基于抗窃听和拜占庭攻击的随机网络编码

赵佳佳 任平安
(陕西师范大学计算机科学学院 西安 710062)

摘 要 随机网络编码目前被广泛应用于实际网络环境中,能够有效提高网络吞吐量。然而网络编码容易受到窃听攻击和拜占庭攻击。提出一种既防窃听,又能有效检测出拜占庭攻击的安全随机网络编码算法。在信源和信宿之间共享秘密信道,该算法通过哈希函数增加少量计算量和少量冗余,实现防窃听攻击和防拜占庭攻击。该算法仅在随机网络编码的基础上改变了信源节点的编码方式和信宿节点的解码方式,中间节点编码方式保持不变,具有较高的编码效应。

关键词 网络编码,窃听,拜占庭,哈希函数,安全信道
中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.09.033

Random Network Coding Based on Anti-eavesdropping and Byzantine Adversaries

ZHAO Jia-jia REN Ping-an
(School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

Abstract Random network coding has been widely applied in the actual network environment, and can effectively improve network throughput. However, network coding is vulnerable to eavesdropping attack and Byzantine attack. This paper presented a random network coding algorithm that can prevent the eavesdropping adversaries and effectively detect Byzantine modification. There is a secret channel sharing between the source and destination, and the algorithm increases a few computations and redundancies to achieve anti- eavesdropping attack and anti- Byzantine attack through the hash function. The algorithm only changes the encoding method of the source node and the decoding method of the destination node based on the random network coding, and the intermediate nodes remain unchanged. It has a high coding efficiency.

Keywords Network coding, Eavesdropping, Byzantine, Hash function, Secure channel

1 引言

Ahlswede 等人[1]首次提出了网络编码理论,与传统路由网络相比,网络编码可以增加多播速率,并提出多播容量为从源节点到目的节点的最大流的最小值。Li, Yeung 和 Cai[2]提出了线性网络编码就可以达到最大多播容量。T. Ho 等人[3,4]提出了随机网络编码,其属于分布式的码构造算法,在网络中参与传输的节点均随机选取系数进行编码,节点将多条输入信道上传输的数据进行随机线性组合,将其发送到输出信道。接收节点收到足够多的线性无关的组合后能以很大的概率正确恢复出信源所发送的信息。

网络编码虽然提高了网络的可靠性和吞吐量,但同时也带来了不可忽视的安全问题,主要包括窃听和污染两类问题。Cai 和 Yeung[5]第一次提出了在多播网络中的信息安全传输问题,他们研究了一个在有向无环多播网络中速率为 h 的多播网络编码,某个窃听者如果能够获取最多 $k(k<h)$ 个独立的消息,那么就有可能修改给定的线性编码使得安全传输的速率为 $h-k$。但在实际的应用中,对安全性的要求不一定要像信息论安全这样高。Bhattad 和 Narayanan[6]介绍了弱安全网络编码,在此网络中攻击者窃听到信源信息运算后的信息,且窃听者窃听到的信道数小于网络最大流,则攻击者不能正确地计算出信源消息。在弱安全网络编码下,不用牺牲网络的吞吐量。

T. Ho 等人[7]研究了网络编码和污染攻击的相互影响,文献中提出了利用网络编码检测攻击敌手存在的方法。Jaggi 等人[8]针对攻击者能力的差别设计了一种适应性的安全网络编码。Nutman 和 Langberg[9]改进了 Jaggi 等人的算法,提高了编码效率。Cai 和 Yeung[10]最早提出了网络纠错编码,纠错编码通过对源信息添加自相关的冗余信息,使得目标节点能够利用这些冗余信息进行纠错。Zhang[11,12]给出了当信道存在信道噪声时网络纠错编码的具体编译码算法。

T. Ho 等人[14]在每个报文中嵌入 Hash 函数值,使接收结点有非常高的概率可以识别到拜占庭攻击。但是在此网络编码中,限定攻击者只能获取部分的信息,当攻击者具有较强的窃听能力时,它可以破译出源消息,进而更改源消息和对应的哈希值,而接收节点则无法检测出消息是否被修改。窃听攻击和拜占庭攻击可能同时出现在同一网络中,这种情况对于网络有很强的攻击破坏能力。

到稿日期:2013-12-04 返修日期:2013-12-31 本文受国家自然科学基金项目:高性能保密计算算法与协议(61070189)资助。
赵佳佳(1988-),男,硕士生,主要研究方向为网络与信息安全;任平安(1963-),男,博士,副教授,硕士生导师,主要研究方向为计算机网络安全。

本文主要利用哈希函数和安全信道对随机单跳网络编码进行改进，提出一种既能防止窃听攻击，又能检测出污染攻击的安全网络编码，仅在随机网络编码的基础上改变了信源节点的编码方式和信宿节点的解码方式。中间节点编码方式保持不变，具有较高的编码效应。

2 基本模型和概念

2.1 网络模型

我们使用一个有向图 $G(V,E)$ 表示一个有向无环网络，V 为节点集合。E 为信道集合，每条边代表一单位容量。F_q 代表一个范围为 q 的有限域。$S\in V$，为网络 G 上的信源节点；$T\subset V$，为信宿节点集合。

在一个 n 维随机网络中，有 n 条虚拟链路向信源发送消息 $M=\{M_1\ M_2\cdots M_n\}$。信源节点 s 和任意中间节点 $w\in V$，将收到的输入边上的所有消息进行线性组合，并发送到输出链路，进行线性组合的系数向量 ζ 均从有限域 F 上随机选取。

对于信宿节点而言，只要收到 n 个源消息 M 的线性组合，并且当 n 个消息的系数矩阵满秩时，即可解码出源消息 M。

2.2 攻击模型

假设 Alice 为信源节点，发送消息给信宿节点。本文考虑其中的一个信宿节点 Bob，其他信宿节点情况与此类似。在窃听模型中，攻击者一般表示为被窃听的信道，在主动攻击模型中，攻击者为网络中的某个节点。在本文的模型中，设定攻击者 Calvin 为网络中某个中间节点，使攻击者既能窃听到输入链路传输到此节点的消息，又能篡改要发送到输出链路的消息，即攻击者既能实现窃听攻击，同时又能实现拜占庭攻击。

Alice 和 Bob 共同享有一个秘密信道，攻击者无法窃听到秘密信道上所传输的信息。Alice 经秘密信道向 Bob 传输一个长度为 τ 的随机数 α，α 在有限域 F_q 上是服从均匀分布的。

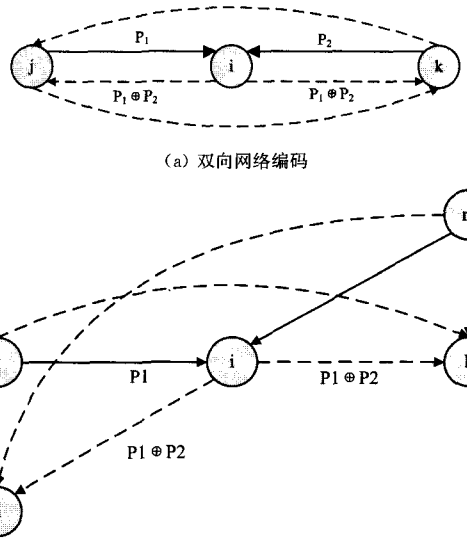
3 安全的网络编码

本文考虑单跳网络中使用的线性异或网络编码方式，该编码方式与 $c=a\oplus b$ 类似。这里，a 和 b 为输入分组，c 为异或之后的输出分组。目前大部分对使用网络编码进行网络优化的研究都仅关注 2 个符号（分组）的编码运算[1]，而且通过对实际系统的研究也发现多于两个符号的网络编码运算会使优化过程极其复杂。因此，本文对网络编码的分析将在使用线性异或网络编码的单跳成对网络中进行。

下面的引理给出了单跳成对网络编码正常工作的要求。

引理 1 在单跳网络编码中，对于节点 k，若想从节点 i 传输的编码分组 $P_c=P_x\oplus P$ 解码出分组 P_x，则该节点需满足以下两个条件：1）节点 k 从节点 i 接收到分组 P_c；2）节点 k 获得了未编码分组 P。

考虑两种节点 k 获得未编码分组 P 的机会：1）通过链路 (k,i) 将 P 传输到节点 i，如图 1(a) 所示的节点 k 处的分组 P_2；2）节点 k 正确地从其他链路侦听到分组 P，如图 1(b) 所示的由节点 k 从链路 (m,k) 侦听到的分组 P_2。根据节点获得未编码分组的这两种方式，定义单跳成对网络中的两种网络编码：1）双向网络编码方式，该方式仅包含机会 1）中的分组；2）侦听网络编码方式，该方式同时包含机会 1）和机会 2）中的分组。



(a) 双向网络编码

(b) 窃听网络编码

图 1 单跳网络编码

本文给出了具体的编译码过程，信源节点通过哈希函数，将原始消息转换 2 次，形成新的要发送的消息。信宿节点通过逆向的解码还原出原始消息。整个过程中，中间节点的编码方式和原编码方式相同，保证了传输信息的高效率。因为哈希函数可以在多项式时间内完成，通过增加少量的计算和少量的带宽，即可构建一个既能有效防止窃听攻击又能检测出拜占庭攻击的安全随机网络编码。

3.1 信源编码

在本文的安全网络模型中，原始信源消息经过 2 次变换，使得消息在传输过程中可以抵挡窃听攻击，并且信宿节点能够检测出消息是否被窜改。在一个 n 维有向无环网络中，信源 Alice 处产生的原始消息 M 形式如下：

$$M=\begin{Bmatrix} m_{11} & m_{12} & \cdots & m_{1k} \\ m_{21} & m_{22} & \cdots & m_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \cdots & m_{nk} \end{Bmatrix}=\begin{Bmatrix} M_1 \\ M_2 \\ \vdots \\ M_n \end{Bmatrix}$$

$M_i(i=1,2,\cdots,n)$ 为原始信息向量，其中 $M_i\in F_q^k$。

在有限域 $GF_{(q)}$ 上选取随机数 α，且服从均匀分布。使用哈希函数 $\theta_1(\cdot):F_q^\tau\to F_q^k$ 使得 $\theta_1(\alpha)\in F_q^k$。我们通过 α 构建新的信息向量，方式如下：

$$\begin{cases} M_1'=M_1+\theta_1(\alpha) \\ M_2'=M_2+\theta_1(\alpha,M_1) \\ \cdots \\ M_n'=M_n+\theta_1(\alpha,M_1,M_2,\cdots,M_{n-1}) \end{cases}$$

经过初次变换，得到新的消息矩阵 $M'=\{M_1'\ M_2'\cdots M_n'\}^{\mathrm{T}}$。

使用哈希函数 $\theta_2(\cdot):F_q^k\to F_q^\gamma$，得到哈希值 $\theta_2(M_i)\in F_q^\gamma$ $(i=1,2,\cdots,n)$ 并附加在 $M_i'(i=1,2,\cdots,n)$ 信息向量之后，使之形成新的向量 M_i'。

$$M'=\begin{Bmatrix} M_1' & \theta_2(M_1) \\ M_2' & \theta_2(M_2) \\ \vdots & \vdots \\ M_n' & \theta_2(M_n) \end{Bmatrix}=\begin{Bmatrix} M_1'' \\ M_2'' \\ \vdots \\ M_n'' \end{Bmatrix}$$

$M_i''=(M_i'\ \theta_2(M_i))$经过两次变换计算后，Alice 在源节点形成了新的信息向量 $M_i''(i=1,2,\cdots,n)$，每个信息向量由 $k+l$位符号组成，前 k 位符号为数据信息 M_i'，后 l 位符号由 M_i 的哈希函数 $\theta_2(M_i)$构成。

3.2 信宿解码

信宿节点 Bob 收到一个消息矩阵 D，其由 n 个线性独立的消息组成。

$$D=M''\times T=\begin{Bmatrix} M_1'' \\ M_2'' \\ \vdots \\ M_n'' \end{Bmatrix}\times T$$

T 为 n 个消息系数组成的系数矩阵。只要系数矩阵满秩，求出 T 的逆矩阵 T^{-1}，即可解码出消息矩阵 M'。

$$D\times T^{-1}=M'\times T\times T^{-1}=\begin{Bmatrix} M_1'' \\ M_2'' \\ \vdots \\ M_n'' \end{Bmatrix}$$

消息向量 $M_i''(i=1,2,\cdots,n)$的前 k 位为数据信息 M_i'，通过密码信道接受到随机数 α，Bob 可以从 M_i'解析出 M_1，从而可以逐步地解析到 M_n。

然后 Bob 通过哈希函数$\theta_2(\cdot)$计算出 $\theta_2(M_i)$，与收到的矩阵进行比较。如果值相同，则说明没有受到拜占庭攻击；如果值不同，就丢弃此消息矩阵 D。

4 安全性分析

4.1 安全机制

在我们的编码方案中，使用了哈希函数处理随机数和信源消息向量 $M_i,i=1,2,\cdots,n$。给定一个消息 m 和哈希函数 $\theta(\cdot),\theta(\cdot)$可以在多项式时间内计算出 m 的哈希值，但是如果给定 m 的哈希值，则不可能计算出原来的消息 m。同样地，给出两个消息 m_1,m_2，使得 $\theta(m_1)=\theta(m_2)$也几乎是不可能的，也就是说不同的 2 个消息得到不同的哈希值的概率非常高。

$$\forall m_1,m_2 \text{ 且 } m_1\neq m_2 \xrightarrow{\text{非常高的可能性}} \theta(m_1)\neq\theta(m_2)$$

对于强哈希函数，有非常低的碰撞攻击可能性，在多项式时间内发现碰撞也是不可能的。

对于窃听攻击，由于随机数 α 是在安全信道传输的，攻击者无法窃听到。即使攻击者窃听到 n 个线性独立的消息，解码出 M'，但还需要破译随机数 α，这对攻击者来讲无疑是巨大的困难。从信息论角度，有

$$I(M_i;M_i+\theta(\alpha,M_1,M_2,\cdots,M_{i-1}))=0,M_i\in M$$

即攻击者得不到 M 的任何有意义的信息，该算法是信息论安全的。

我们假设攻击者知道哈希函数 $\theta_1(\cdot)$和 $\theta_2(\cdot)$，但得不到秘密信道传输的随机数 α。当攻击者窃听到超过 n 个线性独立消息，解码出 M'。

$M_i''=(M_i'\ \theta_2(M_i))$且 $M_i'=M_i+\theta(\alpha,M_1,M_2,\cdots,M_{i-1})$

由于没有得到随机数 α，因此无法解码出 M，此网络编码是防窃听安全的。攻击者虽然知道了哈希函数 $\theta_2(\cdot)$，但是没有解码出 M，因而无法得到正确的哈希值 $\theta_2(M_i)$，此网络编码对于污染攻击也是安全的。我们分别讨论攻击者窃听能力强弱时的两种情况。

情况 1　攻击者窃听能力较弱，无法窃听超过 n 条线性独立的消息，此情况下，攻击者对收到的数据包进行修改转发。

经过信源的编码，网络中传输的每个信息包 p 由 $k+l$ 位符号组成行向量 W_p 来表示，前 k 位符号为数据信息 M_i'，后 l 位符号由 M_i 的哈希函数 $\theta_2(M_i)$构成。经攻击者修改后的数据包 p 可以表示成 W_p+V_p，V_p 是有限域 F_q^{k+l} 上的任意向量。当 V_p 为 0 时，说明信息包 p 没有被修改。

文献[13]对此情况给出了分析，本论文不再赘述。

情况 2　攻击者具有很强的窃听能力，窃听到了超过 n 个线性独立的消息，能够解码出源消息，通过修改源消息和对应的哈希值，使得信宿节点无法检查到消息已经被修改。在我们的模型下，分析此种情况：攻击节点若接受到超过 n 个线性独立的消息。攻击者首先解码出消息矩阵 M'。

$$M'=\begin{Bmatrix} M_1' & \theta_2(M_1) \\ M_2' & \theta_2(M_2) \\ \vdots & \vdots \\ M_n' & \theta_2(M_n) \end{Bmatrix}$$

由 M'，攻击者可以得到源消息向量 M_i 的哈希值 $\theta_2(M_i)$，由哈希值得到源消息向量 M_i 的概率为$\frac{1}{q^k}$。因为 M_i'由 M_i 和$\theta(\alpha,M_1,M_2,\cdots,M_{i-1})$组成，根据哈希函数 $\theta_1(\cdot)$得到 α 的概率为$\frac{1}{q^\tau}$。攻击者破解源消息的概率最高为$\frac{1}{q^{k_\tau}}$。若 q,k,τ 取值较大，解码出源消息的可能性几乎为 0。

4.2 防伪造警报机制

安全机制的一个潜在缺点是节点可能受到 DOS 攻击，即发送和收到伪造警报。本文提出的机制能有效地阻止伪造警报进入分布式网络，同时确保正确包的传送速度不会降低。

首先定义随机矢量为$\vec{t}=\{t_1\cdots t_m\}$，则每个包的效验和为 $f(b_i)=\sum_{k=1}^{m}t_kb_{k,i}$，那么$\vec{f}=\{f(b_1)\cdots f(b_n)\}$。注意到每个效验和 $f(b_i)$都是由一个随机矢量产生的。每个效验包的大小和原始包的大小一样。将这种方法和哈希结合在一起，节点可以快速地在传送过程中确认警报。节点下载信息前，先选取一个随机矢量，计算相应效验和$(\vec{t},\vec{f})$。每个节点独立地选取自己的随机矢量和计算效验和。一旦节点收到警报，看它是否是从“不可靠”窗口发出，或者用效验和进行确认。至此，节点产生所有编码包的线性编码组合包 $e,e=\sum_{i=1}^{n}c_ib_i$，$\vec{c}$是组合因子。为确认包是否遭到攻击，进行以下检查：

$$f(e)=\sum_{k=1}^{m}t_ke_k=\sum_{k=1}^{m}t_k(\sum_{i=1}^{n}c_ib_{k,i})=\sum_{i=1}^{n}c_i(\sum_{k=1}^{m}t_kb_{k,i})$$
$$=\sum_{i=1}^{n}c_if(b_i)$$

结束语　本文借助于秘密信道，提出了一种即能有效防窃听攻击，又能有效检测拜占庭攻击的随机网络编码。本文

利用哈希函数对源消息进行了变化，使用线性随机网络编码，对信源和信宿节点的编译码算法进行了变化，中间节点不需要改变编码方案。通过增加少量的计算复杂度（信源信宿节点）和舍弃少量的带宽，使整个网络达到了理想的安全要求。

参 考 文 献

[1] Ahlswede R, Cai N, Li S-Y R, et al. Network information flow [J]. IEEE Transactions on Information Theory, 2000, 46: 1204-1216

[2] Li S-Y R, Yeung R W, Cai N. Linear network coding[J]. IEEE Transactions on Information Theory, 2003, 49: 371-381

[3] Ho T, Medard M, Shi J, et al. On randomized network coding [C]// 41st Annual Allerton Conference on Communication Control and Computing. Oct. 2003

[4] Ho T, Leong B, Koetter R, et al. Toward a random operation of networks[J]. IEEE Transactions on Information Theory, submitted, 2004

[5] Cai N, Yeung R W. Secure network coding[C]// International Symposium on Information Theory (ISIT) 2002. Lausanne, Switzerland, 2002: 30-50

[6] Bhattad K, Narayanan K R. Weakly secure network coding [C]// Proc. 1st Workshop Netw. Coding Theory Appl, Apr. 2005

[7] Ho T. Networking from a network coding perspective [D]. MIT, 2004

[8] Jaggi S, Langberg M, Katei S. Resilient Network Coding in the Presence of Byzantine Adversaries [C]// 26th IEEE International Conference on Computer Communications. Anchorage: IEEE Press, 2012: 616-624

[9] Nutman L, Langberg M. Adversarial Models and Resilient Schemes for Network Coding [C]// IEEE Intl Symp Inf Theory. Toronto: IEEE Press, 2008: 171-175

[10] Cai N, Yeung R W. Network Coding and Error Correction [C]// IEEE Inform Theory Workshop. Bangalore: IEEE Press, 2002: 119-122

[11] Zhang Z. Network Error Correction Coding in Packetized Networks [C]// IEEE Information Theory Workshop Chengdu, ITW'06. IEEE Press, Chengdu, 2006: 433-437

[12] Zhang Z. Linear Network Error Correction Codes in Packet Networks [J]. IEEE Trans on Inf Theory, 2012, 54(1): 209-218

[13] 韦勇，连一峰. 基于日志审计与性能修正算法的网络安全态势评估模型[J]. 计算机学报，2009，32(4)：763-772

[14] Ho T, Leong B, Koetter R. Byzantine Modification Detection in Multicast Networks with Random Network Coding [J]. IEEE Transactions on Information Theory, 2012, 54(6): 2798-2830

[15] 周业军，李晖，马建峰. 一种防窃听的随机网络编码 [J]. 西安电子科技大学学报，2009，35(1)：696-701

[16] 武广柱，王劲林，齐卫宁. ARLNCStream：自适应随机网络编码流媒体系统[J]. 电子与信息学报，2008，30(1)：25-28

[17] 王汝言，楼芃雯，樊思龙，等. 容迟网络编码节点状态感知的数据转发策略[J]. 重庆邮电大学学报：自然科学版，2013，25(2)：215-220

(上接第 151 页)

[13] Pirretti M, Traynor P, et al. Secure attribute based systems [C]// Proc of the 13th ACM conference on Computer and Communication Security. 2006: 99-112

[14] Yu Shu-cheng, Wang Cong, et al. Attribute Based Data Sharing with Attribute Revocation[C]// Proc of ASIACCS. 2010: 261-270

[15] Wang Guo-jun, Liu Qin, et al. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services [C]// Proc of CCS-2010. 2010: 735-737

[16] Yu Shu-cheng, Wang Cong, et al. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing [C]// Proc of INFOCOM. 2010: 15-19

[17] Wang Guo-jun, Liu Qin, et al. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers[J]. Computers & Security, 2011, 30: 320-331

[18] Nuttapong A, Hideki I. Conjunctive Broadcast and Attribute-Based Encryption [M] // Pairing-Based Cryptograph-Pairing 2009. Springer Berlin Heidlberg, 2009: 248-265

[19] Niroshinie F, Seng W, et al. Mobile cloud computing: A survey [J]. Future Generation Computer Systems, 2013, 29: 84-106

[20] Ibraimi L, Petkovic M, et al. Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes [R]. Centre for Telematics and Information Technology, University of Twente, 2009

[21] Jae H S, Keita E. Efficient Delegation of Key Generation and Revocation Functionalities in Identity-Based Encryption[M]// Topics in Cryptology-CFRSA 2013. Springer Berlin Heidelberg, 2013: 345-358

[22] Yang Kan, Jia Xiao-hua, et al. Attribute-based Fine-Grained Access Control with Efficient Revocation in Cloud Storage Systems [C]// Proc of ASIA CCS. ACM, NY, 2013: 523-528

[23] Junbeom H, Dong K N. Attribute-based access control with efficient revocation in data outsourcing systems[J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(7): 1214-1221

[24] Aggelos K, Moti Y. Group Signatures with Efficient Concurrent Join[C]// Proc of EUROCRYPT 2005. 2005: 198-214

[25] Dalia K. Attribute Based Group Signature with Revocation [R]. Cryptology ePrint archive: report 2007/241

[26] Dan B, Matt F. Identity-Based Encryption from the Weil Pairing [C]// Proc of CRYPTO 2001. 2001: 213-229

[27] Sujata M, Bansidhar M, et al. A secure electronic cash based on a certificateless group signcryption scheme[J]. Mathematical and Computer Modelling, 2013(58): 186-195

[28] Wang Chang-ji, Huang Jia-sen. Attribute-based Signcryption with Ciphertext-policy and Claim-predicate Mechanism[C]// Proc of Seventh International Conference on Computational Intelligence and Security. 2011: 905-909

[29] Keita E, Atsuko M, et al. Toward Dynamic Attribute-Based Signcryption[C]// Proc of ACISP 2011. 2011: 439-443

[30] Fan Chun-i, Wu Chien-nan, et al. Attribute-based strong designated-verifier signature scheme[J]. The Journal of Systems and Software, 2012(85): 944-959