doi:10.3969/j.issn.1000-436x.2013.04.004

# 融合时间戳和同态签名的安全网络编码方法

裴恒利，尚涛，刘建伟
（北京航空航天大学 电子信息工程学院，北京 100191）

**摘 要**：针对无线多跳网络编码的安全性问题，提出了一种融合时间戳和同态签名的安全网络编码方法。在利用基于 RSA 的同态签名方案抵御污染攻击的基础上，引入时间戳设计新型同态签名方案来抵御网络中的重放攻击，以时间戳为源生成网络编码的随机系数来保证签名的同态性。重点分析了本方案产生随机系数的方式对网络编码解码概率的影响，并建立了攻击模型证明方案可同时抵御网络中的污染攻击和重放攻击。性能分析表明本方案与基于 RSA 的同态签名方案开销比值接近于 1。

**关键词**：同态签名；时间戳；污染攻击；重放攻击；网络编码；无线多跳网络
**中图分类号**：TN918 **文献标识码**：A **文章编号**：1000-436X(2013)04-0028-08

# Secure network coding method merged with timestamp and homomorphic signature

PEI Heng-li, SHANG Tao, LIU Jian-wei
(School of Electronic and Information Engineering, Beihang University, Beijing 100191, China)

**Abstract:** A secure network coding method merged with timestamp and homomorphic signature which can solve security issues in wireless multi-hop networks was proposed. The timestamp into RSA-based homomorphic signature scheme was brought and used to produce random coefficients of net it possible to defend pollution attacks and replay attacks simultaneously while maintaining the homomorphic property of the signature. The analysis that mainly focus on was the influence of random coefficients on decoding probability of network coding a security of the proposed scheme. Results indicate that the proposed scheme can defend pollution attacks and replay attacks simultaneously, and the ratio of overhead between RSA-based homomorphic signature scheme and the proposed scheme is approximates 1.

**Key words:** homomorphic signature; timestamp; pollution attack; replay attack; network coding; wireless multi-hop network

## 1 引言

网络编码技术[1]因有利于无线多跳网络传输性能的提升而成为近年的研究热点，但同时它也带来了许多安全问题。例如，在无线多跳网络中，网络编码特别容易受到恶意节点的污染攻击[2]，同时也会遭受传统网络中存在的重放攻击、假冒攻击、篡改攻击、拒绝服务攻击、中间人攻击等[3]。针对污染攻击，Ho 等利用简单多项式散列函数（simple polynomial hash function）在目的节点处对消息的完整性进行验证[4]，然而，中继节点并未参与完整性验证，因此相应地会增加受攻击的数据分组在网络中的传输数量。Gkantsidis 和 Rodriguez 提出的同态散列方案(homomorphic hashing scheme)[5]实现了中继节点对消息完整性的验证，但却需要额外的安全信道来传输原始消息的散列值。随后，Charles 等在同态散列方案的基础上设计了一种同态签名方案(homomorphic signature scheme)[6]，该方案不需要额

收稿日期：2012-06-24；修回日期：2012-11-19
基金项目：高等学校博士学科点专项科研基金资助项目（20091102110004）；国家重点基础研究发展计划（“973”计划）基金资助项目（2012CB315900）；国家自然科学基金资助项目（61272501）
**Foundation Items:** The Specialized Research Fund for the Doctoral Program of igher Education (20091102110004); The National Basic Research Program of China (973 program) (2012CB315900); The National Natural Science Foundation of China (61272501)

外的安全信道，但由于复杂的韦伊配对操作（weil pairing operation）会增加运算的复杂度，因此，其应用受到了限制，而 Yu 等提出的基于 RSA 的同态签名方案[7]则大大降低了同态签名的运算复杂度。Rosario 等[8]对 Yu 的方案进行了改进，将基于 RSA 的同态签名方案设计在整数域中，并通过随机预言模型（random oracle model）证明了该方案的安全性。

虽然同态签名方案能够抵御污染攻击，但由于网络中攻击形式的多样性，设计可同时抵御包含污染攻击在内的多种攻击网络编码签名方案非常重要。尤其是对能量受限的无线传感器网络而言，节点的能量是制约网络性能提升的主要因素，而重放攻击因会大量消耗节点能量而成为此类网络所面临的最棘手的攻击之一。因此，针对能量受限的无线多跳网络，本文在基于 RSA 同态签名方案的基础上设计了一种融合时间戳和同态签名的可同时抵御污染攻击与重放攻击的网络编码签名方案——该方案将对时间戳和对数据的签名有效地结合起来，保证了网络中各节点可以同时认证数据的完整性和时间戳的真实性；并进一步分析了引入时间戳对网络编码解码概率的影响以及对网络开销的影响。

## 2　相关研究

### 2.1　随机线性网络编码

网络编码按照编码系数产生方式的不同可分为随机性网络编码和确定性网络编码，按照编码方式的不同可分为线性网络编码和非线性网络编码[9]。根据无线多跳网络的分布式特点，以下重点介绍随机线性网络编码的具体过程。

网络拓扑如图 1 所示。其中，$A$ 为源节点，$(t_1,\cdots, t_k)$为目的节点，其他各节点为中继节点。源节点将要发送的每一条原始消息 $\boldsymbol{M}_i\ (i=1,\cdots, m)$设定为选自有限域 $Z_q$ 的长度为 $n$ 的向量，其中，$q$ 是预先定义的素数。因此，原始消息 $\boldsymbol{M}_i$ 可表示为 $\boldsymbol{M}_i=(m_{i1},\cdots, m_{in})$。

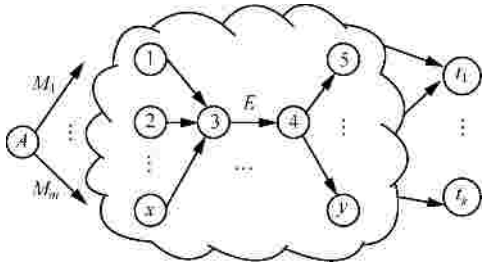


图 1　网络拓扑

在随机线性网络编码中，每一个中继节点将收到的消息线性组合，生成编码消息 $\boldsymbol{E}$ 并转发。因此，$\boldsymbol{E}$ 可表示为该中继节点所收到的消息$(E_1,\cdots, E_k)$的线性叠加，即

$$\boldsymbol{E}=(a_1\cdots a_k)\times\begin{pmatrix}E_1\\ \vdots\\ E_k\end{pmatrix}\bmod q \tag{1}$$

其中，$(a_1\ \cdots\ a_k)$为编码向量，由中继节点随机产生，为使目的节点能够对收到的消息进行解码，在源节点发出的每条原始消息 $\boldsymbol{M}_i$ 前附加一段长度为 $m$ 的单位向量，生成向量 $\boldsymbol{M}_i$’

$$\boldsymbol{M}_i'=(\underbrace{0,\cdots,0}_{i-1},1,\underbrace{0,\cdots,0}_{m-i},m_{i1},m_{i2},\cdots,m_{in}) \tag{2}$$

相应地，中继节点收到的消息向量 $\boldsymbol{E}$’记为

$$\boldsymbol{E}'=(e_1',e_2',\cdots,e_m',e_{m+1}',\cdots,e_{m+n}') \tag{3}$$

其中，$\boldsymbol{M}_i$’、$\boldsymbol{E}$’可统称为扩展消息或扩展向量（augmented message）[10]。为防止攻击者截获从源节点发出的原始消息，源节点对其所要发送的消息也要进行编码，即对要发送的 $m$ 条扩展消息$(M_1', \cdots, M_m')$进行 $m$ 次线性组合，获得 $m$ 条编码消息并转发。

目的节点在收到 $m$ 条线性无关的消息$(E_1', \cdots, E_m')$后，即可得矩阵 $\boldsymbol{U}'$为

$$\boldsymbol{U}'=\begin{pmatrix}e_{1,1}' & \cdots & e_{1,m}' & e_{1,m+1}' & \cdots & e_{1,m+n}'\\ e_{2,1}' & \cdots & e_{2,m}' & e_{2,m+1}' & \cdots & e_{2,m+n}'\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ e_{m,1}' & \cdots & e_{m,m}' & e_{m,m+1}' & \cdots & e_{m,m+n}'\end{pmatrix} \tag{4}$$

将矩阵 $\boldsymbol{U}'$的前 $m$ 列构成的矩阵记作 $\boldsymbol{U}$，后 $n$ 列构成的矩阵记作 $\boldsymbol{V}$，则由式(5)便可将源节点发送的 $m$ 条原始消息解码恢复。

$$(M_1,\cdots,M_m)=\boldsymbol{U}^{-1}\boldsymbol{V} \tag{5}$$

### 2.2　同态签名

同态分为加法同态和乘法同态[11]。给定变量 $X_1$ 和 $X_2$，若对于函数 $F$，存在函数 $f$ 使得式(6)成立，则称函数 $F$ 满足加法同态。

$$F(X_1+X_2)=f\left(F(X_1),F(X_2)\right) \tag{6}$$

若对函数 $F$，存在函数 $f$ 使得式(7)成立，则称函数 $F$ 满足乘法同态。

$$F(X_1\times X_2)=f\left(F(X_1),F(X_2)\right) \tag{7}$$

同态签名便是利用了同态函数保持运算的性质。节点接收的消息与相应签名分别记作$(E_1,\cdots,E_n)$和$(F(E_1),\cdots,F(E_n))$，若当前节点要对接收到消息的线性组合 $a_1E_1+\cdots+a_nE_n$ 生成签名 $S$，如果 $F$ 具有加法同态性，则当前节点可直接由式(8)生成签名。

$$S=f\left(F\left(E_1\right),F\left(E_2\right),\mathrm{L},F\left(E_n\right)\right) \tag{8}$$

其中，由式(8)计算出的签名 $S$ 与 $F(a_1E_1+\cdots+a_nE_n)$ 相等，这样便实现了中继节点在未知源节点私钥的情况下对所要发送的消息进行签名。本文安全网络编码方案中的签名函数具有加法同态性，详见第 3 节中命题 1 的证明。

## 3 安全网络编码方案

在安全网络编码方案中，时间戳信息可以起到两方面作用：一是网络中各节点可以利用时间戳来识别重放消息，以抵御网络中的重放攻击；二是以时间戳为源产生网络编码的随机系数，可以保证网络中各节点能够利用签名函数的加法同态性对编码后的消息产生签名。因此，本文在利用基于 RSA 同态签名方案抵御污染攻击的基础上，引入时间戳设计新型同态签名方案以抵御网络中的重放攻击，并以时间戳为源生成网络编码的随机系数。

网络拓扑如图 1 所示。$A$ 为源节点，不规则区域内的节点为中继节点，$t_1,\cdots,t_k$ 为目的节点，$M_1^{'},\mathrm{L},M_m^{'}$ 表示由原始消息生成的扩展消息，由长度为 $m+n$ 的向量表示。全网采用同步时钟，且所有中继节点均对收到的消息编码。方案中的相关参数如表 1 所示。

方案仍采用传统的基于 RSA 的同态签名方案，但由于在签名方案中引入了时间戳机制，为保证签名仍具有同态属性，方案考虑以时间戳为源生成网络编码的随机系数，具体过程如下。

**Step1** 源节点选取参数。与基于 RSA 的同态签名方案相类似，参数选取过程简述如下。

源节点首先选择 2 个素数 $p$ 和 $q$，其中，$q|(p-1)$ 中通常 $q$ 为 257bit，$p$ 为 1 024bit。然后选择 $m+n+1$ 个不同的元素 $g_1$，$g_2$，…，$g_{m+n+1}$。每个元素均选自 $Z_p$ 且元素 $g_i$ 的形式为 $s^{(p-1)/q} \bmod p$，其中，$s$ 选自 $Z_p$ 且 $s\neq 1$。因此，对任意整数 $t$，$g_j^{tq} \bmod p=1$ 成立。然后，源节点生成 RSA 签名的公钥 $(r,e)$ 和私钥 $d$。其中，$r=uv$，$u$ 和 $v$ 都为素数，为 512bit。一般选定 $r$ 为 1 024bit。令 $f=(u-1)(v-1)$，公钥 $e$ 满足 $\gcd(e,f)=1$，私钥 $d$ 满足 $ed\equiv 1 \bmod f$。因此，对任意整数 $t\in Z_r$，$t^{ed}=t \bmod r$。

表 1 相关参数

| 参数 | 含义 |
|---|---|
| $u, v$ | 512bit 的任意素数 |
| $r$ | $r=uv$，1 024bit，公开参数 |
| $e$ | RSA 签名公钥 |
| $p$ | 任意素数，1 024bit，公开参数 |
| $q$ | 任意素数，257bit，且 $q\|(p-1)$，公开参数 |
| $g_i$ | $g_i\in Z_p$，公开参数 |
| $d$ | RSA 签名私钥 |
| $\boldsymbol{\Phi}$ | $\boldsymbol{\Phi}=(u-1)(v-1)$ |
| $m$ | 源节点发送消息条数 |
| $n$ | 源节点发送消息长度 |
| $k$ | 编码数据的个数，即节点收到 $k$ 个数据之后编码 |
| $w$ | 网络中中继节点的个数 |
| $M_i$ | 源节点 $S$ 要发送的原始消息，以向量形式表示 |
| $M_i^{'}$ | 源节点 $S$ 要发送的扩展消息，以向量形式表示 |
| $E_i$' | 中继节点对接收到的消息线性编码后产生的消息，以向量形式表示 |
| $T_i$ | 时间戳，且 $T_i\in Z_q$ |
| $a_i$ | 网络编码的随机系数，且 $a_i\in Z_p$ |

**Step2** 源节点生成签名。在源节点的签名生成过程中引入了时间戳，对消息和时间戳的组合生成签名。

源节点产生 $m$ 条扩展消息并附上当前时刻作为该条消息的时间戳（需将时间戳 $T_i$ 转换为 $Z_q$ 中的数值），然后用私钥 $d$ 对 $m$ 条消息签名，其中，签名 $\mathrm{SIGN}_d(M_i^{'}\|T_i)$ 如式(9)所示。

$$\mathrm{SIGN}_d(M_i'\|T_i)=\left(\prod_{j=1}^{m+n} g_j^{m_{i,j}^{'}}\cdot g_{m+n+1}^{T_i} \bmod p\right)^d \bmod r \tag{9}$$

**Step3** 中继节点验证签名并生成新的签名。具体过程如下。

中继节点在收到一条消息组合 $\{E^{'}\|T,\ \mathrm{SIGN}_d(E^{'}\|T)\}$ 后，首先判断式(10)是否成立。

$$(\mathrm{SIGN}_d(E'\|T))^e \bmod r=\left(\prod_{j=1}^{m+n} g_j^{e_{i,j}^{'}}\cdot g_{m+n+1}^{T} \bmod p\right) \bmod r \tag{10}$$

如果式(10)成立，则可断定该消息组合没有受到污染攻击，这是因为：若该消息组合在传输过程中的数据部分没有遭到破坏，则式(11)成立。

$$(\mathrm{SIGN}_d(E'\|T))^e \mod r$$
$$=((\prod_{j=1}^{m+n} g_j^{e_j'} \cdot g_{m+n+1}^{T} \bmod p)^d)^e \mod r$$
$$=(\prod_{j=1}^{m+n} g_j^{e_{i,j}'} \cdot g_{m+n+1}^{T} \bmod p) \mod r \quad (11)$$

然后由消息组合中的时间戳部分判断该消息组合是否被重放，如果为重放消息则丢弃。若消息组合在时效范围内，则该节点在收到 $k$ 条消息组合 $\{E_i'\|T_i, \mathrm{SIGN}_d(E_i'\|T_i)\}$ $(i=1,\cdots, k)$后，为保证能够利用同态性质对此 $k$ 条消息组合中数据部分的线性组合进行签名，则需根据当前时刻 $T$ 以及收到的 $k$ 条消息组合中的时间戳$(T_1,\cdots, T_k)$，由式(12)计算出随机系数 $a_1, a_2, \mathrm{L}, a_k$。

$$T = a_1T_1 + a_2T_2 + \mathrm{L} + a_kT_k \bmod q \quad (12)$$

利用该组随机系数对收到的 $k$ 条消息组合中的数据进行线性叠加，得到编码数据 $E'\|T$：即 $E'\|T=a_1(E_1'\|T_1)+\cdots+a_k(E_k'\|T_k)$，并利用签名的同态性质，由 $k$ 条消息组合中的签名生成与 $E'\|T$ 对应的签名 $\mathrm{SIGN}_d(E'\|T)$。

**命题 1**　函数 $\mathrm{SIGN}_d$ 具有加法同态性。

**证明**　设 $\boldsymbol{X}_i=(x_{i1}, \cdots, x_{i(m+n+1)})$ $(i=1, \cdots, k)$是长度为 $m+n+1$ 的向量，则由式(9)可得

$$\mathrm{SIGN}_d(X_i) = (\prod_{j=1}^{m+n+1} g_j^{x_{ij}} \bmod p)^d \bmod r \quad (13)$$

因此

$$\mathrm{SIGN}_d(\sum_{i=1}^{k}(a_iX_i))$$
$$=(\prod_{j=1}^{m+n+1} g_j^{\sum_{i=1}^{k}(a_ix_{ij})} \bmod p)^d \bmod r$$
$$=(\prod_{i=1}^{k}\prod_{j=1}^{m+n+1} g_j^{a_ix_{ij}} \bmod p)^d \bmod r$$
$$=(\prod_{i=1}^{k}(\prod_{j=1}^{m+n+1} g_j^{x_{ij}})^{a_i} \bmod p)^d \bmod r$$
$$=(\prod_{i=1}^{k}(\mathrm{SIGN}_d(X_i))^{a_i} \bmod p)^d \bmod r \quad (14)$$

命题得证。

因此可利用同态性质生成对消息 $E'\|T$ 的签名 $\mathrm{SIGN}_d(E'\|T)$，式(15)给出了该签名的计算式。

$$\mathrm{SIGN}_d(E'\|T) = \prod_{i=1}^{k}(\mathrm{SIGN}_d(E_i'\|T_i))^{a_i} \bmod r \quad (15)$$

然后，节点将消息组合$\{E'\|T, \mathrm{SIGN}_d(E'\|T)\}$转发。

**Step4**　目的节点验证签名并对源节点发送消息解码恢复，具体过程如下。

目的节点在收到一条消息组合后，首先通过式(10)来判断消息是否受到污染攻击，然后等待。当接收到 $m$ 条线性无关的消息组合后，利用式(5)对源节点发送的消息解码恢复。

## 4　安全性分析

本文的安全网络编码方案中假设源节点总是安全的，只有中继节点不可信。攻击者可能会控制中继节点，破坏其所要发送的消息，对网络实施污染攻击；另外，攻击者也可能会控制中继节点，使其重复发送已经发送过的消息，对网络实施重放攻击。

### 4.1　污染攻击的安全性分析

攻击者的污染攻击方式分为 2 种：一是产生伪造消息数据并对其生成有效签名；二是根据攻击者所截获的消息组合中的签名产生与之相匹配的消息数据。

在第一种攻击方式中，攻击者污染中继节点接收到消息组合中的数据部分 $E_i'\|T_i$ $(i=1, \cdots, k)$或直接将伪造的消息数据注入网络，中继节点编码后的消息因此遭到污染。将攻击者污染后的消息记作 $\{\tilde{E}_i'\|\tilde{T}_i \ (i=1, \mathrm{L}, k)\}$，则中继节点编码后的消息与未受攻击时所产生的编码消息 $E'\|T$ 不同，即

$$E'\|T \neq \sum_{i=1}^{k} \tilde{a}_i(\tilde{E}_i'\|\tilde{T}_i) \quad (16)$$

但由于攻击者未知源节点私钥，因此无法对该污染消息生成有效签名，所以攻击无效。

在第二种攻击方式中，攻击者依照截获的消息组合中的签名生成与之匹配的数据，即希望根据所截获的消息组合 $\{E'\|T, \mathrm{SIGN}_d(E'\|T)\}$ 中的签名 $\mathrm{SIGN}_d(E'\|T)$ 推出与之相应的数据 $\tilde{E}'\|\tilde{T}$，且 $\tilde{E}'\|\tilde{T} \neq E'\|T$。因此，该方案的安全性等同于是否可以找到不同于 $E'\|T$ 的数据 $\tilde{E}'\|\tilde{T}$，使得 $\mathrm{SIGN}_d(\tilde{E}'\|\tilde{T}) = \mathrm{SIGN}_d(E'\|T)$，下面将证明其困难度等价于解决离散对数问题。

**命题2**　给定消息$E'\|T$ 和相应签名$\mathrm{SIGN}_d(E'\|T)$，找到不同于 $E'\|T$ 的消息 $\tilde{E}'\|\tilde{T}$，使得$\mathrm{SIGN}_d(\tilde{E}'\|\tilde{T}) = \mathrm{SIGN}_d(E'\|T)$ 的困难度等价于解决离散对数问题。

**证明**　为简化说明，考虑 $m=n=1$ 的特殊情况，

此时，

$$\mathrm{SIGN}_d(E'\|T)=(g_1^{e_1'}g_2^{e_2'}g_3^{e_3'} \bmod p)^d \bmod r \quad (17)$$

问题转化为攻击者希望找到 $E'\|T=(e_1',e_2',e_3')$，使其各元素能够满足

$$\begin{aligned}&(g_1^{e_1'}g_2^{e_2'}g_3^{e_3'} \bmod p)^d \bmod r\\ =&(g_1^{e_1'}g_2^{e_2'}g_3^{e_3'} \bmod p)^d \bmod r\end{aligned} \quad (18)$$

固定 $e_1'$ 和 $e_2'$，令 $x=e_3'$，式(18)变换为

$$g_3^x=g_1^{e_1'-e_1}g_2^{e_2'-e_2}g_3^{e_3'} \quad (19)$$

则问题转化为希望找到 $x$ 使其满足式(19)。可以看出由式(19)求解 $x$ 是一个离散对数困难问题，命题2得证。

该证明可推广到 $m+n>2$ 的情况，限于篇幅，这里不再详述。

### 4.2 重放攻击的安全性分析

在重放攻击中，攻击者截获网络中的消息组合并不断转发或通过控制中继节点使其重复发送已发送过的消息组合，从而达到消耗网络节点能量、占用网络带宽和降低网络吞吐量等目的。

在该攻击中，攻击者有2种攻击方式：直接重放所截获的消息组合或修改所截获消息组合中的时间戳并对其生成有效签名。

在第一种攻击方式中，假设攻击者重放截获的消息组合 $\{E_i'\|T_i,\mathrm{SIGN}_d(E_i'\|T_i)\}$，当网络中某节点在收到该消息组合后，将消息组合中的时间 $T_i$ 与当前时间 $T$ 相比较，如果差值超过门限，则可断定该消息为重放消息，丢弃，攻击无效。

第二种攻击方式相当于污染攻击中的第一种攻击方式：对伪造数据生成有效签名。攻击者由于未知源节点的私钥，因此无法对截获的消息组合中的数据部分进行签名，所以攻击无效。

由以上安全性分析可知，本文提出的安全网络编码方案可同时抵御污染攻击和重放攻击，且攻击成功的困难度等同于解决离散对数困难问题。

## 5 性能分析

### 5.1 开销分析

为了分析安全网络编码的性能，本节重点考虑签名算法所引发的开销，不考虑引入同步计时机制带来的开销。网络中传送的消息组合以 $\{E'\|T,\mathrm{SIGN}_d(E'\|T)\}$ 的形式出现，其中，$E'\|T$ 为数据，以向量形式表示，$\mathrm{SIGN}_d(E'\|T)$ 为签名。由于时间戳 $T$ 的引入使网络开销相较于基于 RSA 的同态签名方案有所增加，现将增加的开销类型分类如下（下文中为叙述简便，称基于 RSA 的同态签名方案为方案 1，本文的引入时间戳的同态签名方案为方案2，且开销均指算法耗费时间）。

1) 参数初始化开销

在初始化过程中，方案2需产生 $m+n+1$ 个模指数运算的底数，即 $(g_1,g_2,\cdots,g_{m+n+1})$ 和一个私钥。因产生私钥的过程仅为简单的模乘和模加运算，远小于产生 $g_i$ 的模指数运算开销，因此下述分析中不考虑产生私钥的开销。

参数初始化阶段耗费时间近似正比于方案所需 $g_i$ 的个数，与方案1相比两者的耗费时间比值近似等于 $(m+n+1)/(m+n)$，且 $m$ 和 $n$ 数值越大该比值越接近于1。

2) 编解码与求解线性方程组的开销

方案1中，网络中的中继节点对收到的消息 $(E_1',E_2',\cdots,E_k')$ 编码，其中，每个向量长度为 $m+n$。由于时间戳的引入，使得每个向量长度增加为 $m+n+1$，因此相应地增加了编解码开销。另外，由于网络中除目的节点以外的每个节点都需要根据当前时间生成随机系数，因此也相应地增加了网络开销。但由于编解码运算与求解线性方程的运算均为简单的模加与模乘运算，因此其所产生的开销与方案1的开销比值近似为1。

3) 计算签名的开销

网络中有2类节点产生签名：源节点和中继节点。由于源节点仅有1个，而中继节点数目较多，因此签名开销主要产生在中继节点。其中，中继节点生成签名的运算如式(9)所示，将方案1中的签名记作 $\mathrm{SIGN}_d(E')$，方案2中的签名记作 $\mathrm{SIGN}_d(E'\|T)$，由于两者均取值于有限域 $Z_r$ 中，且随机系数 $a_i\ (i=1,\cdots,k)$ 均选自有限域 $Z_q$，因此，对两者作 $k$ 次模指数运算的开销比值近似接近于1。

4) 验证签名的开销

中继节点的主要功能是对收到的签名进行验证。验证过程应保证尽可能地快速。然而，由于签名采用基于 RSA 的公钥签名体制，使得签名的验证时间成为了制约网络性能提升的主要因素。因此，衡量方案性能的最重要指标是签名算法的验证时间。

模指数运算是算法效率的制约因素。由式(10)可知，方案 2 的签名验证过程（验证一条消息）需经过 $m+n+2$ 次模指数运算，而方案 1 的签名验证过程仅需运算 $m+n+1$ 次，因此两者的签名验证时间的比值为 $(m+n+2)/(m+n+1)$，且 $m$ 与 $n$ 的值越大，该比值越接近于 1。

由以上分析可知，与方案 1 相比，方案 2 仅在参数初始化与签名验证部分增加了网络的开销，而签名、编解码与求解线性方程所引起的网络开销与方案 1 基本一致。

### 5.2　网络编码解码概率分析

随机线性网络编码中随机系数的生成和选取对目的节点的解码概率有一定影响，而本文网络编码方案中的随机系数通过求解 $k$ 元一次方程组产生，与传统的随机系数的产生方式有所不同，究竟对解码概率有多大影响，需要进一步详细分析。

**命题3**　根据式(12)可解出随机系数 $(a_1, a_2, \text{L}, a_k)$，当用其作为网络中中继节点的编码系数时，目的节点解码概率近似等于随机系数独立均匀选自域 $Z_q$ 的情况，且解码概率 $P$ 的范围如式(20)所示。

$$P \geq (1-d/q)^h \quad (q>d) \tag{20}$$

其中，$d$ 表示网络中目的节点的个数，$q$ 为有限域的大小，$h$ 为源节点所发消息的个数。

**证明**　在随机线性网络编码网络中，若随机系数满足 $Z_q$ 中的均匀分布且相互独立，则目的节点解码概率 $P$ 的取值范围为 $P \geq (1-d/q)^h \quad (q>d)$ [12]。因此，命题 3 可转化为证明式(12)的 $k$ 个解 $(a_1, a_2, \text{L}, a_k)$ 满足独立均匀分布。

用 $(a_1', a_2', \text{L}, a_k')$ 表示独立均匀选自 $Z_q$ 的 $k$ 个系数，$(a_1, a_2, \text{L}, a_k)$ 表示由式(12)解得的 $k$ 个系数。因 $k$ 维单位矩阵 $\boldsymbol{E}_k$ 为向量空间 $\boldsymbol{V}^k$ 的基底，因此，$(a_1', a_2', \text{L}, a_k')$ 可以表示为

$$\begin{pmatrix} a_1' \\ a_2' \\ \text{M} \\ a_k' \end{pmatrix} = r_1 \begin{pmatrix} 1 \\ 0 \\ \text{M} \\ 0 \end{pmatrix} + r_2 \begin{pmatrix} 0 \\ 1 \\ \text{M} \\ 0 \end{pmatrix} + \text{L} + r_k \begin{pmatrix} 0 \\ 0 \\ \text{M} \\ 1 \end{pmatrix} \quad \text{mod } q \tag{21}$$

其中，$\boldsymbol{E}_k = \begin{pmatrix} 1 & 0 & \text{L} & 0 \\ 0 & 1 & \text{L} & 0 \\ \text{M} & \text{M} & \text{O} & \text{M} \\ 0 & 0 & \text{L} & 1 \end{pmatrix}$，$\boldsymbol{V}^k$ 为长度为 $k$ 的所有向量构成的向量空间，$(r_1, r_2, \text{L}, r_k)$ 为均匀独立选自 $Z_q$ 的数。

方程 $T = a_1T_1 + a_2T_2 + \text{L} + a_kT_k \bmod q$ 的解 $(a_1, a_2, \text{L}, a_k)$ 可由式(22)得出。

$$\begin{pmatrix} a_1 \\ a_2 \\ \text{M} \\ a_k \end{pmatrix} = \sum_{i=1}^{k} r_i \begin{pmatrix} \dfrac{1-T_i}{T_1} \\ 1 \\ \text{M} \\ 0 \end{pmatrix} \quad \text{mod } q \tag{22}$$

同样地，$(r_1, r_2, \text{L}, r_{k-1})$ 为均匀独立选自 $Z_q$ 的数。

由式(22)可知，$(a_2, \text{L}, a_k) = (r_1, \text{L}, r_{k-1})$ 满足独立同分布，因此仅需证明

$$a_1 = \sum_{i=1}^{k-1} r_i \left( \frac{1-T_{i+1}}{T_1} \right) \tag{23}$$

满足均匀分布且与 $(a_2, \text{L}, a_k)$ 独立。

根据式(22)和 $(T_2, \text{L}, T_k)$ 之间的相互独立性易知：$r_i[(1-T_{i+1})/T_1]$ $(i=1,2,\text{L},k-1)$ 各变量之间相互独立，由于当 $k$ 足够大时，取值于有限域上的独立随机变量和的极限分布为均匀分布[13]，因此，当 $k$ 取值充分大时，变量 $a_1$ 服从均匀分布。

下面证明($a_1$，…，$a_k$)之间的相互独立性。将 $a_1$ 记作 $X$，$a_i$ $(i=2,\text{L},k)$ 记作 $Y$。则

$$\begin{aligned} &\text{E}(X) = 0\times\frac{1}{q} + 1\times\frac{1}{q} + \text{L} + (q-1)\times\frac{1}{q} = \frac{q-1}{2} \\ &\text{E}(Y) = 0\times\frac{1}{q} + 1\times\frac{1}{q} + \text{L} + (q-1)\times\frac{1}{q} = \frac{q-1}{2} \\ &\text{E}(XY) = \frac{(1+2+\text{L}+q-1)^2}{q^2} = \frac{(q-1)^2}{4} \\ &\Rightarrow \text{E}(XY) = \text{E}(X)\text{E}(Y) \end{aligned} \tag{24}$$

由上述分析可得 $a_1$ 满足均匀分布且与($a_2$,…,$a_k$)相互独立，命题 3 得证。

## 6　仿真分析

### 6.1　时耗分析

利用 NS2 网络仿真软件对本文所介绍的安全网络编码方案进行仿真。其中，传输层采用 UDP 数据流，网络层协议采用洪泛协议，编码尺寸设定为 2，网络拓扑如图 2 所示。A 表示源节点，D 表示目的节点，1、2、3、4、5 节点表示中继节点。

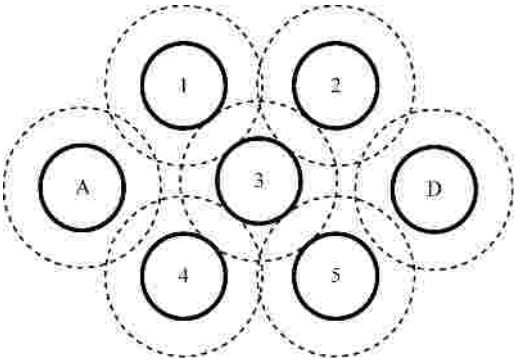


图 2 网络拓扑

改变源节点消息向量中元素的个数 $m$，将基于 RSA 的同态签名方案记为 RSA 方案，所得的算法运行时间对比如图 3 所示。

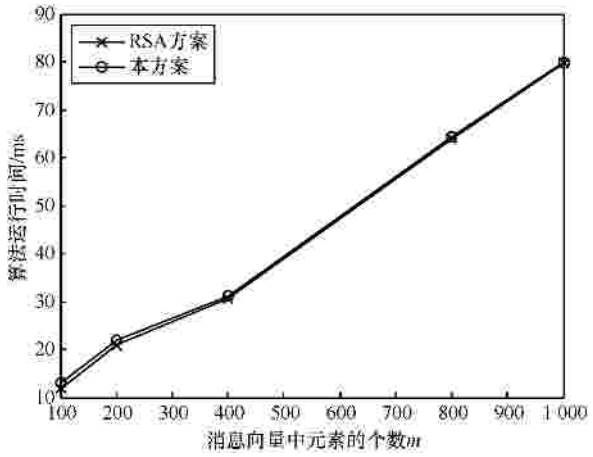


图 3 本方案和 RSA 方案的运行时间对比

从图 3 中可以看出，随着消息向量中元素个数的增加，2 方案的算法运行时间基本呈线性增长。另外，随着 $m$ 的增大，2 方案的曲线基本重合，这是因为算法中引入的时间戳 $T$ 可以看作消息向量 $m$ 中的一个元素，随着 $m$ 值的增大，引入时间戳带来的时耗在整个算法时耗中所占的比重越小。

由上述分析可知，同 5.1 节中的理论分析结果相一致，本方案和 RSA 方案的算法时耗基本一致，并且由于本方案能够同时抵御污染攻击和重放攻击，因此综合考虑算法时耗与安全性能，本方案优于 RSA 方案。

### 6.2 能耗分析

本小节分析了当网络遭遇重放攻击时，本方案、RSA 方案以及未引入安全机制的网络编码方案（简记为编码方案）的节点能耗。

网络中节点所处理的数据分组类型分为 2 种：重放数据分组和非重放数据分组。

对于重放数据分组，3 种方案中节点的处理过程可分为以下 3 点。

1) 本方案。判断其是否为重放分组（表 2 中简记为判断），如果为重放分组，则将其丢弃。

2) RSA 方案。验证签名、编码、计算签名（表 2 中简记为验证编码签名）。

3) 编码方案。编码。

对于非重放数据分组，3 种方案中节点的处理过程可分为以下 3 点。

1) 本方案。验证签名、编码、计算签名。

2) RSA 方案。验证签名、编码、计算签名。

3) 编码方案。编码。

利用 MATLAB 计算上述不同处理过程的运行时间，当消息向量中元素个数 $m$=256 时，得到处理过程的运行时间如表 2 所示。

表 2 不同处理过程的运行时间

| 性能指标 | 处理过程 | | |
|---|---|---|---|
| | 验证编码签名 | 判断 | 编码 |
| 运行时间/ms | 3.501 3 | $0.265\times10^{-5}$ | $5.843\times10^{-2}$ |

利用公式 $W$(能量) = $P$(功率)×$T$(时间) 可计算出每种处理过程对应的能耗。固定网络中非重放数据分组的个数为 10，改变重放数据分组的个数，结合表 2 中的数据，可得 3 种方案中节点的能耗对比如图 4 所示。

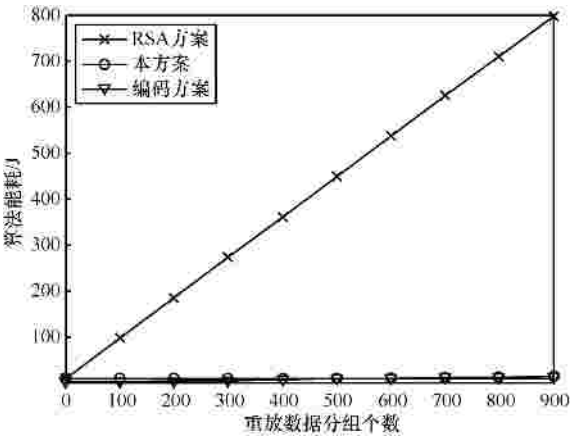


图 4 本方案、RSA 方案以及编码方案的能耗对比

从图 4 中可知，RSA 方案的能耗远远高于其他 2 种方案，因此，在网络遭遇重放攻击时，相较于仅可抵御污染攻击的 RSA 方案，本方案能够很好地节省节点能量，延长节点的生存时间。

图 5 为排除 RSA 方案后，本方案与编码方案的算法能耗对比。

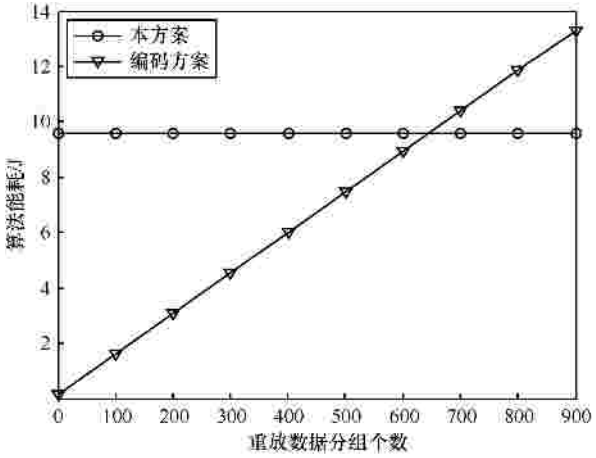


图 5　本方案和编码方案的能耗对比

由图 5 可知，当重放数据分组的个数较小时，相较本方案，编码方案的能耗较小；随着重放数据分组个数的增加，编码方案能耗呈线性增长，而本方案的能耗基本不变。

由上述分析可知，相较于未引入安全机制的网络编码方案，本方案更能够抵御恶意节点重放攻击所带来的能耗，可以更好地延长节点的生存时间。

## 7　结束语

本文的安全网络编码方案利用融合时间戳的同态签名来抵御网络中的污染攻击和重放攻击，为保证中继节点能够利用同态性质对编码后的消息生成新的签名，需要以时间戳为源来生成网络编码的随机系数。文中重点分析了本方案产生随机系数的方式对网络编码解码概率的影响，并建立攻击模型证明方案可同时抵御污染攻击和重放攻击，性能分析表明该方案与基于 RSA 的同态签名方案开销比值接近于 1，因此，网络中各节点并不会因为增加了对时间戳的处理步骤而增长数据处理时间。

## 参考文献：

[1] AHLSWEDE R, CAI N, LI S. Network information flow[J]. IEEE Transactions on Information Flow, 2000, 46(4):1204-1216.

[2] 曹张华, 唐元生. 安全网络编码综述[J]. 计算机应用, 2010, 30(2): 499-505.
CAO Z H, TANG Y S. Survey on secure network coding[J]. Journal of Computer Application, 2010, 30(2):499-505.

[3] PERVAIZ M, CARDEI M, WU J. Routing security in ad hoc wireless networks[J]. Network Security, 2010, 117-142.

[4] HO T, LEONG B, KOETTER R. Byzantine modification detection in multicast networks using randomized network coding[A]. Proceedings of IEEE International Symposium on Information Theory(ISIT)[C]. Massachusetts, USA, 2008. 2798-2803.

[5] GKANTSIDIS C, RODRIGUEZ P. Cooperative security for network coding file distribution[A]. Proceedings of International Conference on Computer Communications(INFOCOM)[C]. Barcelona, Spain, 2006. 367-380.

[6] MENEZES A, OKAMOTO T, VANSTONE S. Reducing elliptic curve logorithms to logorithms in a finite field[J]. IEEE Transactions on Information Theory, 1993, 39(5):1639-1646.

[7] YU Z, WEI Y, RAMKUMAR B. An efficient signature-based scheme for securing network coding against pollution attacks[A]. Proceedings of International Conference on Computer Communications (INFOCOM)[C]. Arizona, USA, 2008. 1409-1417.

[8] GENNARO R, KATZ J, KRAWCZYK H. Secure network coding over the integers[J]. Public Key Cryptography, 2010, 60(56):142-160.

[9] LIM S H, KIM Y H. Noisy network coding[J]. IEEE Transactions on Information Theory, 2011, 57(5):3132-3152.

[10] LIM S H, GERLA M, KRAWCZYK H. Performance evaluation of secure network coding using homomorphic signature[A]. Proceedings of International Symposium on Network Coding(NetCod)[C]. Beijing, China, 2011. 1-6.

[11] SUTAR S G, PATIL G A. Privacy management in cloud by making use of homomorphic functions[J]. International Journal of Computer Applications, 2012, 37(2):13-16.

[12] CAI N, SHI X, MEDARD M. Localized dimension growth in random network coding: a convolutional approach[A]. Proceedings of IEEE International Symposium on Information Theory(ISIT)[C]. St Petersburg, USA, 2011. 1156-1160.

[13] 刘凤梅, 李世取, 黄晓英. 取值于有限域上的独立随机变量和的极限分布定理[J]. 河北工业大学学报, 1999, 1(28):98-102.
LIU F M, LI S Q, HUANG X Y. Limit distribution theorem for a sum of independent random variables whose values belong to a inite field[J]. Journal of Hebei University of Technology, 1999, 1(28):98-102.

## 作者简介：

裴恒利（1990-），女，山东滕州人，北京航空航天大学硕士生，主要研究方向为网络编码、信息安全等。

尚涛（1976-），男，辽宁营口人，博士，北京航空航天大学讲师、硕士生导师，主要研究方向为无线网络通信、网络编码、网络安全等。

刘建伟（1964-），男，山东莱州人，博士，北京航空航天大学教授、博士生导师，主要研究方向为密码学、信息安全、网络安全等。