防窃听攻击的安全网络编码 *

俞立峰[1], 杨 琼[1], 于 娟[2], 沈才樑[1]
(1. 浙江工业职业技术学院, 浙江 绍兴 321000; 2. 复旦大学,上海 200433)

摘 要: 现有的防窃听安全网络编码的研究中,所采用的方法主要有信息论和密码学方法。按照所采用方法的不同,从两方面对现有的防窃听安全网络编码研究中的主要工作进行总结,进而从三个角度对现有的方法进行了分析和比较,对现有方法的优缺点进行了阐述。

关键词: 窃听攻击; *r*-安全网络编码; 强 *r*-安全网络编码; 弱安全网络编码; SPOC; P-coding
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2012)03-0813-06
doi:10.3969/j.issn.1001-3695.2012.03.003

Secure network coding against wiretapping attacks

YU Li-feng[1], YANG Qiong[1], YU Juan[2], SHEN Cai-liang[1]
(1. *Zhejiang Industry Polytechnic College*, *Shaoxing Zhejiang* 321000, *China*; 2. *Fudan University*, *Shanghai* 200433, *China*)

Abstract: In existing research, information theoretical and cryptographic approaches are two main methods adapted to achieve secure network coding to protect against wiretapping. This paper surveyed the existing research works about secure network coding against wiretapping from two aspects according to different approaches. Furthermore, it made analysis and comparison of different methods for achieving secure network coding from three perspectives, and presented their strengths and weaknesses.

Key words: wiretap attacks; *r*-secure network coding; strongly *r*-secure network coding; weakly secure network coding; SPOC; P-coding

0 引言

随着网络通信技术的高速发展以及网络用户数量的快速增长,网络在提供多样化服务的同时,如何提高现有网络资源利用率及传输质量,优化网络,已成为当前网络通信研究的重要课题。在传统多播通信网络中,中间节点仅对接收到的信息进行复制转发,很难达到网络多播的最大传输容量。针对这一问题,Ahlswede 等人[1]提出了网络编码思想,通过对中间节点进行编码处理(使其不仅具备路由功能而且具备编码功能),从而使网络传输容量(最大多播速率)达到最大流传输的理论极限。网络编码思想的提出,立即在理论界引起了广泛的关注,国内外知名大学及研究机构如麻省理工、微软研究院、贝尔实验室、普林斯顿大学、香港中文大学、西安电子科技大学、北京邮电大学等都有团队在积极地开展对网络编码相关理论及应用的研究。

网络编码具有提升网络吞吐量、改善负载均衡、提高带宽利用率、节省无线节点能耗以及增加网络传输健壮性等特点[2]。因此,网络编码思想已被广泛应用到内容分发[3,4]、分布式存储[5]、大规模集成电路设计、无线网络[6]、组播交换[7]等众多研究领域中。其中,在无线网络中的应用主要有:采用网络编码实现无线 Mesh 网络、Ad hoc 网络中的密钥交换[8];采用网络编码的方法来采集传感器数据[9];用网络编码来处理非调谐的收发器[10]等。在内容分发方面的应用最具代表性的是微软以网络编码为核心技术开发出传输容量可高出 BitTorrent 20% ~30% 的"雪崩"系统[3]。此外,网络编码也可以实现一定的安全保密性,如利用网络编码实现网络中数据包的完整性验证[11,12],结合网络编码来实现物理层安全[13~16]。Fragouli 等人[17]采用网络编码来推导重叠网络(overlay network)中的连接丢失率,以及用于被动网络监视[18]等。分布式存储方面,采用网络编码来实现节点故障时存储效率和修复带宽之间的最优均衡[19,20]。

上述的网络编码相关研究都是基于一个理想化的网络环境,而在现实的通信过程中均会面临着一系列的安全问题,如通信被窃听、Byzantine 攻击[21~23]等。在基于网络编码的通信环境下,这些安全问题若得不到很好的解决,将很大程度上影响网络通信的可靠性和有效性,使得网络编码在提升网络吞吐量等各方面的优势得不到很好发挥,并且很有可能较传统网络环境下的通信效率更差。所以,网络编码环境下的安全通信问题成为网络编码甚至通信领域一个亟待解决的大问题,这些问题能否得到有效解决是网络编码能否得以广泛应用的关键。

网络编码的安全问题目前考虑的主要是窃听(被动攻击)和污染(主动攻击)[24]。窃听攻击是指攻击者通过对网络中的某些设备(信道或节点)的监听来收集敏感信息。污染攻击则是指攻击者对所监听到的数据流的某些窜改,或生成一个假的数据流。由于污染攻击需要对消息作相应的修改,易于检测,而窃听攻击方式不对消息作任何修改,所以难以检测。目前防污染网络编码的研究主要有文献[25~28]。本文将主要关注防窃听攻击的网络编码研究,其意义在于:a)大部分的污

收稿日期: 2011-09-24; **修回日期**: 2011-11-19 **基金项目**: 绍兴市重大科技公关项目(2010A21034)

作者简介:俞立峰(1978-),男,硕士,主要研究方向为信息安全;杨琼(1982-),女,硕士,主要研究方向为信息安全(yanghan104@126.com);于娟(1983-),女,博士研究生,主要研究方向为信息安全;沈才樑(1973-),男,副教授,主要研究方向为信息安全.

染攻击都需要基于窃听攻击,即在通过窃听发现目标之后再对目标进行干扰,所以防窃听网络编码在抵制攻击方面更有效,可以达到一举两得的效果;b)对传输敏感信息要求较高的通信网络(如军事网络、银行网络等),在保证传输速率的同时,确保信息不被窃听攻击是安全通信的首要任务,并且需要不惜一切代价来实现保密通信;c)基于网络编码的通信系统中,由于传统的防窃听攻击的安全技术不再适用,对防窃听攻击的安全网络编码的研究已成为一项迫切且具有挑战性的课题。

防窃听网络编码的研究始于 2002 年,当时 Cai 等人[29]将网络编码与信息安全相结合提出一类窃听网络(communication system on a wiretape network,CSWN)模型,并给出了构建安全线性网络编码所需满足的条件。随后,Yeung 等人[30]证明了该安全网络编码构造方法可以以最少的随机序列(随机密钥)实现安全多播信息量的最大化。近来,Cai 等人[31]在文献[29]的基础上就防窃听的安全网络编码进行了更深入的研究,将 CSWN 模型进一步抽象为 *r*-窃听网络模型,并定义了 *r*-安全网络编码。Feldman 等人[32]指出 CSWN 模型(*r*-窃听网络)存在不足,指出构建安全线性网络编码问题等价于找到满足某些扩展的距离属性的线性网络编码,并对 CSWN 模型进行了扩展和简化。

Bhattad 等人[33]指出文献[29]中的安全网络编码实现的安全条件过于严格,于是他们提出了一种弱安全网络编码。Lima 等人[34]在应用随机网络编码的网络中考虑某些节点窃听其入边(信道)上传输的数据,并提出了代数安全标准。Harada 等人[35]提出了一种加强的安全网络编码,即强 *r*-安全网络编码,使得窃听者可窃听到的边数大于 *r* 时,泄露的只是秘密消息向量中最后的若干分量。Silva 等人[36]用最大秩可分(maximum rank separation,MRD)码取代 Ozarow-Wyner 陪集编码中用到的线性码来构造安全线性网络编码,优点是使陪集编码与网络编码无关。为了克服上述安全网络编码在防窃听攻击方面随机密钥的传输冗余和窃听集的特定限制,罗明星等人[37]定义了广义攻击模型,通过推广 all-or-nothing 变换[38],构造了广义组合网络上的安全网络编码,其安全性可由网络容量和窃听集的最小割完全刻画。

目前在国内,网络编码方面,好的研究综述并不多见,仅有黄政等人[39]在介绍网络信息流模型的基础上,针对优化问题的陈述、特点和解法,结合最新的研究成果进行了综述。曹张华等人[40]对安全网络编码的研究和发展进行了综述,详细阐述了通信网络中各种常见的攻击,给出了对抗这些攻击所构建的安全网络编码协议。其着重展示了结合网络编码自身特点而设计的对抗各种攻击的方案,进而对安全网络编码与网络容量及网络开销之间的关系作了简要介绍。另外,随着防窃听网络编码研究的展开,最近两年有很多成果呈现,但是,国内目前还没有专门针对防窃听网络编码的综述。为了填补这一空白,本文将专门对防窃听攻击的安全网络编码的最新研究成果进行分析与总结,以便为以后的相关研究工作提供参考。

按照所采用的方法不同,现有防窃听的安全网络编码大体上可分为两类,即信息论方法和密码学方法。信息论方法是利用合法接收者能获得较窃听者更多的信息这一前提,通过在源消息传输过程中引入足够的噪声到源消息中以达到防窃听的目的。密码学方法则主要通过利用简单的对称加密或同态加密,对网络编码的编码系数进行加密的方式来让窃听者无法对其窃听到的消息进行正确的解码来实现防窃听。本文将按这种分类分别对现有的防窃听安全网络编码的研究进行介绍。

1　信息论方法的安全网络编码

根据安全条件的不同,采用信息论方法的防窃听安全网络编码可分为 *r*-安全网络编码、强 *r*-安全网络编码和弱安全网络编码。其中,强 *r*-安全网络编码的安全条件最高,弱安全网络编码的安全条件最低;*r*-安全网络编码和强 *r*-安全网络编码均要求窃听者在窃听到不超过 *r* 条信道的情况下,不能获得任何关于源消息的信息,所以它们实现的安全称为绝对安全(因为这种安全性是由 Shannon 在文献[41]中提出的,又称做 Shannon 安全),而弱安全网络编码则要求的是窃听者不能获得任何关于源消息的有意义的信息即可。

1.1　*r*-安全网络编码

Cai 等人[31,42]将有窃听攻击的网络抽象为四元组(G,s,T,W)的形式。其中:$G=(V,E)$表示一个有向无环网络,V 为顶点(节点)集,E 为边(信道)集;$s\in T$,为网络 G 上的信源节点;$T\subset V$,为信宿节点集;$W\subseteq P(E)$为若干窃听信道子集构成的集合,$P(E)$ 表示 E 的幂集。通常假定窃听者能获得某一窃听子集 $w\in W$ 中的所有信道上传输的数据,没有窃听者能够同时对两个或两个以上的窃听子集中的信道进行窃听,并且窃听者能窃听到的信道是不随时间变化的。

对于一个窃听网络(G,s,T,W),当对 $\forall w\in W$ 都满足 $|W|\leqslant r$ 时,称该窃听网络为 *r*-窃听网络[29,31,42]。当没有窃听者(即 W 为空集)时,该模型就退化为文献[1,43]中研究的网络编码模型[29,31,42]。另外,该模型还包含香农密码系统[41]、Wire-tap channel Ⅱ[44]和秘密分享模型[45,46]。为了实现有效、可靠的通信,Cai 等人[31,42]基于 *r*-窃听网络模型提出了 *r*-安全网络编码,需要引入随机噪声对要传输的数据进行随机化处理。

定义 1　*r*-安全网络编码。给定一个 *r*-窃听网络(G,s,T,W),设从源节点发出的数据由两部分构成,即 $X=(M,K)$,其中 M 表示信源 s 需要传输的数据,K 为引入的随机噪声。对于该网络上在有限域 F_q 上的一个网络编码 C,当且仅当 C 满足以下两个条件:

a)对 $\forall t\in T$,$H(M|Y_{\mathrm{In}(t)})=0$,$Y_{\mathrm{In}(t)}$ 表示信宿节点从其所有入边($\mathrm{In}(t)$)上接收到的数据,$H(\cdot|\cdot)$表示条件熵。该条件表述的意义为所有的信宿节点都能正确接收到源数据 M。

b)对 $\forall w\in W$,$I(M;Y_w)=0$,其中 Y_w 表示窃听者通过窃听子集 w 中的所有信道获得的数据,$I(\cdot;\cdot)$表示互信息。

该网络编码即称为 *r*-安全网络编码[31,42],其中第一个条件为可解码条件,第二个条件为安全条件。

Cai 和 Yeung 等人[30,31,42]先后证明了 *r*-安全网络编码的最大安全多播速率为 $\omega-r$,其中 ω 为不考虑安全条件的情况下该网络上可达的最大多播速率。进而,他们还分别证明了线性 *r*-安全网络编码的最优性,即采用最少的随机密钥实现了最大速率的安全传输。任何一个可解码的线性网络编码都能被线性地变换成一个 *r*-安全线性网络编码,只要编码域的大小满足 $q>|W|$。这种方法的大体思想是首先假定在给定的网络上已

经存在一个可行的网络编码,然后找到一个满足一定条件(见文献[42]中的引理 4.3、4.4)的转换矩阵 H,采用该矩阵对已有的线性网络编码的全局编码向量进行线性变换便可得到 r-安全网络编码。

Rouayheb 等人[47,48]指出,窃听网络上的安全网络编码问题可视为 Ozarow-Wyner 窃听信道类型Ⅱ[44]在网络上的一个扩展,所以可采用 Ozarow-Wyner 的陪集编码方法实现窃听网络上的安全网络编码通信,只要对应的网络编码满足某些约束。他们将窃听网络上的安全网络编码问题分解成两个子问题,即窃听信道安全编码(也称外部码)的设计和满足额外约束条件的网络编码的设计。此外,Rouayheb 等人还给出了这种编码方式所需编码域的大小的要求。Cai 等人[31]证明了这种安全网络编码的实现方法实际上与他们给出的线性变换的方法是等价的。

受 Ozarow-Wyner 陪集编码方法[47]的启发,Silva 等人[36]提出一种基于 MRD 码的陪集编码的通用安全网络编码模式。该方法的特点就是对网络编码和安全陪集编码的设计可完全分开来考虑,并且它能够很好地与随机网络编码结合。这种方法实际上就是采用一个在 F_q 上非线性的但在其扩域 F_{q^l} 上是线性的陪集编码。基于扩域 F_{q^l},可以用最大秩距离(MRD)码来替换 Ozarow-Wyner 陪集编码模式中的线性最大距离可分(MDS)码,该(MRD)码事实上是 F_q 上秩距离最优的码。在这种编码模式下,窃听者观察到的对传输符号的线性变换实际上是一个秩距离码。

1.2　强 r-安全网络编码

r-安全网络编码中仅考虑攻击者能窃听到的信道数 $|W| \leqslant r$ 的场景,而当存在攻击者能窃听到的信道数大于 r 时,r-安全网络编码就会泄露源消息中的某些信息。于是,Harada 等人提出了强 r-安全网络编码,并给出了相应的构造强 r-安全网络编码的算法。

定义 2　强 r-安全网络编码[35]。给定窃听网络 (G,s,T,W),设从源节点发出的数据为 $X=(M,K)$。对于该网络上在有限域 F_q 上的一个 ω-维线性网络编码 C,其对应的全局编码核为 $\{f_e: e\in E\}$,当 C 为 r-安全网络编码,并且对于任意窃听信道数大于 r 的窃听子集 W 都满足以下条件:

$$\forall \{a_1,a_2,\cdots,a_{j+r-\mathrm{rank}(F_w)}\}\subset\{1,2,\cdots,j\}$$

$$H(M_{a_1},M_{a_2},\cdots,M_{a_{j+r-\mathrm{rank}(F_w)}}\mid Y_w)=\frac{[r+j-\mathrm{rank}(F_w)]_+}{j}H(M)=H(M_{a_1},M_{a_2},\cdots,M_{a_{j+r-\mathrm{rank}(F_w)}})$$

该编码即可称为强 r-安全网络编码,其中 $[a]_+=\max\{a,0\}$,Y_w 为窃听者通过窃听信道获得的数据,$\mathrm{rank}(F_w)$ 为窃听信道子集 w 中所有信道上对应的全局编码向量构成的矩阵的秩。

强 r-安全网络编码能确保在窃听者能窃听到信道数大于 r 时,不泄露源数据 M 中的任意大小为 $r+j-\mathrm{rank}(F_w)$ 的子集 $(M_{a_1},M_{a_2},\cdots,M_{a_{j+r-\mathrm{rank}(F_w)}})$ 的任何信息。基于文献[49]中的线性网络编码构造算法,Harada 等人[35]给出了构造强 r-安全网络编码的算法;同时,他们也给出了将一般的网络编码转换为强 r-安全网络编码的方法。

1.3　弱安全网络编码

r-安全网络编码和强 r-安全网络编码需要采用随机噪声来实现防窃听。为了让合法接收节点能正确接收到源数据,引入的随机噪声也必须随源数据一起传输,所以需要牺牲部分网络带宽来传输随机噪声,即以上两种安全网络编码要以牺牲多播速率为代价。并且它们要求的是让窃听者不能获得任何关于源数据的信息,即窃听者对源数据的不确定性没有因窃取到的数据而降低。事实上在实际应用中并不需要如此严格的安全条件,于是 Bhattad 等人[33]对安全条件进行适当放松,仅要求窃听者不能获得任何关于源数据的有意义信息即可。这种弱安全网络编码的实现并不需要引入随机噪声。

定义 3　弱安全网络码。给定一个 r-窃听网络 (G,s,T,W),设 C 为该窃听网络上的一类线性网络编码。对 $\forall w\in W$,设 w 中所有信道上传送的数据包为 Y_w,对 $\forall m_i\in M$ 都满足 $H(m_i\mid Y_w)=H(m_i)$,Y_w 为窃听者通过窃听信道获得的数据,则称 C 为弱安全网络编码。

Bhattad 等人还证明了信源可以以最大的可达多播速率实现到所有信宿节点的弱安全通信,只要窃听者能够窃听到的信道数量小于该最大可达多播速率(不考虑安全性时对应的网络上网络编码可实现的最大多播速率),并且编码域的大小足够大,可以通过在源节点处对源消息进行矩阵编码以实现弱安全[33]。但是他们没有给出实现弱安全网络编码的具体方法。后来,Silva 等人[50]指出 Bhattad 等人提出的实现弱安全的思路需要外部安全编码与网络编码联合设计,于是他们提出另外一种更通用的实现思路,即采用网络编码域 F_q 的一个扩域 F_{q^l} 上的 MRD 码的陪集编码作为外部的安全编码,这种方法与文献[36]中实现的 Shannon 安全编码方法类似。周业军等人[51]结合随机网络编码提出了一种实现弱安全的安全编码方法,该方法需要引入一个单位的随机密钥。Wei 等人[52]指出前面的一些安全网络编码都需要增加编码域的大小来实现,这样会带来很大的通信开销,于是他们主要针对资源有限的网络,如传感器网络等,设计了高效的实现弱安全的方法;并提出了两种编码模式,一种基本编码模式需要引入一个单位的随机密钥,另一种高级编码模式则无须引入随机密钥,并且可以采用线性反馈移位寄存器来实现编码。罗明星等人[37]采用了广义的 all-or-nothing 变换的方法来实现弱安全。Chang 等人[53]结合网络拓扑提出了一种新的实现最大安全吞吐量的算法,首先尝试寻找适合网络编码的传输拓扑,然后基于该传输拓扑设计能够满足弱安全条件的线性网络编码。

2　密码学方法的安全网络编码

要实现窃听网络上的安全通信,密码学方法中最直接的方式就是采用链路加密方式直接对编码的数据包进行加密再传输。但是,由于链路加密方式需要在每个节点都进行加密、解密,它会给每个节点带来很大的计算开销,从而使整个系统的性能严重下降。所以在网络编码背景下,采用链路加密方式并不可行。现有的基于密码学方法的安全网络编码的研究中主要采用的是端到端的加密方式。下面对密码学方法中的一些主要方法进行介绍。

2.1　SPOC

采用信息论方法的防窃听安全网络编码都是基于窃听者攻击能力有限的假设,面对窃听能力更强的攻击者它们不能起

到有效的抵制作用。于是,Vilela 等人[54]提出了基于密码学方法的 SPOC (secure practical network coding)模式,具体实现过程如下:

a)源节点上的初始化。

(a)选择一种密钥管理机制来实现源和信宿节点之间共享密钥 k 的交换,该共享密钥将用于对初始编码系数进行等长加密。

(b)源生成 ω 个源数据包,可以表示成矩阵的形式 $M=(m_1,\cdots,m_\omega)$,其中每一列对应一个数据包。

(c)源随机选择 ω 个线性无关的编码向量 $(f_1,\cdots,f_\omega)$ 来分别对消息数据包 M 进行编码(线性组合),即 $m'_i=M\cdot f_i=\sum_{j=1}^{\omega}f_{i,j}\cdot m_j$。其中每个编码向量 $f_i=(f_{i,1},\cdots,f_{i,w})^{\mathrm{T}}$,即为 ω-维列向量,得到编码后的数据包:$M'=(m'_1,\cdots,m'_\omega)$。

(d)对每个编码向量使用共享的密钥 k 进行加密:$c_i=E_k(f_i)(1\leqslant i\leqslant\omega)$,得到密文形式的编码向量 $C=(c_1,\cdots,c_\omega)$。

(e)构造新的数据包 $x_i=[u_i,c_i,m'_i]^{\mathrm{T}}(1\leqslant i\leqslant\omega)$,每个新数据包由三部分级联而成。其中 u_i 为第 i 个位置为 1,其他位为 0 的单位列向量,由此得到最终要发送出去的数据包 $X'=\{x'_1,\cdots,x'_\omega\}$。

b)中间节点编码。在每个中间节点上按照标准的随机网络编码方法对数据包进行编码和传输,各信道上 $e\in E$ 传输的数据包为 $y_e=[f'_e,Cf'_e,M'f_e]$。

c)信宿节点解码。当信宿节点 t 接收到 ω 个线性无关的数据包 $y_{e_1},\cdots,y_{e_\omega}$时,便可以执行解码过程:

(a)采用高斯消元解得加密的编码向量 C 和编码的消息 M'。

(b)采用共享的密钥 k 对加密的编码向量 C 进行解码得到编码向量 F。

(c)再对 $[F,MF]$ 进行高斯消元得到原始的消息数据包 M,消息传输完成。

2.2 P-coding

Zhang 等人[55]采用置换加密的方法结合随机线性网络编码本身固有的安全性,提出了一种新的基于密码学的安全网络编码模式 P-coding,它主要适用于随机线性网络编码,实现的是计算安全。P-coding 模式的安全网络编码由三个阶段构成,即源编码阶段、中间再编码阶段和信宿节点解码阶段。具体描述如下:

a)源编码。设网络最大多播的速率为 ω,则源 s 可一次性产生并发出 ω 个数据包 $X=\{x_1,\cdots,x_\omega\}$。在源节点处:

(a)在每个数据包的首部附上其对应的单位向量得到 $x'_i=[u_i,x_i]$,则 $X'=\{x'_1,\cdots,x'_\omega\}$。

(b)为 ω 条虚信道 $\{e_1,\cdots,e_\omega\}$(为表述方便,人为地添加信道,实际中不存在)分别采用随机的方式选择其对应的全局编码核 $\{f_{e_1},\cdots,f_{e_\omega}\}$,并采用选取的全局编码核对 X' 中的数据包执行线性组合,得到各条虚信道上传输的编码消息 $y_{e_i}=X'f_{e_i},1\leqslant i\leqslant\omega$。

(c)对每个编码消息 y_{e_i} 执行置换加密得到它的密文形式 $c_{e_i}=E_k(y_{e_i})$,将密文形式的数据包通过网络发送给信宿。

b)中间节点再编码。中间节点再编码即对源发出的加密后的数据包进行随机网络编码。每条信道 $e\in E$ 上传输的数据包为 $c_e=\sum_{e'\in e\text{的父边}}k_{e',e}\cdot c_{e'}$,其中 $k_{e',e}$ 为随机选择的局部编码核。因为源消息及其对应的全局编码向量的符号被置换加密后重排,并且中间节点对所采用的密钥并不知情,所以它们很难重构出源消息。

c)信宿解码。

(a)对于每个信宿节点 $t\in T$,每当它从其一条入边 e_i 接收到一个加密的数据包 c_{e_i},就可以首先对其执行置换解码:$D_k(c_{e_i})=E_{k-1}(E_k(y_{e_i}))=y_{e_i}$,直到 t 接收到 ω 个线性无关的数据包 $y_{e_1},\cdots,y_{e_\omega}$时,该节点可以得到 $Y_t^{\mathrm{T}}=[F_{\ln(t)},XF_{\ln(t)}]$。其中 $F_{\ln(t)}$ 为以节点 t 入边上的全局编码向量为列构成的矩阵,Y_t^{T} 表示 Y_t 的转置。

(b)采用高斯消元法解出源消息 $Y_t^{\mathrm{T}}=[F_{\ln(t)},XF_{\ln(t)}]\xrightarrow{\text{高斯消元}}[I,X]$。

由于置换函数与线性组合操作是可交换的,中间节点的再编码可以在加密的数据包上透明地执行。显然,这种透明性能够很大程度地提高系统的效率,因为在中间节点上无须任何额外操作。另外,该模式要求通信系统中有一个密钥分发中心,负责产生对称密钥供源和信宿节点离线地获得随机密钥 k。在实现过程中使用置换加密函数时还要求做到:明文的保密和密钥的随机选取。另外,当要传输的数据量很大时,需要对数据分代传输。如果在 P-coding 的整个传输过程中仅使用一个密钥,由于单代的破解可能会发生,这种情况下就会导致其他代的传输泄密。为了解决这一问题,Zhang 等人[55]采用在每一代中都对密钥进行随机扰动的方法,即每一代使用不同的对称密钥进行置换加密。

3 分析与比较

3.1 信息论方法之间的比较

在防窃听安全网络编码研究中,信息论方法的安全网络编码主要有 r-安全网络编码、强 r-安全网络编码和弱安全网络编码。它们之间的主要区别在于:a)实现的安全程度不同,其中强 r-安全网络编码的安全性最高,弱安全网络编码的安全性最低;b)最大安全多播速率不同,r-安全网络编码和强 r-安全网络编码的最大安全多播速率为 $\omega-r$,而弱安全网络编码的最大安全多播速率可达到 ω,其中 ω 为最大网络多播速率;c)实现方法不同,r-安全网络编码和强 r-安全网络编码都需要引入随机噪声,而弱安全网络编码不需要引入随机噪声。

另外,对于构造 r-安全网络编码的不同方法,可从编码所需要的有限域大小、对网络编码的要求以及编码复杂性这几方面来进行比较。编码所需的有限域大小方面,基于 MRD 码的陪集编码模式要求最低,其次是基于 MDS 码的陪集编码,线性变换的编码方式要求最高。对网络编码的要求方面,基于 MRD 码的陪集编码模式是对于任意的可实现最大多播容量的网络编码都可行,但是基于 MDS 码的陪集编码和线性变换的方法则需要网络编码满足一定的条件。编码复杂性方面,都可以在多项式时间内实现。对于基于 MRD 码的陪集编码模式,其唯一的要求就是数据包的长度不能小于网络多播容量,通常这一要求很容易实现。

3.2 密码学方法之间的比较

SPOC 与 P-coding 都是采用密码学中简单加密的方法结合

随机线性网络编码来实现防窃听,其大体思想是通过对编码系数的保护来实现防窃听,它们实现的是计算安全而不是信息论意义上的安全。SPOC 与 P-coding 的主要区别在于:a)加密方法不同,SPOC 采用明文密文等长的加密方法即可,而 P-coding 则采用的是置换加密;b)所带来的开销不同,由于 SPOC 在进行解码时需要执行两轮解码操作,会引入额外的计算开销,而 P-coding 则避免了这种计算开销;c)在存储空间方面,由实现过程可知,SPOC 需要对加密的初始编码向量存储转发,而 P-coding 无须存储额外的编码向量。另外,P-coding 还具有安全、有效、透明、健壮和可扩展的特性[55]。

3.3　信息论方法与密码学方法之间的比较

现有的防窃听安全网络编码中,信息论方法与密码学方法之间的区别主要体现在以下几个方面:

a)两者基于的前提条件不同。信息论方法需要基于窃听者能窃听到的信道数量要少于网络编码的多播速率,否则采用信息论方法无法构造出安全网络编码;密码学方法则基于某些加密方式破译的高计算复杂性的前提,因此它实现的是计算安全。较信息论方法的优点是它不需要假定窃听攻击者的窃听能力是有限的,即使是对于能够窃听到的信道数量达到网络编码的多播速率的窃听者,密码学方法也能实现计算安全。

b)可达的最大安全多播速率不同。信息论方法中除了弱安全网络编码,其他安全网络编码需要传输随机噪声而占用一定量的带宽,所以它们可达的最大安全多播速率为 $\omega - r$;而密码学方法因无须引入随机噪声,其可达的最大安全多播速率与不考虑安全条件的情况下相同,即仍为 ω。

c)密码学方法需要有密钥分发中心负责管理和分发信源与信宿节点共享的密钥,而信息论方法不需要密钥分发中心。

4　结束语

本文分两部分对现有的防窃听安全网络编码的研究工作进行了总结。现有的安全网络编码中,r-安全网络编码和强 r-安全网络编码的安全性要求比较严格,并且需要牺牲部分带宽以传输对源信息进行随机化的随机密钥,这样势必会降低网络的传输速率。通常可以采用降低安全要求的方式来减少传输带宽的开销。弱安全就是一个典型的通过降低安全要求以减少带宽开销的实例,它通常不需要使用随机噪声,所以不需要以牺牲带宽为代价。但是,对于任何窃听网络,只有当所有的窃听信道子集数量都不超过 r 时,才存在 r-安全网络编码或弱安全网络编码[42]。所以,r-安全网络编码、强 r-安全网络编码和弱安全的安全网络编码都需要基于窃听攻击者攻击能力有限的假设,当存在窃听信道数达到最大网络多播速率时,它们都不能有效地实现防窃听。对于这种窃听者能窃听到的信道数量达到最大网络多播速率的情景,因窃听者攻击能力达到最强,所以也称为全能窃听攻击[55],则需要采用密码学的方法。因为密码学的方法无须基于攻击者能力有限的假设,而是攻击者资源有限的假设,实现的是计算安全,但是需要假定有一个密钥分发中心存在。

近几年来对窃听网络上安全网络编码的研究取得了不少的成果,但其中尚存在很多亟待解决的问题:a)当前主要研究的是在单源多播网络场景下的安全网络多播,在其他场景,如多源等,研究甚少,并且还有很多诸如多源场景下安全网络编码容量的确定等问题尚未确定;b)现有的研究工作中主要考虑的是线性网络编码的情况,对于非线性网络编码的安全性研究几乎还是无人问津;c)现有的这些安全网络编码模式中,大部分都对编码域的要求很高,显然给实现带来很多麻烦。那么在给定的有限域上,如何设计实现最优的安全网络编码也还是一个开放的问题。以上这些问题也是将来所要着重研究的工作内容。

参考文献:

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

[2] FRAGOULI C, Le BOUDEC J Y, WIDMER J. Network coding: an instant primer[J]. ACM SIGCOMM Computer Communication Review, 2006, 36(1): 63-68.

[3] GKANTSIDIS C, RODRIGUEZ P R. Network coding for large scale content distribution[C]// Proc of the 24th Annual Joint Conference of IEEE Computer and Communications Societies. 2005: 2235-2245.

[4] LI Bao-chun, NIU Di. Random network coding in peer-to-peer networks: from theory to practice[J]. Proceedings of the IEEE, 2011, 99(3): 513-523.

[5] DIMAKIS A G, RAMCHANDRAN K, WU Y, *et al*. A survey on network codes for distributed storage[J]. Proceedings of the IEEE, 2011, 99(3): 476-489.

[6] FRAGOULI C. Network coding: beyond throughput benefits[J]. Proceedings of the IEEE, 2011, 99(3): 461-475.

[7] KIM M, SUNDARARAJAN J K, MEDARD M, *et al*. Network coding in a multicast switch [J]. IEEE Trans on Information Theory, 2011, 57(1): 436-460.

[8] OLIVERIA P F, BARROS J. A network coding approach to secret key distribution [J]. IEEE Trans on Information Forensics and Security, 2008, 3(3): 414-423.

[9] DIMAKIS A G, PRABHAKARAN V, RAMCHANDRAN K. Ubiquitous access to distributed data in large-scale sensor networks through decentralized erasure codes[C]//Proc of the 4th International Symposium on Information Processing in Sensor Network. 2005: 111-117.

[10] PETROVIC D, RAMCHANDRAN K, RABAEY J. Overcoming untuned radios in wireless networks with network coding [J]. IEEE Trans on Information Theory, 2006, 52(6): 2649-2657.

[11] ZHAO Fang, KALKER T, MEDARD M, *et al*. Signatures for content distribution with network coding[C]//Proc of International Symposium on Information Theory. 2007: 556-560.

[12] YU Zhen, WEI Ya-wen, RAMKUMAR B, *et al*. An efficient signature-based scheme for securing network coding against pollution attacks [C]//Proc of the 27th IEEE International Conference on Computer Communications. 2008: 1409-1417.

[13] LIU Ke-jie, FU Sheng-li, QIAN Yi, *et al*. On the security performance of physical-layer network coding[C]//Proc of IEEE International Conference on Communications. 2009: 1-5.

[14] LIU Wai-xi, YU Sun-zheng, CAI Jun, *et al*. Secure physical layer network coding: challenges and directions[C]//Proc of International Conference on Internet Technology and Applications. 2010: 1-4.

[15] HAY M, SAEED B, LUNG C H, *et al*. Co-located physical-layer network coding to mitigate passive eavesdropping[C]//Proc of the 8th Annual Conference on Privacy, Security and Trust. 2010: 1-2.