# 网络编码理论及应用综述

姚世雄[1],陈 晶[1,*],何 琨[1],杜瑞颖[2]
(1 武汉大学 计算机学院,软件工程国家重点实验室,武汉 430072;
2 武汉大学 地球空间信息技术协同创新中心,武汉 430072)

**摘 要** 指出了网络编码(NC)理论已经日渐成熟,从最开始的实现网络最大流到近来的各种应用,网络编码作为新兴技术被广泛研究. 对基于密码学、信息论、博弈论的网络编码理论进行了分类讨论,随后对安全网络编码技术及其应用作了概括性的描述,提出了开放性的问题,对安全网络编码的应用前景作了展望.

**关键词** 网络编码; 密码学; 信息论; 博弈论
**中图分类号** TP393 **文献标识码** A **文章编号** 1672-4321(2017)02-0115-14

# Survey on Network Coding Theory and Application

*Yao Shixiong*[1], *Chen Jing*[1], *He Kun*[1], *Du Ruiying*[2]
(1 State Key Laboratory of Software Engineering, Computer School, Wuhan University, Wuhan 430072, China;
2 Collaborative Innovation Center of Geospatial Technology, Wuhan University, Wuhan 430072, China)

**Abstract** The network coding (NC) theory has been mature gradually, which was used to achieve the maximum network flow at the beginning and was applied in various aspects recently. As the new technology, NC has been researched widely. In this paper, the NC theory and technology were reviewed. The NC theory was discussed based on the cryptology, information theory and game theory. Additionally, the NC technology and its application were generalized and open research problems were shared. Finally, the prospect of NC application in the future was given.

**Keywords** network coding; cryptography; information theory; game theory

## 1 背景介绍

众所周知,传统的路由机制中传输的信息是不能叠加的,中间节点(例如路由器交换机等)只是对数据包进行存储转发,在多播传输环境中,通常不能实现由最大流最小割定理[1]确定的最大传输容量. 然而,在 2000 年,由香港中文大学的 Rudolf Ahlswede 在 IEEE Transactions on Information Theory 上发表的一篇论文[2]首次提出了网络编码(NC)的概念,并从理论上证明了如果中间节点对传输的信息并非局限于存储转发,而是按照合适的方式进行编码,则该系统能够实现理论上的最大传输率. 随后,香港中文大学的李硕彦教授、杨伟豪教授、蔡宁教授提出了线性网络编码,指出线性网络编码方式可以达到多播方式下的网络容量; 为了解决分布式网络环境中的编码问题,Tracey Ho[3]提出随机网络编码,即随机选取系数进行编码; Koetter Ralf 等[4]提出网络编码的代数框架,即可用代数理论来解决网络编码的系数问题. 这些研究成果进一步地完善和丰富了网络编码理论. 网络编码彻底颠覆了传统通信网络对信息的处理方式,实现了信息论的最大传输率,在信息论领域具有划时代的意义. 其主要优点如下: 1) 提升网络吞吐量,无论是无线还是有线网络,网络节点数越大,网络编码在吞吐量上的优势越明显; 2) 均衡网络负载,将网络流量分布于更广泛的网络上; 3) 提高带宽利用率; 4) 无线网络中节省节点能量消耗; 5) 提高网络链路的鲁棒性.

作为一种极具发展潜力的新兴技术,网络编码已经引起了学术界的广泛关注和高度重视,国外著

收稿日期 2017-04-20 * 通讯作者 陈 晶,教授,博士生导师,研究方向: 信息安全,E-mail: chenjing@whu.edu.cn
作者简介 姚世雄(1988-),男,博士生,研究方向: 信息安全,E-mail: derekysx@whu.edu.cn
基金项目 国家自然科学基金资助项目(61272451; 61572380); 国家重点基础研究发展规划项目(2014CB340600)

名大学和研究机构,例如:加州理工学院[5],麻省理工学院[6],英特尔研究所[7],微软研究院[8],贝尔实验室[9],圣地亚哥通信研究中心[10]等都对网络编码理论开展广泛的研究与应用,国内研究机构也纷纷开始了这方面的研究,例如:清华大学[11],北京大学[12],国防科技大学[13],武汉大学[14],北京航空航天大学[15],北京邮电大学[16],华中科技大学[17]等对网络编码理论进行了探讨与研究.随着研究的深入、应用的扩展和对网络安全需求的进一步提高,研究者发现网络编码在提高性能的同时,也带来了如下一些特有的问题与安全威胁.

(1)网络编码算法中,往往允许中间节点对数据进行编码,而攻击者可以选择路径中的任意节点进行攻击,所以中间节点的参与增加了系统被攻击的可能性.

(2)由于编码后的数据报文可能分别由多条路径进行传输,最终在目的节点进行解码,攻击者可能在其中的部分路径或者部分节点周围进行窃听、篡改、伪造等攻击,所以窃听攻击会更加隐蔽,而污染攻击的影响将更加严重.

(3)在资源受限网络环境中(如无线网络节点能量受限),可能出现合法节点由于节能的自私偏好,为延长自己的服务时间不参与编码而选择只是发送与之对应的目的节点的包,从而造成整个网络系统的性能降低.

如果忽略这些不利因素,面对当前飞速发展的各种网络攻击方式,网络编码所带来优越的性能将很难保证.因此网络编码的安全性从不同的角度出发,有不同的要求:

从密码学的角度考虑,应该包括:1)机密性.要保证传输数据不被非法获取;2)完整性.对于网络编码系统,主动攻击不能篡改或损坏源数据,保证目的节点能够正确解码出源消息;3)真实性.网络中传输的信息及其来源是正确的,是可被验证和可被信任的;4)可追溯性.无线系统的开放性,使得恶意节点很容易入侵到系统中,对非法入侵,伪造数据,能够追溯到恶意本源,对于节点不诚实行为,能够根据审计分析来跟踪安全事件,解决争执;5)新鲜性.为保证网络编码提高网络吞吐率的天然特性,避免网络中重传旧的数据包而浪费网络资源,提高传输效率;6)可用性.利用网络编码,均衡网络负载,平衡各个节点的能量,保证节点的生存时间,保证无线链路的正常传输.

从信息论的角度考虑,应该包括:1)正确性.能够实现错误控制,并改正错误,保证目的节点能够正确解码出源消息;2)弱安全性.在安全要求不是很高的情况下,保证重要信息不被窃取,即重要信息与源信息的条件互信息为0;3)信息论安全性.不出现任何信息泄露,窃听者即使窃听到数据包,也不能获取任何信息,即窃取到的信息与源信息的互信息为0.

从博弈论的角度考虑,应该包括:1)整体利益高于个体利益.防止单个节点为延长自身生存时间,而选择性地发送数据包,导致整个网络系统性能降低;2)抑制攻击.合法节点与非法节点进行博弈,减小攻击造成的影响;3)合理竞争.会话之间相互竞争网络资源,应避免恶性竞争降低网络系统性能.

## 2 网络编码基础

### 2.1 网络编码的基本思想简介

以经典的蝴蝶网络为例,阐明网络编码的基本思想.

如图1所示的通信网络$G=(V,E)$中,$V$表示网络中的节点集,$E$表示边集,$S$是源节点,$T_1$、$T_2$为目的节点,其他节点是中间节点,信道容量为单位容量,源节点$S$要将消息$a$和$b$都发送到两个目的节点$T_1$、$T_2$.

图1($a$)和($b$)均为传统路由方式传输数据,($c$)采用网络编码方式传输数据.由于信道容量为单位容量,很容易发现,在$U$节点处,传统的路由方式只能选择发送$a$或者$b$,在同一时间之内,$T_1$或者$T_2$只能有一个节点能同时收到$a$和$b$;若采用网络编码传输方式,$U$节点对接收到的$a$和$b$进行异或运算$a\oplus b$,然后将$a\oplus b$往后续节点发送,$T_1$接收到$a$和$a\oplus b$就能够通过$a\oplus a\oplus b=b$得到$b$,同理$T_2$也能够得到$a$,这样$T_1$、$T_2$就能够同时收到$a$和$b$.这就是最初提出的网络编码理论,能够实现网络的最大流.

根据网络中的转发节点获取网络编码系数的方式,可以将网络编码分为以下两大类.

(1)集中式——线性网络编码.构造线性网络编码的关键性问题在于确定编码函数的系数.中间节点收到各个链路的信息后,将收到的信息与自身特定的编码系数矩阵进行相应的运算,这些编码系数都是已经确定并且是由中心集中分配的,当一条传输链路上的所有中间编码节点编码后的数据矩阵相互运算之后,到达目的节点如果仍然满足满秩条

件,就能够保证目的节点能够正确解码,从而获得源信息. 集中式编码方案的前提是源节点知道整个网络的拓扑,以此来给中间节点分配编码系数,且网络拓扑是静态的.

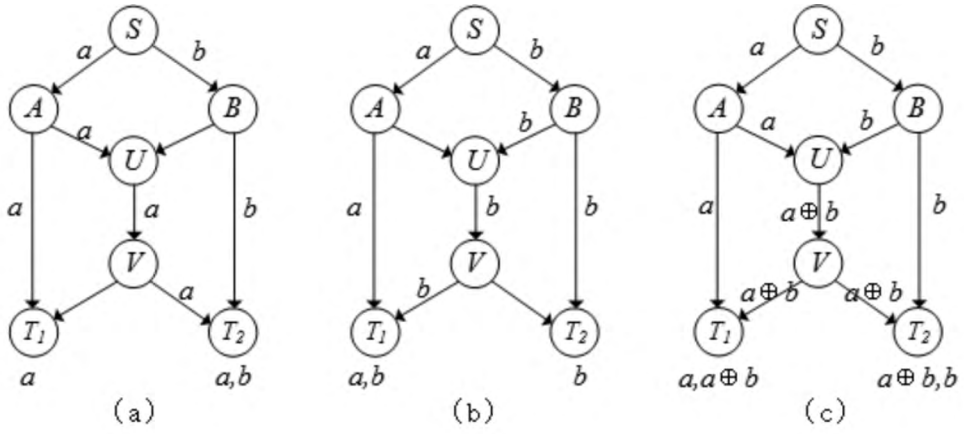


图 1　网络编码基本思想

Fig. 1　Basic idea of network coding

(2) 分布式——随机网络编码. 虽然集中式网络编码便于设计,然而在实际网络中,往往缺少控制中心的管理,而且,各种延迟也会导致网络信息传输的不同步,而分布式网络编码不需要集中式算法的前提信息,如: 网络拓扑、中间节点的编码函数和目的节点的解码函数等,也不依赖任何同步传输的假设,各个节点不需要中心分配编码系数,而是在有限域内随机选择一组元素作为编码系数,随机网络编码在一定概率上不能实现多播容量,但是在概率指数接近编码长度的时候多播链接问题被证明是可行的. 分布式网络编码适用于动态变化的网络拓扑结构,且源节点和中间节点都不需要知道整个网络的拓扑,但目的节点只能概率性的解码源信息.

### 2.2　网络编码的基本概念

根据编码数据流的来源,网络编码可以分为两种形式: 1) 流内(intra-session) 编码[18]: 编码流来自于同一个用户; 2) 流间(inter-session) 编码[19]: 编码流来自于不同的用户.

流内编码通常采用线性网络编码方式,在一个点对点的通信网络 $G=(V,E)$ 中,产生信息的源节点集记为 $V_s=\{s_1,\cdots,s_\sigma\}$,接收信息目的节点集记为 $V_t=\{t_1,\cdots,t_p\}$,其他节点称为中间节点,节点 $i$ 的输入信道和输出信道的集合分别用 $\mathrm{In}(i)$ 和 $\mathrm{Out}(i)$ 表示. 信道上传输的都是基域 $F$ 中的符号,基域 $F$ 是一个有限域,它包括构成源消息和信道上传输的所有符号. 若源节点发送的消息是由基域 $F$ 中的 $\omega$ 个符号组成,则将其表示为 $\omega$ 维行向量 $X\in F_\omega$.

**定义 1**[1]　对于有向无环网络,基域 $F$ 上的 $\omega$ 维线性网络编码由对网络中每个邻接对 $(d,e)$ ($d\in\mathrm{In}(i)$, $e\in\mathrm{Out}(i)$) 定义的标量 $k_{d,e}$ 组成,称之为局部网络编码核. $|\mathrm{In}(i)|\times|\mathrm{Out}(i)|$ 阶矩阵 $K_i=[k_{d,e}]$,其中 $d\in\mathrm{In}(i)$, $e\in\mathrm{Out}(i)$) 称之为节点 $i$ 的局部编码核.

**定义 2**[1]　对于有向无环网络,基域 $F$ 上的 $\omega$ 维线性网络编码由对网络中每个邻接对 $(d,e)$ ($d\in\mathrm{In}(i)$, $e\in\mathrm{Out}(i)$) 定义的 $k_{d,e}$ 标量和定义在每条信道上的 $\omega$ 维列向量 $f_e$ 组成,它们的关系满足下列条件:

$$\text{对 } e\in\mathrm{Out}(i),\ f_e=\sum_{d\in\mathrm{In}(i)}k_{d,e}f_d.$$

$\omega$ 条虚拟信道,$e\in\mathrm{In}(s)$ 对应的向量 $f_e$ 构成向量空间 $F^\omega$ 的标准基. 向量 $f_e$ 称为信道 $e$ 的全局编码核.

在网络编码理论中,线性网络编码理论的研究与应用最为广泛,而局部编码核和全局编码核在线性网络编码中起着至关重要的作用,是线性网络编码理论不可或缺的元素.

流间编码通常采用 XOR 编码方式,即对接收到的数据包进行异或运算,通常需要有侧信息或辅助信息辅助目的节点正确解码,如图 1 描述的例子中,$a$ 作为 $a\oplus b$ 的侧信息辅助 $T_1$ 解码出 $b$.

本文后续描述中所涉及的符号定义如表 1 所示.

表1 文中涉及符号定义一览表

Tab.1 Definition of the notations involved

| 符号 | 含义 | 符号 | 含义 |
|---|---|---|---|
| $G$ | 有向图 | $\sum_i$ | 策略空间 |
| $V$ | 节点集 | $u_i$ | 效用函数 |
| $E$ | 边集 | $F$ | 博弈模型 |
| $X$ | 源节点发送数据 | $S(S_i)$ | 源节点 |
| $x_i$ | $X$ 分成 $n$ 个子块 | $T(T_i)$ | 目的节点 |
| $N$ | 博弈参与者集合 | $y(e)$ | 全局编码向量 |
| $x_{i,j}$ | 每个子块 $x_i$ 再细分为 $m$ 个小块 | $A$ | 所有窃听边集 |
| $C$ | $C=(c_1,c_2,\cdots,c_n)$ 为编码系数 | $A_i$ | $A_i \subseteq E, A_i \in A$ 表示被窃听的边集 |

## 3 安全网络编码理论基础

### 3.1 基于密码学的安全网络编码

#### 3.1.1 对数字签名的应用

数字签名的原理示意图如图2所示,假定源S与宿T通信,S向T发送消息M,首先S计算Hash,它是消息M的函数,即Hash=H(M),H表示Hash函数. E为公钥加密函数,D为解密函数,PR为S的私钥,PU为S的公钥. S计算出M的Hash值后,用其私钥对Hash值进行加密,再将消息连同加密过的Hash值一起发送给T,T接收到消息后,首先计算消息$M'$的$Hash'$值,然后对附在$M'$后面的部分用S的公钥PU解密得出Hash,再将Hash与$Hash'$进行比较,如果一致,T能够相信消息是S发送的.

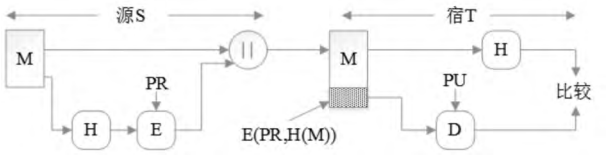


图2 数字签名原理示意图

Fig.2 Schematic diagram of digital signature

Qiming Li 在文[20]中分析了Krohn的验证技术(基于同态加密Hash函数的验证技术),指出该方法有很高的计算和通信开销,因而在某些场景中不宜被应用,并提出了一些方法对该问题进行改进,以减少计算和通信开销,并同时可以提供安全保护. 其基本的认证方案: 数据$X$被分成$n$个块$x_1,\cdots x_n$,每一个块又被分成$m$个子块: $x_{i,1},\cdots,x_{i,m}$,其中,$x_{i,j}$属于乘法群$Z_p^*$($p$为一个大素数). 哈希函数$H$用于为每一个块提供哈希值$h_1,\cdots,h_n$. 每一个哈希值需要$m$个生成器$g_1,\cdots,g_m \in Z_p^*$,第$i$个块的哈希值$h_i$是由公式$h_i=\prod_{j=1}^{m} g_j^{x_{i,j}} \bmod p$计算而来. 可以看出哈希函数$H$具有同态性,即对于任意两个块$x_i$和$x_j$来说,有$H(x_i)H(x_j)=H(x_i+x_j)$. 这些哈希值预先分配给可靠的节点. 当收到一个编码块$x$,$x$是源数据$n$个块在编码系数$C=(c_1,\cdots,c_n)$下的线性组合,每一个节点都可以利用$x$,$C$和哈希值$h_1,\cdots,h_n$以及哈希函数$H$的同态性能来验证$x$的完整性,整个过程如图3所示. 特别的,节点只需要检验是否满足等式$H(x)=\prod_{i=1}^{n} h_i^{c_i} \bmod p$. 这个方案有两个固有的局限性,第一,基于哈希函数$H$的计算开销比较大; 第二,在验证单个数据包的时候,方案中所有的参数包括所有的哈希值都要预先分配.

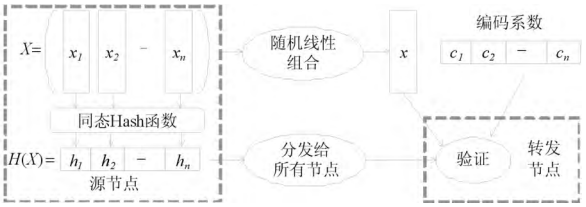


图3 同态Hash过程概要

Fig.3 Outline of homomorphic hash process

为了提高计算效率,提了基于VSH-DL(基于离散对数的VSH)的方法,VSH-DL是VSH[21](非常平滑哈希)函数的变体. VSH以及其变体的基本原理是利用小素数作为群的生成器,这样能够很大地提高哈希函数计算效率. 但是,VSH函数在动态验证过程中并不能提供同态性能. Zhen Yu 在文[22]中提出了基于公钥密码的签名方案,源用RSA私钥为每条消息产生签名,并将签名附在相应的消息后面,其他的节点包括发送者通过源的公钥对接收到的消息进行验证. 此方案是基于同态签名函数,保证任何一条消息的签名是由输入消息的签名组成的. 这样,只要每一个节点在它发出的消息上附带签名,发送者在不需要知道源节点私钥的情况下可以给它自己输出的消息产生一个有效的签名. David Mandell Freeman 在文[23]中提出了一个通用的框架能够将有特定性能的签名方案转换成线性同态签名方案. 同态签名方案的安全性遵循相同计算假设(被用来证明潜在签名方案的安全性),这个系统相比于先前的用在标准模型的

同态签名具有弱安全性.

3.1.2　对消息认证码的应用

消息认证码( MAC) 又称为密码校验和,是一种认证技术[24],原理如图 4 所示,假定源 S 与宿 T 通信, S 向 T 发送消息 M 则 S 计算消息和密钥的 hash 函数值 MAC,即 MAC = C( $K_1$,M) ,其中 C 为 MAC 函数,$K_1$ 为共享密钥,MAC 为消息认证码. E 为对称加密函数,D 为解密函数,对称密钥 $K_2$ 为双方共享. 消息连同 MAC 值一起被加密然后发送给 T,T 接收到密文后解密得出消息 $M'$ 和 $MAC'$,再通过函数 C 对消息 $M'$ 和 $K_1$ 进行运算,其结果与收到的 $MAC'$ 进行比较,如果一致,T 能够相信消息是 S 发送的. 若去掉方案中虚线框的部分( 采用对称加密,也可采用非对称加密) ,不影响认证功能,但是保密性无法保证.

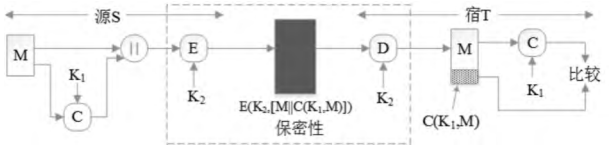


图4　消息认证与保密性

Fig. 4　Massage authentication and confidentiality

经典的 MAC 设计不能完美兼容网络编码,这是因为每个中间节点对其接收到的所有的编码包,先要验证与之对应的 MAC,所有的编码包验证通过后,再进行编码、转发,过高的计算复杂度会影响中间节点的处理速率,消耗能量,增大网络延迟,但基于通用的 Hash 函数 MAC 能完美地适用于网络编码. Anya Apavatjrut 在文[25]中介绍了三种不同的 MAC 设计方案,均可用来阻止污染攻击. 基于 Hash 函数的 MAC( HMAC) 和 MDx-MAC,其软件执行速度比 DES 这样的对称分组密码要快. 但 Hash 函数不依赖于密钥,因此不能直接用于 MAC,HMAC 方案将密钥加入到现有的 Hash 函数中,具有良好的消息认证性能,不仅不需要修改现有的 Hash 函数,还保持了 Hash 函数原有的性能,并且对密钥的使用和处理也较为简单,嵌入的 Hash 的强度,决定了认证机制抗密码分析的强度,HMAC 的基本结构可以参见文[24].

分组密码链接-消息认证码( CBC-MAC 或 CCM) 依赖于分组密码,其关键算法包括 AES 加密算法,计数器( CTR) 工作模式和基于密码的消息认证码( CMAC) ,在加密和 MAC 算法中共用一个密钥,CBC-MAC 的工作过程可以参见文[24]. 这种消息认证码能提供强安全性,适用于需要认证和加密的应用环境中.

基于 UHFs 的消息认证码具有同态性,即一次验证过程可以验证一组消息,很大程度地减小了计算开销和能量消耗,提高验证效率,适用于数据包较多,需要批量认证的环境. 但是如果一组消息中有一个消息出错,会导致这一组消息的验证失败,这时可以通过二分法重新构建分组,多次验证可找出污染消息.

文[26]中首次提出了一个基于对称密钥的方案,不仅能够过滤污染消息还能在发送节点对收到的 MACs 进行 XOR 编码,这样编码节点需要验证的 MAC 的数量不会增加. 方案利用了具有同态性的基于通用哈希函数( UHFs) 的 MAC,它能够将 MAC 融合在 XOR 网络编码系统中,方案能够减少因数据完整性保护所需的额外通信空间. 方案假设所有的节点通过概率密钥预分配算法随机分配密钥,每一个节点在全局密钥池里选固定数量的密钥,通过控制密钥池的大小和每个节点获取的密钥数量,确保任意两个节点在一定概率下能找到共享密钥,这样,每个发送者可通过与源节点的共享密钥来验证接收的消息认证码.

Zhaohui Tang 在文[27]中提出了一种多接受者同态认证编码( MRHA-code) ,源与每个验证者共享独立的密钥,并为每条消息和每个验证者附带一个标识符,如果有 $N$ 个验证者,这个方法能够阻止任何 $N$-1 个验证者之间相互勾结欺骗第 $N$ 个验证者,然而这个方法需要源节点存储大量的密钥,中间节点传输大量的标记. 此方法源自信息论环境中的验证编码,该方案提高了验证编码的性能,使其能在网络编码环境中适用,还扩展了多接受者的认证编码概念,并在此基础上加入了同态性能.

同态消息验证码能完美地兼容网络编码系统,并且减小了中间节点的计算开销,允许中间节点在不知道密钥的情况下生成一个能够被最终的目的节点认证的标签,也就是说这种方法可以使目的节点分辨并丢弃污染数据包,但是不能阻止污染包网络中的扩散,而且这种方法通常需要假设在发送节点和接收节点之间存在一种共享密钥,这在某些场景中是不适用的,如无线网络中,污染包的扩散消耗了中间节点的能量,影响合法数据的传输率.

3.1.3　基于密码学网络编码应用小结

网络编码的安全性问题已经被众多学者所关注,基于密码学的方案很多. 通常,对称密码方案比公钥密码方案具有更高的计算效率,但是具有很大的局限性,如数字签名只能利用公钥密码. 文[28]对基于公钥加密的密码学网络编码技术的实际可行性做了评价分析,基于公钥的方法可以分为两类: 1) 基于同态

Hash 的方案;2) 基于同态签名的方案. 由于消息认证码一般是基于 Hash 函数,因此这里将同态 Hash 与同态签名进行比较,前者具有更高效的计算效率,但是需要随包传输一定长度的签名信息或者是为中间节点和目的节点预分配信息. 因此当预分配是可行的时候,同态 Hash 方案更易被接收. 同态签名仅适合于对数据包进行线性组合的网络编码系统,而且需要较大的计算开销,但是不需要预分配或者附带签名信息. 表2 将相关文献中的各种属性做了定性比较.

表2 基于密码学安全网络编码相关文献对比

Tab. 2 Contrast about the literature of network coding based on cryptography

| 比较项 | 文[20] | 文[22] | 文[23] | HMAC | 文[25] CBC-MAC | UHF | 文[26] | 文[27] MRHR |
|---|---|---|---|---|---|---|---|---|
| 是否具有同态性 | 是 | 是 | 是 | 否 | 否 | 是 | 是 | 是 |
| 计算开销 | 较小 | 较小 | 较小 | 大 | 大 | 较小 | 小 | 较小 |
| 通信开销 | 小 | 小 | / | 大 | 大 | 小 | 大 | 大 |
| 是否预分配信息 | 是 | 否 | 否 | 否 | 否 | 否 | 是 | 是 |
| 加密方式 | 公钥 | 公钥 | 公钥 | 公钥 | CBC | 公钥 | 对称 | 公钥 |
| 安全性 | 抗污染攻击 | 抗污染攻击 | 弱安全 | 抗污染攻击 | 抗污染攻击 | 抗污染攻击 | 抗污染攻击 | 抗污染攻击 |

### 3.2 基于信息论的安全网络编码

网络编码的基本思想源自于信息论,可以把它看作是 Shannon 信息理论的延伸.

Marco Di Renzo 在文[29]中总结了基本的信息论结论,这些结论奠定了该领域后续研究工作的基础,文章介绍并总结了最近的分析、设计、最优结果,称之为网络纠删码,这对有损耗的网络,如无线网络中高效地利用网络编码是很有帮助的.

对于安全网络编码系统的安全性,根据信息论的安全需求可以分为两类:信息论安全[30]和弱安全[31]. 信息论安全的要求是当且仅当窃听者窃听到的消息与源消息的互信息为0,即不允许任何信息泄露. 在实际情况中,有时候安全需求不需要这么严格,弱安全要求不允许任何有意义的信息泄露,即窃听者窃听到的消息与源消息的条件互信息为0. 二者明显的区别在于,弱安全允许信息泄露,但是这些信息不能解码出有用信息,而信息论安全则不允许任何信息泄露.

众多学者基于不同的网络环境和所传输数据的安全等级需求,分别实现了安全网络编码系统中的两种安全需求. Danilo Silva 等[32]讨论了安全网络编码系统同时抵御窃听攻击和污染攻击的问题,在网络环境中,源节点给每个目的节点发送 $n$ 个数据包,敌手可以任意选取 $u$ 条链路进行窃听,并且向网络中注入 $t$ 个错误数据包,系统的目标就是实现零错误传输,即面对敌手的信息论安全,另外这个目标是在通用网络环境中实现,即独立于网络的拓扑结构和采用的网络编码方式. 在这样的要求下,每次传输的数据包个数的上界是 $n-u-2t$,给出了一种基于 *rank-metric* 编码的方案能够达到传输的最大值,并且有很低的编码解码复杂度. 此方案不仅兼容随机网络编码,而且,满足最严格的零错误零信息泄露的需求,实现完全可靠完全安全的通信.

Jin Wang 等[33]研究了在安全单播网络中应对被动攻击时,满足信息论安全需求下的最佳线性网络编码的设计问题. 提出的最佳线性网络编码的设计目标有三点:1) 满足信息论安全;2) 最大化单播流的传输率;3) 最小化添加随机符号的数量. 首次明确了在信息论安全需求下的最大安全传输率问题,并且转化其为受限的最大网络流问题. 设计出高效的二项式算法能够找出最佳传输拓扑,并在最佳传输拓扑的基础上,设计了能够满足上述三个要求的确定性线性网络编码. 文[34]中介绍了依赖于信道编码技术信息论安全方法,信道编码技术利用传播信道的固有随机性来加强数字通信系统的安全性. 文章分为两个部分,第一部分确定一个内在安全通信图(iS-graph),这个随机图用来描述在一个大规模网络中如何建立安全连接. 第二部分展示了安全的网络链接是如何随着无线传播效果、链路的保密率阈值以及合法节点与窃听节点噪声强度的变化而变化.

Cai Ning 在文[35]中提出了一种将信息安全与网络编码相结合的模型,在此模型中,网络的部分信道集合被给出,这样窃听者就能够访问该集合中的任何一条信道(仅仅只能访问一条),但是窃听者得不到被传输消息的任何信息. 通常情况下,为了保护信息在发送过程中不被泄露,发送者生成一个密钥 K 独立于源消息 M,发送者先通过安全信道将密钥 K 发送给接收者,然后通过公共信道发送 M + K,接收者作为一个合法节点在接收到 K 和 M + K 之后,就能获取源消息 M,因为 M = (M + K) - K. 要保证信息不被泄露,就要确保公共信道和安全信道的消息不能同时被非法的窃听者获取. 据此,作者为安全网络编码提出了一个模型,称之为"窃听网络",这个窃听网络由通信网络和窃听信道子集组成. 对于这样的窃听网络,

如果窃听者能够访问任何窃听信道子集,却不能获取保密消息的任何信息,而所有的合法目的节点能够零错误解码出保密消息,那么这样的网络编码方案就是安全的. 特别地,在一个窃听网络中,窃听集合的任何子集基数不大于 r,则称这样的窃听网络为 r-WN( WN 指 wiretap network) ,一个网络编码方案对于 r-WN 是安全的,称为 r-secure. 即在一个 r-secure 网络编码方案中,一个窃听者通过访问 r 条信道不能获取保密消息的任何信息. 显而易见,如果存在 r-secure 网络编码,那么 r 严格小于源节点到任何一个目的节点的最大流值,因为,如果窃听者能够访问到源节点到目的节点的最小割上的所有信道,窃听者将能够获取保密消息.

信息论的安全需求主要针对窃听攻击,根据传输数据的安全等级需要,设计不同级别的安全方案,以达到弱安全或信息论安全.

### 3.3　基于博弈论的安全网络编码

网络编码能够获得高可靠性,高吞吐率等高性能的一个重要前提条件是假设所有的用户都是合作的,然而,在很多实际应用中,用户很可能为将自己的利益最大化,而拒绝参与合作传输,例如: 部分节点为了使其所在的单播流的数据传输率最高,或者节点为保证自身足够的生存时间,而选择性地发送数据包等等,这些都可能会影响整个网络的性能,为解决这些问题,博弈论被引进到安全网络编码方案中. 博弈的基本要素包括三种元素: 参与人集合 $N = [1,2,\cdots,I]$,每个参与者 $i$ 的纯策略空间 $\sum_i$ 以及每个参与人的收益函数 $u_i$,博弈基本模型为 $F = (N,(\sigma_i),\{u_i\})$. 参与者 $i$ 指做决策的个体,其目标是通过选择合适的策略来最大化自己的收益; 参与人的策略 $s_i \in \sum_i$,表明参与人选择的行动,混合策略 $\sigma_i$ 是纯策略上的一种概率分布; 收益 $u_i$ 指的是在所有的参与人都选择了各自的策略且博弈已经完成之后,参与人 $i$ 获得的收益.

在单播应用中,用户在本质上并没有兴趣将自己的消息提供给与自己配对节点之外的其它节点,或者是替其它节点转发消息,这样的自私行为势必会影响到网络吞吐量. Jennifer Price [36] 提出一个网络编码博弈方案来检查自私用户的网络编码策略对网络效率的影响,其中,自私节点作为博弈参与者,其策略集合是节点的编解码方案( 包括编码函数,块大小,比例等等) ,通过分析表明,该方案能够确保用户积极地参与到期望的合作通信中,即使用户可以完全自主地选择编码方式.

在文 [37] 中,Jennifer 以经典的蝴蝶网络及其拓展的网络模型为例,提出一种基于博弈的网络编码方案,不仅能够实现网络容量,还能确保均衡的出现. 广义的蝶形网络如图 5 所示,是一个度为 2 的三层网络,有两个单播流,链路$(S_1,D_1)$ 和$(S_2,D_2)$ 受限于提供侧信息( 冗余信息) ,这些信息仅用来辅助 $S_2$ 到 $T_2$ 和 $S_1$ 到 $T_1$ 的信息进行解码. 由此可知链路$(S_1,D_1)$ 和$(S_2,D_2)$ 不会参与到编码或者直接发送的选择之中. 拓展的蝶形网络如图 6 所示,存在$(S_1,T_1)$ 和$(S_2,T_2)$ 链路,能传输 $S_1$ 到 $T_1$ 的数据,$S_2$ 到 $T_2$ 的数据,还能够传输侧信息,在这种情况下,$S_i$ 是发送新信息还是侧信息是由整个网络的网络方案决定的,而 $S_i$ 以标记数据包的方式决定发送到节点 $A$ 的数据包是通过编码还是路由的方式继续往下传播,同样,发送到 $D_i$ 的数据是发送到 $T_i$ 还是 $T_{-i}$,或者同时发送到两个接收者,$S_i$ 选择的标记即构成编码册.

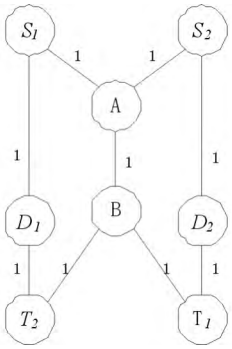


图 5　广义的蝶形网络

Fig. 5　Generalized butterfly network

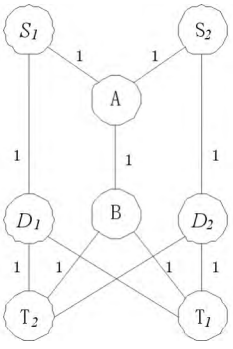


图 6　拓展的蝶形网络

Fig. 6　Extended butterfly network

在拓展的蝶形网络中,约定一个简单的编码方案,它有如下性能: 1) 网络编码只在 $A$ 节点执行,网络中的其他节点只是转发信息; 2) $A$ 节点将来自 $S_1$ 和 $S_2$ 的信息分成两个部分: 需要编码的部分和需要路由的部分; 3) 被指派为编码的信息在 $A$ 节点进行简单的异或( XOR) 运算,被指派为路由部分的信息

按照传统的路由方式进行发送. 假设网络的编码方案是固定的,而且为所有博弈者所知.

对两种编码方案进行比较: 1) A 节点对所有接收到的消息进行网络编码; 2) A 节点对保证目的节点能够解码的最少信息进行编码,其他信息以路由的形式发送. 在这个博弈方案中,源节点合理地选择传输策略,中间节点的编码方案能够使编码和路由相结合. 中间节点的网络编码方案的选择不仅仅决定了整个网络的吞吐量,还能影响理性和自私用户的行为.

Jason R. Marden 在文[38]中提出了以单播会话作为自私的决策者(决策者可以是单播会话中的源节点或者是编码节点)的非合作博弈方案. 在共享网络资源的条件下,多重单播在相互独立的信息流中会建立竞争关系,完全分布式网络将整个网络环境中的节点或者会话看作是独立的博弈者,针对网络资源的利用进行博弈. 这样做的好处是分布式算法将中央优化问题分解,博弈者独立解决分解的小问题从而减小原来中央控制节点的计算和协调开销; 缺点是这样做可能导致次优方案的发生,每个博弈者在未知整个问题的完整信息的情况下,独立的选择每一个子问题的最优的方案可能导致整个问题的次优性能.

Angelos Antonopoulos 在文[39]中介绍了在数据分发场景中提出博弈论的介质访问控制策略. 在 Ad hoc 网络中,数据分发是非常困难和复杂的,因为在这样的网络中缺乏基础设施,并且,无线链路也缺乏稳定性. 然而,网络编码的出现,能够为通信提供鲁棒性和多样性,提高服务质量. 数据分发的目标是在网络链路和节点中共享大量的数据包,节点的目标有两个: 1) 在合理的时间内完成数据分发; 2) 最大化自身的生存时间. 因此在数据分发的过程中,源节点需要在传输数据和节约能源之间做出权衡. 这篇文章为数据分发提出了能源效率博弈论介质访问策略,作者用"分发访问博弈"(DAG)来定义网络节点在节约能量和促进数据分发之间的一种均衡状态. 作者的方案能够满足以下两个要求: 1) 在不影响服务质量的前提下,利用基于能量博弈论技术提高系统的能量效率; 2) 提出了一种通用的访问方案,能够应用于各种无线标准中.

Mohsenian-Rad A-H 在文[40]中提出了流间(inter-session)网络编码的重复博弈,即动态博弈. 作者提出,在一个网络环境中,若用户有大量数据包需要传输,在用户不间断地传送很多数据包的时候,就可以将博弈的历史记录(记录在之前的博弈中,其他用户是否参与合作,提供目的节点解码需要的包)考虑进来,根据历史博弈记录来计划将来的行动. 可是重复编码博弈并不能简单地促使用户之间的合作,其关键挑战在于用户之间的合作不能明确定义. 作者引入了议价问题,即在数据传输之前,各用户之间找到一个相互接收的网络编码速率. 重复博弈进行的时候,用户可以根据上一阶段其他用户的选择来做确定自己这一阶段的动作. 通过这样的激励机制,就可以促使整个博弈达到完美均衡状态.

表3对博弈论在网络编码系统中的应用做了一个概括性的总结,从表格中可以发现,博弈论的应用主要针对用户节点的自私行为,并且多用静态博弈形式,博弈论在安全网络编码中的应用还有很大的发展空间.

表3 博弈论应用相关文献的比较

Tab. 3 Contrast about the literature of network coding application based on game theory

| 比较项 | 文[36] | 文[37] | 文[38] | 文[39] DAG | 文[40] |
|---|---|---|---|---|---|
| 网络环境 | 单播应用 | 单播应用 | 多重单播 | 数据分发 | 流间编码 |
| 博弈冲突 | 节点自私行为 | 节点自私行为 | 竞争网络资源 | 节点自私行为 | 节点自私行为 |
| 博弈者 | 自私节点 | 源节点 | 单播会话(源节点或编码节点) | 自私节点 | 源节点 |
| 策略集 | 节点的编解码方案 | 编码节点收到数据包的动作(编码或直接发送) | 单播会话选择路径 | 是否分发数据包 | 确定编码包和非编码包的比例 |
| 博弈目的 | 促进合作,实现整体利益 | 实现整个网络的吐吞率的提高 | 抑制恶性竞争,合理分配网络资源 | 实现节约能量和数据分发之间的均衡 | 利用历史博弈记录控制节点将来行为,实现完美均衡 |
| 博弈形式 | 静态 | 静态 | 静态 | 静态 | 动态(重复博弈) |

# 4　安全网络编码技术的研究与应用

## 4.1　安全网络编码技术的研究

### 4.1.1　基于层次( 物理层,网络层,应用层) 的编码技术

Zhenzhen Gao 和 Yu-Han Yang 在文 [41] 中提出了一个基于物理层编码( PNC) 方案可以抵御窃听攻击. 在这个方案中, "训练符号"第一次由目的节点传输,由于链路通道的互惠共享,每一个用户节点能够获得一个它自身到目的节点 D 的链路状态信息,这个是窃听者无法获得的. 利用链路状态信息为每个节点设计反窃听编码,目的节点能够成功解码源信息,但是窃听者的解码有很高的错误率. 文 [42] 中同样是基于物理层的模拟网络编码( ANC) ,根据网络编码的固有特性设计了一个双非毗邻监测点方案探测恶意的拜占庭攻击. 由于 ANC 不需要假设任何标识符号,载波相位和载波频率同步,所以这个方案的实施具有实际可行性. 文 [43] 提出了一个新的物理层线性网络编码方案,应用于空间复用多进多出双向传播信道( spatial-multiplexing MIMO two-way relay channels) ,在这种环境中,发送者并不需要知道链路状态信息( CSI) . 文 [44] 对 PNC 进行介绍,讨论了近期关于无线通信、无线信息论、无线网络三个领域中的关键性成果,调查了 PNC 中的一个关键问题: 同步问题,最后对 PNC 的应用也进行了拓展,PNC 不仅适用于无线网络,还适用于光纤网络. 文 [45] 通过分析网络编码的优点和发展分析了一种新颖的无线视频中的安全网络编码框架,并展示了在网络编码层的操作实现三个目标: 1) 满足规定的安全保障的同时减少加密操作的次数; 2) 将轻量级的安全方案与无线视频中的分层编码和流协议相结合; 3) 可扩展的视频流域网络编码相匹配. 方案的成果在于: 1) 对延迟比较敏感的应用设计了安全机制,能够在获得鲁棒性的同时在可控复杂度的情况下不损失安全性; 2) 对可扩展视频进行分层编码; 3) 对方案性能以及开销做了分析.

文 [46] 提出了一个新的安全网络编码模型 2-LSNC,该模型提高了窃听者要想获得秘密信息所需要占用的链路数量,并分析了资源开销和安全级别的折中点. 两层安全网络编码建立了一个称为"安全防护水平"的度量标准,并且文中提出的模型符合该标准. 作者指出,当网络规模和链路数量达到一个临界点时,该模型比 Cai 和 Yeung 提出的模型消耗更少. 文 [47] 研究了线性网络编码系统对抗既是窃听者又是干扰者的敌手安全问题. 系统的目标是在有攻击者出现时可以达到"零错误"通信,即信息论安全. 并且该系统是通用的,无论任何网络拓扑或任何底层编码都可以适用.

### 4.1.2　基于网络流的编码技术: 流内编码,流间编码

文 [48] 根据如何利用网络编码的优势,将系统分为两种编码系统: 流内编码和流间编码系统,并且系统地分析了这两类框架的组件,确定了那些能够严重降低系统性能的潜在安全漏洞. 首次分析了基于网络编码的实际无线系统中所有组件的安全性. 文 [49] 针对无线 mesh 网络流内编码系统,提出了一个轻量级的方案——DART ( Delayed Authentication with Random Transformation) ,利用了基于时间认证随机线性变换组合的方法来防御污染攻击. 作者在 DART 基础上确定了最佳发送策略提高系统性能,并且提出了高效的攻击者身份认证方案,能够迅速隔离攻击节点,选择合适传输路径. 文 [50] 也提出了一种基于线性代数的零空间方法对抗流内网络编码系统污染攻击的方案. 文 [40] 介绍了一种流间网络编码动态博弈,作者提出的激励策略能够刺激用户参与到流间网络编码中. 对于 2-flow downlink 场景,文 [51] 首次优化了流间网络编码( inter-session NC) 方案,它对于时间变化信道( time-varying channel) ,是可证最优的. 这个方案是一个新的线性 INC 操作,不用传统的 XORing. 作者提出了一个 queue-length-based 方案,能够协助新的 INC 操作,并且能够很好地使用时间变化信道.

### 4.1.3　基于单播,多播的网络编码技术

文 [38] 中提出了一个框架结构,允许每个单播会话在响应局部信息时,能够独立适应它的路由决策. 方案将一个单播会话作为一个自私的决策者,在一个非合作的博弈论中,这种方法需要设计本地开销函数和单播会话的决策规则,这样就可以在一个共享的网络环境中获得一个令人满意的系统性能,对比分布式算法性能,本方案可以通过集中控制器来实现最佳性能. 文 [37] 通过博弈论的方法处理了这些在单播网络中的协调合作问题. 在源与目的节点之间实现给定的网络编码方案,会引发网络编码博弈. 在一个自治合理的单播流网络中,网络编码方案的性能与网络编码博弈性能是相关的.

文 [52] 解决了在相同的源和目的节点之间安全的单播和多流线性网络编码的建模与优化设计问

题,这个设计将拓扑结构的形成和安全线性网络编码整合在一起. 设计的目的在于: 1) 在安全的单播多流场景中为线性网络编码的设计制定了一个安全的单播路由协议; 2) 线性网络编码的设计能实现最大的安全传输率; 3) 提供了一个有效的近似算法能够获得接近最优的拓扑来将有限域最小化. 文[53]设计了一个安全的线性网络编码来对抗窃听攻击,并在满足弱安全需求的前提下,使得源和目的结点之间的多重单播数据流传送速率最大. 作者证明了该问题是NP问题,并给出了一个有效的启发式算法. 文章首先试图找到一个满足网络编码的转发拓扑,然后在该拓扑结构的基础上,设计弱安全的线性网络编码机制. 文[54]设计了一种线性网络编码,在满足弱安全的同时,使得相同源和目的结点之间的多重单播流转发数据率最大. 作者首先证明了安全单播路由问题等价于受限的不相交路径问题,继而提出了一个高效的算法能够在一个多项式时间内找到最佳单播拓扑,基于此拓扑设计确定性线性网络编码方案. 文[33]同样先以高效的算法找到最佳传输拓扑,在此拓扑的基础上设计最优线性网络编码,满足单播流的传输速率最大化,添加的随机符号数量最小化.

文[55]设计了一个无条件安全的认证码用于多播网络编码,由一个可信的权威来计算和分发关键数据给目的节点和中间节点,这个方法允许目的节点和中间节点验证消息的完整性,探测并丢弃正在传播的恶意信息,这样在到达目的节点前,污染被终止. 文[56]研究了如何以最小的投资来隐藏传播给多接收者的数据流,与传统的加解密方法比较,此方法的优点在于1. 比加解密有更低的CPU使用率; 2. 在被窃听时除了可以混淆有效负载信息,还能隐藏编码信息; 文[57]展示了一种通过利用多个统计独立的消息对窃听者保持保密的方法来消除信息丢失率. 对时延敏感的数据在无线多播中的传输时,不同的接收者可能会丢失不同的数据包,这是一个挑战. 基于网络编码的多播容易受到错误包注入攻击即污染攻击,而现有的解决方案要么有很高的计算开销,要么具有很高的数据包丢失率. 文[58]针对时延敏感数据的网络编码多播,提出了一种基于编码包的零空间性能的高效认证机制,使接收者能够以很高的概率探测出伪造的数据包,并且设计了一个基于Markov决策过程的自适应调度算法,能够在给定时间限制范围内,最大化可以接收的已被认证的数据包数量.

安全网络编码技术迅速发展,针对不同的应用环境,从不同的技术角度,应对不同的攻击形式,表4对相关文献方案特性进行了对比.

表4 安全网络编码方案技术对照表

Tab. 4 Comparison of the technologies of related network coding schemes

| 文献 | 应用环境 | 编码层次 | 编码形式 | 抗攻击类型 | 安全需求 | 特性 |
|---|---|---|---|---|---|---|
| [36] [37] | 单播博弈 | / | / | / | / | 防止节点自私行为影响整个网络系统性能 |
| [40] | 博弈 | / | 流间 | / | / | 刺激用户节点参与到流间编码方案 |
| [42] | / | 物理层 | / | 拜占庭攻击 | / | 双非毗邻看门狗方案 |
| [49] | / | / | 流内 | 污染攻击 | / | 基于时间的认证随机线性变换组合的方法 |
| [50] | / | / | 流内 | 污染攻击 | / | 基于线性代数的零空间方法 |
| [53] | 多重单播 | / | / | 窃听攻击 | 弱安全 | 设计弱安全网络编码机制; 数据传输率最大 |
| [41] | / | 物理层 | / | 窃听攻击 | / | 利用链路状态信息设计编码 |
| [44] | / | 物理层 | / | / | / | 研究了同步问题,拓展PNC应用 |
| [45] | 无线视频传输 | 网络层 | / | / | 轻量级安全 | 减少加密次数 |
| [47] | / | 底层 | / | 窃听攻击,污染攻击 | 信息论安全 | 方案具有通用性,不限制网络拓扑 |
| [52] | 单播多流 | / | / | / | 弱安全 | 寻找拓扑设计LNC方案; 实现最大传输率 |
| [54] | 多重单播 | / | / | 窃听攻击 | 弱安全 | 多重单播转发速率最大 |
| [55] | 多播网络 | / | / | 污染攻击 | / | 需要可信的权威计算并分发预信息 |
| [56] | 多接收者 | / | / | 窃听攻击 | / | 计算开销低,信息隐藏防窃听 |
| [57] | 无线多播 | / | / | 窃听攻击,污染攻击 | / | 消除信息丢失率 |
| [58] | 时延敏感多播网络 | / | / | 污染攻击 | / | 基于编码包的零空间性能的高效认证机制探测污染包,提出基于Markov决策过程的自适应调度算法 |

### 4.2　安全网络编码应用

网络编码技术使得网络各方面的性能得到很大的提升,因此网络编码技术应用在各个领域: 数据存储、数据共享、多媒体数据传输等等.

文 [59] 在分布式数据存储中运用网络编码技术,利用同态指纹识别进行完整性检查,并能够保证网络编码的代数结构,允许检验者快速定位损坏的数据块. 文 [60] 利用网络编码的优势来进行完整性检查,并对基于网络编码的云存储提出了一个网络编码审计——远程数据完整性检查方案. 此方案是基于对称密钥的协议,对基于网络编码的分布式云存储系统进行存储数据的完整性检查. 文 [61] 为多云存储(NNCloud)提出了一个基于代理人的系统,目的是在一个云存储永久失败时能够比较划算地进行修复. 文 [62] 阐述了关于在分布式存储系统中利用网络编码减少修复开销的问题,并提出了三类修复问题: 1) 精确修复(丢失的信息可以精确再生); 2) 功能修复(修复前后,只保持相同的 MDS 编码的性能); 3) 精确修复系统部分(系统部分能够精确重建,非系统部分按照功能模型修复).

表 5　安全网络编码的应用

Tab. 5　Application of network coding theory

| 应用方向 | 主要性能和用途 | 相关文献 |
|---|---|---|
| 数据存储 | 主要包括分布式存储和云存储的应用,主要利用网络编码技术进行数据完整性检查以及数据的保护,减少修复开销等. | [59] [60] [61] [62] |
| 数据共享 | 无线网络数据共享系统中,用户向基站上传数据通常是基于加密的 SIM 卡传输,而下载的安全性可利用网络编码方案,在保证良好的安全性的前提下,提高网络的吞吐量. | [63] |
| 多媒体数据传输 | 无线网络带宽不能很好地满足多媒体数据的传输,容易出现严重的丢包情况,网络编码技术能够减少加解密次数,降低延迟,一定程度上避免因为丢包导致的问题. | [64] [65] |

文 [63] 提出了一个在无线网络中,通过协调器分层传输来进行数据共享的系统,主要集中于会议组间的安全数据连接,分层传输能够提高网络的吞吐量,分层调制也可以用来提高网络吞吐量. 在安全单播、安全广播和网络编码三种方案中进行比较,数据共享系统方案中使用协调器分层传输时网络编码方案是最有效的.

目前,在无线网络中的多媒体应用持续增长,但是无线网络的带宽却不能很好的满足该需求,因为无线网络中通常会遇到受限的带宽、不可靠的通道、多变的拓扑、多样异构的节点类型、分散的环境以及高丢包率等,为保证低延迟低丢包率的多媒体传输环境,引进了安全网络编码技术. 文 [64] 对已经存在的无线网络中多媒体传输的网络编码技术进行了总结. 文 [65] 通过分析网络编码的优点和发展分析了一种新颖的在无线视频中的安全网络编码框架,并展示了在网络编码层的操作实现三个目标: 1) 满足规定的安全保障的同时减少加密操作的次数; 2) 将轻量级的安全方案与无线视频中的分层编码和流协议相结合; 3) 可扩展的视频流域网络编码相匹配. 方案的成果在于: 1) 对延迟比较敏感的应用设计了安全机制,能够在获得鲁棒性的同时,在可控复杂度的情况下不损失安全性; 2) 对可扩展视频进行分层编码; 3) 对方案性能以及开销做了分析.

## 5　开放性问题

网络编码理论及应用还存在如下开放性问题.

(1) 同态签名等密码学方案需要较大的计算通信开销. 无线设备、终端已经成为人们生活中不可或缺的重要元素,无线信息传输的安全性不容忽视,同样无线设备、终端的能量需求必须考虑,密码学方案固然能够在安全信息传输中起到很好的作用,但是对于无线设备来说,其计算开销和能量开销亟待优化.

(2) 应对的攻击形式较为单一,比如针对污染攻击提出的同态签名,不一定能抵抗随机伪造攻击等安全威胁等. 防御技术不断发展,黑客的攻击技术也是多种多样,在信息化的今天,一个安全的信息系统应该能够抵御多种形式的攻击.

(3) 需要额外的安全信道或者方案针对的网络拓扑较为特殊,缺乏一般性. 安全信道通常用来传输密钥或者希望不被攻击者获取的信息,通过安全信道的传输的信息量较小. 另外有些方案针对的网络拓扑较为特殊,比如方格网络等. 因此我们需要设计更具一般性的方案,能够适用于任何网络或者对于绝大部分网络拓扑.

(4) 方案多是基于物理层的方案,上层或者跨层编码方案的研究可以作为研究的关注点之一. 虽然跨层思想在无线网络的优化设计领域中已经有 20 多年的历史,但是将其运用到网络编码系统的设计方案还

很少,在将来的研究中,可以结合跨层思想来设计安全网络编码系统.

(5) 许多网络编码方案局限于XOR编码,对于其他编码方式可能不适用.目前有很多方案仅适用于XOR编码或者是确定性的线性网络编码,虽然在应对特殊安全问题的时候,我们可以采用特殊编码方法,但是更希望方法具有一般性,能够解决一类安全问题.

## 参 考 文 献


[1] Raymond W. Yeung. 信息论与网络编码 [M]. 蔡 宁,译. 北京: 高等教育出版社,2011:422.

[2] Rudolf Ahlswede, NingCai, Shuo-Yen Robert Li. Network information flow [J]. IEEE Transactions on Information Theory, 2000,46:1204-1216.

[3] Tracey Ho, Muriel Medard. On Randomized Network Coding [J]. Proceedings of the Annual Allerton Conference on Communication Control and Computing. 2003,41(1):11-20.

[4] Koetter Ralf, Muriel Médard. An algebraic approach to network coding [J]. IEEE/ACM Transactions on Networking, 2003(11):782-795.

[5] Jia-Qi Jin, Tracey Ho, Harish Viswanathan. Comparison of Network Coding and Non-Network Coding Schemes for Multi-hop Wireless Networks [C]// IEEE. 2006 International Symposium on Information Theory. Seattle, USA: IEEE, 2006:197-201.

[6] Desmond S. Lun, NiranjanRatnakart, Ralf Koett. Achieving Minimum-Cost Multicast: A Decentralized Approach Based on Network Coding [C]// IEEE. Proceedings of INFOCOM. Miami, USA: IEEE, 2005:1608-1617.

[7] Feng Xue, Sumeet Sandhu. PHY-layer network coding for broadcast channel with side information [C]//IEEE. Information Theory Workshop. Tahoe City, USA: IEEE, 2007:108-113.

[8] Christos Gkantsidis, PabIo Rodriguez. Network Coding for Large Scale Content Distribution [C]//IEEE. Proceedings of INFOCOM. Miami, USA: IEEE, 2005:2235-2245.

[9] Tracey Ho, Muriel Médard, Ralf Koetter. An Information-Theoretic View of Network Management [J]. IEEE Transactions on Information Theory, 2005(51):1295-1312.

[10] Randall Dougherty, Christopher Freiling, and Kenneth Zeger. Insuffciency of Linear Coding in Network Information Flow [J]. IEEE Transactions on Information Theory, 2005(51):2745-2759.

[11] Jianping He, Jiahai Yang, Changqing An. A Study of Collisions in Wireless Network Coding System [C]// IEEE. 1st IFIP. Dubai, United Arab Emirates: IEEE, 2008:1-5.

[12] Huo Qiang, Song Lingyang, Li Yonghui, Jiao Bingli. Novel multihop transmission schemes using selective network coding and differential modulation for two-way relay networks. [C]//IEEE. International Conference on Communications (ICC). Budapest, Hungary: IEEE, 2013:5924-5928.

[13] Xianlong Jiao, Xiaodong Wang, Xingming Zhou. Active Network Coding based High-Throughput Optimizing Routing for Wireless Ad Hoc Networks [C]//IEEE. Wireless Communications. Dalian, China: IEEE, 2008:1-5.

[14] Jing Chen, Ruiying Du, Qian Wang, Shixiong Yao. Secure Routing Based on Network Coding in Wireless Sensor Networks [C]// IEEE. Proceeding of the 12th International Conference on Trust, Security and Privacy in Computing and Communications. Melbourne, Australia: IEEE, 2013:58-64.

[15] Wang gang, Dai xia,Liyonghui. Network Sharing of Multi-Protocol Data Flows in Congestion Networks [J]. IEEE Transactions onVehicular Technology. 2013(11):1-9.

[16] Zhao Mingfeng, Zhou Yajian,RenDongxiao, Yang Yixian. A minimum power consumption scheme for two-way relay with physical-layer network coding [C]// IEEE. 2010 2nd International Conference on Network Infrastructure and Digital Content. Beijing, China: IEEE, 2010:704-708.

[17] Wang Wei, Yu Li, Zhu Guangxi, Dai Rui. A Novel Approach in Network Coding Based on Shuffle Coding [C]//IEEE. Proceedings of 2007 International Symposium on Intelligent Signal Processing and Communication Systems. Xiamen, China: IEEE, 2007:8-11.

[18] Szymon Chachulski, Michael Jennings, Sachin Katti. Trading Structure for Randomness in Wireless Opportunistic Routing [C]//ACM. Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications. Kyoto, Japan: ACM, 2007:169-180.

[19] S. Katti, H. Rahul, W. Hu and D. Katabi. Xors in the air: practical wireless network coding [C]//ACM. Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications. Pisa, Italy: ACM, 2006:243-254.

[20] Qiming Li, John C. S. Lui, Dah-Ming Chiu. On the Security and Efficiency of Content Distribution Via Network Coding [J]. IEEE Transactions onDependable and Secure Computing, 2012(9):211-221.

[21] Scott Contini, Arjen K. Lenstra, and Ron Steinfeld. VSH, an Efficient and Provable Collision-Resistant Hash Function [J]. Advances in Cryptology-EUROCRYPT,2006: 165-182

[22] Yu Zhen, Wei Yawen, Ramkumar. An efficient signature-based scheme for securing network coding against pollution attacks [C]//IEEE. The 27th Conference on Computer Communications. Phoenix, USA: IEEE, 2008: 1409-1417.

[23] David Mandell Freeman. Improved Security for Linearly Homomorphic Signatures: A Generic Framework [J]. International Association for Cryptologic Research, 2002: 697-714

[24] William Stallings. **密码编码学与网络安全——原理与实践** [M] 5 版. **王张宜, 杨 敏, 杜瑞颖,等译. 北京: 电子工业出版社,** 2012.

[25] Anya Apavatjrut, Wassim Znaidi, Antoine Fraboulet. Energy efficient authentication strategies for network coding [J]. Concurrency and Computation: Practice and Experience, 2012, 24(10): 1086-1107.

[26] Kazuya Izawa, Atsuko Miyaji, KazumasaOmote. Lightweight integrity for XOR network coding in wireless sensor networks [C]//ISPEC. International Conference on Information Security Practice and Experience. Hangzhou, China: Springer, 2012: 245-258.

[27] Zhaohui Tang, Hoon Wei Lim. Multi-receiver Homomorphic Authentication Codes for Network Coding [J]. IACR Cryptology ePrint Archive, 2012(2012): 447-470.

[28] Seung-Hoon Lee, Mario Gerla, Hugo Krawczyk. Performance Evaluation of Secure Network Coding using Homomorphic Signature [C]//IEEE. 2011 International Symposium on Network Coding. Beijing, China: IEEE, 2011: 1-6.

[29] Di Renzo Marco, IezziMichela, Graziosi Fabio. Beyond routing via network coding: An overview of fundamental information-theoretic results [C]// IEEE. 2010 21st International Symposium on Personal Indoor and Mobile Radio Communications. Istanbul, Turkey: IEEE, 2010: 2745-2750.

[30] CaiNing, Yeung Raymond W. Secure network coding [C]// IEEE. 2002 International Symposium on Information Theory. Lausanne, Switzerland: IEEE, 2002: 323.

[31] Bhattad, Kapil, Narayanan. Weakly secure network coding [J]. NetCod, 2005(104): 1-6.

[32] Danilo Silva, Frank R. Kschischang. Universal Secure Error-Correcting Schemes for Network Coding [C]// IEEE. 2010 International Symposium on Information Theory Proceedings. Austin, USA: IEEE, 2010: 2428-2432.

[33] Jin Wang, Jianping Wang, Kejie Lu. Optimal design of linear network coding for information theoretically secure unicast [C]//IEEE. International Conference on Computer Communications. Shanghai, China: IEEE, 2011: 757-765.

[34] Pedro C. Pinto, Joao Barros, Moe Z. Win. Secure Communication in Stochastic Wireless Networks—Part I: Connectivity [J]. IEEE Transactions on Information Forensics and Security, 2012(7): 125-138.

[35] Cai, Ning, Yeung Raymond W. Secure network coding on a wiretap network [J]. Information Theory, 2011(57): 424-435.

[36] Price Jennifer, Javidi Tara. A game-theoretic approach to coding for information networks [C]//IEEE. 46th Annual Allerton Conference on Communication, Control, and Computing. Urbana-Champaign, USA: IEEE, 2008: 1397-1402.

[37] Price Jennifer, Javidi Tara. Network coding games with unicast flows [J]. Selected Areas in Communications, 2008(26): 1302-1316.

[38] Marden Jason R, Effros Michelle. A game theoretic approach to network coding [C]//IEEE. Information Theory Workshop on Networking and Information Theory. Volos, Greece: IEEE, 2009: 147-151.

[39] Antonopoulos Angelos, Verikoukis Christos. Game theoretic network coding-aided MAC for data dissemination towards energy efficiency [C]// IEEE. 2012 International Conference on Communications (ICC). Ottawa, Canada: IEEE, 2012: 5630-5634.

[40] Mohsenian-Rad A-H, Huang Jianwei, Wong Vincent W. S. Bargaining and price-of-anarchy in repeated inter-session network coding games [C]//IEEE. 2010 Proceedings on INFOCOM. San Diego, USA: IEEE, 2010: 1-9.

[41] Gao Zhenzhen, Yang Yu-Han, Liu KJRay. Anti-eavesdropping space-time network coding for cooperative communications [J]. Wireless Communications, 2011(10/11): 3898-3908.

[42] VaibhavPandit, Jung Hyun Jun, Dharma P. Agrawal. Inherent Security Benefits of Analog Network Coding for the Detection of Byzantine Attacks in Multi-Hop Wireless Networks. [C]// IEEE. 2011 8th International Conference on Mobile Adhoc and Sensor Systems. Valencia, Spain: IEEE, 2011: 697-702.

[43] Guo, Jiajia and Yang, Tao and Yuan, Jinhong and Zhang, Jian A. Design of linear Physical-layer network coding for MIMO Two-way relay channels without transmistter CSI [C]// IEEE. 2015 Wireless Communications and Networking Conference (WCNC). New Orleans, USA:

IEEE, 2015:1-6.

[44] Liew Soung Chang, Zhang Shengli, Lu Lu. Physical-layer network coding: Tutorial, survey, and beyond [J]. Physical Communication, 2013(6):4-42.

[45] Lu'isa Lima, Steluta Gheorghiu, Jo ~ao Barros. Secure Network Coding for Multi-Resolution Wireless Video Streaming. Selected Areas in Communications [J]. IEEE Journal on, 2010,28(3):377-388.

[46] Mehdi M. Hassanzadeh, Mohammad Ravanbakhsh, and Oyvind Ytrehus. Two Layer Secure Network Coding [C]// IEEE. International Symposium on Telecommunications. Tehran, Iran: IEEE, 2008:7-12.

[47] Chung Chan . Universal Secure Network Coding by Non-linear Secret Key Agreement [C]// IEEE. Proceedings of the 2012 International Symposium on Network Coding. Cambridge, USA: IEEE,2012:97-102.

[48] Jing Dong, Reza Curtmola, Ruben Sethi. Toward Secure Network Coding in Wireless Networks: Threats and Challenges [C]//IEEE. 4th Workshop on Secure Network Protocols. Orlando, USA: IEEE,2008:33-38.

[49] Jing Dong, Reza Curtmola, Cristina Nita-Rotaru. Practical Defenses Against Pollution Attacks in Wireless Network Coding [J]. ACM Transactions on Information and System Security, 2011,14(1):7.

[50] Andrew Newell, Cristina Nita-Rotaru. Split Null Keys: A Null Space Based Defense for Pollution Attacks in Wireless Network Coding [C]// IEEE. 9th Annual Communications Society Conference on Sensor, Mesh and AdHoc Communications and Networks. Seoul, South Korea: IEEE, 2012:479-487.

[51] Wei-Cheng Kuo, Chih-Chun Wang. Robust and optimal opportunistic scheduling for downlink 2-flow inter-session network coding with varying channel quality [C]// IEEE. Proceedings on INFOCOM. Toronto, Canada: IEEE,2014: 655-663.

[52] Jin Wang, Jianping Wang, Kejie Lu. Modeling and Optimal Design of Linear Network Coding for Secure Unicast with Multiple Streams [J]. IEEE Transactions on Parallel and Distributed Systems, 2013,24(10):2025-2035.

[53] Xiangmao Chang, Jin Wang, Jianping Wang. On Achieving Maximum Secure Throughput Using Network Coding Against Wiretap Attack [C]//IEEE. Distributed Computing Systems (ICDCS). Genova, Italy: IEEE, 2010:526-535.

[54] Jin Wang, Jianping Wang, Kejie Lu. Optimal Linear Network Coding Design for Secure Unicast with Multiple Streams [C]// IEEE. 2010 Proceedings on INFOCOM. San Diego, USA: IEEE, 2010:1-9.

[55] FrédériqueOggier, HananeFathi. An authentication code against pollution attacks in network coding [J]. IEEE/ACM Transactions on Networking, 2011, 19(6): 1587-1596.

[56] A. Hessler, T. Kakumaru, H. Perrey. Data obfuscation with network coding [J]. Computer Communications, 2012, 35(1):48-61.

[57] Matsumoto Ryutaroh, Hayashi Masahito. Secure multiplex network coding [C]//IEEE. 2011 International Symposium on Network Coding (NetCod). Beijing, China: IEEE, 2011:1-6.

[58] Tuan T. Tran1, Hongxiang Li, Lingjia Liu. Secure Network-Coded Wireless Multicast for Delay-Sensitive Data [C]// IEEE. 2012 International Conference on Communications (ICC). Ottawa, Canada, IEEE, 2012: 1943-1947.

[59] Rongfei Zeng, Yixin Jiang, Chuang Lin. A Distributed Fault/Intrusion-Tolerant Sensor Data Storage Scheme Based on Network Coding and Homomorphic Fingerprinting [J]. Parallel and Distributed Systems, 2012,23(10): 1891-1830.

[60] Anh Le, AthinaMarkopoulou. NC-Audit: Auditing for network coding storage [C]//IEEE. 2010 International Symposium on Network Coding (NetCod). Cambridge, USA: IEEE, 2010:155-160.

[61] Yuchong Hu, Henry C. H. Chen, Patrick P. C. Lee. Applying Network Coding for the Storage Repair in a Cloud-of-Clouds [J], NCCloud:2012:21-28.

[62] Dimakis Alexandros G, Ramchandran Kannan, Wu Yunnan. A survey on network codes for distributed storage [J]. Proceedings of the IEEE, 2011,99(3): 476-489

[63] Keiichi Mizutani, Thomas Haustein, Kei Sakaguchi. Multi-user data sharing using coordinator with network coding and layered transmission [C]//VDE. 18th European Wireless Conference. Poznan, Poland: VDE, 2012:1-5.

[64] Twisa Mehta, Zunnun Narmawala. Survey on Multimedia Transmission using Network Coding over Wireless Networks [C]//IEEE. 2011 Nirma University International Conference on Engineering (NUiCONE). Ahmedabad, India: IEEE, 2011:1-6.