文章编号:1001 - 9081(2011)07 - 1868 - 04
doi:10.3724/SP.J.1087.2011.01868

限定节点查看信息的网络编码签名方案

冯　帆,王彩芬,罗　海,于志轩
(西北师范大学 数学与信息科学学院,兰州 730070)
(262721969@qq.com)

摘　要:现有网络编码研究关注的是信息传送效率的增加而忽略了网络编码使信息在网络传送中过于泛滥,这对信息的安全造成威胁。为了解决这个问题,设计了限定节点查看消息的网络编码签名方案。依据网络环境中需要查看信息节点的个数,提出了两种方案:一是少数节点查看信息,使用接收节点的公钥签名,而只有拥有公钥对应私钥的节点才可以解密得到信息的方法;二是多个节点之间通信,为了避免没有权限的节点查看信息,需要通信的节点预先建立会话钥,利用会话钥进行签名信息传递的方法。新方案通过权限限制了节点查看到信息的内容,从而保证了信息在网络中的安全性。新方案使用网络编码有效的在提高信息传送效率的同时保证了信息在网络中传送的安全性。

关键词:网络编码;节点限定;签名;公钥;私钥;权限
中图分类号:TP393.08　　**文献标志码**:A

Network coding signature scheme with limitation of nodes to check news

FENG Fan, WANG Cai-fen, LUO Hai, YU Zhi-xuan
(*College of Mathematics and Information Science, Northwest Normal University, Lanzhou Gansu* 730070, *China*)

Abstract: The existing network coding research focuses on the increase of the transmission efficiency of information on the network yet ignoring the information's overflow in the transmission caused by the network coding, which poses a threat to information security and even all message in the network's can be revealed by network nodes. In order to solve this problem, a new method was designed. Based on the different number of information nodes needed to check in different network environments, there are two solutions: one is only a few nodes, using the public key signature of receiving information node, can check information. Meanwhile only the nodes with the private key corresponds to the public key can decrypt and get information. The other one is communication between multiple nodes. In order to avoid that the node with no permission checks information, session keys should be established between communication nodes and be used to transfer the information. The new scheme limits the nodes to check the information though the authority, and consequently ensures the security of information in the network. The usage of network coding in new scheme effectively improves the efficiency of information transmission while assuring the safety of transferring information in the network.

Key words: network coding; node limition; signature; security of internet; public key; private key; authority

0　引言

2000 年,香港中文大学的 R. W. Yeung 和 N. Cai 首次提出了网络编码,其核心思想是在网络中参与传输的节点,其输出边上传输的数据可以通过该点多条输入边上传输的数据的某种线性或非线性变换得到,而参与传输的所有节点对数据的变换应保证最终所有接收节点可以正确恢复出信源所发送的信息[1]。

Alshwede 等人[2]以著名的"蝴蝶网络"(Buttery Network)模型为例,阐述了网络编码的基本原理。如图 1 所示的"单信源二信宿"蝴蝶网络,设各链路容量为 1,S 是信源节点,Y 和 Z 是信宿节点,其余为中间节点。根据"最大流最小割"定理,该多播的最大理论传输容量为 2,即理论上信宿 Y 和 Z 能够同时收到信源 S 发出的 2 个单位的信息,也就是说能同时收到 $b1$ 和 $b2$。图 1(a)表示的是传统的路由传输方式,节点 W 执行存储和转发操作。假定 W 转发信息 $b1$,则链路 WX、XY 和 XZ 上传输的信息均为 $b1$,虽然信宿 Z 收到 $b1$ 和 $b2$,但信宿 Y 却只能收到 $b1$(同时收到一个多余的 $b1$),因此信宿 Y 和 Z 无法同时收到 $b1$ 和 $b2$,该多播不能实现最大传输容量。

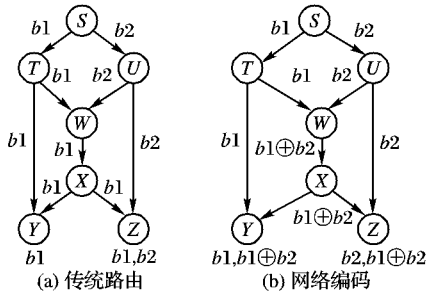

图 1　"单信源二信宿"蝴蝶网络

图 1(b)表示的是网络编码方法,节点 W 对输入的信息进行模二加操作,然后将操作结果 $b1 \oplus b2$ 发送至输出链路

收稿日期:2011 - 01 - 04;**修回日期**:2011 - 02 - 25。
基金项目:国家自然科学基金资助项目(61063041);国家教育部科学技术研究重点项目(208148)。
作者简介:冯帆(1985 -),男,甘肃庆阳人,硕士研究生,主要研究方向:信息安全、密码学;　王彩芬(1963 -),女,河北安国人,教授,博士生导师,博士,主要研究方向:密码学、电子商务协议的设计与分析;　罗海(1981 -),男,安徽巢湖人,硕士研究生,主要研究方向:信息安全、密码学;　于志轩(1983 -),男,甘肃兰州人,硕士研究生,主要研究方向:信息安全、密码学。

WX,然后又通过链路 XY 和 XZ,最终达到信宿 Y 和 Z。Y 收到 $b1$ 和 $b1 \oplus b2$ 后,通过译码操作 $b1 \oplus (b1 \oplus b2)$ 就能解出 $b2$,因此,信宿 Y 同时收到了 $b1$ 和 $b2$。同理,信宿 Z 也同时收到 $b1$(通过译码操作 $b2 \oplus (b1 \oplus b2)$)和 $b2$。由此,基于网络编码的多播实现了理论上的最大传输容量[3]。

现有研究关注了网络编码的种种优点,都在强调信息通过网络编码后在网络中传输效率的增加,而忽视了一个问题,那就是当网络中的信息都使用网络编码传递时,信息就会在很短的时间内遍布整个网络,导致信息传播的泛滥,这样的结果导致信息的安全性受到了威胁,在网络中的任何节点,都有可能看到信息的内容,这样就无法保证信息的保密性,而在一些信息安全保密性要求比较高的网络中使用现有的网络编码传输信息也就失去了意义。

在信息保密的大前提下,我们根据网络环境中需要接收消息的节点个数的不同,提出了两种不同的解决方案,以保证信息在这两种网络环境中都可以安全保密地传输。

1　背景知识

1.1　随机线性网络编码

在确定性的网络编码中,中间节点的编码向量需要依据网络的拓扑结构进行预先的确定,但在实际的网络中,网络的拓扑结构经常会发生变化,特别是在无线网络中,每次网络拓扑结构发生变化时,都需要对编码向量进行重新确定。而随机的网络编码只要求中间节点自己随机地在某有限域中进行编码系数的选择,而无需对整个网络的拓扑结构有任何的了解。

用一个非循环的有向图 $G=(V,E)$ 表示整个网络,V 为网络中所有节点的集合,E 为网络中所有边的集合。源点 S 想要发送 m 个消息到一个目的节点集合 $R=\{r_1,r_2,\cdots,r_t\}$,这 m 个消息可表示为以下向量形式:$X_1',X_2',\cdots,X_m'$。其中,$X_i'=(x_{i1}',x_{i2}',\cdots,x_{im}') \in F_q^m (i=1,2,\cdots,m)$,为了方便目的节点解码,一般会在原始消息后面附带上其全局编码向量。原始消息的全局编码向量一般为一组相互正交的单位向量,即:

$$X_i=(x_{i1}',x_{i2}',\cdots,x_{im}',\underbrace{0,\cdots,0}_{i},1,\underbrace{0,\cdots,0}_{m}) = (x_{i1},x_{i2},\cdots,x_{in},x_{i,n+1},\cdots,x_{i,n+m}) \in F_q^{m+n};i=1,2,\cdots,m$$

源点将这 m 个消息广播出去。

在任意一中间节点 v 处,其输出的消息向量为其接收到的消息向量的线性组合,即:$w=\sum_{i=1}^{J} c_i w_i$,其中 $w_i=(w_{i1},w_{i2},\cdots,w_{in},\beta_{i1},\cdots,\beta_{im})$,$(\beta_{i1},\cdots,\beta_{im})$ 是消息 w_i 的全局编码向量,而局部编码向量 $C=(c_1,c_2,\cdots,c_l) \in F_q^l$ 由该中间节点 v 在有限域 F_q 上随机选取。显然,对于任意的 $w_i=(w_{i1},w_{i2},\cdots,w_{in},(\beta_{i1},\cdots,\beta_{im})$,有 $w_i=\sum_{j=1}^{m}\beta_{ij}X_j$。当目的节点收到 m 个线性无关的消息向量 $w_1,w_2,\cdots,w_m$,由于 $w_i=\sum_{j=1}^{m}\beta_{ij}X_j$,则有 $\begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_m \end{bmatrix} \begin{bmatrix} X_1 \\ X_2 \\ \vdots \\ X_m \end{bmatrix}$,令 $B=\begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_m \end{bmatrix}$,则有 $\begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{bmatrix} = B \begin{bmatrix} X_1 \\ X_2 \\ \vdots \\ X_m \end{bmatrix}$。

两边都乘以 B^{-1},可得:$\begin{bmatrix} X_1 \\ X_2 \\ \vdots \\ X_m \end{bmatrix} = B^{-1} \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{bmatrix}$。

1.2　同态网络编码签名方案[4]

本方案采用固定长度的公钥和固定长度的单位向量。具体方案内容详见文献[4]。首先对这个签名方案做一简单介绍。此方案由四个部分组成。

1.2.1　构造 $Setup(1^k,N)$

选择一个安全参数 1^k 和一个有效的整数 N。

1)生成一个双线性组 $G=(G_1,G_2,G_T,e,\varphi),G_1,G_2,G_T$ 的素数阶 $p>2^k$。选择生成元 $g_1,g_2,\cdots,g_N \xleftarrow{R} G_1\backslash\{1\}$,并且 $h \xleftarrow{R} G_2\backslash\{1\}$;

2)选择 $\alpha \xleftarrow{R} F_p$,并且定义 $u:=h^\alpha$;

3)定义哈希函数 $H:Z\times Z \to G_1$;

4)公钥为 $PK:=(G,H,g_1,\cdots,g_N,h,u)$,私钥为 $SK:=\alpha$。

1.2.2　签名 $Sign(SK,id,m,v)$

给定秘密的私钥 $SK:=\alpha$,定义 $id \in \{0,1\}^k$,整数 m 指明签名空间,一个分量 $v \in F_p^N$,计算 $n:=N-m$,输出签名:$\sigma:=\left(\prod_{i=1}^{m}H(id,i)^{v_{n+1}}\prod_{j=1}^{n}g_j^{v_j}\right)^\alpha$。

1.2.3　联合 $Combine(PK,id,\{(\beta_i,\sigma_i)\}_{i=1}^{l})$

给定一个公钥 PK,一个文件的编号 id,l 对权重 $\beta_i \in F_p$ 和签名 σ_i,计算输出:$\sigma:=\prod_{i=1}^{l}\sigma_i^{\beta_i}$。

1.2.4　验证 $Verify(PK,id,m,y,\sigma)$

给定一个公钥 $PK=(g_1,g_2,\cdots,g_N,h,u)$ 和编号 id,一个指明签名空间的整数 m,一个签名 σ,向量 $y \in F_p^N$,设定 $n:=N-m$,并且定义:

$\gamma_1(PK,\sigma) \xlongequal{\text{def}} e(\sigma,h)$ 和 $\gamma_2(PK,id,m,y) \xlongequal{\text{def}} e\left(\prod_{i=1}^{m}H(id,i)^{y_{n+i}}\prod_{j=1}^{n}g_j^{y_j},h\right)$。如果 $\gamma_1(PK,\sigma)=\gamma_2(PK,id,m,y)$ 则算法输出 1,否则输出 0。1 表示验证通过,0 表示验证失败。文献[4]中已做了详细证明,这里不再证明。

1.3　基于用户口令的组密钥交换协议[5]

具体协议内容详见文献[5],首先对这个协议做以下简单描述:

一个信息发送源 S,和若干个信息接收端 C_i,每一个 C_i 与发送源 S 分享自己的一个口令 pw_i。

1)一个素数 q 的循环群 G,g 是 G 的生成元;

2)一对加解密算法 (E,D);

3)三个单项哈希函数 H_1,H_2,H_3。

通过两轮交换信息生成会话钥如下:

第一轮　S 选择 n 个随机数 $s_1,s_2,\cdots,s_n \in Z_q^*$,计算 $t_1=E_{pw_1}(g^{s_1}),t_2=E_{pw_2}(g^{s_2}),\cdots,t_n=E_{pw_n}(g^{s_n})$,然后发送 t_i 到 C_i,同时每一个 C_i 选择一个随机数 $x_i \in Z_p^*$,计算 $y_i=E_{pw_i}(g^{x_i})$,然后广播 y_i。S 和 C_i 用 pw_i 解密得到的 y_i 和 t_i,然后共享 $sk_i=H_1(sid \| g^{s_i x_i})$,其中 $sid=y_1 \| y_2 \| \cdots \| y_n$。

第二轮　S 随机选择一个秘密的 $K \in Z_p^*$,并且为每一个 $1,2,\cdots,n$ 计算 $k_i=K \oplus sk_i$ 和 $\varphi_i=H_2(sk_i \| S)$,然后 S 向所有的 C_i 广播 k_i 和 φ_i,与此同时,C_i 计算并且广播 $\eta_i=$

$H_2(sk_i \| C_i)$,S 验证每一个 η_i 防止字典攻击,C_i 验证每一个 φ_i,当 C_i 验证通过,计算 $K = k_i \oplus sk_i$,并得到会话钥 $sk = H_3(SID \| K)$,其中 $SID = s\ id \| k_1 \| k_2 \| \cdots \| k_n$。协议的安全性已经在文献[2]中做了详细的证明。

2 本文方案

为了防止网络环境中所有的用户都可以查看到网络中的信息,使得网络中的信息安全性得到提高,依据网络环境中需要查看信息的节点的个数提出了不同的解决方案,保证了信息通过网络编码后传递虽然信息遍布整个网络,但是没有权限的节点无法查看到信息内容。

2.1 方案一

方案一适用于网络中少数节点之间为保证信息的保密性传输消息,其思想是通信双方协商互用对方的公钥签名,而接收到信息的节点只有使用签名时所用公钥相对应的私钥解密,才可以解读信息的内容,从而保障了其他节点无法正确查看信息。本方案是在文献[4]的基础上做了改进,从而适应了特定网络环境的需要。

假设 S 表示发送信息节点,C 表示接收信息节点。SK 表示私钥,PK 表示公钥。

优点 保证通信节点之间信息保密传送,即使消息通过网络编码在网络中泛滥传递,也可以保证信息的安全性。

缺点 因为每次通信都要使用接收节点的 PK 签名,接收节点要使用自己的 SK 解密,这样使得通信的代价增大,并且每次通信都限定了通信节点的个数。

如果少数节点之间在网络中秘密通信,S 可以利用 C 的 PK 签名信息后在网络中传输,C 接收后只有通过自己的 SK 解密才可以得到信息。其他节点即使得到消息也无法解密查看到正确的信息内容。具体描述如下。

2.1.1 构造 $Setup(1^k,N)$

选择一个安全参数 1^k 和一个有效的整数 N。

1)生成一个双线性组 $G = (G_1,G_2,G_T,e,\varphi)$,$G_1,G_2,G_T$ 的素数阶 $p > 2^k$。选择生成元 $g_1,g_2,\cdots,g_N \xleftarrow{R} G_1\backslash\{1\}$,并且 $h \xleftarrow{R} G_2\backslash\{1\}$;

2)选择 $\alpha \xleftarrow{R} F_p$,并且定义 $u := h^\alpha$;

3)定义哈希函数 $H: Z \times Z \to G_1$;

4)公钥为 $PK := (G,H,g_1,\cdots,g_N,h,u)$,私钥为 $SK := \alpha$。

2.1.2 签名 $Sign(PK,id,m,v)$

给定的公钥为 $PK = (g_1,\cdots,g_N,h,u)$,定义 $id \in \{0,1\}^k$,整数 m 指明签名空间,一个分量 $\boldsymbol{v} \in F_p^N$,设定 $n := N - m$,输出签名:$\sigma := \left(\prod_{i=1}^{m} H(id,i)^{v_{n+1}} \prod_{j=1}^{n} g_j^{v_j}\right)^u$。

这个签名和文献[4]相似,但是使用了接收信息的节点的公钥签名,保证了只有拥有使用签名时的公钥对应的私钥解密才可以得到正确的消息内容,从而实现了在网络中限定节点查看信息。

2.1.3 联合 $Combine(SK,id,\{(\beta_i,\sigma_i)\}_{i=1}^{l})$

秘密的私钥为 SK,一个文件的编号 id,l 对权重 $\beta_i \in F_p$ 和签名 σ_i,计算输出 $\sigma := \prod_{i=1}^{l} \sigma_i^{\beta_i}$。

2.1.4 验证 $Verify(SK,id,m,y,\sigma)$

给定一个私钥 $SK := \alpha$ 和编号 id,一个指明签名空间的整数 m,一个签名 σ 和向量 $\boldsymbol{y} \in F_p^N$,计算 $n := N - m$,并且定义 $\gamma_1(SK,\sigma) \xlongequal{\text{def}} e(\sigma,h)$ 和 $\gamma_2(SK,id,m,\boldsymbol{y}) \xlongequal{\text{def}} e\left(\prod_{i=1}^{m} H(id,i)^{y_{n+i}} \prod_{j=1}^{n} g_j^{y_j},\alpha\right)$ 如果 $\gamma_1(SK,\sigma) = \gamma_2(SK,id,m,\boldsymbol{y})$ 则算法输出 1,否则输出 0。1 表示验证通过,0 表示验证失败。

证明

令 $\{(v_k,\sigma_k)\}_{k=1}^{l}$ 是一个分量的消息—签名对,对于所有的 k 而言 $\gamma_1(SK,\sigma_k) = \gamma_2(SK,id,m,v_k)$。

令 $\beta_1,\beta_2,\cdots,\beta_l \in F_p$,$y = \sum_{k=1}^{l} \beta_k v_k$,$\sigma := Combine(SK,id,\{(\beta_k,\sigma_k)\}) = \prod_{k=1}^{l} \sigma_k^{\beta_k}$,根据 e 的性质,可以得到

$$\gamma_1(SK,\sigma) = e\left(\prod_{i=1}^{m} \sigma_i^{y_{n+i}},h\right) = e\left(\prod_{i=1}^{m} H(id,i)^{y_{n+i}} \prod_{j=1}^{n} g_j^{y_j},\alpha\right) \prod_{k=1}^{l} e(\sigma_k,h)^{\beta_k} = \prod_{k=1}^{l} \gamma_1(SK,\sigma_k)^{\beta_k}$$

$$\gamma_2(SK,id,m,y) = e\left(\prod_{i=1}^{m} H(id,i)^{y_{n+i}} \prod_{j=1}^{n} g_j^{y_j},\alpha\right) = e\left(\left(\prod_{i=1}^{m} H(id,i)^{\sum_{k=1}^{l}\beta_k v_{k,n+i}}\right)\left(\prod_{j=1}^{n} g_k^{\sum_{k=1}^{l}\beta_k v_{k,j}}\right),\alpha\right) = e\left(\left(\prod_{k=1}^{l}\prod_{i=1}^{m} H(id,i)^{\beta_k v_{k,n+i}}\right)\left(\prod_{k=1}^{l}\prod_{j=1}^{n} g_j^{\beta_k v_{k,j}}\right),\alpha\right) = \prod_{k=1}^{l} e\left(\prod_{i=1}^{m} H(id,i)^{v_{k,n+i}} \prod_{j=1}^{n} g_j^{v_{k,j}},\alpha\right)^{\beta_k} = \prod_{k=1}^{l} \gamma_2(SK,id,v_k)^{\beta_k}$$

得证 $\gamma_1(SK,\sigma) = \gamma_2(SK,id,m,y)$ 的正确性。

2.2 安全性证明

攻击者要阅读自己没有权限查看的信息,就必须通过询问被攻击者以试图得到被攻击者的私钥,这样才能解密信息,下面就利用密钥交换的安全性基于离散对数问题的困难性,Diffie-Hellman 能够抵抗离散对数攻击这一原理予以证明该方案的安全性。

假设 A 为攻击者,构造一个算法 B,输入 $g \in G_1,h,z \in G_2$,且 $z = h^x$,输出 $\omega \in G_1$,算法 B 模拟哈希函数 H 以及方案一中的算法 $Setup$ 和 $Sign$。

2.2.1 $Setup$

当 A 询问 $Setup(1^k,N)$,算法 B 做如下工作:

1)建立一个双线性组 $G = (G_1,G_2,G_T,e,\varphi)$,$G_1,G_2,G_T$ 的素数阶 $p > 2^k$;

2)选择随机的 $s_1,t_1,s_2,t_2,\cdots,s_N,t_N \in F_p$,设定 $g_j = g^{s_j}\varphi(h)^{t_j}$,其中函数 φ 为同态映射,$j = 1,2,\cdots,N$;

3)输出公钥 $PK := (G,H,g_1,\cdots,g_N,h,z)$,$H$ 为算法 B 模拟的哈希函数。

2.2.2 $Hash\ query$

当 A 询问 $H(id,i)$ 的值时,算法 B 做如下工作:

1)如果 $H(id,i)$ 已经被询问过,则返回 $H(id,i)$;

2)如果 $H(id,i)$ 没有被询问过,选择随机的 $\zeta_i,\tau_i \in F_p$,设定 $H(id,i) := g^{\zeta_i}\varphi(h)^{\tau_i}$。

2.2.3 $Sign$

当 A 在向量空间 $\boldsymbol{V} \subset F_p^N$ 上询问一个签名,基向量 $\boldsymbol{v}_1,\cdots,\boldsymbol{v}_m \in F_p^N$,算法 B 做如下工作:

1)选择 $id \xleftarrow{R} \{0,1\}^k$,当 i 时的 $H(id,i)$ 被询问过了,那

么模拟失败,其中 $i \in \{1,2,\cdots,m\}$;

2)设定 $n:=N-m$,计算 $i=1,2,\cdots,m$ 时的 $\zeta_i=-\sum_j^n s_j v_{ij}$,设定 $s:=(s_1,s_2,\cdots,s_n,\zeta_1,\zeta_2,\cdots,\zeta_m)$;

3)选择 $i=1,\cdots,m$ 时的 $\tau_i \xleftarrow{R} F_p$,设定 $t:=(t_1,\cdots,t_n,\tau_1,\cdots,\tau_m)$;

4)设定 $i=1,\cdots,m$ 时的 $H(id,i):=g^{\zeta_i}\varphi(h)^{\tau_i}$;

5)计算 $\sigma_i:=\varphi(z)^{v_{it}}$;

6)输出 id 和 $\sigma:=(\sigma_1,\cdots,\sigma_m)$。

2.2.4　*Output*

如果 B 没有做上面的工作,最后 A 输出一个 m 长的签名 σ,一个代号 id 和一个非零的向量 $\boldsymbol{y}$。

1)如果 id 不是签名询问选择过的代号,对 $i=1,\cdots,m$ 时的 $H(id,i)$ 执行哈希询问,设定 $s:=(s_1,\cdots,s_n,\zeta_1,\cdots,\zeta_m)$ 和 $t:=(t_1,\cdots,t_n,\tau_1,\cdots,\tau_m)$;

2)如果 id 是签名询问选择过的代号,让 s 和 t 等于那次询问时的向量;

3)设定 $n:=N-m$,并输出:

$$\omega:=\left(\frac{\prod_{i=1}^{m}\sigma_i^{y_{n+i}}}{\varphi(z)^{ty}}\right)^{1/(sy)} \tag{1}$$

当公钥 PK 对应的私钥 SK 是 x,对于每一个向量 $\boldsymbol{v}_i$ 我们都可以根据 B 模拟的算法 Sign 和哈希询问,以及 B 的输出签名 σ 得到:

$$\left(\prod_{i=1}^{m}H(id,i)^{v_{i,n+1}}\prod_{j=1}^{n}g_j^{v_{i,j}}\right)^x=\varphi(z)^{v_{it}} \tag{2}$$

而由算法 B 模拟的真正签名为:

$$\left(\prod_{i=1}^{m}(g^{\zeta_i}\varphi(h)^{\tau_i})^{v_{i,n+1}}\prod_{j=1}^{n}(g^{s_j}\varphi(h)^{t_j})^{v_{i,j}}\right)^x=(g^{sv_i}\varphi(h)^{tv_i})^x \tag{3}$$

因为构造的 $s\in V^{\perp}$,所以对于每一个 i 来说 $sv_i=0$,则 $\varphi(z)=\varphi(h)^x$。

假设 B 没有做如上工作,攻击者 A 输出一个签名 σ,一个代号 id,一个非零向量 $\boldsymbol{y}$,设定 $\sigma:=(\sigma_1,\cdots,\sigma_m)$,那么如果 $Verify(SK,id,m,y,\sigma)=1$,则:

$$e\left(\prod_{i=1}^{m}\sigma_i^{y_{n+i}},h\right)=e\left(\prod_{i=1}^{m}H(id,i)^{y_{n+i}}\prod_{j=1}^{n}g_j^{y_j},\alpha\right)$$

由式(3)可得:$e(g^{sy}\varphi(h)^{ty},z)=e(g^{x(sy)}\varphi(z)^{ty},h)$,再由式(1)和式(2)以及 e 的性质可得:$\prod_{i=1}^{m}\sigma_i^{y_{n+i}}=g^{x(sy)}\varphi(z)^{ty}$。

当 $sy\neq 0$ 时,可根据 B 输出的 ω 计算出 g^x,这与 Diffie-Hellman 能够抵抗离散对数攻击这一原理相矛盾,说明攻击失败,且 $sy=0$ 的概率是 $1/p$ [4],即证明此方案是安全的。

2.3　方案二

方案二适用于网络环境中许多节点之间需要传递信息通信,又为了避免没有权限查看信息的节点查看到网络中传输信息的内容。其思想是多个需要通信的节点首先协商建立通信会话钥,然后使用协商好的会话钥签名、解密消息,得到真正的信息内容,从而保证信息在网络中即使泛滥传递,也可以确保通信节点之间信息传递的安全性,使得信息得以有限的阅读。

会话钥是在需要通信的节点在交互通信中产生的,并且可以防止攻击者进行字典攻击,确保了会话钥的安全性,保证了信息的安全。详细证明参见文献[5]。这里不再详细证明。

假设　S 表示会话的发起者,C 表示会话参与者,SK 表示私钥,PK 表示公钥。会话钥 sk。

优点　在支持多节点之间信息通信的前提下,保证了通信组中信息传递的安全性,非通信组成员无权查看通信组成员之间传递的信息,确保了组成员之间信息的安全,从而限定了查看信息的节点。

缺点　在节点相互通信之前,通信节点之间必须首先协商建立通信会话钥,然后使用会话钥对传递信息进行签名、解密通信,这样就增加了第一次通信时的代价,但是在长期确定、不变的通信组内利用此方案进行通信前的协商组密钥的代价就微乎其微了。具体描述如下:

2.3.1　构造 *Setup*

选择一个安全参数 1^k 和一个有效的整数 N。

1)生成一个双线性组 $G=(G_1,G_2,G_T,e,\varphi),G_1,G_2,G_T$ 由素数 $p>2^k$ 决定。选择生成元 $g_1,\cdots,g_N \xleftarrow{R} G_1\backslash\{1\}$;

2)定义哈希函数 $H:Z\times Z\to G_1$;

3)一个素数 q 的循环群 G_q,f 是 G_q 的生成元;

4)一对加解密算法 (E,D);

5)三个单项哈希函数 H_1,H_2,H_3。

生成会话钥第一轮:

S 选择 n 个随机数 $s_1,\cdots,s_n\in Z_q^*$,计算 $t_1=E_{PK_1}(f^{s_1})$,$\cdots,t_n=E_{PK_n}(f^{s_n})$,然后发送 t_i 到 C_i,同时每一个 C_i 选择一个随机数 $x_i\in Z_p^*$,计算 $y_i=E_{SK_i}(f^{x_i})$,然后广播 y_i。S 和 C_i 分别用 C_i 的 PK_i,SK_i 解密得到的 y_i 和 t_i,然后共享 $sk_i=H_1(sid\|f^{s_ix_i})$,其中 $sid=y_1\|y_2\|\cdots\|y_n$。

生成会话钥第二轮:

S 随机选择一个秘密的 $K\in Z_p^*$,并且为每一个 $1,2,\cdots,n$ 计算 $k_i=K\oplus sk_i$ 和 $\varphi_i=H_2(sk_i\|S)$,然后 S 向所有的 C_i 广播 k_i 和 φ_i,与此同时,C_i 计算并且广播 $\eta_i=H_2(sk_i\|C_i)$,S 验证每一个 η_i 防止字典攻击,C_i 验证每一个 φ_i,当 C_i 验证通过,计算 $K=k_i\oplus sk_i$,并得到会话钥 $sk=H_3(SID\|K)$,其中 $SID=sid\|k_1\|k_2\|\cdots\|k_n$。

2.3.2　签名 $Sign(sk,id,m,v)$

会话钥 sk 只有通信节点才秘密的知道,定义 $id\in\{0,1\}^k$,整数 m 指明签名空间,一个分量 $\boldsymbol{v}\in F_p^N$,计算 $n:=N-m$,输出签名:$\sigma:=\left(\prod_{i=1}^{m}H(id,i)^{v_{n+1}}\prod_{j=1}^{n}g_j^{v_j},sk\right)$。

2.3.3　联合 $Combine(sk,id,\{(\beta_i,\sigma_i)\}_{i=1}^{l})$

会话钥 sk,一个文件的编号 id,l 对权重 $\beta_i\in F_p$ 和签名 σ_i,计算输出:$\sigma:=\prod_{i=1}^{l}\sigma_i^{\beta_i}$。

2.4　验证 $Verify(sk,id,m,y,\sigma)$

会话钥 sk,编号 id,一个指明签名空间的整数 m,向量 $\boldsymbol{y}\in F_p^N$,一个签名 σ,计算 $n:=N-m$,并且定义 $\gamma_1(sk,\sigma)\overset{\text{def}}{=\!=}e(\sigma,sk)$ 和 $\gamma_2(sk,id,m,y)\overset{\text{def}}{=\!=}e(\prod_{i=1}^{m}H(id,i)^{y_{n+i}}\prod_{j=1}^{n}g_j^{y_j},sk)$,如果 $\gamma_1(sk,\sigma)=\gamma_2(sk,id,m,y)$ 则算法输出 1,否则输出 0。1 表示验证通过,0 表示验证失败。

(下转第 1879 页)

时,从密钥路径的建立概率与妥协节点比率之间的关系来进一步验证算法的抗节点妥协性能。

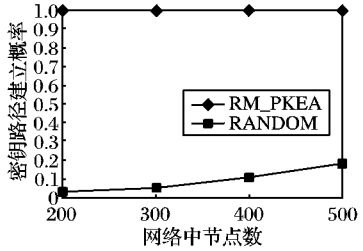

图 1　密钥路径建立概率随网络规模变化情况

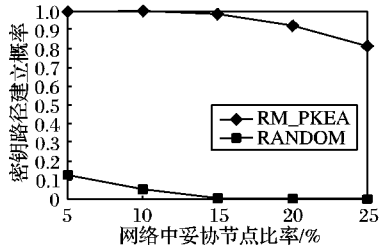

图 2　密钥路径建立概率随妥协节点比例变化情况

由图 2 可知,本文提出的新方法在网络中存在妥协节点时,密钥路径的建立概率要远远优于传统的基于密钥预置技术的对偶密钥建立算法。特别地,即便是网络中存在大量的妥协节点时,本文提出的新方法仍能在很大程度上保证非妥协节点之间的安全通信。

4　结语

本文研究传感器网络中的对偶密钥建立技术,提出了一种动态对偶密钥建立算法,与传统的单纯基于密钥预置技术的对偶密钥建立算法相比,新算法具有 100% 的概率来建立邻节点之间的直接对偶密钥,从而使得能以更短的路径来建立节点直接的间接对偶密钥路径,能更有效地保障传感器网络的通信安全。

参考文献:

[1] POTTIE G, KAISER W. Wireless sensor networks[J]. Communications of the ACM, 2000, 43(5): 51 – 58.

[2] 成奋华, 周顺先, 王雷. 传感器网络中基于对偶编码的随机密钥建立算法研究[J]. 计算机应用, 2010, 30(6): 1495 – 1497.

[3] WEI REIZHONG, WU JIANG. Product construction of key distribution schemes for network[C]// Proceedings of ACM SIG Symposium on Applied Computing. New York: ACM, 2005, 3357: 280 – 293.

[4] SHEU J P, CHENG J C. Pair-wise path key establishment in wireless sensor networks[J]. Computer Communications, 2007, 30(11/12): 2365 – 2374.

[5] EESCHNAURE L, GLIGOR V D. A key-management scheme for distributed sensor networks[C]// Proceedings of the 9th ACM Conference on Computer and Communication Security. New York: ACM, 2002: 41 – 47.

[6] CHAN HAOWEN, OERRIG A, SONG D. Random key predistribution schemes for sensor networks[C]// IEEE Symposium on Research in Security and Privacy. Washington, DC: IEEE Computer Society, 2003: 197 – 213.

[7] LIU DONGGUANG, NING PENG. Establishing pairwise keys in distributed sensor networks[J]. ACM Transactions on Information and System Security, 2005, 8(1): 41 – 77.

[8] 王雷, 林亚平, 陈治平, 等. 超立方体系统中基于安全通路向量的容错路由[J]. 软件学报, 2004, 15(5): 783 – 790.

(上接第 1871 页)

两个方案的正确性证明类似,这里不再做详细证明。

方案二的安全性首先依赖于通信节点之间组密钥建立过程的安全性,其次依赖于签名过程的安全性。组密钥的生成过程是安全的,并且可以防止字典攻击,这点在参考文献[5]中以得到了详细的证明,而签名过程是在方案一的基础上改进得来,所以也是安全的。

3　结语

网络编码是针对网络组播业务而提出的有效的数据传输方式,但是现实中网络编码的应用还远未普及,基于网络编码的理论和新应用不断涌现,网络编码正给现有的网络带来了革命性的变化,但从研究的深度来看,仍处于探索阶段,有很多尚未解决和探索的领域。本文针对目前研究只重视网络信息的传输效率而忽略了信息通过网络编码后在网络中传输泛滥的特点,使得网络中的任意节点都可能阅读信息,为保证网络中信息的安全性做了一些改进,根据网络环境中需要查看信息的节点个数,提出了两种解决方案,这样就限定了节点查看消息的权利,从而保证了信息的安全性。

对于网络编码中限定节点查看消息的研究还很不足,不仅仅局限于当前两种方案,在具体网络应用环境中,还会有不同的方式来确保信息在提高传输效率的同时保证信息的安全性,是今后学习和研究中值得关注的地方。

参考文献:

[1] 代青. 浅谈网络编码技术[J]. 电脑知识与技术, 2009, 5(26): 7383 – 7384, 7389.

[2] AHLSWEDE R, NING CAI, LI S Y R, *et al*. Network information flow[J]. IEEE Transactions on Information Theory, 2000, 46(4): 1204 – 1216.

[3] 陶少国, 黄佳庆, 杨宗凯, 等. 网络编码研究综述[J]. 小型微型计算机系统, 2008, 29(4): 583 – 592.

[4] BONEH D, FREEMAN D, KATZ J, *et al*. Signing a linear subspace: Signature schemes for network coding[C]// PKC' 09: Public-key Cryptography, LNCS 5443. Berlin: Springer, 2009: 68 – 87.

[5] NAM J, HAN S, PARK M, *et al*. Enhancing security of a group key exchange protocol for user with individual passwords[C]// The 2009 International Conference on Computational Science and Applications 2009, LNCS 5593. Berlin: Springer, 2009: 173 – 181.

[6] WU Y, CHOU P A, JAIN K, *et al*. A comparison of network coding and tree packing[C]// IEEE International Symposium on Information Theory. New York: IEEE, 2004: 143.

[7] HO T, MEDARD M, KOETTER R, *et al*. An information-theoretic view of network management[J]. IEEE Transactions on Information Theory, 2005, 51(4): 1295 – 1312.

[8] HO T, LEOND B, CHANG YU-HAN, *et al*. Network monitoring in multicast networks using network coding[C]// IEEE International Symposium on Information Theory. New York: IEEE, 2005: 1977 – 1981.

[9] YUN A, CHEON J, KIM Y. On homomorphic signatures for network coding[J]. IEEE Transactions on Computers, 2010, 59(9): 1295 – 1296.

[10] YAN WEN-JIE, YANG MING-XI, LI LA-YUAN, *et al*. Short signatures for multi-source network coding[C]// 2009 International Conference on Multimedia Information Networking and Security. Washington, DC: IEEE Computer Society, 2009: 458 – 462.