窃听攻击下子空间码的安全性

刘宴涛[1] 王雪冰[2]
(渤海大学工学院 锦州 121000)[1] (中国石油大学胜利学院 东营 257061)[2]

摘 要 子空间码与随机线性网络编码相结合的网络系统具有编译码复杂度低、无需附加编码矢量和非相干通信等优点,曾被用于网络纠错。针对子空间码在窃听攻击下的安全性能,将攻击者猜测信源消息的成功概率作为子空间码的安全性度量。基于 Cai 和 Yeung 提出的网络窃听模型,采用线性代数和组合学方法,定量计算了攻击者的猜测概率并得到了闭式解。分析结果表明,子空间码具有概率意义下的弱安全性,但与许多完美安全或弱安全编码方案相比,子空间码具有复杂度低、灵活性高、拓扑不受限、可对抗多边窃听等优势,因此子空间码适用于计算受限且安全性能要求不高的应用。

关键词 网络安全,窃听攻击,子空间码
中图法分类号 TP393 **文献标识码** A

Security of Subspace Code against Wiretap Attacks

LIU Yan-tao[1] WANG Xue-bing[2]
(College of Engineering, Bohai University, Jinzhou 121000, China)[1]
(Shengli College, China University of Petroleum, Dongying 257061, China)[2]

Abstract The network system in combination of subspace code and random linear network coding has the advantages of low complexity of encoding and decoding, there is no need to attach coding vectors, and noncoherent communications, and it has been applied for network error correcting. This paper addressed the security of subspace code against wiretap attacks. The security performance is measured in the probability with which the attacker guesses source messages. Based on the wiretap network model proposed by Cai and Yeung, we quantitatively calculated the guess probability with the methods of linear algebra and combinatorics and obtained its closed form solution. The result shows that subspace code has weak security in the sense of probability. Compared to many coding schemes with perfect security or weak security, however, subspace code benefits from low complexity, high flexibility, topology independence, and capability of fighting wiretaps on multiple links. As a result, subspace code is suitable to network applications with limited calculations and moderate security requirements.

Keywords Network security, Wiretap attack, Subspace code

1 引言

窃听攻击是指攻击者通过窃听通信链路中传输的数据以获取有用信息,属于被动攻击的一种形式。由于窃听攻击不干扰正常的通信过程,因此不易被通信方察觉。在对抗窃听攻击方面,不同的通信传输机制表现出不同的能力。一般来讲,网络的传输机制可以分为两大类:路由和编码。传统路由网络采用存储-转发的传输机制,网络节点只被允许忠实地转发数据包,而不允许对收到的数据包做任何改动,因此网络链路上传输的数据包和信源发出的数据包是相同的,只要窃听者截获了链路上的数据包,就可以获得信源的消息,可见路由机制是一种"所见即所得"的传输方式。在路由网络中,通常采用信源至信宿端到端加密的方法来对抗窃听攻击。网络编码采用存储-编码-转发的传输机制,即允许中间节点对接收到的数据包进行编码操作从而产生新的数据包向后继节点转发,因此网络链路上传输的数据包并不是信源发出的原始数据包,可见网络编码属于一种"所见非所得"的传输机制。在这种机制下,无论是授权接收方还是窃听攻击者,如果想通过译码恢复信源消息,必须具备两个条件[1]:1)接收到足够多的数据包;2)掌握全部的编码规则,如全局编码矢量等。授权接收方是具备这两个条件的,但对于非授权的窃听者来说,则需要具备比对路由网络攻击更强的能力。由此可见,在对抗窃听攻击方面,编码网络比路由网络具有天然的优势和更好的性能。图 1 比较了路由网络和编码网络的传输机制,其中,有限字母集取为有限域 F_5,信源消息为 d_1 和 d_2,在编码网络中传输的数据 d_3 和 d_4 对应的全局编码矢量分别为$(g_{11},g_{12})=(1,1)$,$(g_{21},g_{22})=(1,2)$,编码如下:

$$d_3=g_{11}d_1+g_{12}d_2=1*1+1*2=3$$

$$d_4=g_{21}d_1+g_{22}d_2=1*1+2*2=0$$

由图 1 可知,路由网络中传输的数据是信源数据的精确再现,而编码网络中传输的数据则与信源数据完全不同。

本文受国家自然科学基金项目(61471045,61227001)资助。

刘宴涛 男,博士,副教授,主要研究方向为 ad hoc 网络、网络编码和网络仿真等;王雪冰(1974-),男,硕士,副教授,主要研究方向为软件定义网络、公共安全网络和车际网络等,E-mail:bbxxww2002@163.com。

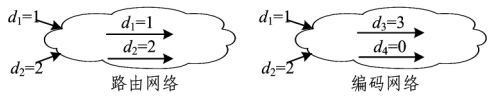


图 1　路由网络与编码网络的比较

进一步，如果对编码网络的攻击者具有更强的攻击能力使得上述两个必要条件能够得到满足，则窃听者可以破译信源消息。在这种情况下，为了探索更强有力的安全网络编码方案，Cai 和 Yeung [2] 提出了窃听网络模型（Wiretap Network Model-WNM）：

定义 1[2]　WNM 由四元组(G,S,R,A)构成：

1）有向无环图 $G=(V,E)$，V 和 E 分别代表顶点集和边集。

2）源节点 $S\in V$。

3）一组接收节点 $R=\{r_i:r_i\in V\}$。

4）窃听边集 $\mathrm{A}=\{A:A\subset E\}$，窃听者可以窃听 A 的某个实例（又称窃听图样）。

还有一种 WNM 的定义[3]不是指定窃听边的集合，而是限制窃听边的数目，如$|A|\leqslant r$，本文称其为 r-WNM。

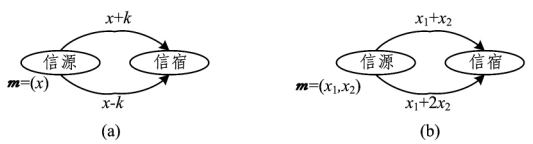
基于 WNM 或 r-WNM，研究者提出了很多安全网络编码方案。根据安全强度的不同，这些方案可以被划分为 3 类：弱安全[4]、完美安全[5]和强安全[6]。以下用 $\boldsymbol{m}=(m_1,\cdots,m_n)$ 表示信源消息，用 $\boldsymbol{y}_A$ 表示在边集 A 上被窃听的符号集合。

1）弱安全是指保护每个信源符号 m_i 不被窃听者解析，即 $H(m_i|\boldsymbol{y}_A)=H(m_i)$。弱安全可以基于精心设计的线性网络编码[4,7]、加密[8-13]或变换[14]实现，其优势在于复杂度低且安全网络容量与非安全编码容量相同，即没有网络容量损失。

2）完美安全又称信息论安全[5]，旨在保护信源的信息量不被泄露，即满足 $H(\boldsymbol{m}|\boldsymbol{y}_A)=H(\boldsymbol{m})$。完美安全网络编码方案可以基于预编码[3,5]、陪集码[15]或秩度量码[16]。完美安全实现了对信源信息的最大程度保护，但完美安全网络编码复杂度高且不可避免地存在着网络容量的损失。

3）如果完美安全被打破，则窃听者一定可以获得关于信源的部分信息量，在这种情况下，强安全编码[6]应用秘密分享策略极大地减少了信息量的泄露。

图 2 示出了两种简单的完美安全和弱安全编码方案，字母集取为有限域 F_3。其中，图 2(a)为 $r=1$ 完美安全的 1-WNM，信源符号 x 首先与随机符号 k 进行运算，然后发到网络链路上，无论窃听者截获哪条边上的符号，都无法获得关于 $\boldsymbol{m}$ 的信息，即 $H(\boldsymbol{m}|\boldsymbol{y}_A)=H(\boldsymbol{m})$；图 2(b)是 $r=1$ 弱安全的 1-WNM，该方案不使用随机符号，网络链路上传输的是信源符号 x_1 和 x_2 的线性组合，不难验证 $H(x_i|\boldsymbol{y}_A)=H(x_i)$，也就是说窃听者仅仅通过单一链路截获的数据无法求解 x_1 和 x_2，但$I(\boldsymbol{m};\boldsymbol{y}_A)>0$，即窃听者可以获得关于信源消息 $\boldsymbol{m}$ 的部分信息。



(a)完美安全　　(b)弱安全

图 2　完美安全与弱安全的比较

子空间码与随机线性网络编码相结合具有编译码复杂度低、不需要附加编码矢量和非相干通信等优点，曾被用于网络纠错。基于 r-WNM 模型，本文分析了子空间码在窃听攻击下的安全性能。本文第 2 节给出了子空间码的工作原理；第 3 节定量计算了在使用子空间码的随机网络编码系统中，窃听者猜测信源消息的成功概率；第 4 节将子空间码和一些完美安全和弱安全编码方案做了比较和讨论；最后对全文进行总结。

2　子空间码

子空间码属于阵列码的一种，与矢量编码不同，阵列码使用矩阵表示信源消息。在子空间码中，消息被映射为一个 n 维全矢量空间的某个子空间，消息码字被表示为子空间的基向量排成的矩阵。传输时，信源把该矩阵的全部行向量发到网络中，这些向量经历网络中间节点的网络编码操作后到达信宿节点，信宿根据收到的向量计算和识别子空间，从而完成译码。后文把定义在有限域 F_q 上的 n 维全矢量空间记为 F_q^n。图 3 是基于 4 维矢量空间 F_5^4 的一个子空间码编码网络，其中两个消息‘A’和‘B’对应的子空间如下：

‘A’$=\{(1000),(0100),(0010)\}$

‘B’$=\{(0100),(0010),(0001)\}$

以消息‘A’的传输为例：信源向网络中发送的是‘A’所对应的子空间的 3 个基向量，经过网络的传输和随机网络编码操作，信宿收到 3 个向量，通过对子空间的计算和比对，信宿可以识别出消息符号‘A’。

图 3　子空间码传输示意

在子空间码的码书中，如果全部许用码字所对应的子空间的维数相同，则称该子空间码为恒维子空间码。恒维子空间码由于编译码简单获得了最广泛的研究和应用。Kötter 和 Kschischang[17]针对子空间码定义了一种子空间距离度量 $d(A,B):=dim(A+B)-dim(A-B)$，并利用该距离的最小距离译码，从而实现对随机网络编码系统的网络纠错。Zhang 等[18]巧妙地利用了线性网络编码的子空间保持特性提出了一种高效的子空间鉴权方法用于对抗污染攻击。Fang 等[19]为了对抗非法数据篡改，为发送的子空间生成数字签名并发送到网络中，网络节点如果检测到接收的数据包不属于该子空间则丢弃，从而尽可能早地发现并阻止污染蔓延。目前，针对子空间码的研究主要集中在网络纠错和对抗主动攻击等方面，然而在窃听攻击的敌对环境中，采用子空间码的随机网络编码系统的安全性能尚属未知。针对这一问题，本文采用概率和组合学的方法着重分析了恒维子空间码在对抗窃听攻击时的安全性能。

3　子空间码的安全性分析

子空间码使用随机网络编码作为底层传输网络，但是定性地看，子空间码的安全性要优于标准的随机网络编码[20]，这是因为后者要求在数据包中附加全局编码矢量用于信宿端译码，这种方式将导致一旦网络中传输的数据包被截获，窃听者将同时获得编码矢量和码字，从而增加了码字被破译的风险；而在使用子空间码的编码网络中，只有码字在网络中传输，数据包中不需要附加编码矢量，因此降低了码字被破译的

风险。下面对子空间码的安全性做定量分析。

3.1 问题描述

考察一个随机线性编码网络，信源信宿使用基于 F_q^n 的 k 维子空间码，网络中存在着一个窃听者 Eve 能够窃听到 l 条链路上传输的数据矢量，假设 Eve 掌握子空间码的全部先验知识，包括码书和全空间 F_q^n 等。从这个意义上讲，Eve 和授权接收者具有相同的知识，只不过授权接收者能够接收到 k 个数据矢量[1)]，而 Eve 只能接收到 l 个数据矢量。Eve 的目的是通过这 l 个数据矢量识别出信源发送的消息，因此 l 度量了 Eve 的攻击能力：如果 $l\geqslant k$，则 Eve 可以毫无疑义地译码，此时 Eve 和授权接收者具有相同的能力；如果 $l<k$，则 Eve 不能精确地译码，然而它能够以一定的概率 P_l 猜测出信源发送的是哪一条消息。可见，这个猜测概率 P_l 定量地描述了子空间码的安全性，此概率越大，则安全性越差。下面我们应用线性代数和组合学方法计算这一概率。在此之前，首先给出组合学的一个计数结果：矢量空间 F_q^n 的全部 k 维子空间的数目为：

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)} \tag{1}$$

这个数在组合学[21]中也被称为高斯系数。在恒维子空间码中，假设全部 k 维子空间都被用于许用码字，则码书的大小就是该系数。

3.2 猜测概率 P_l

下面具体计算 P_l，显然 P_l 应该是 n,l,k,q 的函数。不失一般性，记 l 个被截获的矢量为 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_l$，则有

定理 1 在向量空间 F_q^n 中，包含矢量 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_l$ 的 k 维子空间的个数为：

$$M_l=\frac{(q^{n-l}-1)(q^{n-l-1}-1)\cdots(q^{n-k+1}-1)}{(q^{k-l}-1)(q^{k-l-1}-1)\cdots(q-1)} \tag{2}$$

证明：首先，不失一般性，记包含矢量 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_l$ 的 k 维子空间的基为 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_l,\boldsymbol{V}_{l+1},\cdots,\boldsymbol{V}_k$，由于 $\boldsymbol{V}_{l+1}$ 不能等于 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_l$ 的任何线性组合，因此 $\boldsymbol{V}_{l+1}$ 有 q^n-q^l 个可能的取值。同理，如果记 $\boldsymbol{V}_i:(l+1\leqslant i\leqslant k)$ 的可能取值的个数为 $N(\boldsymbol{V}_i)$，则有：

$$\begin{cases} N(\boldsymbol{V}_{l+1})=q^n-q^l \\ N(\boldsymbol{V}_{l+2})=q^n-q^{l+1} \\ \cdots \\ N(\boldsymbol{V}_k)=q^n-q^{k-1} \end{cases} \tag{3}$$

因此，包含 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_l$ 的全部可能的 k 维子空间的基的个数为：

$$(q^n-q^l)(q^n-q^{l+1})\cdots(q^n-q^{k-1}) \tag{4}$$

其次，分析某个具体的包含 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_l$ 的 k 维子空间 S_i 的基的个数。仍然记 S_i 的基为 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_l,\boldsymbol{V}_{l+1},\cdots,\boldsymbol{V}_k$，经过同样的分析可以得到 $\boldsymbol{V}_i:(l+1\leqslant i\leqslant k)$ 可能取值的个数为 $N'(\boldsymbol{V}_i)$：

$$\begin{cases} N'(\boldsymbol{V}_{l+1})=q^k-q^l \\ N'(\boldsymbol{V}_{l+2})=q^k-q^{l+1} \\ \cdots \\ N'(\boldsymbol{V}_k)=q^k-q^{k-1} \end{cases} \tag{5}$$

因此，对于某一特定的 k 维子空间 S_i 来说，包含 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_l$ 的可能的基的个数为：

$$(q^k-q^l)(q^k-q^{l+1})\cdots(q^k-q^{k-1}) \tag{6}$$

联立式(4)和式(6)，可以得出包含 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_l$ 的不同的 k 维子空间的个数为：

$$\begin{aligned} M_l &= \frac{(q^n-q^l)(q^n-q^{l+1})\cdots(q^n-q^{k-1})}{(q^k-q^l)(q^k-q^{l+1})\cdots(q^k-q^{k-1})} \\ &= \frac{(q^{n-l}-1)(q^{n-l-1}-1)\cdots(q^{n-k+1}-1)}{(q^{k-l}-1)(q^{k-l-1}-1)\cdots(q-1)} \end{aligned} \tag{7}$$

由于假设 F_q^n 的全部 k 维子空间都用于许用码字，因此 M_l 就是包含被截获矢量 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_l$ 的可能的码字(即子空间)个数。另外，对比式(1)不难发现，式(1)正是式(2)在 $l=0$ 时的特殊情况。为了计算 P_l，进一步假设信源的消息服从均匀分布，即 F_q^n 的全部 k 维子空间服从等概分布。基于此，当 Eve 截获了 $\boldsymbol{V}_1,\cdots,\boldsymbol{V}_l$ 时，其准确猜测出信源发送的子空间的概率为：

$$P_l=\frac{1}{M_l}=\frac{(q^{k-l}-1)(q^{k-l-1}-1)\cdots(q-1)}{(q^{n-l}-1)(q^{n-l-1}-1)\cdots(q^{n-k+1}-1)} \tag{8}$$

取参数 $n=8,q=2,k=6$，绘制 P_l 与 l 的函数关系如图 4 所示。由图 4 可知，P_l 随 l 的增大而增大，也就是说 Eve 截获的数据包越多，其猜中的概率就越大。

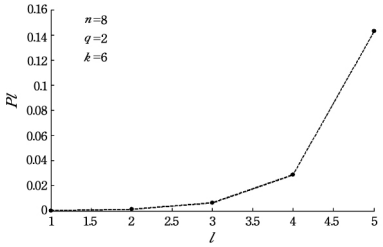


图 4 猜测概率 P_l 随着 l 的增大而增大

此外，为了观察 P_l 与 k 的函数关系，取 $l=k-1$，此时有

$$P_l=\frac{(q-1)}{(q^{n-k+1}-1)} \tag{9}$$

P_l 和 k 的函数关系如图 5 所示，由图 5 可知在有限域 F_q、矢量维数 n 和截获的数据矢量个数 l 都固定的情况下，恒维子空间码的维数 k 越小，安全性能越好。

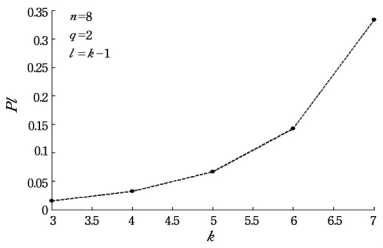


图 5 P_l 随着 k 的增大而增大

3.3 信息泄露

计算 Eve 从 l 条被窃听的边上获取的信息量如下：

$$\begin{aligned} I(\boldsymbol{m};\boldsymbol{y}_A) &= H(\boldsymbol{m})-H(\boldsymbol{m}|\boldsymbol{y}_A) \\ &= \log\begin{pmatrix} n \\ k \end{pmatrix}_q - \log(M_l) \\ &= \log\left[\frac{(q^n-1)\cdots(q^{n-l+1}-1)}{(q^k-1)\cdots(q^{k-l+1}-1)}\right] \\ &\quad (\text{比特}/\ l\ \text{矢量}) \end{aligned} \tag{10}$$

1) 以下默认节点接收的数据矢量彼此独立。

4　比较与讨论

由式(10)可知，在使用子空间码的网络中存在着信息泄露，因此子空间码不满足完美安全。然而，需要说明的是很多安全网络编码方案是以增加系统复杂度为代价的，系统安全性的提升要付出额外的开销，比如预编码[5]、陪集码[15]、加密[8-13]或复杂的网络编码算法[7]等，而子空间码的复杂度和开销远远低于这些方法。

以文献[7]为例，Adeli 和 Liu 设计了一种线性网络编码算法用于实现 1-WNM。该算法的基本思想很简单：为了防止任何一个消息符号 m_i 从任意一条链路泄露出去，只需要保证网络中任意一条链路的全局编码矢量不等于单位矢量 $\boldsymbol{u}_k=(0,\cdots,0,1,0,\cdots,0)$ 或 $\boldsymbol{u}_k$ 的倍数即可。为此，他们提出了一个本地编码矢量分配策略，如图 6 所示，该方法为某个节点 t 分配本地编码矢量时，需要检测该节点的所有输出边是否满足上述约束条件，即需要保证：

$$\boldsymbol{g}(e_j')=\sum_{i=1}^{|in_t(t)|}l_{ij}\cdot\boldsymbol{g}(e_i)\neq m\cdot\boldsymbol{u}_k \tag{11}$$

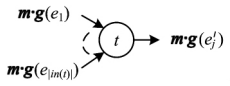


图 6　网络节点的编码

图 6 和式(11)中，l_{ij} 是本地编码系数，e_i 表示节点 t 的入边，e_j' 表示节点 t 的出边，$g(e)$ 是边 e 的全局编码矢量。这种编码矢量的分配和检测要对网络中所有节点和所有边依拓扑序进行。因此，即使针对固定拓扑网络，该方法也需要引入大量的迭代才能保证式(11)成立，从而导致了非常高的计算复杂度。这一问题对于动态拓扑网络更为严重，很可能迭代还没有完成，网络拓扑就已经发生变化，因此导致该方法不可用。与文献[7]相比，子空间码具有明显的优势。首先，文献[7]仅仅针对 1-WNM 有效，即窃听者只能从单一链路窃听数据包，如果窃听者能窃听多条链路，则该方法失效；而子空间码则实现了 r-WNM($r\geqslant1$)在概率意义上的安全，因此适用范围更广。在图 4 中，点($l=1$，$P_l=0.0004$)对应着子空间码针对 1-WNM 的安全性能，可见 Eve 猜测成功的概率 P_l 是很小的，也就是说该子空间码系统针对 1-WNM 的安全性是很高的。其次，子空间码的编译码复杂度远远低于文献[7]，在应用子空间码的系统中，信源只需要把消息映射为子空间，网络的中间节点只需要执行常规的随机网络编码操作，信宿需要根据接收到的 k 个数据矢量计算和识别子空间，这可以应用高斯消去法完成，复杂度为 $O(kn)$。最后，由于子空间码的非相干通信属性对拓扑变化不敏感，因此子空间码既适用于固定网络又适用于移动网络，而文献[7]仅能工作于固定网络。子空间码和文献[7]的比较如表 1 所列。

表 1　子空间码与文献[7]的比较

网络编码方案	拓扑	复杂度	适用性
文献[7]	固定	高	1-WNM
子空间码	可变	低	r-WNM

除了低复杂度外，与许多安全编码方案相比，子空间码在灵活性和适用性上还具有的一些优势，比如：所有的完美安全编码和基于加密的弱安全编码方案都需要在信源信宿之间增加一条额外的私密链路，用于在信源信宿之间分享编码矩阵、密钥或 Hash 函数等，这无疑进一步增加了系统的复杂性和安全风险，子空间码则免除了这一要求。此外，大部分完美安全编码方案仅仅是针对固定拓扑网络有效的。几种安全网络编码方案的比较如表 2 所列。

表 2　安全网络编码方案的比较

编码方案	安全级	拓扑	方法	私密链路
文献[3,5,15-16]	完美	固定	预编码	需要
文献[8]	弱	可变	加密	需要
文献[10]	弱	可变	Hash 函数	需要
文献[7]	弱	固定	网络编码算法	不需要
文献[9,11]	弱	可变	置换加密	需要
子空间码	概率	可变	无	不需要

结束语　本文定量分析了子空间码在窃听攻击下的安全性能。基于 Cai 和 Yeung 的网络窃听模型，以其截获的数据包个数 l 来度量窃听者的攻击能力，以窃听者成功猜中信源消息的猜测概率 P_l 来度量子空间码的安全性能。应用线性代数和组合学方法，计算得到 P_l 的闭式解。分析结果表明，子空间码不具备完美安全性，但具有概率意义下的弱安全性。此外，相比许多完美安全和弱安全编码方案，子空间编码具有编译码复杂度低、灵活度高、不依赖网络拓扑和私密链路且可对抗 r-WNM 等优点。因此，子空间码适用于中等安全要求且计算能力受限的网络应用。

参 考 文 献

[1] LI S Y R, CAI N, YEUNG R W. Linear Network Coding[J]. IEEE Transactions on Information Theory, 2003, 49(2): 371-381.

[2] CAI N, YEUNG R W. Secure Network Coding [C]// International Symposium on Information Theory (ISIT'02). 2002: 323.

[3] FELDMAN J, MALKIN T, STEIN C, et al. On the capacity of secure network coding [C] // Proc. of Allerton Conference. 2004: 1-10.

[4] BHATTAD K, NARAYANA K R. Weakly secure network coding[C] // Proc. First Workshop on Network Coding, Theory, Appl. (NetCod'05). 2005: 1-6.

[5] NING C, YEUNG R W. Secure Network Coding on a Wiretap Network[J]. IEEE Transactions on Information Theory, 2011, 57(1): 424-435.

[6] HARADA K, YAMAMOTO H. Strongly secure linear network coding[M]. Oxford University Press, 2008.

[7] ADELI M, LIU H. On the Inherent Security of Linear Network Coding [J]. Communications Letters, IEEE, 2013, 17 (8): 1668-1671.

[8] VILELA J P, LIMA L, BARROS J. Lightweight security for network coding[C] // Proc. 2008 IEEE Int. Conf. on Comm.. 2008: 1750-1754.

[9] YAWEN W, ZHEN Y, GUAN Y. Efficient Weakly-Secure Network Coding Schemes against Wiretapping Attacks[C] // 2010 IEEE International Symposium on Network Coding (NetCod). 2010: 1-6.

[10] ADELI M, HUAPING L. Secure network coding with minimum overhead based on hash functions[J]. Communications Letters, IEEE, 2009, 13(12): 956-958.

[11] PENG Z, YIXIN J, CHUANG L, et al. P-Coding: Secure Network Coding against Eavesdropping Attacks[C] // 2010 Proceedings IEEE INFOCOM. 2010: 1-9.

[12] 武萌，吴蒙. 防窃听的弱安全网络编码[J]. 计算机技术与发展，2014(10): 167-169.

[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] 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):237-246.
[15] EL ROUAYHEB S Y,SOLJANIN E. On Wiretap Networks II [C]// IEEE International Symposium on Information Theory, 2007(ISIT 2007). 2007:551-555.
[16] SILVA D,KSCHISCHANG F R. Security for wiretap networks via rank-metric codes[C]// IEEE International Symposium on Information Theory,2008(ISIT 2008). 2008:176-180.
[17] KOETTER R,KSCHISCHANG F R. Coding for Errors and Erasures in Random Network Coding[J]. IEEE Transactions on Information Theory,2008,54(8):3579-3591.
[18] ZHANG P,JIANG Y,LIN C,et al. Padding for Orthogonality: Efficient Subspace Authentication for Network Coding[C]// Infocom 2011. 2011:1026-1034.
[19] FANG Z,KALKER T,MEDARD M,et al. Signatures for Content Distribution with Network Coding[C]// IEEE International Symposium on Information Theory, 2007 (ISIT 2007). 2007: 556-560.
[20] TRACEY H,MEDARD M,KOETTER R,et al. A Random Linear Network Coding Approach to Multicast [J]. IEEE Transactions on Information Theory,2006,52(10):4413-4430.
[21] VAN LINT J H,WILSON R M. A Course in Combinatorics (2nd ed)[M]. Cambridge,U. K. :Cambridge Univ. Press,2001.

(上接第 350 页)

的几个等级的集合中进行比对,而新模型通过计算安全值,将主客体安全特性通过更加精细的方法表达出来,然后再通过安全限进行规范和约束,打破了集合的约束,将主体所能访问的客体范围与自身安全值相关,每个主体都拥有自己单独的可访问空间,而不再是有限的几个集合之间进行比较,增加访问控制的灵活度,使得主客体间的访问控制进一步规范化。

(2)关于安全限在访问控制中的安全方面。本文尝试将主体安全值放大到一个特定的范围,从而增加其可同时读写的客体的范围,增加访问控制的灵活性,但是,这同样存在部分隐患,当主体的保密值扩展为保密值限时,主体就可以在适当范围内同时读写部分比自身安全值高的或比自身安全值低的客体,这样势必会影响客体的安全特性,而本文采取的方法并不能详尽规避其中所有缺点,如隐蔽通道的问题(若主体通过特定方法将自身安全限系数无限放大,那么主体就可以读写全局所有客体)。另外,由于本文对客体安全特性的调整方法只允许保密值上行和完整值下行,全局的客体整体保密值趋势和完整值趋势固定,那么随着时间推移,势必会造成极端现象,从而导致只有极高保密值和极低完整值的主体才能读写客体,使得访问控制灵活性下降,因此这部分还需进行进一步研究与发展。

(3)关于访问控制模型计算量方面。本文借鉴 ABAC 细粒度访问控制的优点,尝试将属性值集合映射为可计算的特定值的集合,并对其计算方法进行约束定义,结合属性权重的特点,从细粒度方向对实体安全特性进行评估计算,从而得出一个可以用来相互比对的精确的数值,在这一过程中,需要大量的计算来保证读取的安全性,因此访问速度势必有所影响,但通过对安全值的计算,结合 BLP 和 Biba 的访问特点,既保证了基于属性的访问控制的细粒度特性,也保证了访问控制模型的灵活性,如果主体或客体属性发生变化,那么其对应的安全值同样也会发生变化,其可访问或可被访问的集合同样发生变化。

(4)关于强制访问控制规则方面。本文通过对 BLP 和 Biba 综合模型的改进,使其适应安全值环境需求,成功建立了一个基于保密值和完整值的强制访问控制模型,由于安全值是可以用来比对的,因此实体间的访问控制可以通过策略进行强制化,而安全值是系统通过属性值来对主客体进行安全评估的值,故主客体之间的访问控制可以完全通过 BLP 和 Biba 的访问控制规则来规范约束,具有很高的保密性和完整性。

结束语 本文通过对安全值计算环境的搭建,综合 BLP 和 Biba 的特点,建立了一个基于属性的兼顾保密性、完整性为一体的综合强制访问模型,通过对安全值上下限的定义,对信息上下行约束条件和规则的重新制定,不仅保证了访问模型的灵活性,同时又继承了 BLP 和 Biba 访问模型的优点,具有很高的实用性和安全性。但在属性权重和安全值的计算方面,还需要做进一步的考虑和完善;同时在环境属性的归约方面,本文也没有进行深入研究。下一步,在完善属性权重的设置和安全值计算的同时,要融入环境属性的变化和迁移特性以进一步提升综合强制模型的可用性和安全性。

参 考 文 献

[1] 徐亮,谭煌. BLP 改进模型的形式化描述及自动化验证[J]. 计算机工程,2013,39(12):130-135.
[2] 马萌,唐卓,李仁发,等. 基于条件随机场的改进 BLP 访问控制模型[J]. 计算机科学,2015,42(8):138-144.
[3] ZHANG J,YUN L J,ZHOU Z. Research of BLP and Biba dynamic union model based on check domain[C]// Preceedings of the seventh International Conference on Machine Learning and Cybernetics. Kunming,2008:12-15.
[4] 周向军. 基于 BLP/Biba 的混合云计算数据中心安全访问控制模型[J]. 信息安全与技术,2016,7(1):63-65.
[5] 于芳芳,马建红. 基于多优化技术的 ABAC 模型[J]. 计算机应用与软件,2015,32(11):312-316.
[6] 邹佳顺,张永胜,高艳. 云环境下基于使用控制的 ABAC 模型研究[J]. 计算机应用研究,2014,31(12):3692-3694.
[7] 倪川,黄志球,王珊珊,等. 基于属性的支持策略本体推理的访问控制方法研究[J]. 计算机科学,2015,42(3):96-101.
[8] 毋涛,张帆. 云计算下基于属性的访问控制方法[J]. 计算机系统应用,2016,25(2):231-234.
[9] BALAMURUGAN B,SHIVITHA G N,MONISHA V,et al. A Honey Bee Behaviour inspired novel Attribute-Based Access Control using Enhanced Bell-Lapadula Model in Cloud Computing[C]// International Conference on Innovation Information in Computing Technologies(ICIICT). IEEE,2015:1-6.
[10] BELL D,LAPADULA L. Secure Computer Systems:Mathematical Foundations and Model:echnical Report M74-244[R]. MITRE Corp. ,Bedford,MA 1973.
[11] BIBA K J. Integrity Considerations for Secure Computer Systems: EST TR-76-372[R]. ESD/AFSC, Hanscom AFB, Bedford, MA 1977.
[12] HU V C,FERRAIOLO D,KUHN R,et al. Guide to attribute based access control (ABAC) definition and considerations (draft)[J]. NIST Special Publication,2013,800(162).