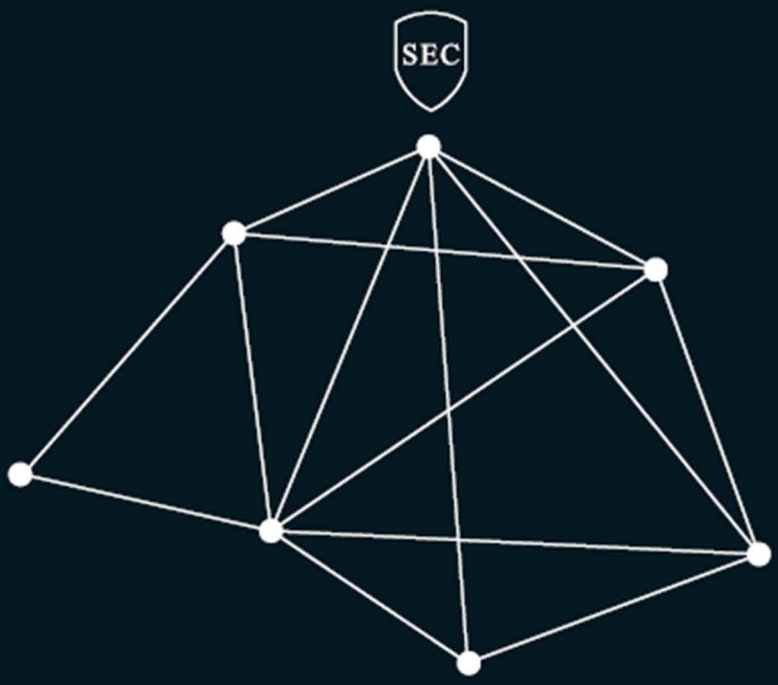


无线网络编码安全研究

RESEARCH ON
CODING SECURITY OF
WIRELESS NETWORKS

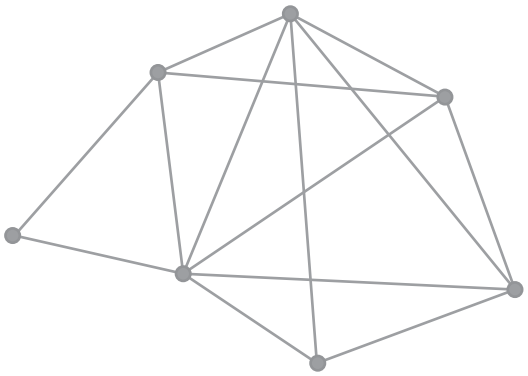
宁佐廷 史伟奇 刘绪崇 著

湖南大学出版社

无线网络编码安全研究

RESEARCH ON
CODING SECURITY OF
WIRELESS NETWORKS

宁佐廷 史伟奇 刘绪崇 著



湖南大学出版社·长沙

内 容 简 介

本书以无线网络编码为核心，对无线网络编码缓存管理、编码方案及其安全性进行了深入研究。其中，对无线网络编码策略中数据包乱序、包丢失和缓存约束的问题，现有编码易导致数据多次传输的问题，无线网络编码防窃听采用传统安全手段开销大的问题，无线网络编码防污染攻击中现有方法带来的每个节点计算开销大、时延高的问题，进行了有针对性的研究，并提出了具体的解决方案与对策。

图书在版编目（CIP）数据

无线网络编码安全研究/宁佐廷，史伟奇，刘绪崇著．—长沙：湖南大学出版社，2020.12

ISBN 978-7-5667-1701-6

Ⅰ.①无… Ⅱ.①宁… ②史… ③刘… Ⅲ.①无线网—编码—侦听—安全技术—研究 Ⅳ.①TN915.08

中国版本图书馆 CIP 数据核字（2018）第 284583 号

无线网络编码安全研究

WUXIAN WANGLUO BIANMA ANQUAN YANJIU

著　　者：宁佐廷　史伟奇　刘绪崇
责任编辑：尚楠欣　　**责任校对：**陈鹏金
印　　装：北京虎彩文化传播有限公司
开　　本：710 mm×1000 mm　1/16　**印张：**9　**字数：**130 千
版　　次：2020 年 12 月第 1 版　**印次：**2020 年 12 月第 1 次印刷
书　　号：ISBN 978-7-5667-1701-6
定　　价：36.00 元

出 版 人：李文邦
出版发行：湖南大学出版社
社　　址：湖南·长沙·岳麓山　　**邮　　编：**410082
电　　话：0731-88822559(营销部)，88821174(编辑室)，88821006(出版部)
传　　真：0731-88822264(总编室)
网　　址：http://www.hnupress.com
电子邮箱：liuwangfriend66@126.com

序　言

随着无线网络技术及应用的飞速发展，无线网线已成为人们日常生活中不可或缺的部分。与此同时，人们对无线网络的性能要求也越来越高，如要求更快的网速、更快的搜索响应和更安全的网络服务等。但现有的无线网络技术还不能满足用户的使用要求，如何满足用户对无线网络的高性能要求，成为网络技术研究者需要迫切解决的问题。而要提升网络性能（如带宽利用率、吞吐量、网络时延及安全性等），网络编码成为一个非常适合且非常有效的技术手段。

目前市面上有一些关于网络编码方面的书籍，但这些书籍大部分都是从网络编码的应用方面进行阐述和分析，仅少部分涉及了网络编码的安全性分析，而关于无线网络编码安全方面的书籍几乎没有。本书基于传统网络对无线网络编码安全性进行了分析，并且探讨了未来网络结构中网络编码的安全性问题，如分析了软件定义网络 SDN 中网络编码的安全性问题。

本书从专业研究人员的角度出发，分三个部分介绍了无线网络编码及其安全性。第一部分，介绍了无线网络编码的研究背景、研究意义及相关方法。第二部分，介绍了现有无线网络编码安全性所包含的两个方面，即窃听攻击和污染攻击，且介绍了抵抗这两种攻击的方法。第三部分，从未来网络的角度阐述了网络编码对未来网络的重要意义。重点介绍了命名数据网络中网络编码的研究价值和应用价值。

本书可供从事网络编码及其安全性研究的专业人员使用。读者需要具备计算机操作系统、网络编码、计算机网络等方面的预备基础知识。作

者在专著后面列出了详细的参考文献，读者及相关研究人员可以从中找到相应的背景知识。

本书涉及的内容广泛、专业，不仅融入作者多年的网络编码研究成果和经验，更包含了对未来网络等相关前沿技术的研究。囿于知识和经验，本书中不当之处在所难免，恳请广大读者提出宝贵意见。

谢　鲲

2018 年 6 月 16 日

前　言

无线网络编码很大程度上是基于无线网络的媒介开放特性实现的，特别是异或编码。而一般情况下，无线网络下的异或编码，其性能主要取决于缓存和数据包调度策略。因此，研究一种高效实用的编码管理策略和更先进的编码方案，对网络性能的提升具有重要的价值。同时，无线网络开放的媒介特性使得它容易遭受攻击，如窃听攻击和污染攻击，这给无线网络编码的研究和应用前景蒙上了阴影。因此，研究安全性高且开销相对较低的安全网络编码方法对无线网络编码研究是具有十分重要的意义。本书以无线网络编码为核心，对无线网络编码缓存管理、编码方案及其安全性进行了深入研究，主要工作及创新点如下：

(1)针对无线网络编码策略中数据包乱序、包丢失和缓存约束的问题，本书提出了基于数据包交换与调度的无线网络编码数据包管理策略。无线网络中，采用网络编码能进一步提升网络吞吐量，降低端到端传输时延。然而，在编码缓存满的情况下，现有的编码策略并没有充分考虑到数据包乱序的情况。同时，在缓存满的情况下，对于新获得的数据包，现有的策略是要么丢弃要么用其替换缓存中已有的数据包，但这两种处理方法都基于一定的前提条件和假设。而在实际网络中，情况往往是十分复杂的。针对这些情况，本书提出了在一般网络条件下的无线网络编码策略。该策略不仅考虑了数据包乱序、数据包概率丢失等问题，而且充分考虑了编码缓存约束的问题。在编码缓存满的情况下，对于新的数据包，本书采用预丢弃措施，同时记录丢弃数据包 ID，该数据包 ID 包含了数据包对应源节点和包序号信息。在数据包乱序的情况下，本书根据编码缓存

内数据包信息及每条流的发送数据包信息，在满足编码条件的情况下，调整缓存内数据包顺序，从而进一步提升网络性能。

(2)针对现有异或编码导致的多次数据传输问题，本书提出了组群异或编码方案。网络编码从编码关系的角度分为线性网络编码和非线性网络编码两种。在线性网络编码中，异或编码是轻量级且开销非常小的一种编码方案，该方案操作简单，具有很好的成效。然而，异或编码由于采用成对异或操作的方式，属于原子编码操作，因此，对编码节点而言，在编码数据包数量比较大的情况下，编码次数多。而且，在缓存满的条件下，节点需要多次调度和多次向源节点请求数据包，极大地影响了网络性能，如增加了网络时延等等。针对这些缺陷，本书提出了组群异或编码方案，该方案将满足编码条件的数据包一次性进行异或编码，然后再逐级从每条流减少一个数据包进行编码，以此类推，直到最后完成一条流一个数据包的原子编码操作。这种编码方案，极大地提升了编码效率，减少了数据包传输次数，降低了网络时延。

(3)针对无线网络编码防窃听采用传统安全手段开销大的问题，本书提出了基于 IBC 算法的安全防窃听网络编码方案。现有的无线网络编码防窃听方案主要有两种：同态哈希和同态签名。这两种方案通过同态加密的方法，将发送的数据包进行哈希或签名，而攻击者很难通过窃听的方法获取有效信息，从而提高了传输编码数据包的安全性。但是，这两种方案共同的缺陷就是网络中的每个编码节点计算开销非常大，计算时延也高。针对这些不足，本书提出了基于 IBC 算法的安全防窃听网络编码方案，该方案区别于传统的非对称加密方法，公钥即节点身份标识，如 IP 等。同时，加密的对象只是编码系数，减少了计算数据量。该方案极大地降低了编码节点的计算复杂性，同时很好地达到了防窃听攻击的目的。

(4)针对无线网络编码防污染攻击中现有方法带来的每个节点计算开销大、时延高的问题，本书提出了高性能、低开销的安全防污染攻击方案。现有的防污染攻击方案可以归纳成两类：数据验证和纠错。数据验证是基于公钥加密体系，如同态哈希和同态签名，这类方案给网络中每个节点带来了复杂的计算开销，因此，它将不可避免地造成高计算时延。后

一类方案，也就是纠错，它主要是对每个数据块进行纠正从而确保收到的数据不被污染。然而，这种方案的局限在于只能对数量非常受限的污染数据包进行纠正。针对这两类方案的缺点，本书提出了高性能、低开销的防污染攻击方案。该方案利用了密钥预分发和消息验证码（MAC）。基于多播特性，合法节点使用目的节点密钥为每个数据生成多个 MACs。每个 MAC 附加在源数据后面。因此，每个节点能使用各自的密钥对收到的数据进行验证，并且能对污染数据进行过滤。

（5）结合未来网络 SDN，研究 SDN 下网络编码的安全性。通过允许中继节点在发送数据包之前对接收的数据包进行编码，网络编码扩大了多播应用程序的容量。但它很容易受到污染攻击。有人提出了一些签名方案来阻止这种攻击，但是大多数签名方案都需要同态，不能轻松生成和管理密钥。本书提出了一种基于软件定义网络的安全交换网络编码方案。在该方案中，复杂的安全组播管理与基于 SDN 的快速数据传输分离。根据服务需求和网络状态，将多个多播集聚合到一个多播组中。然后，控制器使用网络编码路由聚合组，只有受信任的交换机才能通过广播加密加入网络编码。该方案可以利用传统的无同态密码体制，大大降低了计算复杂度，提高了传输效率。

本研究受湖南省科技重大专项资助，项目号：No.2017SK1040。

宁佐廷

2018 年 6 月 16 日

目　次

1 绪 论

1.1 研究背景

随着无线网络技术及应用的飞速发展，无线网络已成为人们日常生活中不可或缺的部分。与此同时，人们对无线网络的性能要求也越来越高，如要求更快的网速、更快的搜索响应和更安全的网络服务等。但现有的无线网络技术还不能满足用户的使用要求，如何满足用户对无线网络的高性能使用要求，成为每个网络技术研究者需要迫切解决的问题。而要提升网络性能（如带宽利用率、吞吐量、网络时延及安全性等），网络编码成为一个非常适合且非常有效的技术手段。

网络编码[1][2]最初是在通信领域中由香港中文大学的李硕彦、蔡宁和杨伟豪等提出来的。其核心思想就是允许中继节点对收到的数据进行编码操作，通过这种操作，极大地提升了网络吞吐量，减少了网络时延，均衡了网络负载。网络编码技术是计算机网络通信领域一项十分重要的技术。越来越多的国内外研究者将目光投向网络编码，并使其迅速成为一个重点研究领域。同时，由于网络编码技术本身涉及通信理论、数学理论、矩阵理论、计算机科学、编码和密码学等，因此该技术也对这些研究领域的发展产生了非常重要的推动作用。网络编码结合编码和路由技术，使得中继节点能对接收的数据进行编码组合，并将编码后的数据包以多播的方式发送出去；而目的节点在收到编码后的数据包后，可以根据数据

包中对应的编码系数，对编码数据进行解码，从而获得对应的原始数据。网络编码通过突破传统的存储转发局限，使得网络的中继节点获得网络流传输的理论上限。区别于传统的路由技术，网络编码彻底颠覆了现有通信网络中的信息处理和信息传输的方式，如图 1-1 所示。正是网络编码的这些特性，使得对网络编码的研究从开始的组播网络容量分析、时空复杂性分析和算法理论等方面延伸到实际应用层面。同时，网络编码通过最大程度地利用网络信道，在单信源网络中使得节点与信源之间的信息传输率达到最大。与传统的存储转发路由技术相比，网络编码可以节省数据传输次数，特别在无线网络尤其无线传感网络中，它能极大地节约节点的传输能耗，提升数据传输效率。在数据分发应用上，网络编码可以充分利用多条链路进行数据传输。信息的多链路传输，很大程度上减少了网络节点拥塞等约束，对均衡网络负载有很大的帮助。而且，网络编码的数据恢复效用，对数据丢失具有很好的容错性和鲁棒性。

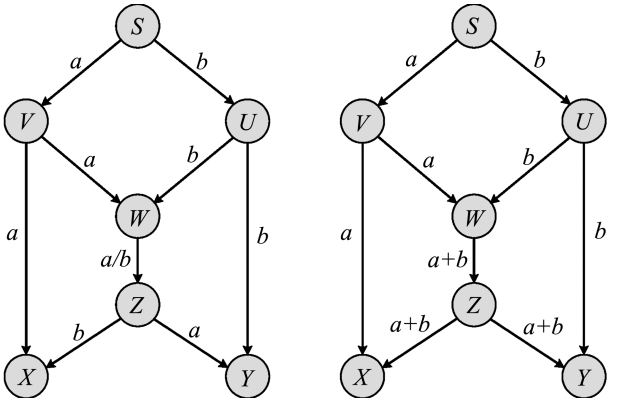


图 1-1　网络编码与传统路由对比图

无线网络的一些特性使得它与有线网络有很大的不同。无线网络的内在属性(如广播传输、媒介共享和时变)使得它可以更好地利用网络编码获得性能增益。由于无线网络传输介质共享的特性，可以通过无线媒介开放实现网络编码网络性能的最大化提升。如图 1-2 所示，中继节点 R 在收到源节点 S_A 与 S_B 的数据包后，可以对其进行编码操作，如将两

条流的数据包两两异或操作形成编码数据包 $P_1 \oplus Q_1$，$P_2 \oplus Q_2$，然后广播出去。而目的节点能获取附近源节点发送的数据包，例如目的节点 D_A 获得到 Q_1，Q_2，然后将收到的编码数据包如 $P_1 \oplus Q_1$ 与得到的数据包 Q_1 进行异或解码操作，最终得到原始数据包。采用同样的方法，目的节点 D_B 也可以获得对应的原始数据包，使无线网络编码对网络性能的增益最大化。

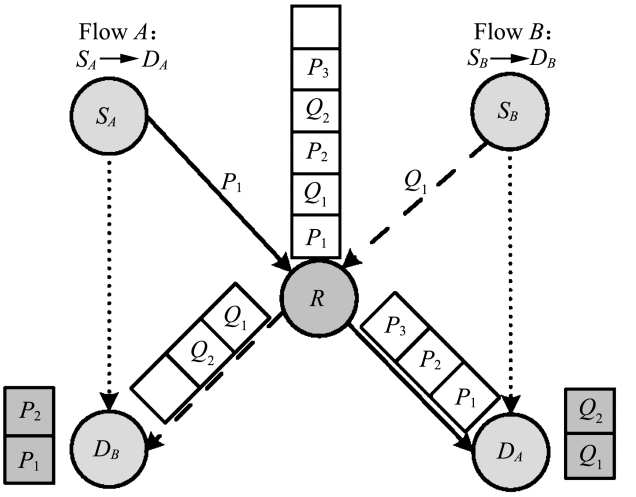


图 1-2 无线网络编码图

然而，无线网络编码[3][4]也因其编码数据包的特性使得它容易遭受攻击，给其应用带来很大的威胁。无线网络编码遭受的威胁主要有两种：窃听攻击[5]和污染攻击[6]。一方面，一些攻击者通过无线窃听，蓄意向其他节点发送伪造/篡改数据包以达到破坏编码数据包的目的；另一方面，无线网络编码面对污染攻击特别脆弱，恶意攻击者通过向合法节点发送污染数据包，使得合法节点编码形成的数据包也遭受污染，进而使得网络中存在大量污染数据，导致目的节点无法解码获得原始数据，有时甚至会造成网络瘫痪。

(1)防窃听的网络编码[7][8]。

现有的防窃听网络编码方法主要有两种，即信息论的方法和密码学

的方法。一般情况下，合法接收者获得的有效信息较窃听者获取的信息多，信息论的方法是通过在信息的源头对发送的编码消息加入随机数以对发送消息进行校验，最终达到防窃听的目的。这种方法基于消息校验码技术。密码学的方法是采用密码技术对网络编码系数进行加密，从而使得窃听者即使在数据包被窃取的情况下也无法对数据进行解密，因此也就无法对编码数据进行解码，无法获取有效信息，从而达到防窃听的目的。

(2)防污染的网络编码[9][10]。

污染攻击是指攻击者在通过无线窃听获取数据包信息后，将窃听到的数据进行恶意修改、伪造或者部分删除等操作，使得网络中传输的数据遭到破坏。特别在网络编码网络中，遭到破坏的数据将被其他节点进一步编码，使得污染进一步扩散，造成目的节点无法解码恢复所需要的原始数据包。这极大地浪费了网络资源，尤其对于无线网络，污染攻击导致宝贵的能耗浪费，有时甚至导致网络崩溃。现有的防污染攻击方法主要有两种：一种是利用同态签名体制，另一种是利用消息的代数结构。

1.2 研究意义

无线网络编码(特别是异或编码)很大程度上是基于无线网络的媒介开放特性实现的。而一般情况下，对于无线网络下的异或编码，其性能主要取决于缓存和数据包调度策略。因此，研究一种高效实用的缓存管理策略和更先进的编码方案，对网络性能的提升具有重要的价值。本书围绕无线网络编码缓存管理策略和编码方案，重点解决缓存管理中的数据包调度和交换问题，同时解决了传统两两异或编码存在的多次数据包传输和调度问题。

同时，无线网络开放的媒介特性使得它容易遭受攻击，如窃听攻击和污染攻击，这给无线网络编码的研究和应用前景蒙上了阴影。因此，研究安全性高且开销相对较低的安全网络编码方法对无线网络编码具有十分

重要的意义。围绕编码安全问题，本书重点解决防窃听和防污染攻击方案中普遍存在的计算、时延开销高及污染检测不及时的问题。

上述研究的意义还在于：

(1)用于流量管理。

网络编码能极大地提升网络吞吐量，平衡网络负载，提升网络性能。网络节点会根据网络流量确定哪些是编码节点，找出最优路径和最大吞吐量，选择最佳数据包传输和分发路径，这对网络中节点的流量均衡有很大的现实意义。因此，网络编码能很好地应用于流量管理中。

(2)用于数据分发。

无线网络的广播特性使得多个流在同一个节点汇聚的机会很大，因此，无线网络具有更多的编码机会。大规模的数据分发有着广泛的应用背景，基于存储和转发的 IP 组播是实现数据分发的一种有效手段。采用基于网络编码的组播技术，能够有效节约网络资源，提升数据分发系统的服务质量(quality of service，QoS)，显著降低信息传输的实施成本。

(3)用于网络管理。

网络编码对于均衡网络负载、提升网络吞吐量和节省传输能耗具有极大的帮助，因此，在网络管理中，使用网络编码能更好地分配和协调网络资源，最大化带宽利用率。特别地，在大型骨干网络中，对关键节点的编码操作能降低网络拥塞程度，减少数据传输次数和传输时延。同时，通过对关键节点的编码操作，能更好地对网络资源进行管理，提升网络性能，也能方便资源配置。

(4)用于网络安全。

网络安全对网络的应用而言非常重要，安全网络编码可以在很大程度上能解决传统的密码学手段带来的计算复杂性和信息冗余等问题。安全网络编码通过对编码系数或者部分编码系数进行加密操作，隐藏了数据传输的核心部分。同时，由于安全网络编码只是加密编码系数，其计算复杂度得以极大的降低，节点资源开销小，特别对于无线网络而言，宝贵而有限的能源能得到充分应用。

1.3 主要工作及关键技术挑战

本书以无线网络编码为核心，对无线网络编码缓存管理、编码方案及其安全性进行深入研究，主要工作分为如下几个部分：提出基于数据包交换与调度的无线网络编码缓存管理策略，提出组群异或无线网络编码方案，提出防污染攻击的安全网络编码方案和基于 SDN 广播加密的安全网络编码方案。研究工作的关系框图如图 1-3 所示。

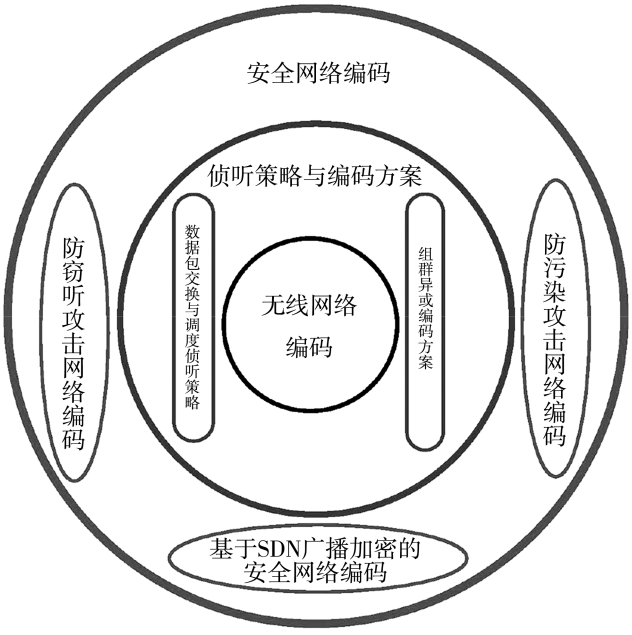


图 1-3 研究工作的关系框图

(1)针对无线网络编码缓存管理策略中数据包乱序、数据包丢失和缓存约束的问题，本书提出了基于数据包交换与调度的无线网络编码缓存管理策略。

无线网络中，采用网络编码能进一步提升网络吞吐量，降低端到端传输时延。然而，在缓存满的情况下，现有的缓存管理策略并没有充分考虑到数据包乱序的情况。同时，在缓存满的情况下，对于新获得的数据包，现有的策略是要么丢弃，要么用其替换缓存中已有的数据包，但这两种处理方法都基于一定的前提条件和假设。而在实际网络中，情况往往是十分复杂的。针对这些情况，本书提出了在一般网络条件下的无线网络编码策略。该策略不仅考虑了数据包乱序、数据包概率丢失等问题，而且充分考虑了编码缓存约束的问题。在缓存满的情况下，对于新获得的数据包，本书采用预丢弃措施，同时记录丢弃数据包 ID，该数据包 ID 包含了数据包对应源节点和数据包序号信息。而在数据包乱序的情况下，本书根据缓存内数据包信息及每条流的发送数据包信息，在满足编码条件的情况下，调整缓存内数据包顺序，从而进一步提升网络性能。

(2)针对现有异或编码导致的多次数据传输问题，本书提出了组群异或网络编码方案。

网络编码从编码关系的角度分为线性网络编码和非线性网络编码。在线性网络编码中，异或编码是轻量级且开销非常小的一种编码方案，该方案操作简单，具有很好的成效。然而，由于异或编码采用成对异或操作的方式，属于原子编码操作，因此，对编码节点而言，在编码数据包数量比较大的情况下，编码次数多。而且，在缓存满的条件下，节点需要多次调度和多次向源节点请求数据包，极大地影响了网络性能，如增加了网络时延等。针对这些缺陷，本书提出了组群异或编码方案，该方案将满足编码条件的数据包一次性进行异或编码，然后再逐级从每条流减少一个数据包进行编码，以此类推，直到最后完成一条流一个数据包的原子编码操作。这种编码方案极大地提升了编码效率，减少了数据包传输次数，降低了网络时延。

(3)针对采用传统安全手段无线网络编码防窃听开销大的问题，本书提出了基于 IBC 算法的安全防窃听网络编码方案。