计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2022,31(5):254–261 [doi: 10.15888/j.cnki.csa.008531]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

抗 BGP 中间人攻击的无证书签名方法①

韩增杰, 胡　杨, 姚志强

(福建师范大学 计算机与网络空间安全学院, 福州 350117)
通信作者: 姚志强, E-mail: yzqfzfj@fjnu.edu.cn

摘　要: 边界网关协议用于自治域之间交换网络可达信息, 但面临中间人攻击威胁, 因此提出一种改进的无证书多重签名方案并将其应用于边界网关协议. 在该方案中域间路由须按照路由传递顺序对其进行签名, 自治系统对多重签名验证成功才可接收路由, 且自治系统的公私钥与可信中心交互生成, 签名消息的长度固定, 计算高效. 通过安全性分析, 证明基于无证书的有序多重签名方案在随机预言机模型下具有不可伪造性, 将其应用到边界网关协议中可以抵抗中间人攻击.

关键词: 无证书签名; 多重签名; 中间人攻击; 前缀劫持; 边界网关协议; 签名方案

引用格式: 韩增杰,胡杨,姚志强.抗 BGP 中间人攻击的无证书签名方法.计算机系统应用,2022,31(5):254–261. http://www.c-s-a.org.cn/1003-3254/8531.html

Prevention of Man-in-the-middle Attacks on BGP Using Certificateless Signatures

HAN Zeng-Jie, HU Yang, YAO Zhi-Qiang

(College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China)

Abstract: The border gateway protocol (BGP) is used to exchange network reachability information between autonomous systems, but it is threatened by man-in-the-middle attacks. Therefore, an improved certificateless multi-signature scheme is proposed and applied to BGP. The inter-domain routing must be signed according to the route delivery order, and the autonomous systems can receive the route only after the multi-signatures are verified successfully. The public and private keys to the autonomous systems are generated interactively with the trusted center with a fixed length of the signature message and efficient calculations. The security analysis proves that the proposed scheme cannot be fabricated under the random oracle model and is valid for resisting the man-in-the-middle attacks on BGP.

Key words: certificateless signature; multi-signature; man-in-the-middle attack; prefix hijacking; border gateway protocol (BGP); signature scheme

边界网关协议 (border gateway protocol, BGP) 的作用是在不同的自治系统之间传递路由, 通过 BGP 提供的各种路由属性为自治系统通信提供最佳路径. 由于 BGP 协议的通信双方无条件信任彼此, 自治系统不验证路由信息的有效性, 因此容易受到中间人攻击[1]. BGP 的中间人攻击主要包括前缀劫持攻击和路径伪造攻击. 中间人可以宣布自己为目标前缀的起源, 通告一个比目标前缀更长的虚假路由, 其余的 BGP 路由器在接收到这些虚假的通告后将其放到路由表中传送数据. 如果中间人将劫持的路由信息丢弃, 则通信双方不可达, 产生路由黑洞; 如果中间人把自己作为中转中心, 将受害者路径重定向到目标网络, 原始路径依旧可达, 恶意的中间人可以随时窃听双方的通信, 导致消息泄露. 中间人攻击能够得逞的原因是由于缺少对路由消

① 基金项目: 国家自然科学基金 (61872090, 61972096); 福建省引导性科技项目 (2019H0010)
收稿时间: 2021-08-02; 修改时间: 2021-09-09, 2021-09-22; 采用时间: 2021-10-19; csa 在线出版时间: 2022-02-21

息来源以及对 AS-PATH 路径的认证, 目前针对中间人攻击的研究方案主要分为两大类, 一类是以 S-BGP 为代表的安全扩展技术, 另一类是当发生中间人攻击时及时响应的异常检测技术. 在使用证书的 BGP 安全扩展方案中, 证书的颁布和撤销都是复杂的过程, 而无证书方法只需要引入可信的第三方与用户交互生成公私钥即可, 不需要引入证书, 因此本文提出无证书的签名方法来防止中间人攻击.

1 相关研究

针对 BGP 的中间人攻击, S-BGP[2] 通过公钥基础设施为每个 AS 颁发证书来验证路由的起始源, 通过签名的方式使得攻击者无法劫持, 但由于 S-BGP 采用基于证书的安全扩展方案来防御中间人攻击, 在域间路由验证时会产生较大的计算开销和存储代价, 难以实施. 文献 [3] 提出一种改进的 BGP 路由源认证方案. 将从 RP 获取的 ROA 证书附加到更新报文中, 接收端从 RP 申请可信的 ROA 证书公钥并进行解密, 通过与更新报文比较从而验证路由源的真实性. 文献 [4] 针对路由传输路径上的负载变化提出了前缀劫持检测系统 LDC, 攻击者发动前缀劫持后流量负载会发生异常. 文献 [5] 根据 BGP 在受到中间人攻击时路由控制平面路径和真实转发路径不一致的特征, 提出一种针对中间人攻击的实时检测系统, 但该方案无法检测延长距离为 1 的中间人攻击. 文献 [6] 提出了一种实时检测与缓解系统 ARTEMIS, 由 AS 本身检测和自动缓解针对其自身前缀的劫持, 该方案利用控制面板监视的最新进展实时检测前缀劫持, 并且会进行自动缓解. Li 等人[7] 提出了针对 BGP 的特殊中间人攻击 Tiger 攻击, Tiger 攻击不会破坏路由在控制平面和数据平面一致性, 因此可以规避现有的检测方案. Alkadi 等人[8] 针对前缀劫持提出了一种实时处理方法 OGI, 通过 AS 本身来检测由被劫持节点引起的可疑传输自治系统. 邓海莲等人[9] 从 Route Views 系统获取路由信息, 根据路由变化的幂律性建立正常域间路由模型, 从而检测前缀劫持和路径篡改等异常行为. 大多数针对 BGP 的中间人攻击检测系统通常是在前缀劫持发生后进行的检测机制, 因此无法从根本上解决 BGP 的中间人攻击.

为解决基于身份的密码体制中私钥生成中心 (PKG) 可能造成的伪造签名攻击, Al-Riyami 等人[10] 提出了无证书公钥密码体制. 该体制通过引入可信中心 KGC 来产生用户的部分私钥, 用户根据随机生成的秘密值产生另一部分私钥, 完整私钥由用户自己保存. 陈亚萌等人[11] 提出的基于双线性对的无证书签名方案成员交互次数过多, 效率较低. 刘帅等人[12] 提出的基于椭圆曲线的无证书签名方案在计算效率上有一定的提升, 但是签名长度不固定, 会随着签名人数的增加而改变.

将无证书公钥密码体制和有序多重签名结合构造成无证书的有序多重签名, 既可以解决传统签名方案中公钥合法性和私钥托管问题, 又可以解决签名时多个签名人无法有序验证的问题. 罗文俊等人[13] 提出一种不含双线性对运算的无证书签名方案, 计算效率较高, 但是该方案的签名长度不固定, 且签名人数越多, 通信效率越低. 秦艳琳等人[14] 提出的无证书有序多重签名方案被许艳等人[15] 通过安全性分析证明其无法抵抗伪造攻击, 许艳等人对方案进行改进从而使其能够抵抗伪造攻击. 但是杜红珍等人[16] 提出许艳等人的方案存在不足, 并且通过修改后发现其验证过程需要 n+1 个双线性对计算, 计算效率大大降低. 孙玉等人[17] 提出的多重签名方案没有验证签名者的顺序, 各个签名成员可以私自改变签名顺序从而伪造签名.

为了从根本上解决 BGP 协议中存在的中间人攻击, 本文从有序多重签名出发, 结合无证书签名方案的优势, 在路由传递过程中源 AS 和传播 AS 需要按序对路由信息进行多重签名, 路由信息接收者通过正确的签名顺序对其进行验证, 从而解决域间路由在传递过程中的路径认证问题. 该方案不仅解决了传统公钥密码体制中存在的证书管理问题和基于身份的密码体制中秘钥生成中心伪造签名的问题, 同时能够抵抗边界网关路由协议的中间人攻击.

2 无证书有序多重签名方案

无证书多重签名方案通常是以双线性对为工具构造的, 也有研究人员提出不含双线性对的无证书有序多重签名方案, 本文采用基于双线性对的多重数字签名方案, 其安全性是基于离散对数和计算性 Diffie-Hellman 问题, 这里不再赘述双线性对和困难问题定义.

无证书有序多重签名方案的步骤如下:

(1) 初始化系统参数: KGC 生成参数 *params*、系统主密钥和系统公钥, 将 *params* 对用户公开.

(2) 生成秘密值: 用户 N_i 随机生成秘密值, 并根据参数 *params* 生成部分公钥.

(3) 生成部分私钥: KGC 验证用户的身份, 并根据参数 *params* 生成对应的部分私钥发送给用户 N_i.

(4) 生成完整公私钥: 用户 N_i 通过参数 *params* 验证部分私钥, 生成完整公钥和完整私钥.

(5) 用户签名: 输入消息 m 和 *params* 生成部分签名σ_i, 并将部分签名发送给后续签名成员.

(6) 验证签名: 验证上一个签名成员的签名结果σ_i是否正确. 若正确, 则继续签名, 否则停止签名.

为简述方便, 将方案中使用的符号和含义列于表 1. 无证书有序多重签名方案主要包括注册阶段、签名阶段和整体验证阶段, 其中注册阶段包括 KGC 初始化系统参数及用户公私钥的生成; 签名阶段包括每个用户的部分签名; 整体验证阶段是对生成的完整签名进行验证. 下面详述无证书有序多重签名方案的具体过程:

(1) 注册阶段

1) 初始化系统参数: KGC 选择椭圆曲线上的点构成阶为 q 的循环群 G 和 G_T, 其中, q 为大素数, G 为加法循环群, 记为 $(G, +)$, G_T 为乘法循环群, 记为 $(G_T, \cdot)$, 双线性映射 e: $G\times G \to G_T$. 选择两个安全的哈希函数 H_1 和 H_2, 其中, H_1:$\{0, 1\}^*\times G\times G\to Z_q^*$, H_2:$\{0, 1\}^*\to Z_q^*$. KGC 随机选择$s\in Z_q^*$, 计算 $P_0=sP$, 其中, P 为群 G 的一个生成元, s 为系统主密钥由 KGC 安全保存, P_0 为系统公钥, 将参数 $params=\{G, G_T, q, e, P, P_0, H_1, H_2\}$对用户公开.

2) 生成用户部分公钥: 用户 N_i 将自己的用户身份 ID_i 发给 KGC, 随机选择$x_i\in Z_q^*$作为秘密值, 生成用户的部分公钥 P_i, 将部分公钥发送给 KGC.

$$P_i = x_iP \tag{1}$$

3) KGC 为用户生成部分私钥: KGC 验证用户 N_i 的身份 ID_i, 为用户生成$r_i\in Z_q^*$, 计算 R_i、Q_i、z_i, 通过安全信道将 (R_i, z_i) 发送给用户 N_i.

$$\begin{cases} R_i = r_iP \\ Q_i = H_1(ID_i, R_i, P_i) \\ z_i = r_i + Q_is \end{cases} \tag{2}$$

4) 用户生成完整公私钥: 用户收到 (R_i, z_i) 后, 计算 Z_i, 验证 $Z_i=R_i+H_1(ID_i, R_i, P_i)P_0$ 是否成立, 若不成立, 则返回到第 2 步重新计算; 若成立, 则用户的完整公钥为 (P_i, R_i, Z_i), 计算 w_i, 用户的完整私钥为 (x_i, w_i).

$$\begin{cases} Z_i = z_iP \\ w_i = (z_i + x_iH_1(ID_i, R_i, P_i))^{-1} \end{cases} \tag{3}$$

表 1 符号说明

符号	含义
G, G_T	循环群
P	生成元
q	大素数
H_1, H_2	哈希函数
Q_i, V_i, h_{1i}, h_{2i}	哈希值
N_i, ID_i	用户身份标识
s	系统主私钥
P_0	系统公钥
x_i	用户秘密值
P_i, R_i, Z_i	用户公钥
x_i, w_i	用户私钥
r_i, d_i, g_i	随机数
S	签名者身份集合
T_i	字符串
A, A_1, A_2	攻击者
D	挑战者
L_1, L_2, L_3, L_4	查询表
$\perp$	未知值
T_m	模乘运算开销
$\|G\|$	椭圆曲线上点的长度

(2) 签名阶段

1) 第一个签名用户对消息 m 进行部分签名:

① 选择随机数$d_1\in Z_q^*$, 计算 D_1:

$$D_1 = d_1P \tag{4}$$

② 计算 V_1, 其中, S 为 n 个签名者的身份集合, 记为 $S=\{ID_1, ID_2, \cdots, ID_i, \cdots, ID_n\}$, T_i 是长度为 n 的$\{0, 1\}^n$ 字符串, 其中, 第 $n–i+1$ 位为 1, 其余位为 0.

$$V_1 = H_2(m \| P_1 \| Z_1 \| P_0 \| S \| T_1 \| D_1) \tag{5}$$

③ 用户 N_1 对消息 m 的部分签名结果为$Sign_1$, 令 $\sigma_1 = Sign_1$, 用户 N_1 将部分签名结果(m,σ_1,D_1), 发送给下一个待签名用户.

$$Sign_1 = (x_1H_2(m \| P_1 \| Z_1 \| P_0 \| S \| T_1 \| D_1) + d_1)w_1 \tag{6}$$

2) 第 i 个签名用户 N_i 收到上一个用户的签名结果 (m,σ_{i-1},D_{i-1}), 首先对σ_{i-1}进行验证, 若验证不通过, 则停止签名. 无证书有序多重签名的正确性通过双线性对性质计算易得:

$$\prod_{i=1}^{n} e((D_i + V_iP_i)(R_i + (P_0 + P_i)Q_i)^{-1}, P) = e(\sigma_n, P) \tag{7}$$

通过上式验证用户的部分签名和完整签名. 验证过程如下:

① 计算 Q_j、V_j, 其中, $1 \leqslant j \leqslant i–1$:

$$\begin{cases} Q_j = H_1\left(ID_j, R_j, P_j\right) \\ V_j = H_2\left(m \| P_j \| Z_j \| P_0 \| S \| T_j \| D_j\right) \end{cases} \tag{8}$$

② 验证等式:

$$e(\sigma_{i-1}, P) = \prod_{j=1}^{i-1} e((D_j + V_j P_j)(R_j + (P_0 + P_j)Q_j)^{-1}, P) \tag{9}$$

3) 若式 (9) 成立, 则用户 N_i 对上一个用户的签名结果进行签名:

① 选择随机数$d_i \in Z_q^*$, 计算 D_i:

$$D_i = d_i P \tag{10}$$

② 计算 V_i:

$$V_i = H_2(m \| P_i \| Z_i \| P_0 \| S \| T_i \| D_i) \tag{11}$$

③ 则用户 N_i 对消息 m 的部分签名结果为$Sign_i = (x_i V_i + d_i) w_i$, 令$\sigma_i = Sign_i + \sigma_{i-1}$, 用户 N_i 将部分签名结果(m, σ_i, D_i), 发送给下一个待签名用户.

(3) 整体验证阶段

最终得到完整签名(m, σ_n, D_n), 验证式 (12) 是否成立:

$$\prod_{i=1}^{n} e((D_i + V_i P_i)(R_i + (P_0 + P_i)Q_i)^{-1}, P) = e(\sigma_n, P) \tag{12}$$

其中, $1 \leqslant i \leqslant n$, 若等式成立, 则签名正确, 否则签名错误.

3 效率分析

为方便计算, 本文将双线性对运算记为 BP, 椭圆曲线上的点乘计算记为 A, C 表示一次模乘运算, D 表示一次模逆运算, H 表示使用了一次哈希函数, 忽略模加和模减运算, 根据双线性对运算的性质, 验证公式右边可以化简为一个双线性对, 一次签名使用了一次哈希函数. 从表 2 可以看出在整体验证阶段, 文献 [15] 的方案需要 n+1 次双线性对运算, 而本文方案和文献 [16] 仅需要两个双线性对运算, 且比文献 [16] 在整体验证时少了 n 倍的哈希运算.

表 2 与其他方案比较

方案	注册阶段	签名阶段	整体验证
文献[13]	6A+3C+2H	2A+4C+2H	2nC+3nH
文献[15]	3A+2C+H	A+C+2H	(n+1)BP+2nA+3nH
文献[16]	3A+2C+H	A+C+2H	2BP+2nA+3nH
本方案	5A+C+D+H	A+2C+H	2BP+2nA+nD+2nH

表 2 中, 根据文献 [18] 和文献 [19] 提供的数据, 本文用 T_m 代表模乘运算所需的计算开销, 则模的取逆运算≈11.60T_m, 椭圆曲线标量乘运算≈29.00T_m, 映射到点的哈希运算≈29.00T_m, 双线性配对运算≈87.00T_m. 设置签名成员 n=5, 在 I5-4590、16 GB 内存和 Windows 7 操作系统环境下本方案在注册阶段用时为 0.63 ms, 签名阶段用时为 0.20 ms, 整体验证阶段用时为 2.75 ms. 从表 3 可以看出, 在安全性方面, 文献 [13] 无法抵抗第 2 类攻击者且签名长度不固定, 文献 [15] 提出的方案被杜红珍等人[16] 证明无法抵抗第 1 类攻击者和第 2 类攻击者, 本文在第 5.2 节对签名过程进行了详细的分析, 证明本方案能够同时抵抗这两类攻击者的伪造签名攻击. 通过在相同实验环境下分析得出本方案总体计算效率要高于文献 [15] 和文献 [16]: 文献 [15] 在签名阶段用时 0.29 ms, 在整体验证阶段用时 4.24 ms; 文献 [16] 在签名阶段的用时 0.29 ms, 在整体验证阶段的用时 3.06 ms. 本方案较文献 [15] 在整体验证效率上提升了约 35%, 较文献 [16] 在注册阶段提升了约 31%. 因注册阶段的效率基本相同, 考虑到各成员只进行一次注册阶段, 而签名过程需要多次验证, 因此随着签名人数的增多, 本方案的优势越明显. 同时本方案的签名长度固定, 验证者只需要验证最后产生的完整签名即可, 属于紧凑的有序多重签名.

表 3 安全性对比

方案	签名长度	第1类攻击者	第2类攻击者
文献[13]	不固定	安全	不安全
文献[15]	$\|G\|$	不安全	不安全
文献[16]	$\|G\|$	安全	安全
本方案	$\|G\|$	安全	安全

4 方案在 BGP 中的应用

4.1 基于无证书多重签名的 BGP 方案

基于证书的 BGP 安全扩展技术存在不足, 因此本文将无证书有序多重签名引入到 BGP 的路由信息认证中, 解决 S-BGP 的证书颁发和撤销的复杂问题. 基于无证书多重签名的 BGP 安全方案主要分为 KGC 初始化阶段、自治系统注册认证阶段、发布路由阶段和路由传播阶段.

(1) KGC 初始化阶段

KGC 初始化过程同无证书签名方案一致, 随机选择$s \in Z_q^*$, 计算 P_0=sP, 其中, P 为群 G 的一个生成元, s 为系统主密钥由 KGC 安全保存, P_0 为系统公钥, 将参数 $params$=$\{G, G_T, q, e, P, P_0, H_1, H_2\}$对用户公开.

(2) 自治系统注册认证阶段

自治系统需要向 KGC 注册, 获得合法成员身份:

1) 自治系统 AS_n 将自己的身份信息发给 KGC, 随机选择$x_i \in Z_q^*$作为秘密值, 生成部分公钥 $P_i=x_iP$, 将部分公钥发送给 KGC.

2) KGC 验证自治系统的身份后, 为其生成$r_i \in Z_q^*$, 计算 $R_i=r_iP$、Q_i、z_i, 通过安全信道将 (R_i, z_i) 发送给自治系统.

$$\begin{cases} Q_i = H_1(ID_i, R_i, P_i) \\ z_i = r_i + Q_i s \end{cases} \tag{13}$$

3) 自治系统收到 (R_i, z_i) 后, 计算 $Z_i=z_iP$, 验证 $Z_i=R_i+H_1(ID_i, R_i, P_i)P_0$ 是否成立, 若不成立, 则返回到第 2 步重新计算; 若成立, 则自治系统的完整公钥为 (P_i, R_i, Z_i), 计算 w_i, 自治系统的完整私钥为 (x_i, w_i).

$$w_i = (z_i + x_i H_1(ID_i, R_i, P_i))^{-1} \tag{14}$$

(3) 发布路由阶段

待发布路由的自治系统发布路由条目, 并且为其签名: 自治系统选择随机数$d_1 \in Z_q^*$, 计算 $D_1=d_1P$, 计算 V_1, 其中, S 为 n 个传输自治系统的身份集合, 记为 $S=\{ID_1, ID_2, \cdots, ID_i, \cdots, ID_n\}$, T_i 是长度为 n 的$\{0, 1\}^n$ 字符串, 其中, 第 $n–i+1$ 位为 1, 其余位为 0. 签名结果为 $Sign_1$, 令$\sigma_1= Sign_1$, 路由发布者将路由信息和签名结果(m,σ_1,D_1)发送给临近的自治系统.

$$\begin{cases} V_1 = H_2(m \| P_1 \| Z_1 \| P_0 \| S \| T_1 \| D_1) \\ Sign_1 = (x_1 H_2(m \| P_1 \| Z_1 \| P_0 \| S \| T_1 \| D_1) + d_1) w_1 \end{cases} \tag{15}$$

(4) 路由传播阶段

当前自治系统收到路由信息时, 需要验证签名结果, 若验证通过则将路由条目添加到路由表, 并将路由信息继续传输, 验证不通过则丢弃路由.

验证过程如下: 计算 Q_j, V_j, 其中, $1 \leqslant j \leqslant i–1$; 验证等式:

$$\begin{cases} e(\sigma_{i-1}, P) = \prod_{j=1}^{i-1} e((D_j + V_j P_j)(R_j + (P_0 + P_j)Q_j)^{-1}, P) \\ Q_j = H_1\left(ID_j, R_j, P_j\right) \\ V_j = H_2\left(m \| P_j \| Z_j \| P_0 \| S \| T_j \| D_j\right) \end{cases} \tag{16}$$

4.2 方案分析

4.2.1 抗伪造性

无证书的公钥密码体系中存在两类攻击者: 第 1 类攻击者 A_1 可以替换签名者的公钥进行签名, 但不知道系统主密钥; 第 2 类攻击者 A_2 可以获取系统主密钥, 但不能替换签名者的公钥. 本文通过定理 1 和定理 2 证明无证书多重签名无法被伪造.

定理 1. 在随机预言机模型下, 如果攻击者 A_1 能够以不可忽略的概率伪造出多重签名, 则挑战者 D 可以通过 A_1 解决 CDH 问题.

假设攻击者拥有最大优势已经获得 n–1 个签名者的签名, 即攻击者已经获得了 n–1 个签名者的私钥, 可以伪造出这 n–1 个签名者的签名, 为了证明本方案难以抵抗伪造性, 攻击者需要在多项式时间内以一个不可忽略的概率伪造出最后一个签名者的签名. D 已知 P, $X=aP$, $Y=bP$, 如果可以求出 abP, 则称 D 可以通过 A_1 解决 CDH 问题.

模拟过程如下:

D 将结合 CDH 困难问题模拟本方案, 选择椭圆曲线上的点构成阶为 q 的循环群 G 和 G_T, 其中, q 为素数, G 为加法群, G_T 为乘法群, 双线性映射 $e:G\times G\rightarrow G_T$. 选择两个安全的哈希函数 H_1 和 H_2, 其中, $H_1:\{0, 1\}^*\times G\times G\rightarrow Z_q^*$, $H_2:\{0, 1\}^*\rightarrow Z_q^*$. D 设置系统公钥 $X=xP=P_0$, 其中, P 为群 G 的一个生成元, 系统主密钥 x 对 D 未知, D 构造询问用户的身份集合 $S=\{ID_1, ID_2, \cdots, ID_i, \cdots, ID_{qc}\}$. D 维护 4 张表: L_1 对应用户的秘密值询问, L_2 和 L_4 分别对应哈希函数 H_1 和 H_2 的询问, L_3 对应用户的部分私钥询问, 将 $params=\{G, G_T, q, e, P, P_0, H_1, H_2\}$发送给 A_1, A_1 进行如下询问:

(1) 秘密值询问: A_1 询问 ID_i 的秘密值, 如果 L_1 列表中包含 (ID_i, x_i, P_i), 则 D 将 x_i 返回给 A_1, 否则 D 选择随机数$x_i \in Z_q^*$, 并计算 $P_i=x_iP$, 将 x_i 发送给 A_1, 在 L_1 列表中记录 (ID_i, x_i, P_i).

(2) 公钥替换询问: A_1 替换用户 N_i 的公钥, 输入用户的身份 ID_i 和被替换之后的公钥 P_i'以及私钥 x_i', D 更新列表 L_1.

(3) H_1 询问: A_1 输入 (ID_i, R_i, P_i), 如果 L_2 列表中包含 (ID_i, R_i, P_i, h_{1i}), 则将 h_{1i} 返回给 A_1, 如果 L_2 列表中没有相关信息, 则分两种情况讨论:

1) 若 $i\neq n$, D 随机选择$g_i \in Z_q^*$, 计算 $h_{1i}=g_iP$, 同时在 L_2 列表中记录 (ID_i, R_i, P_i, h_{1i}).

2) 若 $i=n$, D 随机选择$g_i \in Z_q^*$给 A_1, 计算 $h_{1i}=g_iY$, 同时在 L_2 列表中记录 (ID_i, R_i, P_i, h_{1i}).

(4) 部分私钥询问: A_1 询问用户 N_i 的部分私钥, 分

两种情况讨论:

1) 如果 $i=n$, 停止询问, 终止模拟过程;

2) 如果 $i\neq n$, 随机选择 z_i, 并计算 $Z_i=z_iP$ 和 $R_i=z_iP-h_{1i}P_0$, 记录到 L_3 表中.

(5) 公钥询问: A_1 询问用户 N_i 的公钥, 分两种情况讨论:

1) 如果 $i\neq n$, 查找用户 N_i 的公钥 (R_i, P_i, Z_i);

2) 如果 $i=n$, D 随机选择 r_i, 计算 R_i, 查找 P_i, 计算 Z_i, 同时更新 L_2 表;

(6) H_2 询问: 输入 $(m, P_i, Z_i, P_0, S, T_i, D_i)$, 如果 L_4 列表中包含 $(m, P_i, Z_i, P_0, S, T_i, D_i, h_{2i})$, 则返回 h_{2i}, 否则 D 随机选择 $h_{2i}\rightarrow Z_q^*$给 A_1, 同时在 L_4 列表中记录 $(m, P_i, Z_i, P_0, S, T_i, D_i, h_{2i})$.

(7) 部分签名询问: A_1 使用用户身份 ID_i 向 D 询问消息 m 的签名. 如果 $i=n$, 则停止签名, 停止模拟过程; 如果 $i\neq n$, 则 D 查询 L_2 表和 L_3 表, 计算$w_i=(z_i+x_ih_{1i})^{-1}$, 得到用户 N_i 的完整公私钥, 则用户 N_i 对消息 m 的签名为$Sign_i=(x_ih_{2i}+d_i)w_i$.

(8) 伪造签名: 通过上述询问过程得到一个完整签名(σ_n, D_n), D 验证式 (17) 是否成立来判断签名结果:

$$e(\sigma_n,P)=e((d_n+h_{2n}x_n)(r_n+sg_nY+x_nh_{1n})^{-1},P)\prod_{i=1}^{n-1}e(\sigma_{n-1},P) \tag{17}$$

若成立, 则根据分叉引理, 选择不同的哈希函数 h'_{2n}, 通过重放 A_1, D 可以得到对消息 m 的另一个有效签名(σ'_n, D_n), 验证式 (18) 是否成立:

$$e(\sigma'_n,P)=e((d_n+h'_{2n}x_n)(r_n+sg_nY+x_nh_{1n})^{-1},P)\prod_{i=1}^{n-1}e(\sigma_{n-1},P) \tag{18}$$

若成立, 则式 (17) 和式 (18) 相除可求解 sY 即 abP, 从而解决 CDH 困难问题, 这与定理 1 矛盾, 因此 A_1 无法伪造签名.

定理 2. 在随机预言机模型下, 如果攻击者 A_2 能够以不可忽略的概率伪造出多重签名, 则挑战者 D 可以通过 A_2 解决 ECDLP 问题.

假设攻击者拥有最大优势已经获得 n–1 个签名者的签名, 即攻击者已经获得了 n–1 签名者的私钥, 可以伪造出这 n–1 个签名者的签名, 为了证明本方案难以抵抗伪造性, 攻击者需要在多项式时间内以一个不可忽略的概率伪造出最后一个签名者的签名. D 已知用户 n 的公钥 U 和 P, 如果可以求出 u, 则可以通过 A_2 解决 ECDLP 问题.

模拟过程如下:

挑战者 D 选择椭圆曲线上的点构成阶为 q 的循环群 G 和 G_T, 其中, q 为素数, G 为加法群, G_T 为乘法群, 双线性映射 e: $G\times G\rightarrow G_T$. 选择两个安全的哈希函数 H_1 和 H_2, 其中, H_1: $\{0, 1\}^*\times G\times G\rightarrow Z_q^*$, H_2: $\{0, 1\}^*\rightarrow Z_q^*$. D 随机选择$s\in Z_q^*$, 计算 $P_0=sP$, 其中, P 为群 G 的一个生成元, s 为系统主密钥, P_0 为系统公钥, D 维护 4 张表: L_1 对应用户的秘密值询问, L_2 和 L_4 分别对应哈希函数 H_1 和 H_2 的询问, L_3 对应用户的部分私钥询问, 将 $params=\{G, G_T, q, e, H_1, H_2, P, P_0\}$和系统主密钥 s 发送给攻击 A_2, A_2 进行如下询问:

(1) H_1 询问: D 构造询问用户的身份集合 $S=\{ID_1, ID_2, \cdots, ID_i, \cdots, ID_{qc}\}$, A_2 输入 (ID_i, R_i, P_i), 如果 L_2 列表中包含 (ID_i, R_i, P_i, h_{1i}), 则 D 将 h_{1i} 返回给 A_2, 如果 L_2 列表中没有相关信息, 则 D 随机选择 $h_{1i}\rightarrow Z_q^*$给 A_2, 同时在 L_2 列表中记录 (ID_i, R_i, P_i, h_{1i}).

(2) 秘密值询问: A_2 询问 ID_i 的秘密值, 分两种情况讨论:

1) 如果 $i\neq n$, D 选择随机数$x_i\in Z_q^*$, 计算 $P_i=x_iP$, 将 x_i 发送给 A_2, 在 L_1 列表中记录 (ID_i, x_i, P_i).

2) 如果 $i=n$, 令 $P_i\leftarrow U$, 将 $(ID_i, \perp, P_i)$ 记录到表 L_1 中.

(3) 部分私钥询问: A_2 询问 ID_i 的部分私钥 z_i, D 选择两个随机数$a_i, b_i\in Z_q^*$, 其中, $r_i\leftarrow a_i$, $h_{1i}\leftarrow b_i$, 计算 $R_i=r_iP$, 将 (ID_i, R_i, h_{1i}) 记录到表 L_2 中, 计算 $z_i=r_i+sh_{1i}$, 计算 $Z_i=z_iP$, 在 L_3 中记录 (ID_i, z_i, Z_i).

(4) 公钥询问: A_2 询问 ID_i 的公钥, D 查询表 L_1、L_2、L_3, 将完整公钥发给 A_2.

(5) H_2 询问: A_2 输入 $(m, P_i, Z_i, P_0, S, T_i, D_i)$, 如果 L_4 列表中包含 $(m, P_i, Z_i, P_0, S, T_i, D_i, h_{2i})$, 则返回 h_{2i}, 否则 D 随机选择 $h_{2i}\rightarrow Z_q^*$给 A_2, 同时在 L_4 列表中记录 $(m, P_i, Z_i, P_0, S, T_i, D_i, h_{2i})$.

(6) 部分签名询问: A_2 使用用户身份 ID_i 向 D 询问消息 m 的签名. 如果 $i=n$, 则停止签名, 停止模拟过程; 如果 $i\neq n$, 则 D 查询 L_2 表和 L_3 表, 计算$w_i=(z_i+x_ih_{1i})^{-1}$, 得到用户 N_i 的完整公私钥, 则用户 N_i 对消息 m 的签名为$Sign_i=(x_ih_{2i}+d_i)w_i$.

(7) 伪造签名: 通过上述询问过程得到完整签名(σ_n, D_n), D 通过验证式 (19) 是否成立来判断签名:

$$e(\sigma_n,P)$$
$$=e((d_nP+h_{2n}\bar{x}P)(z_nP+\bar{x}Ph_{1n})^{-1},P)\prod_{i=1}^{n-1}e(\sigma_{n-1},P) \tag{19}$$

若成立, 则根据分叉引理, 选择不同的哈希函数 h'_{2n}, 通过重放 A_2, D 可以得到对消息 m 的另一个有效签名(σ'_n,D_n), 验证式 (20) 是否成立:

$$e(\sigma'_n,P)$$
$$=e((d_nP+h'_{2n}\bar{x}P)(z_nP+\bar{x}Ph_{1n})^{-1},P)\prod_{i=1}^{n-1}e(\sigma_{n-1},P) \tag{20}$$

若成立, 则式 (19) 和式 (20) 相除可求解 u 的值, 从而解决 ECDLP 困难问题, 这与定理 2 矛盾, 因此攻击者 A_2 无法伪造签名.

4.2.2 抗中间人攻击

在 BGP 中, 恶意的中间人通过伪造路由信息的方式, 使其在控制层面的转发路径和真实传输路径不一致, 导致面临威胁. 本方案中发布或者转发路由信息的自治系统需要向 KGC 注册身份信息, KGC 通过运营商验证自治系统的合法身份后才会向其分配部分私钥和完整的公钥. 其次在路由传递过程中包含了自治系统的身份集合$\{ID_1, ID_2, \cdots, ID_i, \cdots, ID_n\}$, 恶意的中间人无法伪造身份信息. 当中间人使用新的身份 ID 进行签名后, 下一个自治系统会通过原始的身份集合进行验证. 由于签名时的随机数发生改变, 根据无证书有序多重签名方案的验证方式, 下一个自治系统将无法验证, 则会停止签名, 并将验证失败的路由条目丢弃. 本方案通过签名的方式确保路由条目没有被篡改, 当攻击者和受害者前缀网络所在的自治系统相邻时同样满足上述的验证过程, 因此本方案也解决文献 [5] 方案存在的不足. 同时本方案存在用来表明签名顺序的 0-1 字符串, 每个自治系统都有固定的签名顺序, 各个自治系统不能擅自改变签名顺序来伪造签名.

5 结论

本文针对边界网关路由协议存在的中间人攻击威胁, 将无证书公钥密码体制和有序多重签名结合, 提出一种无证书的有序多重签名方案, 并对私钥生成过程和签名过程进行改进. 与同类型方案相比, 本文提出的签名方案在计算效率上有一定的提升, 同时能够抵抗 BGP 的中间人攻击.

参考文献

1 Conti M, Dragoni N, Lesyk V. A survey of man in the middle attacks. IEEE Communications Surveys & Tutorials, 2016, 18(3): 2027–2051.

2 Kent S, Lynn C, Seo K. Secure border gateway protocol (S-BGP). IEEE Journal on Selected Areas in Communications, 2000, 18(4): 582–592. [doi: 10.1109/49.839934]

3 贾佳, 延志伟, 耿光刚, 等. 一种改进的 BGP 路由源认证机制. 计算机系统应用, 2017, 26(1): 240–245. [doi: 10.15888/j.cnki.csa.005541]

4 Liu YJ, Su JS, Chang RKC. LDC: Detecting BGP prefix hijacking by load distribution change. 2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum. Shanghai: IEEE, 2012. 1197–1203.

5 黎松, 段海新, 李星. 域间路由中间人攻击的实时检测系统. 清华大学学报 (自然科学版), 2015, 55(11): 1229–1234.

6 Sermpezis P, Kotronis V, Gigis P, *et al*. ARTEMIS: Neutralizing BGP hijacking within a minute. IEEE/ACM Transactions on Networking, 2018, 26(6): 2471–2486. [doi: 10.1109/TNET.2018.2869798]

7 Li Q, Zhang XW, Zhang X, *et al*. Invalidating idealized BGP security proposals and countermeasures. IEEE Transactions on Dependable and Secure Computing, 2015, 12(3): 298–311. [doi: 10.1109/TDSC.2014.2345381]

8 Alkadi OS, Moustafa N, Turnbull B, *et al*. An ontological graph identification method for improving localization of IP prefix hijacking in network systems. IEEE Transactions on Information Forensics and Security, 2020, 15: 1164–1174. [doi: 10.1109/TIFS.2019.2936975]

9 邓海莲, 刘宇靖, 葛一漩, 等. 域间路由异常检测技术研究. 信息网络安全, 2019, (11): 63–70.

10 Al-Riyami SS, Paterson KG. Certificateless public key cryptography. 9th International Conference on the Theory and Application of Cryptology and Information Security. Taipei: Springer, 2003. 452–473.

11 陈亚萌, 程相国, 王硕, 等. 基于双线性对的无证书群签名方案研究. 信息网络安全, 2017, (3): 53–58. [doi: 10.3969/j.issn.1671-1122.2017.03.009]

12 刘帅, 陈建华. 无双线性对的无证书签名方案及其在配电网中的应用. 计算机科学, 2020, 47(9): 304–310. [doi: 10.11896/jsjkx.200500002]

13 罗文俊, 李长英. 一种不含双线性对的无证书有序多重签名方案. 计算机应用研究, 2012, 29(4): 1427–1429. [doi: 10.3969/j.issn.1001-3695.2012.04.063]

14 秦艳琳, 吴晓平. 高效的无证书有序多重签名方案. 通信学

报, 2013, 34(7): 105–110.
15 许艳, 黄刘生, 田苗苗, 等. 可证安全的高效无证书有序多重签名方案. 通信学报, 2014, 35(11): 126–131.
16 杜红珍, 温巧燕. 改进的无证书有序多重签名方案. 通信学报, 2015, 36(10): 56–61. [doi: 10.11959/j.issn.1000-436x.2015196]
17 孙玉, 刘贵全. 安全高效无证书有序多重签名方案. 重庆邮电大学学报 (自然科学版), 2016, 28(3): 431–434, 442.
18 Karati A, Islam SKH, Biswas GP. A pairing-free and provably secure certificateless signature scheme. Information Sciences, 2018, 450: 378–391.
19 He DB, Zeadally S, Xu BW, *et al*. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Transactions on Information Forensics and Security, 2015, 10(12): 2681–2691. [doi: 10.1109/TIFS.2015.2473820]