抗万能攻击的安全网络编码

徐光宪 付 晓

(辽宁工程技术大学电子与信息工程学院 葫芦岛 125105)

摘 要 提出了一种能够抵抗万能攻击者的安全网络编码算法。在敌人可以窃听所有节点和信道及污染 z_0 个链路的情况下,该算法利用稀疏矩阵对信源信息进行矩阵变换,增强了信息的抗窃听能力,并利用列表译码法在信宿处进行译码,对污染攻击进行检测和排除。理论分析和仿真结果表明,该算法能够在多项式时间内设计完成,能够抵抗窃听和污染等安全性攻击,使得原本的随机网络编码以很高的概率达到弱安全的要求;同时提高了编码速率,减小了存储空间的占用。更重要的是,该算法仅在原随机编码体制的基础上对信源和信宿进行了修改,中间节点保持不变。

关键词 网络编码,万能攻击,稀疏矩阵,列表译码,弱安全,编码速率

中图法分类号 TP309.7 **文献标识码** A

Secure Network Coding Against the Omniscient Adversaries

XU Guang-xian FU Xiao

(Electronic and Information Engineering, Liaoning Technical University, Huludao 125105, China)

Abstract A secure network coding algorithm against the omniscient adversaries was presented. While the adversary can eavesdrop all links and jam z_0 links, the algorithm transforms the source news with sparse matrix to enhance the data anti-wiretapping capacity. In order to detect and eliminate pollution attacks, the receiver uses list decoding algorithm to recover the source news. The theoretical analysis and simulations both confirm that this algorithm can be designed and implemented in polynomial time, resistant eavesdropping and pollution attacks. At the same time, this algorithm can also make the standard random network coding to achieve the weakly secure condition at a high probability, increase the encoding rate and reduce the occupied memory space. Furthermore, only the source and destination need to be modified, and intermediate nodes implement a classical distributed network code.

Keywords Network coding, Omniscient attack, Sparse matrix, List decoding, Weakly secure, Encoding rate

1 前言

2000年,Ahlswede等[1]基于网络信息流的概念,首次提出了网络编码的思想,即允许网络节点对来自不同链路的信息进行编码组合,这样便可以实现网络流量的最大化。对于网络编码的应用研究已经证明,网络编码多播传输和线性网络编码均可以实现网络的最大流,并且,所有的算法都可以在多项式时间内设计完成[2-4]。虽然网络编码的初衷在于提高网络的吞吐量、实现网络最大流,但是进一步的研究发现,它也是一种安全网络传输的好方式。

在网络通信中,搭线窃听和污染攻击是破坏数据安全传输的常用手段。针对上述安全性问题,2002年,Cai等[5]首先论述了网络编码在安全方面的应用,最先研究了单源无圈网络中数据的安全多播问题,给出了搭线窃听的网络通信模型,并且构造了信息论意义下安全的网络编码。之后又有许多学者在Cai的基础上开展了很多卓有成效的研究。在抗搭线窃听的安全网络编码得到广泛研究的同时,针对有更大隐患的污染攻击,研究者也取得了一些重要的研究成果。Ho等[6]最先研究了网络编码和污染攻击的相互影响,给出了利用网络编码检测攻击敌手存在的体制。然而,搭线窃听和污染攻击很有可能同时出现在同一网络中,称具有此种能力的攻击者为万能攻击者,它对于网络系统有很强的攻击和破坏能力。

文献[5]仅对具有有限窃听能力的攻击者进行了分析,其所提出的网络模型并不能对污染攻击进行检测与抵抗;赵慧,卓新建等[7]在K. Jain[8]研究的基础上,提出了一种安全性定理,并证明在编码节点处使用伪随机函数更能确保信源消息不被恶意攻击者获取。然而,该算法没有考虑到对污染攻击的抵抗,并且需要知道整个网络的拓扑结构,不适宜用于大规模网络和无线网络。文献[6]的算法对污染攻击仅能够进行检测,而不能进行错误纠正,并且对于窃听攻击的抵御能力较弱。蒋铭勋等[9]提出了一种网络编码污染数据的检测分析方法,结合了同态哈希函数和线性空间签名进行污染检测,但其同样不能对污染信息进行错误纠正。Jaggi等[10]针对有线网络,讨论了抗污染的信息论上的速率最优解,然而需要中心化设计且复杂度较大。Jaggi等[11]提供了分布式解决方法,其可以在多项式时间内设计完成。然而,其对于抗窃听能力的

到稿日期:2011-09-25 返修日期:2012-02-24 本文受辽宁省重点实验室项目(2009S051)资助。

徐光宪(1977—),男,博士,副教授,主要研究方向为信号处理与编码;付 晓(1988—),女,硕士生,主要研究方向为信息论与编码,E-mail:fx09291108@163.com。

考虑较少，并且对于存储空间的需求较大。周亚军等[12]利用消息空间的所有子空间上的一种度量，给出了一种安全的纠错网络编码。然而，其在传输过程中需要一条秘密信道，针对万能攻击者，该算法的安全性较差。

网络编码在执行过程中伪装了数据，并且能有效地承载数据，但同时也在节点处增加了额外的计算和存储要求，增加了节点的复杂性。因此，需要设计合适的网络编码方案来抵抗具有强大能力的万能攻击者，同时降低网络编码节点的复杂性。文献[13]讨论了信息论安全和弱安全两种不同的安全性，并且给出了每种安全性的编码域。周亚军等[14]指出采用弱安全方案可以在保证文件不被攻击者获取的同时，降低安全网络编码的复杂性、提高传输效率。对于网络编码的节点复杂性优化，申肖肖等[15]采用伪范德蒙德矩阵来改善 P2P 网络编码的分发及 P2P 网络编码的安全性能。然而，文献[16]已经证明，在优化节点复杂性方面，稀疏矩阵中的对角矩阵具有更大的优势。文献[16]的算法在降低编码节点复杂性和提高解码速率方面有了很大的改善，但其未提及对于污染攻击的检测与纠正。

综上所述，本文首先提出了万能攻击者模型(即攻击者有强窃听能力和主动污染能力)，然后基于稀疏矩阵和列表译码法对文献[16]的编解码算法进行改进，提出了能够抵抗万能攻击者的安全网络编码算法。理论分析和仿真验证表明，该算法达到了弱安全性的要求，并有效地降低了网络节点的复杂性。

2 基本模型与概念

2.1 网络模型

为了简化对问题的分析，我们主要集中讨论一类无延时、非循环的单信源多信宿多播通信网络。对于一个无环多播网络 $G=(V,E)$，V 是点的集合，E 是信道的集合，为了构造网络码[1]，令 $GF(q)$ 为 q 阶有限域(这里 q 为一个大素数)。

网络编码　一个定义在 $G=(V,E)$ 上的 n 维线性网络码，对 G 中的每条边 $e\in E$ 分配一个向量 $u(e)$，称其为信道 e 的“全局编码核”(global encoding kernel)，使其满足：

(1)分配给信源 X 的向量空间为 $z(X)=GF_n(q)$，即一个 n 维向量空间；

(2)分配给边 $e\in E$ 的向量必须是所有到达节点 $tail(e)$ 的边上的向量的线性组合($tail(e)$ 指边 e 的尾节点)；若 e 的尾节点是信源 X，则 e 上的向量从 $z(X)$ 中选取；

(3)在每个信宿节点上，必须有能够恢复信源信息的特定函数操作。

用 $z(S)$ 表示节点 S 的向量空间，并注意到，对于任何非源节点 S，$z(S)$ 是到达 S 的所有边上向量的所有可能线性组合的集合。因此可以很容易判断出，对于任意 $e\in E$，有 $u(e)\in z(tail(e))$。

信源 A　A 产生不可压缩的数据信息，并利用编码算法将这些信息编码，然后将编码后的信息分组为 b 个数据包为一组的若干组。这样，A 就可以通过网络将这些数据信息传送给信宿。文中提到的编码算法将在第 4 节介绍。

信宿 B　B 将接收到的数据包整合组成矩阵 Y。整合的过程是这样的，Y 的第 i 行 Y_i 对应第 i 个接收到的数据包，然后 B 利用矩阵 Y 进行译码，从而恢复出 A 发出的数据信息 X。具体的译码算法将在第 4 节介绍。

总的来说，令 M 为 A 要传给 B 的数据信息，A 利用编码算法将 M 编码，这样获得编码后的数据信息 X。A 再通过网络将信息 X 传输出去，中间节点按照基本网络编码将信息进一步处理后，最后传送到信宿 B。B 将接收到的消息组成 Y，对 Y 进行译码解出信息 X，进而得到信源原始消息 M。

弱安全　弱安全指的是攻击者仅仅得到了信源信息运算后的比特(如异或)，且其不能够恢复信源的片段。这样，攻击者没有得到关于 M 的任何有意义的信息，即信源信息 M 仍旧是安全的[13,14]。

2.2 万能攻击模型

文献[11,12,17]中的秘密信道共享模型指出，在 A 与 B 之间存在一条安全的秘密信道可以无误地传送数据信息，这样便增加了网络系统本身的安全性；而文献[5,18]中所假设的攻击者只具有有限的窃听能力，并且不向数据信息中注入污染信息，所以文献[5,18]中的安全算法仅能抵抗较弱的窃听攻击。

不同于以上文献中所出现的攻击者，本文所假设的攻击者隐藏在网络中，可以窃听 A 与 B 之间的任何信道，而且具有恶意的攻击行为，会向链路所传送的信息中注入污染信息包。在本文中，定义这样的攻击者为万能攻击者 C。

令 z_o 表示攻击者 C 所能够污染的链路的数量，Z 表示 C 所注入的污染信息，则 Z 是一个 $z_o\times n$ 矩阵。

3 万能攻击模型中的网络编码列表译码法

3.1 列表译码法

列表译码法是通过改进传统线性分组码的伴随式译码算法而提出的一种低复杂度的译码法。在基本网络编码中，由于信源中未加入冗余，在有污染攻击存在的情况下，信宿 B 不可能唯一解出原始信源数据信息。然而，B 却可以对这些结果进行列表译码，即接收者鉴定出一些可能是信源数据信息的结果。一旦建立起这些列表，在信源中加入冗余便可进一步求出唯一的信源数据。网络编码与列表译码法的结合是本文译码算法的核心内容。

3.2 信源信息的处理

首先，对编码后的信源信息 X 进行划分，用分块矩阵 $[H\quad R\quad I]$ 来表示。其中，H 表示由原始消息 M 编码后的数据符号所构成的 $b\times(n-\Delta n-b)$ 矩阵；R 表示为进一步求得 X 而加入的冗余符号组成的 $b\times\Delta n$ 矩阵；I 是一个用来记录全局编码向量的 $b\times b$ 单位矩阵。将 X 写入列向量 W_X(在编码算法中会详细介绍)。令 $D=(d_{ij})$ 为 $b\Delta n\times bn$ 阶冗余矩阵，其中 d_{ij} 在 F_q 中独立均匀选取。则构成 R 的 $b\Delta n$ 个冗余符号可由式(1)求解得到：

$$DW_X=0 \tag{1}$$

式中，D 对于信源 A、信宿 B 和攻击者 C 是公开的，所以 R 也是公开的，该译码算法不需要秘密信道。

3.3 网络编码列表译码法

在网络编码中，中间节点对来自不同输入链路的信息进行随机线性组合，则信宿 B 接收到的信息可以表示为：

$$Y=JX+J'Z \tag{2}$$

即

$$Y=[J\,|\,J']\begin{bmatrix}X\\Z\end{bmatrix} \tag{3}$$

式中，J 和 J' 分别表示从信源 A 和攻击者 C 发出的数据信息包到 B 所接收到的线性独立的数据信息包集合的线性映射，即转移矩阵。

信宿 B 首先从 Y 中选取线性独立的 $b+z_o$ 列构成一个子矩阵 Y^S，并且 Y^S 必须包含 Y 的后 b 列（即 I 的对应列），Y^S 中另外的 z_o 列为任意选取的。令 X^S 和 Z^S 分别表示 X 和 Z 在 Y^S 中的对应列，则有：

$$Y^S=[J\mid J']\begin{bmatrix}X^S\\Z^S\end{bmatrix} \tag{4}$$

由于 Y^S 是 Y 的列向量所张成的线性空间，且 Y^S 的秩为 $b+z_o$[11]，因此 Y^S 是可逆的，且 $Y=Y^SF$，则：

$$F=(Y^S)^{-1}Y \tag{5}$$

由式(3)—式(5)推得：

$$Y=[J\mid J']\begin{bmatrix}X^SF\\Z^SF\end{bmatrix} \tag{6}$$

由于线性随机网络编码中的编码向量是随机选取的，因此很大概率上 J 和 J' 均是可逆的，则对比式(3)、式(6)可得：

$$X=X^SF \tag{7}$$

$$Z=Z^SF \tag{8}$$

信宿 B 运用以上线性列表译码法得到式(7)、式(8)。此时，令 F_1 表示 F 的前 z_o 列，F_2 表示 F 的余下 b 列，X_1^S 表示 X^S 的前 z_o 列。因为在最初构成 X 最后 b 列的单位矩阵 I 和信源信息矩阵的其他部分经受了同样的线性变换（即网络编码），所以式(7)可以写为：

$$X=X_1^SF_1+F_2 \tag{9}$$

X 可由式(1)、式(9)唯一解得[11]，从而信宿 B 可成功恢复出原始信源信息 M。

4 抗万能攻击的安全网络编码算法

本文提出了一种新颖的能够抵抗万能攻击者的安全网络编码算法。在信源的编码算法中，利用稀疏矩阵及其逆矩阵对信源信息数据进行矩阵变换，以达到抵抗强窃听攻击和降低网络编码节点复杂性的目的；在信宿译码算法中，信宿 B 利用编码后的数据矩阵，首先生成一个低维线性列表，之后对其进行列表译码。B 将网络编码与列表译码相结合，以达到排除污染信息的目的。

4.1 信源的编码算法

假设信源和信宿共享有一个随机数生成器，信源信息数据 M 经过一系列变换，最后得到处理后的信息 X，其处理流程如图 1 所示。具体的算法处理过程如下：

1)首先，信源在有限域 F_q 上选取一个随机数 P，然后在随机数生成器上生成 $l_1,l_2,\cdots,l_b$，并重新排列，得到如下形式的对角矩阵：

$$L=\begin{pmatrix}l_1&&&\\&l_2&&\\&&\ddots&\\&&&l_b\end{pmatrix} \tag{10}$$

2)设 $M'=(M_1,M_2,\cdots,M_b)L=(\beta_1,\beta_2,\cdots,\beta_b)$。重新组合$(\beta_1,\beta_2,\cdots,\beta_b)$得消息 K：

$$K=\begin{pmatrix}k_{11}&k_{12}&\cdots&k_{1n-\Delta n-b}\\k_{21}&k_{22}&\cdots&k_{2n-\Delta n-b}\\\cdots&\cdots&\ddots&\cdots\\k_{b1}&k_{b2}&\cdots&k_{bn-\Delta n-b}\end{pmatrix}=\begin{pmatrix}\beta_1\\\beta_2\\\cdots\\\beta_b\end{pmatrix} \tag{11}$$

3)选取一组线性无关的向量 $g_i\in F_{q^{n+1}}$，$i=1,2,\cdots,b$，生成如下行列式：

$$G=\begin{pmatrix}P&&&\\&g_2&&\\&&\ddots&\\&&&g_b\end{pmatrix} \tag{12}$$

其中，第一个信息包是信源所选取的随机数 P。

4)设 $H=G^1K$，则：

$$H=G^{-1}\begin{pmatrix}\beta_1\\\beta_2\\\ddots\\\beta_b\end{pmatrix}=\begin{pmatrix}h_{11}&h_{12}&\cdots&h_{1n-\Delta n-b}\\h_{21}&h_{22}&\cdots&h_{2n-\Delta n-b}\\\vdots&\vdots&\ddots&\vdots\\h_{b1}&h_{b2}&\cdots&h_{bn-\Delta n-b}\end{pmatrix} \tag{13}$$

5)求解方程(1)获得加入 X 的冗余矩阵符号，并构成 R。同时向 X 中加入一个 $b\times b$ 阶单位矩阵 I，则得到 $X=[H\quad R\quad I]$。令 W_M^T 表示将 M 所有列向量一列接一列地依次串联所得到的新的列向量，W_M 表示 W_M^T 的转置。则将 X 表示为列向量 $W_X=[W_H\quad W_R\quad W_I]^T$。$W_X$ 为最后信源要传输到网络中的消息。

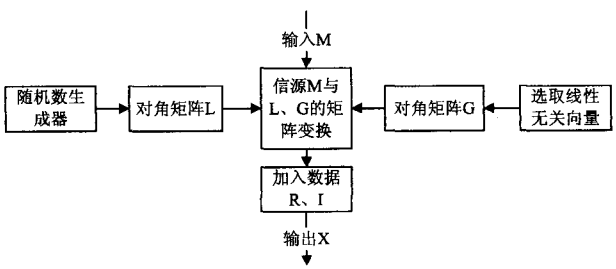

图 1 信源编码流程图

4.2 信宿的译码算法

信宿将接收到的数据信息包整合组成矩阵 Y，并通过如下步骤译码，以获得原始信源消息 M。

1)求解方程(1)得到冗余数据 R。

2)用万能攻击模型中的列表译码法(式(1)、式(9))得到唯一的 X。又因为有 $X=[H\quad R\quad I]$，所以可进一步得到 H。

3)信宿从 H 中译码得到 K：

$$K=GH=G\begin{pmatrix}h_{11}&h_{12}&\cdots&h_{1n-\Delta n-b}\\h_{21}&h_{22}&\cdots&h_{2n-\Delta n-b}\\\vdots&\vdots&\ddots&\vdots\\h_{b1}&h_{b2}&\cdots&h_{bn-\Delta n-b}\end{pmatrix} \tag{14}$$

4)从 G 中可得到信源最初选取的随机数 P，以 P 为种子，在随机数生成器中得到向量$(l_1,l_2,\cdots,l_b)$，从而可进一步得到 L。

5)原始信源消息 $M=(M_1,M_2,\cdots,M_b)$可用式(15)唯一解得：

$$M=(M_1,M_2,\cdots,M_b)=M'L^{-1}$$

$$=(\beta_1,\beta_2,\cdots,\beta_b)\begin{pmatrix}l_1&&&\\&l_2&&\\&&\ddots&\\&&&l_b\end{pmatrix}^{-1} \tag{15}$$

5 编码体制的通用安全性

在该编码方案中，网络中间节点的随机编码系数在有限

域 F_q 上选取，而信源节点中对随机线性网络编码的线性变换矩阵在上述有限域的扩域中选取，以此来达到编码的通用性。

对于强窃听攻击，该安全网络编码算法能够以很高的概率达到弱安全的要求，其证明过程与文献[17]类似。只要攻击者得不到信源开始所选取的随机数 P，他便不能得到关于 M 的全局编码向量，进而无法得到关于 M 的任何有意义的信息[14]。由于 G 对于攻击者 C 是安全的(证明过程不再赘述)，因此随机数 P 对于 C 也是安全的。又

$$ML=(M_1,\cdots,M_b)\begin{pmatrix} l_1 & & \\ & \ddots & \\ & & l_b \end{pmatrix}=(\beta_1,\cdots,\beta_b) \tag{16}$$

则

$$(M_1,\cdots,M_b)=(\beta_1,\cdots,\beta_b)\begin{pmatrix} l_1 & & \\ & \ddots & \\ & & l_b \end{pmatrix}^{-1} \tag{17}$$

显然，因为随机数 P 对于攻击者 C 是安全的，则($l_1,\cdots,l_b$)对于 C 是安全的。所以，即使当攻击者得到所有信息包 $\beta_1,\cdots,\beta_b$ 时，攻击者 C 也无法得到关于($M_1,\cdots,M_b$)的任何信息。从信息论角度，有

$$I(M_i;ML)=0,M_i\in M \tag{18}$$

即攻击者得不到 M 的任何有意义的信息，该算法也达到了弱安全的要求。

对于污染攻击，由网络编码列表译码法可以得出抗万能攻击的安全网络编码算法能够以高于 $1-q^{n\varepsilon}$ (ε 为某个小正数)的概率解出 X[19]，即排除污染信息，达到信息的安全传输要求。所以，无论对于网络中存在的两类安全性威胁还是能力强大的万能攻击者，该安全网络编码算法都是通用安全的。

6 仿真实验及性能分析

本文提出的编码算法对信源进行矩阵变换操作，且在中间节点进行线性网络编码，由于它运用了稀疏矩阵，因此其编码复杂度由 $O(m^2n)$ 降为 $O(mn)$。本文译码算法利用低复杂度线性列表译码算法，由于信源中加入了冗余，因此译码算法复杂度为 $O((mn)^3)$[19]。由此可见，本文提出的抗万能攻击的安全网络编码方案具有较低的复杂度，并且节省了大量存储空间。

使用 matlab 对编码算法进行仿真并取得实验数据。选取 6 个不同大小的文件进行编码处理，分别从编码速率和占用存储器空间两方面来验证抗万能攻击的安全网络编码的性能。

如图 2 所示，与文献[17]给出的安全网络编码算法相比，在编码同样大小的文本文件时，本文算法的编码速率有显著的提高，在某些情况下可达到 1.5MB/s。而且，随着所需编码文件的增大，传统安全网络编码的编码速率减小，这种情况可能是由于内存读取的开销和缓存大小引起的[20]。如图 3 所示，从 0.5MB 到 2MB 不等的文件经过改进的编码方案编码后，所占用的存储器空间为 0.003MB 左右，与传统编码方案所占用的空间相比，大大减小了。经更多的仿真实验验证，文件的增大不会影响抗万能攻击的安全网络编码算法对于文件所占用空间的压缩性能，并且在接收端通过译码可恢复出原文件[16]。具体实验数据如表 1 所列。

表 1 仿真实验数据

原文件占用空间 (M)	编码后占用空间 (M)	传统编码速率 (M/s)	该算法编码速率 (M/s)
0.50	0.002	0.11	0.45
0.72	0.002	0.11	0.64
0.98	0.003	0.04	0.83
1.28	0.003	0.03	1.06
1.60	0.004	0.03	1.31
2.00	0.004	0.03	1.52

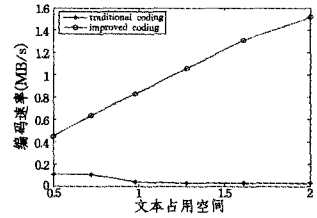

图 2 编码速率的比较

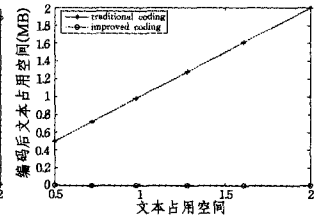

图 3 存储空间占用情况比较

结束语 本文提出了一种新颖的抗万能攻击的安全网络编码算法，利用稀疏矩阵与列表译码法的特性，结合线性随机网络编码，对信源和信宿编解码算法进行了改变。该算法不需要知道网络拓扑，其内部节点不需要任何新的功能，且它对有线和无线网络均适用。

经理论特性分析和实验结果验证，抗万能攻击的安全网络编码算法在攻击者有强窃听能力和主动污染能力的情况下，能够以很高的概率达到弱安全的要求，而且还具有很高的编解码速率和较低的复杂度，节省了大量存储空间，有效地减小了开销。

参 考 文 献

[1] Ahlswede R, Ning Cai, 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 Transactions on Information Theory, 2003, 49(2): 371-381

[3] Koetter R, Medard M. An algebraic approach to network coding [J]. IEEE/ACM Transaction on Networking, 2003, 11(5): 782-795

[4] Jaggi S, Sanders P, Chou P A, et al. Polynomial time algorithms for multicast network code construction [J]. IEEE Transactions on Information Theory, 2005, 51(6): 1973-1982

[5] Cai N, Yeung R. Secure network coding [C]// IEEE International Symposium Information Theory. 2002, 2: 323

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

[7] 赵慧，卓新建. 等. 一种基于网络拓扑的安全网络编码算法分析[C]//通信理论与技术新进展—第十三届全国青少年通信学术会议论文集. 2008: 844-846

[8] Jain K. Security based on network topology against the wiretapping attack [J]. IEEE Wireless Communication, 2004, 11(1): 68-71

[9] 蒋铭勋，崔巍. 随机线性网络编码污染数据的检测分析[J]. 计算机工程，2010, 36(24): 107-112

[10] Jaggi S, Langberg M, Ho T, et al. Correction of Adversarial Errors in Networks [C]// International Symposium on Information Theory. Sept. 2005: 1455-1459

(下转第 114 页)

mod n 中 $x \notin [a,b]$，Alice 可以通过如下方法来欺骗 Bob：一是找到一个 x'，r' 且 $x' \in [a,b]$ 使得 $g^{x'}h^{r'} \bmod n = g^x h^r \bmod n$，再用 x' 代替 x 执行零知识证明式(1)－式(4)，这需要解离散对数，在计算上是不可能的；二是找到一个 $x' \in [a,b]$ 且 $g^x \bmod n = g^{x'} \bmod n$，由于 Alice 不知道 n 的分解，因此这也是不可能的，否则与强 RSA 假设矛盾。在上两项都不可能被攻破的情况下，Alice 要欺骗成功，则需要攻击式(1)－式(4)。因为攻破每一个公式的成功概率均小于 2^{-t+1}[10]，所以 Alice 成功欺骗的概率小于 $4 \times 2^{-t+1} = 2^{-t+3}$。例如，当安全参数 t 取值 80 时，Alice 成功欺骗的概率小于 2^{-77}。

2)匿名性：sign 协议的式(1)－式(4)都是统计零知识证明，具有无限计算能力的攻击者也不能求解出相应的离散对数。Bob 从 Alice 获得的公开数据有 $E(x,r)$、E_1、E_2、U、E_3、E_4、E_5、F、u，其中包含 x、y_1、y_2、α、ω、r、r_1、r_2、r_3、r_4，未知数共 10 个，而方程却有 9 个，攻击者可以猜测出一个未知数，再决定其他随机数，它们都是合法解。因而 Bob 不能从此过程中获取 TPM 的相关信息，这保障了匿名性。

3)撤消性：在本方案中，如果 Prover 所在 TPM 泄露了匿名认证密钥(x,r)，则(x,r)将被加入至撤消列表中。当 Verifier接到请求时，检查是否存在(x',r')，使得 $E(x',r') \stackrel{?}{=} E(x,r)$，如果相等，则可以判断事务请求来自一个被撤消的无效 TPM，Verifier 拒绝为其提供服务。

在本方案中，Prover 共执行 1 次签名，生成和验证消息认证码各 1 次，生成密钥 1 次；CA 执行 1 次签名验证，生成和验证消息认证码各 2 次；DAA Issuer 共执行 1 次签名，1 次签名验证，生成和验证消息认证码各 1 次，生成密钥 1 次；共需要执行 24 个复合模指数运算及 8 个 hash 运算。而在原 DAA 方案中，Issuer 生成密钥 1 次，Prover 签名 3 次，共执行 43 次复合模指数及 20 个 hash 运算。可以看到，本方案的 join 协议比 DAA 方案的复杂不少，但是本方案的 join 协议解决了 Issuer 与 Verifier 的共谋问题，而且 Prover 获得 DAA 证书后，CA 不再参与 sign 过程，因此 CA 不会成为性能瓶颈；而本方案的复合模指数运算和 hash 运算数量比原 DAA 方案少得多，因而总体运算效率有较大提高。

对于选择的参数，假设 $|n| = 1024$bit，$|b-a| = 512$bit，$T = 512$，$l = 40$，$t = 80$，$s = 40$，$s_1 = 40$，$s_2 = 552$。根据文献[10]，sign 协议仅需要发送 13222bit 数据。因此，本方案的 sign 协议通信量也是比较少的。

结束语 直接匿名认证是可信计算平台的重要功能。面对复杂的网络环境和不断涌现的各种攻击手段，设计具有高安全性和高效率的直接匿名认证方案具有重要意义。本文通过引入可信第三方以及使用特定区间承诺值证明机制，使改进的 DAA 认证方案具有较高的安全性和效率，解决了已有协议的安全隐患。

参 考 文 献

[1] Trusted Computing Group. Trusted Computing Platform Alliance(TCPA) Main Specification Version 1. 1b[EB/OL]. http://www.trustedcomputinggroup.org,2011-08-20

[2] Brickell E, Camenisch J, Chen L. Direct anonymous attestation [EB/OL]. http://eprint.iacr.org/2004/205.pdf,2011-08-20

[3] Brickell E, Chen L, Li J. A new direct anonymous attestation scheme from bilinear maps[C]//Proceedings of the 1st International Conference on Trusted Computing and Tpust in Information Technologies. Berlin: Springer-Verlag, 2008: 166-178

[4] He Ge, Tate S R. A direct anonymous attestation scheme for embedded devices[C]//Proc of the 10th International Conference on Practice and Theory in Public-key. Springer-Verlag, 2007: 16-30

[5] 陈小峰，冯登国. 一种基于双线性映射的直接匿名证明方案[J]. 软件学报，2010，21(8)：2070-2078

[6] Brickell E, Chen Li-qun, Li Jiang-tao. Simplified security notions of direct anonymous attestation and a concrete scheme from pairings[C]//The Conference on Trusted Computing(TRUST 2008). Villach, Austria, 2008: 315-330

[7] 杨亚涛，曹陆林，李子臣，等. 基于 XTR 机制改进的直接匿名认证方案[J]. 计算机科学，2011，38(4)：141-144

[8] 张京良，马育珍，王育民. 承诺值在特定区间的高效证明[J]. 西安电子科技大学学报：自然科学版，2006，33(6)：949-952

[9] Rudolph C. Covert identity information in direct anonymous attestation[C]//Proceedings of the 22nd IFIP TC-11 International Information Security Conference(SEC2007) on New Approaches for Security, Privacy and Trust in Complex Environments. Springer, Boston, 2007: 443-448

[10] Fujisaki E, Okamoto T. Statistical zero knowledge protocols to prove modular polynomial relations[C]//Proceedings of CRYPTO' 97. Berlin: Springer-Verlag, 1997: 16-30

[11] Boudot F. Efficient Proofs That a Committed Number Lies in an Interval[C]//EUROCRYPT 2000, LNCS l 807. Berlin Heidelberg: Springer-Verlag, 2000: 431-444

[12] Ge He. An Anonymous Authentication Scheme for Trusted Computing Platform[EB/OL]. http://eprint.iacr.org/2005/445.pdf,2011-08-20

(上接第 91 页)

[11] Jaggi S, Langberg M, Katti S, et al. Resilient Network Coding in the Presence of Byzantine Adversaries [J]. IEEE Transactions on Information Theory, 2008, 54(6): 2596-2603

[12] 周亚军，李晖，马建峰. 一种安全的纠错网络编码[J]. 电子与信息学报，2009，31(9)：2237-2241

[13] Bhattad K, Narayanan K R. "Weakly Secure Network Coding" [EB/OL]. http://netcod.org/papers /06Bhattad N-final.pdf, 2007-05-22

[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

[15] 申肖肖，李晖. P2P 网络编码技术研究[D]. 西安：西安电子科技大学，2010

[16] 徐光宪，付晓. 基于稀疏矩阵的低复杂度安全网络编码算法[J]. 计算机工程，38(9)：55-57

[17] 周亚军，李晖，马建峰. 防污染和防窃听的网络编码[D]. 西安：西安电子科技大学，2009

[18] 张岩. 一种改进的安全网络编码方案的研究[J]. 南京邮电大学学报，2009：962-966

[19] 马松雅，罗明星，杨义先. 抗 Byzantine 攻击的安全网络编码研究综述 [C]//中国电子学会第十五届信息论学术年会暨第一届全国网络编码学术年会论文集(下册). 2008

[20] 董学文，牛文生，马建峰，等. Ad-hoc 路由协议的串空间安全性扩展[J]. 计算机科学，2011，38(7)：51-54