防窃听的弱安全网络编码

武 萌,吴 蒙
(南京邮电大学,江苏 南京 210003)

摘 要:网络编码可以达到网络的最大理论多播容量,它的提出是通信领域的一项重要突破。在网络编码实际应用中,安全问题不可忽视。文中提出了一种防窃听的弱安全 VSWNC 算法。首先 VSWNC 要求信源信宿共享一个随机数生成器;其次信源端可用随机种子 r 在随机数生成器上生成一个范德蒙行列式 P,随后用 P 对信源信息进行预编码处理;最后信宿端可通过 r 得到 P 从而正确解码。把 VSWNC 算法应用于随机网络编码中,在牺牲少量带宽的情况下能保证以概率 1 达到弱安全要求。

关键词:网络编码;弱安全;窃听网络
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2014)10-0167-03
doi:10.3969/j.issn.1673-629X.2014.10.040

A Weakly Secure Network Coding against Wiretap Attack

WU Meng, WU Meng
(Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Network coding can achieve the theoretical multicast capacity of a network, and it is an important breakthrough in communication field. The security is an important issue when network coding is used in practical network. In this paper, provide a VSWNC algorithm, which is weakly secure network coding algorithm against wiretap attack. Firstly, in VSWNC algorithm the source and the destination share a random number generator. Secondly, in source node, a Vandermonde determinant P is generated using random number r in the random number generator and source message can be pre-coded using matrix P. Finally, user node can decode correctly using matrix P achieving from r. Using VSWNC in random network coding, can achieve the weakly secure condition at probability of one with sacrificing a small amount of capacity.

Key words: network coding; weakly secure; network of wiretap

0 引 言

网络编码由 Ahlswede 等人[1]在 2000 年首次提出,其思想是允许网络中间节点对其收到的信息进行编码整合后再转发。随后 Li 等人[2]证明了线性网络编码可获得网络最大组播容量。网络编码引来的安全问题主要分为窃听攻击和拜占庭攻击两种,比普通网络的安全问题更不容忽视,将严重影响网络的可靠性和有效性。文中主要研究防窃听攻击的安全网络编码问题。Cai 等人[3]提出了防窃听的安全网络编码思想,随后 Cai 等人[4-5]进一步提出了 r-安全网络编码算法,并给出了构造线性网络编码的充要条件及编码构造的优化方法。以上这些安全网络编码算法均为基于信息论安全。Bhattad 等人[6]提出了弱安全网络编码,只要窃听者无法获得任何有用信息即可。Harada 等人[7]提出了一种强安全网络编码,其在窃听者一次可窃听到的边数大于 r 时,保证只有秘密消息向量中最后的若干分量被泄露。罗明星等人[8]定义了广义攻击模型,推广了 All-or-nothing 变换。俞立峰等人[9]对现有防窃听的安全网络编码的方法做了总结分析和比较。王骁等人[10]提出了一种基于哈希函数安全网络编码算法。徐光宪等人[11]提出了基于混沌序列的低开销的安全网络编码方案。王永建等人[12]从网络覆盖方向研究基于网络编码的无线传感器网络的防窃听技术。刘琼等人[13]利用大素数及其本原根提出基于信息论安全的网络编码方案。

收稿日期:2013-11-07 **修回日期**:2014-02-15 **网络出版时间**:2014-07-17
基金项目:江苏省高校自然科学研究重大项目(10KJA510035)
作者简介:武 萌(1988-),女,河南三门峡人,硕士研究生,研究方向为无线通信中的信号处理;吴 蒙,教授,博士生导师,研究方向为无线通信与信息安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20140717.1229.021.html

1 网络编码

1.1 网络编码基本概念

通信网络可用有向图 $G=(V,\varepsilon)$ 来表示,其中 V 代表节点集合, ε 代表边集合, $\varepsilon=\{(u,v)\mid u,v\in V\}$。节点包含信源 s,中间节点和信宿节点 t。文中主要研究单信源多信宿无环网络。信宿集合用 T 表示,假设有 k 个信宿,则 $T=\{t_1,t_2,\cdots,t_k\}$ $(i=1,2,\cdots,k)$。信源 s 发出的信息为

$$\boldsymbol{X}=\begin{bmatrix}x_{11} & x_{12} & \cdots & x_{1M}\\ x_{21} & x_{22} & \cdots & x_{2M}\\ \vdots & \vdots & \ddots & \vdots\\ x_{N1} & x_{N2} & \cdots & x_{NM}\end{bmatrix}=\begin{bmatrix}\boldsymbol{X}_1\\ \boldsymbol{X}_2\\ \vdots\\ \boldsymbol{X}_N\end{bmatrix}$$

其中, $\boldsymbol{X}_i\in M$, M 为信源信息集, N 小于网络多播容量,即网络的最大流最小割值。

网络编码具有全局编码核 $\boldsymbol{f}_e$ ($e\in\varepsilon$)。每个信道 $e\in\varepsilon$ 上传输的消息为 $Y_e=f_e(X)\in F$, F 为传输字符集。除信宿节点外其他节点均不能识别和恢复信源消息 X。在线性编码中, $\boldsymbol{f}_e$ 为线性函数,则 $\boldsymbol{f}_e$ 为 N 维向量,所有边上的全局编码向量构成矩阵 $\boldsymbol{F}$。

1.2 防窃听安全网络编码模型

Cai 和 Yeung 提出了一种防窃听的网络模型,表示为(G,S,T,W)。

定义 1:网络窃听模型。

(1) G 为文中介绍的无环单源多信宿有向图;

(2) S 为信源节点,产生随机信息 X^n ;

(3) T 为信宿节点集合,信宿节点可以无差错地恢复信源发出的信息 X^n ;

(4) W 为窃听集, $W=\{W_1,W_2,\cdots,W_k\}$ 。 W 中的边都有可能完全被窃听者窃听, W_i 中包含若干个信道,这些信道是窃听者一次能窃听到的信道。 W_i 中信道的编码向量组成的矩阵为窃听矩阵 $\boldsymbol{\omega}_i$,则窃听者收到的信息为 $\boldsymbol{\omega}_i\boldsymbol{X}$ 。

为了保护信源发出的信息不被窃听者窃听,可对信源信息进行随机化处理。

$$\boldsymbol{X}=(X_1,X_2,\cdots,X_n)=(m_1,m_2,\cdots,m_{n-r},k_1,k_2,\cdots,k_r)$$

其中, $(m_1,m_2,\cdots,m_{n-r})$ 表示原始信息; $(k_1,k_2,\cdots,k_r)$ ($k_i\in K$, K 为密码字符集)表示随机密钥。

定义 2:t-窃听网络。

如果一个网络的窃听集中所有子集包含的信道数不超过 t,则这个网络就称为 t-窃听网络。 t-窃听网络上的安全网络编码称为 t-安全网络编码。

1.3 安全条件

信息论安全是指窃听者无法获得任何信源发出的消息。

定义 3:在窃听网络(G,S,T,W)中,网络编码若是信息论安全的,必须满足如下条件:

(1)解码条件:对于任何信宿节点 $t\in T$,获得的信息包由 $\varphi_t(M,K)$ 表示,则对于任意 $M_1,M_2\in M$,只要 $M_1\neq M_2$,则 $\varphi_t(M_1,K_1)\neq\varphi_t(M_2,K_2)$, K_1,K_2 可能相等也可能不相等。

(2)安全条件:对于任何窃听集 W,有 $H(M\mid Y_W)=H(M)$,其中 Y_w 表示 $e\in W$ 上的传输的信息包。

在实际应用中,没有必要在任何情况下都保证信息论安全。只要窃听者无法获得任何关于信源消息的有用信息即可。

定义 4:如果窃听者无法通过正确解码获得 m_i ($i=1,2,\cdots,n-r$) ,则网络编码是弱安全的。

由于弱安全网络编码放宽了安全条件,相对于信息论安全来说,可以提高编码的最大多播速率。

如图 1 所示,网络的多播容量为 2,图中 x_1,x_2 代表源信息, r 代表随机密钥。图 1(a)中每条边上传送的信息均为 $ax_1+br(b\neq0)$,可得 $I(x_1\mid ax_1+br)=0$,因此(a)中描述的编码算法是信息论安全的,此网络中信息论安全的最大速率为 1。(b)中每条边上传送的信息为 $ax_1+bx_2(a,b\neq0)$,可知当 a 和 b 都不为 0 时, $I(x_1\mid ax_1+bx_2)=0$, $I(x_2\mid ax_1+bx_2)=0$,即此编码算法是弱安全的,可达到多播容量 2。在弱安全条件下,信源信息可以不含有随机密钥,即 $\boldsymbol{X}=(X_1,X_2,\cdots,X_n)=(m_1,m_2,\cdots,m_n)$。

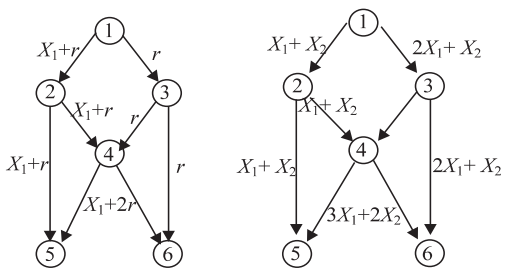

图 1 编码算法示意图

图 1 中源节点传输信源消息的线性组合,即 $\boldsymbol{PX}$,由文献[3,5]可知,通过选取合适的矩阵 $\boldsymbol{P}$, 可以使一般的网络编码转变为安全网络编码,分别达到信息论安全和弱安全。

2 VSWNC 编码算法

VSWNC 是利用范德蒙行列式的弱安全网络编码算法,它假设信源信宿共享一个随机数生成器。信源发出的消息为 $\boldsymbol{X}$,信宿收到的消息为 $\boldsymbol{Z}$,则 $\boldsymbol{Z}=\boldsymbol{FX}$。

2.1 信源端编码

(1)信源在有限域 M 上选取一个随机数 r,然后用这个初值 r 在随机数生成器生成 $N-1$ 个随机数。 r_1,

$r_2,\cdots,r_{N-1}$ 这 $N-1$ 个数构成范德蒙行列式。种子 r 是对窃听者保密的。

$$\boldsymbol{P}=\begin{bmatrix}1 & 1 & \cdots & 1\\ 1 & r_1 & \cdots & r_{N-1}\\ \vdots & \vdots & \ddots & \vdots\\ 1 & r_1^{N-1} & \cdots & r_{N-1}^{N-1}\end{bmatrix}$$

(2) $\boldsymbol{X}$ 左乘 $\boldsymbol{P}$ 可得到 $\boldsymbol{X}'=\boldsymbol{PX}$。

$$\boldsymbol{X}'=\begin{bmatrix}x'_{11} & x'_{12} & \cdots & x'_{1M}\\ x'_{21} & x'_{22} & \cdots & x'_{2M}\\ \vdots & \vdots & \ddots & \vdots\\ x'_{N1} & x'_{N2} & \cdots & x'_{NM}\end{bmatrix}$$

(3) 在 $\boldsymbol{X}'$ 后加入单位冗余得到 $\boldsymbol{Y}$,其中 $p_1,p_2,\cdots,p_{N-1}$ 为 M 上的随机数。

$$\boldsymbol{Y}=\begin{bmatrix}x'_{11} & x'_{12} & \cdots & x'_{1M} & r\\ x'_{21} & x'_{22} & \cdots & x'_{2M} & p_1\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ x'_{N1} & x'_{N2} & \cdots & x'_{NM} & p_{N-1}\end{bmatrix}$$

经过以上变换,信源就把 $\boldsymbol{Y}$ 传输出去。$\boldsymbol{Y}$ 在网络中进行网络编码,则 $\boldsymbol{Z}=\boldsymbol{FY}$。

2.2　信宿端解码

(1) 信宿收到 $\boldsymbol{Z}$ 后可用公式 $\boldsymbol{Y}=\boldsymbol{F}^{-1}\boldsymbol{Z}$ 获得 $\boldsymbol{Y}$,然后得到 r 和 $\boldsymbol{X}'$。

(2) 信宿以 r 为种子,访问随机数生成器,可以获得 $r_1,r_2,\cdots,r_{N-1}$,进而得到 $\boldsymbol{P}$。

(3) $\boldsymbol{X}=\boldsymbol{P}^{-1}\boldsymbol{X}'$,这样信宿就可以获得信源信息 $\boldsymbol{X}$。

2.3　安全性分析

定理 1:当窃听者窃听到的信道数 k 小于网络多播容量时($k<n$),此编码译码算法可以达到弱安全的要求。

证明:信源在信道中传输的信息是 $\boldsymbol{X}$ 的变换 $\boldsymbol{Y}$。首先要保证信宿可以正确解码。因为矩阵 $\boldsymbol{P}$ 是满秩可逆矩阵,信宿可以通过对 $\boldsymbol{P}$ 求逆,由公式 $\boldsymbol{X}=\boldsymbol{P}^{-1}\boldsymbol{X}'$ 解码。因此 VSWNC 编码方式满足解码条件。

若使得此编码能够达到弱安全的要求,需满足

$$H(\boldsymbol{X}_i\mid\boldsymbol{\omega}_i\boldsymbol{Y})=0\quad i=1,2,\cdots,N \tag{1}$$

先忽略 $\boldsymbol{Y}$ 中最后一列的冗余信息,即证明

$$H(\boldsymbol{X}_i\mid\boldsymbol{\omega}_i\boldsymbol{X}')=0\quad i=1,2,\cdots,N \tag{2}$$

为了达到公式(2),则必须满足

$$\boldsymbol{b}_i\boldsymbol{\omega}_i\boldsymbol{P}\neq\boldsymbol{I}_{N,j}\quad\forall\boldsymbol{b}_i,i,j \tag{3}$$

其中,$\boldsymbol{I}_{N,j}$ 表示 $N\times N$ 单位矩阵的第 j 行;$\boldsymbol{b}_i$ 是为一 N 维向量。

式(3)两边同乘以 $\boldsymbol{P}^{-1}$ 得:

$$\boldsymbol{b}_i\boldsymbol{\omega}_i\neq\boldsymbol{I}_{N,j}\boldsymbol{P}^{-1}\quad\forall\boldsymbol{b}_i,i,j \tag{4}$$

只要 $\boldsymbol{P}^{-1}$ 的任一行向量都不在 $\boldsymbol{\omega}_i$ 的行向量张成的空间上就能满足条件。当 $\boldsymbol{P}$ 由随机数生成器生成后,在 $\boldsymbol{P}^{-1}$ 行向量张成的空间外选择编码矩阵 $\boldsymbol{F}$ 中的行向量,就可满足式(4)。由此定理 1 得证,选取合适的编码矩阵 $\boldsymbol{F}$,存在用此编码方法构造的网络编码符合弱安全的要求。

推论 1:在一个多播容量为 n 的网络中,如果同时被窃听的信道数小于 n,则此网络编码能达到的最大传输速率为 $n-n/m$,编码复杂度为 $O(n^2m)$。

证明:由文献[5]可知,弱安全网络编码可以获得最大传输速率为网络最大流 n,VSWNC 算法引入了冗余为 n 个,因此 VSWNC 算法获得的最大传输速率为 $mn/m-n/m=n-n/m$。

定理 2:在一个多播容量为 n 的网络中,当使用随机网络编码时,如果同时被窃听的信道数小于 n,则此网络编码可以以概率 1 达到弱安全要求。

证明:如果窃听者无法获得 $\boldsymbol{X}$ 到 $\boldsymbol{Y}$ 的变换矩阵,则无法获得有用的信源信息,这样便能达到弱安全的要求。一般情况下,窃听者不会和信源信宿共享同一个随机数生成器,在这种情况下,即使窃听者获得到种子 r,也无法获得产生范德蒙行列式的随机数 $r_1,r_2,\cdots,r_{N-1}$,因此无法获得关于 $\boldsymbol{X}$ 的任何有用信息。这样此编码方法便能以概率 1 满足弱安全要求。

3　结束语

文中针对网络编码中的窃听问题,提出了一种满足弱安全的 VSWNC 算法。VSWNC 算法只需要对信源信息进行预编码,其他节点的编码算法保持不变,在被窃听的信道数小于多播容量时,可达到弱安全的要求。此算法要求信源信宿共享一个随机数生成器,保证信宿通过随机种子可得到矩阵 $\boldsymbol{P}$。同时为了给信宿传送随机种子,编码引入了少量冗余,使最大传输速率降低为 $n-n/m$。在应用随机网络编码时,VSWNC 算法可以以概率 1 达到弱安全的要求。文献[14]中提出,当信源信宿间共享秘密信道时可以以概率 1 达到弱安全,且达到理论多播容量。但在现实网络中尤其是无线网络中保证一个秘密信道的代价是很大的,文中的算法虽然最大传输速率略低于理论多播容量,但易实现。

参考文献:

[1] Ahlswede R, Cai Ning, Li S Y R, et al. Network information flow[J]. IEEE Transactions on Information Theory, 2000, 46(4):1204-1216.

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

(下转第 173 页)

存储,文件服务器主要将上传的文件集中存储。

系统能较好地支持 Ms Office、PDF、TXT 等各类文档的在线预览,能够将支持的各类文档按页转化为 SWF 动画帧,最终通过 Flexpaper 分页进行在线预览,且文档内容可以进行有效缩放。系统文件服务器主要配置:CPU 为 Intel 至强 E5-2600,内存为 8 G。在此配置下对于小于 1 M 的文档,系统转化为 PDF 文件的时间不超过 2 s,生成 SWF 文档的时间小于 5 s;Web 服务器主要配置:CPU 为 Intel 至强 E5-4600,内存为 12 G。在此配置下,针对文档在线预览响应时间低于 1 s,基本能够满足用户文档在线预览的需求。

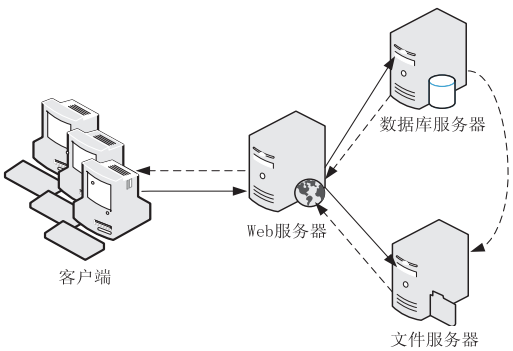

图 3　系统部署图

4　结束语

文中提出了一套在线文档预览解决方案,并在 SSH 框架技术基础上,实现了类似百度、豆丁功能的文库系统,较好地解决了文档在线预览功能,同时实现了基于 RBAC 的细粒度文档安全访问控制机制。目前,该系统已经应用到单位业务工作中,基本满足了单位内部文档管理需求,下一步系统将在文档全文检索方面进行完善。

参考文献:

[1] 陈晗鸣. 基于 PDM 的船舶文档管理系统设计与开发[J]. 舰船科学技术,2012,34(12):131-135.

[2] 王延刚,何　斌,宋　伟,等. 面向工程机械的文档信息管理系统的设计与实现[J]. 计算机与现代化,2013(1):185-188.

[3] 张　奎,李　哲,苑庆涛. 基于网盘的项目文档在线管理系统[J]. 西安邮电学院学报,2012,17(4):71-74.

[4] 陈天河. Struts,Hibernate,Spring 集成开发宝典[M]. 北京:电子工业出版社,2007.

[5] 三扬科技. Struts 核心技术与 JavaEE 框架整合开发实践[M]. 北京:电子工业出版社,2008.

[6] 孙卫琴. 精通 Hibernate:Java 对象持久化技术详解[M]. 北京:电子工业出版社,2006.

[7] Roughley L. Practical Apache Struts2 Web 2.0 projects[M]. [s. l.]:APress,2007.

[8] Linwood J, Minter D. Beginning Hibernate[M]. [s. l.]: APress,2010.

[9] Seddighi A R. Spring persistence with Hibernate[M]. [s. l.]:Packt Publishing Limited,2009.

[10] Fisher M,Partner J,Bogoevici M,et al. Spring integration in action[M]. [s. l.]:Manning Publications,2012.

[11] 李海峰. MVC 模式架构的应用研究[J]. 自动化与仪器仪表,2013(1):4-6.

[12] 赵　伟,王志华,周　兵. 基于 MVC 的 e-ERP 系统的设计与实现[J]. 计算机应用与软件,2013,30(2):106-109.

[13] 李　刚. 轻量级 JavaEE 企业应用实战-Struts2+Spring+Hibernate 整合开发[M]. 第 3 版. 北京:电子工业出版社,2008.

[14] 刘　伟,冯　伟,刘友江. 基于 SSH 和 Acegi 的 Web 应用框架的设计与实现[J]. 软件导刊,2011,10(7):122-124.

[15] 姬朝阳,唐红喜. 基于 SSH 的日志统计分析系统的分析与设计[J]. 计算机技术与发展,2010,20(8):212-216.

(上接第 169 页)

[3] Cai Ning, Yeung R W. Secure network coding[C]//Proc of IEEE international symposium on information theory. [s. l.]: IEEE,2002.

[4] Cai Ning, Yeung R W. Secure network coding on a wiretap network[J]. IEEE Trans on Information Theory, 2011, 57(1):424-435.

[5] Cai Ning, Chan T. Theory of secure network coding[J]. Proceedings of the IEEE,2011,99(3):421-437.

[6] Bhattad K, Naraynan K R. Weakly secure network coding[C]//Proc of the 1st workshop on network coding, theory, and applications. [s. l.]:[s. n.],2005.

[7] Harada K, Yamamoto H. Strongly secure linear network coding[J]. IEICE Trans on Fundamentals of Electronics, Communications and Computer Sciences, 2008, E91-A(10): 2720-2728.

[8] 罗明星,杨义先,王励成,等. 抗窃听的安全网络编码[J]. 中国科学:信息科学,2010,40(2):371-380.

[9] 俞立峰,杨　琼,于　娟,等. 防窃听攻击的安全网络编码[J]. 计算机应用研究,2012,29(3):813-818.

[10] 王　骁,郭网媚,肖鹤玲,等. 基于哈希函数的高效完善安全网络编码算法[J]. 华中科技大学学报:自然科学版,2013,41(5):102-104.

[11] 徐光宪,李晓彤,罗荟荟. 一种基于混沌序列的安全网络编码设计与分析[J]. 计算机科学,2013,40(5):147-149.

[12] 王永建,许俊峰,杨余旺,等. 基于网络编码的传感器网络防窃听技术[J]. 清华大学学报:自然科学版,2011,51(10):1341-1344.

[13] 刘　琼,潘　进,刘　炯. 基于信息论安全的防窃听网络编码方案[J]. 计算机工程,2012,38(22):107-110.

[14] 周亚军,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,2009,36(4):696-701.

防窃听的弱安全网络编码

作者： 武萌， 吴蒙
作者单位： 南京邮电大学,江苏 南京,210003
刊名： 计算机技术与发展 ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2014(10)