用	73
4.10 隐患和参数	75
参考文献	76
第5章 网络编码和用户协同在LTE网络流和下载服务上的应用	79
5.1 引言	79
5.2 eMBMS中的Raptor码	82
5.3 包丢失图样	84
5.4 基于用户协同的丢失恢复	86
5.5 网络编码应用于用户协同	89
5.6 仿真结果	91
5.7 结论	93
参考文献	93
第6章 CONCERTO: 现实世界MANET系统中的一些基于网络编码的经验	96
6.1 引言	96
6.1.1 无线MANET面临的挑战	97
6.1.2 CONCERTO解决方案	97
6.2 CONCERTO综述	98
6.3 网络编码	100
6.3.1 前期工作	100
6.3.2 CONCERTO网络编码	100
6.4 子图构造	102
6.4.1 算法	102
6.4.2 实现	103
6.5 网络编码传输协议	104
6.5.1 MANET中的可靠传输	104
6.5.2 转发协议架构	104
6.5.3 网络编码传输协议的主/从架构	105
6.5.4 半可靠从转发引擎算法	106
6.5.5 全可靠从转发引擎算法	107
6.6 网络编码的效益	108
6.6.1 广播、多播和单播的统一机制	108
6.6.2 对于路由环路的鲁棒性	108
6.6.3 对于链路或节点故障的鲁棒性	109
6.6.4 提供低延迟链路层编码	109
6.6.5 极端机会路由	110

6.6.5.1	长跳	110
6.6.5.2	大量的有损链路	111
6.7	现场实验的基础设施	111
6.7.1	硬件	111
6.7.2	基准系统	112
6.7.3	通信方案	113
6.7.4	评估方法	114
6.8	实验结果及分析	114
6.8.1	实验场景	114
6.8.2	实验结果	117
6.8.2.1	地面战术场景	117
6.8.2.2	空中战术场景的结果	121
6.8.2.3	战术场景下的文件传输结果	122
6.9	总结和展望	122
6.9.1	总结	122
6.9.2	展望	123
6.10	致谢	123
	参考文献	123
第7章	安全网络编码：保密与可靠通信中的界和算法	125
7.1	引言	125
7.2	模型	126
7.2.1	威胁模型	126
7.2.2	网络和码字模型	127
7.3	窃听安全	128
7.3.1	相干情况	128
7.3.2	非相干情况	130
7.4	干扰安全	131
7.4.1	相干情况	131
7.4.2	非相干情况	134
7.4.3	加密场景	137
7.5	存在窃听和干扰对手时的保密传输	139
7.5.1	相干情况	139
7.5.2	非相干情况	140
7.6	其他方案	141
7.7	总结	142
7.8	致谢	142

参考文献	142
第8章 网络编码和数据压缩	148
8.1 引言	148
8.2 模型和符号	150
8.3 一般联合信源网络编码的速率区域特性	151
8.4 无损组播的容量结果	152
8.4.1 无边信息场景	153
8.4.2 汇聚节点具有边信息的场景	153
8.5 实用的方法	154
8.6 附录	155
参考文献	157
第9章 网络编码的标度律	160
9.1 引言及基本设定	160
9.2 有损链路下的无线广播	161
9.2.1 延迟标度增益	161
9.2.2 扩展	164
9.2.2.1 拓扑扩展	164
9.2.2.2 动态到达	166
9.2.2.3 流入流量的延迟灵敏度	167
9.2.3 吞吐量-延迟权衡	168
9.3 大规模移动 Ad Hoc 网络中的编码	172
9.3.1 示例: 在 i.i.d 移动模型下的吞吐量-延迟权衡	173
9.3.2 对多播通信流的扩展	176
9.3.3 对现有成果的总结	178
9.3.4 结论	179
参考文献	180
第10章 网络编码在容断网络中的应用	183
10.1 引言	183
10.2 容断网络与随机线性编码的背景介绍	184
10.2.1 网络模型	184
10.2.2 DTN 路由方案回顾	185
10.2.2.1 DTN 广播路由方案	185
10.2.2.2 DTN 单播路由方案	186
10.2.3 随机线性编码	187
10.3 设计空间	188
10.4 广播通信中的编码效益	190

10.4.1 编码有利于提高能效	190
10.4.2 实际的 RLC 广播方案	191
10.5 单播应用中的编码效益	192
10.5.1 网络编码减少分组投递延迟	193
10.5.1.1 最小分组投递延迟	193
10.5.1.2 实现最小分组投递延迟的概率	195
10.5.1.3 其他指标	197
10.5.2 网络编码对延迟-传输次数的权衡关系的改善	198
10.5.3 关于 RLC 效益的讨论	199
10.5.3.1 不同带宽和缓存限制的影响	199
10.5.3.2 分代管理的影响	200
10.5.3.3 控制信令的影响	201
10.5.4 对网络编码方案的建模研究	201
10.5.5 其他关于在单播应用中使用 RLC 方案的研究工作	203
10.5.5.1 优先编码协议	204
10.5.5.2 两跳方案中的最优控制	204
10.5.5.3 在 DTN 中基于网络编码进行安全通信	204
10.6 开放性问题	205
10.6.1 短消息应用的 RLC 效益	205
10.6.2 多播通信中的 RLC 方案	205
10.7 总结与结束语	206
参考文献	206

网络编码入门

第 1 章 网络编码入门

Frank R. Kschischang

加拿大, 多伦多, 多伦多大学, 电子与计算机工程系

摘要

本章是学习网络编码的入门教程, 侧重讲述单源多播问题。首先, 本章将回顾一些常用的结论, 例如: 网络的多播容量等于划分该网络中的源节点和目的节点的最小割的容量; 通过定义在某足够大的有限域上的线性网络编码, 可以实现该多播容量且存在计算该网络编码系数的高效算法; 当选取网络编码系数的有限域足够大时, 可以无限逼近该多播容量。此外, 本章还将讨论实际应用中非常重要的一种网络编码——非相干随机网络编码。在非相干随机网络编码下, 源节点和目的节点都没有关于网络中的具体网络编码操作的先验信息。本章的最后将证明对于一般的网络流问题, 仅使用线性网络编码并不能实现网络的最大吞吐量, 并给出了若干反例。

关键词

图和网络、多播容量、线性网络编码、线性信息流算法、随机线性网络编码、非相干网络编码、非线性网络编码。

1.1 蝶形网络

网络编码建立在一个简单而广泛的概念的基础上: 在包交换网络中, 中间节点不仅仅是简单地路由转发接收到的数据包, 而是对它们进行一些函数操作并计算、转发操作结果。下面将举例说明网络编码带来的好处, 第一个例子引自 Ahlswede, Cai, Li 和 Yeung 等人编著的关于网络编码的开创性论文^[1], 网络编码这个新兴研究领域也正是起源于此。

图 1-1a 所示的有向图称为“蝶形网络”, 它是一个包交换网络模型。在该网络中, 源节点 s 需要将信息多播给两个目的节点 t 和 u 。有向图的每一条有向边代表一条无差错包传输信道, 每个信道利用 (Channel Use) 可以传输 1 个长为 m 比特的数据包。源节点希望以尽可能高的速率与两个目的节点通信。蝶形网络的一个关键特征是它包含一条瓶颈链路, 即图 1-1a 中从节点 b 到节点 c 的有向边 (用边 (b, c) 表示)。

解决该多播问题的一种“路由方法”如图 1-1b 所示。源节点在第一个时隙分别给与它相连的两个中间节点发送数据包 x 和 y , 网络将 x 转发给目的节点 t 和 u , 将 y 转发给目的节点 u 。在第二个时隙中, 源节点发送数据包 y 和 z , 网络将 z 转发给目的节点 t 和 u , 将 y 转发给目的节点 t 。两个时隙结束后, 两个目的节点都能够接收到 x 、 y 、 z 这 3 个数据包。使用该路由方法能够在两个时隙内传输给目的节点 3 个不同的数据包, 因此该方案的多播吞吐量为 1.5 包/信道利用。这里将网络“信道”的一次“使用”定义

为每条网络边传输最多一个数据包。该多播吞吐量已被证明是使用路由方法能够实现的 最大吞吐量。

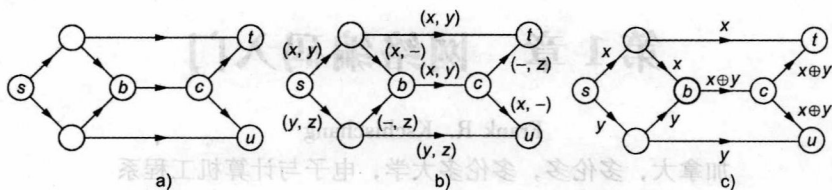


图 1-1

a) 包含“瓶颈链路”(b、c)的蝶形网络 b) 使用“路由方法”解决多播问题：在 2 个时隙内将 3 个数据包 x 、 y 、 z 路由转发给两个目的节点 (“—”表示在该时隙内信道空闲) c) 使用“网络编码方法”解决多播问题：在瓶颈链路上发送 x 、 y 的模二和(异或) $x \oplus y$ ，使得两个目的节点均能恢复出 x 和 y ，实现 2 数据包/时隙的传输

然而，使用图 1-1c 所示的“网络编码方法”能够实现 2 包/信道利用的多播吞吐量。该方法中，第一个时隙源节点仍分发两个数据包 x 和 y ，与“路由方法”不同的是，节点 b 将转发这两个数据包的模二和 $x \oplus y$ (将 x 和 y 按位异或)，而不是只转发 x 、 y 中的一个。目的节点 t 接收到数据包 x 和 $x \oplus y$ ，并根据它们恢复出 x 和 y ($x \oplus (x \oplus y) = y$)。同样地，目的节点 u 也可以从它接收到的两个数据包中恢复出 x 和 y 。网络编码方法以网络中间节点的编码操作和目的节点的解码操作为代价，提升了网络的多播吞吐量，并突破了使用“路由方法”所能实现的吞吐量上限。

那么，我们是否可以做得更好呢？容易看出，对于上述蝶形网络，答案是“不”。节点 t 和节点 u 仅通过两条边连接到网络，因此在单位时间内这两个节点最多只能接收两个数据包（一般地，一个网络的最大多播吞吐量取决于分割源节点和目的节点的最小“割集”——引自“最大流最小割”定理，后文将给出详细讨论）。图 1-1c 中所示的网络编码方法能够实现网络多播吞吐量的最大可能值，因此它是一个最优方案。

另一个例子是在无线中继网络中经常考虑的“无线蝶形网络”。考虑如图 1-2 所示的网络结构，两个位于山谷的小站 s 和 t 不能直接通信，它们需要通过位于山顶的中继节点 r 进行通信（通过无线信道）。假设该场景中的所有无线设备都只能工作在“半双工”模式，也就是说，1 个节点在 1 个时隙内只能接收或发送（而不能同时收发）1 个信号。此外，中继节点 r 在 1 个时隙内只可能接收到来自两个山谷小站中其中一个（而不是全部）的信号，但是两个山谷小站都能接收到中继节点广播的信号。假设通信目标是 s 发送数据包 x 给 t ， t 发送数据包 y 给 s （数据包的长度均为 m 比特）。



图 1-2 “无线蝶形网络”，山谷小站 s 和 t 可通过中继节点 r （广播方式）进行通信的无线半双工中继网络

使用“路由方法”可以在4个时隙内实现该通信目标：(1) s 发送 x 给 r ；(2) r 广播 x 给 t ；(3) t 发送 y 给 r ；(4) r 广播 y 给 s 。

使用“网络编码方法”时，仅需要3个时隙就可以实现该通信目标：(1) s 发送 x 给 r ；(2) t 发送 y 给 r ；(3) r 将 $x \oplus y$ 同时广播给 s 和 x 。由于 s 小站本来就有数据包 x ，因此它可以通过计算 $x \oplus (x \oplus y)$ 得到数据包 y ，相似地， t 也可以恢复出数据包 x 。该示例再一次证明了“网络编码方法”以网络中间节点的编码操作和目的节点的解码操作为代价，提升了网络的多播吞吐量，并突破了使用路由方法所能实现的吞吐量上限。

上述两例给我们上了重要的一课：要想充分利用通信网络的信息传输容量，光靠改进路由算法一般来说是不够的。尽管很多教科书在描述包交换网络时都将“数据包流”比喻为“货物流”，但是从蝶形网络示例中可以看出这种比喻从根本上来说就是不合适的。实际上，和在高速公路上行驶的汽车不同，多个信息数据包可以通过多种方式（如“线性叠加”）有效地结合在一起，而目的节点可以从这些结合后的信息中恢复出原始信息。本章乃至于本书都是基于这个简单思想的延拓。

本章结构如下：1.2节给出了通信网络在多播场景下的一个基本图论模型。1.3.1节给出了一个从最大流最小割理论推导出的重要定理：网络的最大多播吞吐量等于分割源节点和目的节点的最小“割集”的容量；1.3.2节详细描述了线性网络编码，该编码方法的本地编码操作只能是定义在有限域上的线性操作；1.3.3节进一步证明了使用定义在一个充分大的有限域上的线性网络编码可以实现网络的多播吞吐量上限。对于给定的网络，1.4.1节中给出了能够解决特定多播问题的网络编码系数的有效生成方法；1.4.2节主要讲述了随机线性网络编码，该编码方法的编码系数随机选取自某域，而不是预先设计好的。当域足够大时，随机选取的编码系数可以获得和预先设计最优的编码系数近似相同的性能。1.5节中证明了相对于路由方法，编码方法的多播吞吐量增益可以无限大。1.6节主要讲述的是非相干随机网络编码。使用非相干随机网络编码时，源节点和目的节点都没有关于网络中具体网络编码操作的先验信息。1.7节中讨论了实现网络编码的字母表所需具备的性质，并给出了若干个关于流问题的示例，这些示例说明（一般情况下）仅使用线性网络编码不足以实现网络的最大传输速率。

网络编码的相关文献日益增多，除本篇之外，其他关于网络编码的入门资料可参考文献[2-5]。

注意，本章中作如下约定： $|X|$ 表示有限集 X 包含的元素的数量；矩阵用粗体字母表示，如 $\mathbf{A}$ ； $\mathbf{I}$ 表示单位矩阵； $\mathbf{e}_i$ 表示第 i 列为1的单位向量 $(0, \dots, 0, 1, 0, \dots, 0)$ 。

1.2 图和网络

1.2.1 组合包网络

下面给出的图论模型虽然不是完全意义上的一般模型，但却足以表征网络编码的主

要思想。

一个组合包网络 $N = (V, E, S, T, A)$ 包括:

- 1) 有限有向无环多重图 $G = (V, E)$, 其中 V 表示图 G 的顶点集合, E 表示图 G 的有向边的多重集合。
- 2) 无重复源节点集合 $S \subset V$ 。
- 3) 无重复目的节点集合 $T \subset V$ 。
- 4) 有限的数据包符号集 A , $|A| \geq 2$ 。

图 G 中的顶点代表包交换网络中的通信节点, 有向边代表通信节点之间的无差错传输信道。有向边 (u, v) 具有单位容量, 即每条边每次只能将 1 个数据包 (从符号集 A 中选取的一个符号) 从点 u 传送给点 v 。如果要进行更大容量 (必须为整数) 的传输, 可以在点 u 和点 v 之间连接若干条平行边, 因此 G 是一个多重图。为了避免多条平行边之间相互混淆, 我们给多重集合 E 的每条边分配一个标号, 分别是 $e_1, e_2, \dots, e_{|E|}$, 每条边都是一组顶点的有序对, 且对于 $j \neq i$, 允许 $e_i = e_j$ 。

对于顶点 $v \in V$, 我们用 $I(v)$ 表示所有进入点 v 的边的集合, 用 $O(v)$ 表示所有从点 v 出发的边的集合。一般来说, 对于一个给定的网络, 我们可以通过引入“虚拟节点”来实现 $S \cap T = \emptyset$, 其中, S 为所有源节点的集合, 且满足 $\forall s \in S, I(s) = \emptyset$; T 为所有目的节点的集合, 且满足 $\forall t \in T, O(t) = \emptyset$ 。

与图论中的设定相同, 图 G 中从顶点 $u \in V$ 至顶点 $v \in V$ 的任意 (有向) 路径都可表示为一个由有向边 $(u, v_1), (v_1, v_2), (v_2, v_3), \dots, (v_{l-2}, v_{l-1}), (v_{l-1}, v)$ 组成的有限序列, 该序列中的每个元素都是有向边集合 E 中的元素。如果一条有向路径的两个端点相同, 那么这条路径就被称为图的一个环。包交换网络定义中的“无环”指的是该网络的多重图 G 中不存在环。

对于顶点 $u, v \in V$, 如果 $v = u$ 或者图 G 中存在一条从 u 到 v 的有向路径, 就称 u 可达 v 。上述可达性意味着 V 是部分有序的, 通常可以被进一步扩展为兼容的全体有序, 又称为拓扑有序。拓扑有序的概念将在 1.4.1 节中使用到。

在有向边 $(u, v) \in E$ 上进行的操作是将点 u 发出的数据包 $p \in A$ 无差错地交付给点 v 。所有边都允许处于空闲状态 (即不传输数据包), 并假设点 v 具有它的所有入边的状态信息 (空闲状态的边可以从 E 中等效移除)。在后文讨论的线性网络编码中, 用传输零数据包来表示这些“空闲边”。

组合包网络中的组合逻辑指的是: 顶点 v 的出边集合 $O(v)$ 中的任一非空闲边上传输的数据包是来自其入边集合 $I(v)$ 中的所有非空闲边的数据包 (当 v 为源节点时, 则为它自己产生的数据包) 的函数。对于一个实际网络实现, 在节点 v 输出的数据包函数被计算好并发送出去之前, 进入节点的数据包是需要被缓存的。这里不考虑由传输、缓存以及对数据包的处理引起的时延。

节点 v 使用的函数被称为 v 的本地编码函数。例如, 当 v 只有路由功能时, 它的出边上发送的数据包可以看做是对入边上接收到的数据包的复制。而网络编码的基本思想是对进入节点的所有数据包进行更一般性的本地编码操作, 而不仅仅是简单的复制, 从而获得性能上的效益。

对于组合包网络 N ，一次信道利用指的是为 E 中的每一条非空闲边都分配一个具体的数据包（取自集合 A ），也可以看做是网络中的节点对特定本地编码函数的一次实现。换言之，一次信道利用中的本地编码函数是固定的，且网络中的每条边最多被使用一次。当然，对于不同的信道利用，本地网络编码函数可以不同，图 1-1b 中给出的“路由方法”可以说明这一点。

本章以在每次信道利用中网络所传输的数据包数量（包/信道利用）作为单位来度量网络的传输效率。如前所述，图 1-1b 所示的蝶形网络的多播速率为 1.5 包/信道利用，图 1-1c 则可达到 2 包/信道利用。需要注意的是，这里提到的“数据包”所包含的信息量取决于符号集 A 的规模 $|A|$ 。以包/信道利用为单位度量的速率可以通过乘以 $\log_2 |A|$ 比特/数据包将其转化为以比特/信道利用为单位度量的速率。只有在比较使用不同规模的符号集的网络时，如在允许改变符号集规模的条件下，上述两种度量单位才会存在差异。

本节所述的组合网络模型并不具备完全意义上的一般性。在无线传输环境下，需要综合考虑无线信道的广播特性（即一次传输可能会被多个目的节点接收）和无线环境的多址特性（多个节点同时发送时可能会在接收端产生相互干扰），并对该模型进行修正。此外，本模型没有明确考虑中断率（链路不完全可靠的概率）、时延（或其他时序逻辑中关于时间的概念）及可能存在的反馈信道（图论中的环），但使用该组合网络模型足以阐明网络编码的主要思想。

1.2.2 网络信息流

我们用 $S = \{s_1, s_2, \dots, s_{|S|}\}$ 表示所有源节点的集合。假设每个源节点 $s_i \in S$ 都有无穷多个待发送的数据包，而目的节点 $t \in T$ 只需重建子集 $D_t \subseteq S$ 中的源节点发送的数据包。 D_t 表示 t 点播的源节点集合。

假设 s_i 有数据包 $p_1, p_2, p_3, \dots$ 待发送， n 次信道利用后， t （通过对这 n 次信道利用中来自 $I(t)$ 的数据包进行特定的函数运算）可以恢复出 k 个源数据包 $p_1, p_2, p_3, \dots, p_k$ ，那么就说 t 能够以速率 $r_t = k/n$ （单位：包/信道利用）解码 s_i 的信息。我们要求源节点 $s_i \in S$ 以同一传输速率 r_i （包/信道利用）服务所有点播它的目的节点。给定网络中的点播集 $\{D_t: t \in T\}$ 以速率 $(r_1, r_2, \dots, r_{|S|})$ 可达指的是：通过选择本地编码操作（可以是时变的）和 n ，所有目的节点都能以给定速率重建它点播的源信息。

关于上述一般网络信息流的一个重要的特殊情况就是多播问题，其中 $\forall t \in T, D_t = S$ ，即每个目的节点都点播了所有源节点的信息。

还有其他一些比较重要的特殊情况，如单点单播（网络中仅有 1 个源节点 s 和 1 个目的节点 t ，且满足 $D_t = \{s\}$ ）和多点单播（ $S = \{s_1, s_2, \dots, s_L\}$ ， $T = \{s_1, s_2, \dots, s_L\}$ 且满足 $D_{s_i} = \{s_i\}$ ， L 是大于 1 的整数）等。

在接下来的章节中，首先将考虑单源多播问题，并证明当数据包符号集是一个足够大的有限域时，使用线性网络编码能够实现最大多播速率。然而我们也将看到，对于一般的网络信息流问题，仅使用线性网络编码通常不足以使网络达到最大速率。