第 36 卷 第 4 期 计 算 机 工 程 2010 年 2 月
Vol.36 No.4 Computer Engineering February 2010
·安全技术· 文章编号：1000—3428(2010)04—0112—03 文献标识码：A 中图分类号：TP309

基于 WAP 的双向认证密钥协商方案

郑 旋，卢建朱，付 杰
(暨南大学信息科学技术学院，广州 510632)

摘 要：PKI 用证书管理公钥。无线网络设备的能量、计算能力和存储容量有限，限制了带证书的数字签名的应用。针对上述问题，利用布鲁姆过滤器技术，结合公钥密码体制，提出一种不带数字证书的、适用于无线移动场景的双向认证密钥协商方案，并对其进行性能分析和安全性分析。结果证明，该方案结合计数型布鲁姆过滤器技术，更容易实现用户与接入点的动态管理。

关键词：布鲁姆过滤器；公钥；双向认证

Mutual Authentication Key Agreement Scheme Based on WAP

ZHENG Xuan, LU Jian-zhu, FU Jie
(College of Information Science and Technology, Jinan University, Guangzhou 510632)

【Abstract】PKI uses certificate to manage public key. The application of digital signature carrying certificate is restricted for the limited computing power and memory capacity of wireless terminal device. Aiming at this problem, this paper uses Bloom filter and combines with public key cryptography, proposes a scheme of mutual authentication and key exchange for WAP which is suitable for the environment of wireless, and makes an analysis of the performance and safety about the proposed scheme. Results prove that this scheme can make use of counting Bloom filter to implement the dynamic management of users and user points.

【Key words】Bloom filter; public key; mutual authentication

1 概述

目前国内无线局域网的标准主要采用 WAPI 和 IEEE 802.11i 2 种双向认证机制，它们对 WLAN 安全性有很大的提高，但也存在一些安全隐患。WAPI 的认证不能抵抗重放攻击、密钥一致性攻击等。IEEE 802.11i 缺乏对接入点(Access Point, AP)的认证，有遭受假冒 AP 攻击的可能。文献[1]提出一种线性双向认证密钥交换协议，该协议能在低性能的无线设备和高性能服务器之间建立可靠的无线通信。文献[2]提出一种新的安全协议，该方案能抵抗未知密钥共享攻击。文献[3]基于文献[4]方法提出一种更有效的协议，上述协议都是基于公钥密码系统。文献[5]用对称加密方法设计了一个双向认证协议，运行速度快，但移动用户须存储整个网络中所有 AP 的身份标识。

本文利用文献[6]中布鲁姆过滤器和计数型布鲁姆过滤器的思想，将它们与公钥数字签名相结合，提出一种不带数字证书的无线应用协议(Wireless Application Protocol, WAP)双向认证密钥协商方案。在认证过程中，用户与接入点通过布鲁姆过滤器分别验证对方公钥的真实性，不用传输数字证书或寻求 AS 的帮助，从而提高了认证效率，降低了通信成本。移动用户只须存储对应 AP 的过滤器数据，不再要保存 AP 的身份标识，节约了存储空间。

2 预备知识

布鲁姆过滤器[7]是一种空间效率较高的随机数据结构，可以判断一个元素是否属于某个集合。在初始状态时，布鲁姆过滤器是一个包含 m 位的位数组，每一位都置为 0。假设集合 $S=\{s_1,s_2,\cdots,s_n\}$，$\{h_i\}_{i=1}^{k}$ 是 k 个相互独立的哈希函数，其中，$h_i:S\mapsto\{0,1,\cdots,m\text{-}1\}$。为了判断 s 是否为集合 S 中的元素，对每个 h_i 计算 $h_i(s_j)$。如果所有 $h_i(s_j)$ 的位置都是 1($1\leq i\leq k$)，则 $s_j\in S$，否则 $s_j\notin S$。有时会把不属于该集合的元素误认为属于该集合，其错误率大小是可估计的，本文假设 $k_n<m$，且各个哈希函数是完全随机的。当集合 $S=\{s_1,s_2,\cdots,s_n\}$ 的所有元素都被 k 个哈希函数映射到 m 位的位数组时，这个数组中某一位还是 0 的概率是：$(1-\frac{1}{m})^{kn}\approx \mathrm{e}^{-kn/m}$，因此，其错误率 $f=(1-(1-\frac{1}{m})^{kn})^k\approx(1-\mathrm{e}^{-kn/m})^k=\mathrm{e}^{k\ln(1-\mathrm{e}^{-kn/m})}$。为了使元素查询时的错误率降到最低，令 $g=k\ln(1-\mathrm{e}^{-kn/m})$，只要让 g 取到最小，f 就取到最小。因为 $\frac{dg}{dk}=\ln(1-\mathrm{e}^{-kn/m})+\frac{kn}{m}\frac{\mathrm{e}^{-kn/m}}{1-\mathrm{e}^{-kn/m}}$，所以当 $\frac{dg}{dk}=0$ 时，g 能取得最小值，k 要满足 $k=\frac{m}{n}\ln 2$，得到 $f_{\min}=(\frac{1}{2})^{\frac{m}{n}\ln 2}=(1.618\ 5)^{\frac{m}{n}}$。

3 双向认证密钥协商方案的设计

认证系统成员由移动设备(Mobile Equipment, ME)、AP 和认证服务器(Authentication Server, AS)组成，如图 1 所示。

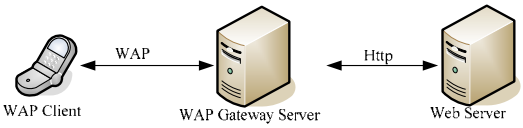

图 1 系统模型

基金项目：国家自然科学基金资助项目(60773083)
作者简介：郑 旋(1984－)，女，硕士，主研方向：无线网络安全；卢建朱，副教授、博士；付 杰，硕士
收稿日期：2009-06-22 **E-mail**：smile_355@126.com

该认证系统包括 3 个阶段：系统初始化，双向认证密钥协商过程和用户或接入点的撤销与添加。

V_{M_i} 表示移动用户 U_i 的身份认证信息，V_{B_j} 表示接入点 B_j 的身份认证信息。在 ME 端和 AP 端事先各安装一个布鲁姆过滤器，在 AS 端安装 2 个布鲁姆过滤器和一个计数型布鲁姆过滤器，安装计数型布鲁姆过滤器是为了便于实现移动用户和接入点的撤销和添加。

基于椭圆曲线的数字签名具有密钥短、处理速度快、带宽要求低等优点，在双向认证过程中，本文选择椭圆曲线数字签名算法(Elliptic Curve Digital Signature Algorithm, ECDSA)。令 F_q 是一个有限域，q 是一个素数，AS 选择合适的椭圆曲线构造点集 $E(F_q)$，G 是 $E(F_q)$ 的 n 阶生成元，FR 是 F_q 中的一个元素，选取安全的 hash 函数 $h(\cdot)$，得到系统参数 $D=(q,E(F_q),FR,G,n,h)$。

3.1 系统初始化

令(PK_{U_i}， SK_{U_i})表示 ME U_i 的公钥和私钥，(PK_{B_j}， SK_{B_j})表示 AP B_j 的公钥和私钥。AS 首先分别为每个用户 U_i 和接入点 B_j 分配不同的密钥对(PK_{U_i}， SK_{U_i})和(PK_{B_j}， SK_{B_j})，然后构造集合：$S_U=\{<U_1,PK_{U_1}>,<U_2,PK_{U_2}>,\cdots,<U_i,PK_{U_i}>\}$；$S_B=\{<B_1,PK_{B_1}>,<B_2,PK_{B_2}>,\cdots,<B_j,PK_{B_j}>\}$，由于#{}表示集合的基数，因此#{ S_U }=N, #{ S_B }= N'，其中，$N \gg N'$。

利用系统提供的 k 个相互独立的哈希函数 $\{h_l(\cdot)\}_{l=1}^{k}$ (如 SHA-1)，AS 端应用布鲁姆过滤器技术计算 1 个 m bit 的 $\boldsymbol{v}_U$ 向量，记为 $\boldsymbol{v}_U=v_U^0v_U^1\cdots v_U^{m-1}$，其中，对于 v_U^i， $i\in[0,m-1]$，满足：

$$v_U^i=\begin{cases}1, & \text{if}\exists l\in[1,k],\ j\in[1,N],\ \text{s.t.}\ h_l(U_j\,\|\,PK_{U_j})=i\\ 0, & \text{otherwise}\end{cases}$$

使得 $<U_j,PK_{U_j}>\in S_U$，当且仅当所有哈希函数 $h_l(U_j\,\|\,PK_{U_j})=i$ 的分量 $v_U^i=1$。用类似的方法计算 p bit 的 $\boldsymbol{v}_B$ 向量，记为 $\boldsymbol{v}_B=v_B^0v_B^1\cdots v_B^{p-1}$。使得 $<B_j,PK_{B_j}>\in S_B$，当且仅当所有哈希函数 $\left\{h_l(B_j\,\|\,PK_{B_j})\right\}_{l=1}^{t}=i$ 的分量 $v_B^j=1$， $i\in[0,p-1]$， $j\in[1,N']$。

AS 端应用计数型布鲁姆过滤器对 $\boldsymbol{v}_U$ 计算向量 $\overline{\boldsymbol{v}}_U=\overline{v}_U^0\overline{v}_U^1\cdots\overline{v}_U^{m-1}$，对于 $\overline{v}_U^i$， $i\in[0,m-1]$，满足：$\overline{v_U^i}=\#\{(U_j\,\|\,PK_{U_j})\,|\,h_l(U_j\,\|\,PK_{U_j})=i,\ \text{for}\ \exists l\in[1,k],\ j\in[1,N]\}$。

类似地，得到 $\boldsymbol{v}_B$ 的对应向量 $\overline{\boldsymbol{v}}_B=\overline{v}_B^0\overline{v}_B^1\cdots\overline{v}_B^{p-1}$，对每个整数 $i\in[0,p-1]$ 有 $\overline{v_B^i}=\#\{(B_j\,\|\,PK_{B_j})\,|\,h_l(B_j\,\|\,PK_{B_j})=i$， for $\exists l\in[1,t],\ j\in[1,N']\}$。

最后 AS 将 ECDSA 签名方案中的系统公共参数 D 和向量 $\boldsymbol{v}_U$ 预装载到每个 AP 端，同时将 D 和向量 $\boldsymbol{v}_B$ 预装载到每个 ME 端，并将 $\overline{\boldsymbol{v}}_B$ 和 $\overline{\boldsymbol{v}}_U$ 秘密保存。

3.2 双向认证密钥协商过程

假设(PK_{U_i}， SK_{U_i})= (d_iG,d_i) 和(PK_{B_j}， SK_{B_j})= (d_jG,d_j)，其中，$d_i,\ d_j\in[1,n-1]$。ME 端 U_i 向 AP 端 B_j 请求服务。为了防止假冒攻击，在获取服务之前要实现双向认证。

在双向认证过程中，U_i 和 B_j 操作如下：

(1) U_i 向 B_j 发送 $U_i\,\|\,PK_{U_i}$，启动双向认证。

(2) B_j 将 $B_j\,\|\,PK_{B_j}$， V_{B_j}， (C',D')和 N_{B_j} 发送给合法注册的用户 U_i。

1)验证 U_i 是合法注册的用户。B_j 应用 AS 端的 k 个相互独立的哈希函数 $\{h_l(\cdot)\}_{l=1}^{k}$ 计算 $\boldsymbol{v}_U[h_l(U_i\,\|\,d_iG)]=?1$。当且仅当所有的 $l\in[1,k]$，满足 $\boldsymbol{v}_U[h_l(U_i\,\|\,d_iG)]=1$，则 d_iG 为 U_i 真实的公钥。若验证 PK_{U_i} 为真，则继续下一步；若为假，则取消连接。

2) B_j 生成关于认证信息 V_{B_j} 的签名(C',D')。选取一个随机数 r_j， $r_j\in[1,n-1]$。计算 $r_jG=(x_j,y_j)$， $C'=x_j \bmod n$ ($C'\neq 0$)， $D'=r_j^{-1}(h(V_{B_j})+C'd_j)(\bmod n)$ ($D'\neq 0$)。

3) B_j 生成一个随机数 N_{B_j}，将 $B_j\,\|\,PK_{B_j}$， V_{B_j} (C',D')和 N_{B_j} 发送给 U_i。

(3) U_i 向合法真实的接入点 B_j 发送 V_{M_i} 及其签名(C,D)，以证明自己的合法身份。

1)验证 B_j 是合法注册的接入点。应用类似方法，U_i 计算 $\boldsymbol{v}_B[h_l(B_j\,\|\,d_jG)]=?1$。当且仅当所有的 $l\in[1,t]$，若满足 $v_B[h_l(B_j\,\|\,d_jG)]=1$，则 d_jG 为 B_j 真实的公钥。若验证 PK_{B_j} 为真，则继续第 2)步；若为假，则取消连接。

2) U_i 验证 B_j 的认证信息 V_{B_j} 的真实性。U_i 接收到(C',D')后，对其进行验证。首先检查 C',D'，若 $C',D'\notin[1,n-1]$ 则表示签名无效；否则计算 $u_1=h(V_{B_j})D'^{-1}(\bmod n)$， $u_2=C'D'^{-1}(\bmod n)$， $X=u_1G+u_2d_jG$。若 $X=0$，则表示签名无效；否则 $X=(x_j,y_j)$，计算 $V=x_j \bmod n$。若 $V\neq C'$，则表示签名无效，否则表示签名有效。若签名有效，则认为 B_j 为可信接入点，继续第 3)步；若签名无效，则取消连接。

3) U_i 生成关于认证信息 V_{M_i} 的签名。选取一个随机数 r_i， $r_i\in[1,n-1]$。计算 $r_iG=(x_i,y_i)$， $C=x_i \bmod n$ ($C\neq 0$)， $D=r_i^{-1}(h(V_{M_i})+Cd_i)(\bmod n)$ ($D\neq 0$)。

4) U_i 随机选取一个整数 N_{U_i}，向合法 B_j 发送 V_{M_i}，(C,D)及 N_{U_i}。

(4) B_j 验证 U_i 认证信息 V_{M_i} 的真实性。

B_j 接收到(C,D)后，用已通过验证的 U_i 公钥 d_iG 验证签名。若验证签名有效，则说明 U_i 为可信用户，双方可用会话密钥 $ck=h(N_{U_i},N_{B_j})$ 进行通信；若验证签名无效，则取消连接。具体过程如图 2 所示。

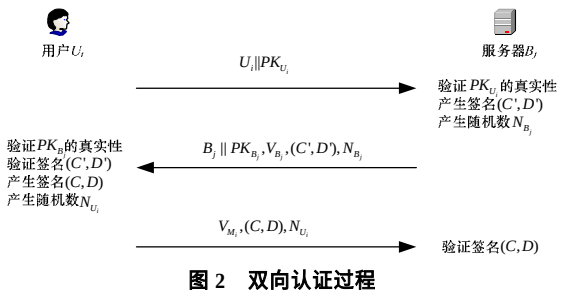

图 2 双向认证过程

由此可见，用户 U_i 和接入点 B_j 都向对方表明了自己的合法身份，实现了双向认证。

3.3 用户或接入点的撤销与添加

当有人员变动、发现欺诈用户或者有新的接入点加入、发现欺诈接入点等情况时，AS 端利用计数型布鲁姆过滤器技

术实现用户或接入点的添加、撤销。

3.3.1 用户或接入点的撤销

假设撤销用户 U_j，AS 端执行以下操作：

(1) 检查 U_j 端的哈希值 $\{h_l(U_j \| PK_{U_j})\}_{l=1}^{k}$。若有 $h_l(U_j \| PK_{U_j}) = i$，则 AS 端的 $\overline{v_U^i}$ 做减 1 操作。

(2)根据更新的 $\overline{\boldsymbol{v}_U}$ 向量，AS 端可获得一个新的 $\boldsymbol{v}_U'$ 向量，记为 $\boldsymbol{v}_U' = v_U^{0'} v_U^{1'} \ldots v_U^{m-1'}$。此时 $v_U^{i'}$ =1，当且仅当 $\overline{v_U^i} \geq 1$；否则 $v_U^{i'}$ =0。

(3)计算 $\boldsymbol{v}_{\triangle U} = \boldsymbol{v}_U' \oplus \boldsymbol{v}_U$ ($\oplus$ 表示异或运算)，删除 $\boldsymbol{v}_U$ 向量。显然，$\boldsymbol{v}_{\triangle U}$ 是一个 m bit 向量，且至多有 k bit 置 1。

(4)AS 端将向量 $\boldsymbol{v}_{\triangle U}$ 发送给每个 AP 端。

(5)AP 端根据 $\boldsymbol{v}_{\triangle U}$ 向量更新 $\boldsymbol{v}_U$ 向量。若 $v_{\triangle U}^i = 1$，则 $\boldsymbol{v}_U^i$ =0，$i \in [0, m-1]$。

这样就完成了一个用户的撤销。用户 U_j 撤销后，也将其对应的 PK_{U_j} / SK_{U_j} 密钥对销毁。用类似的方法可以实现 AP 的撤销，AS 由更新的 $\overline{\boldsymbol{v}_B}$ 向量得到 $\boldsymbol{v}_{\triangle B}$ 向量后发送给每个 ME，ME 根据 $\boldsymbol{v}_{\triangle B}$ 向量更新 $\boldsymbol{v}_B$ 向量。最后将其对应的 PK_{B_j} / SK_{B_j} 密钥对销毁。

3.3.2 新用户或新接入点的添加

假设有新用户 U_j 要求入网，U_j 首先在 AS 端进行注册。AS 利用布鲁姆过滤器技术，将 $< U_j, PK_{U_j} >$ 映射到{0,1,…, m-1}的范围中，获得更新的 $\boldsymbol{v}_U$ 向量，利用计数型布鲁姆过滤器技术获得更新的 $\overline{\boldsymbol{v}_U}$ 向量。使用与撤销用户相同的方法，AS 根据更新的 $\boldsymbol{v}_U$，$\overline{\boldsymbol{v}_U}$ 向量计算得到 $\boldsymbol{v}_{\triangle U}$ 向量，将 $\boldsymbol{v}_{\triangle U}$ 发送给每个 AP 端，然后 AP 端对向量 $\boldsymbol{v}_U$ 进行更新，若 $\boldsymbol{v}_{\triangle U}^i = 1$，则 $\boldsymbol{v}_U^i$ =1，$i \in [0, m-1]$。这样就实现了新用户的添加。应用同样的方法可实现新接入点的添加。

4 性能分析与安全性分析

由于 ME 端是属于低性能的无线设备，而 AP 端是较 ME 端性能更高的设备，因此本文只对 ME 端进行性能和安全性分析。

4.1 性能分析

在本方案的认证过程中，ME 端需完成的计算有：k 次哈希运算，一次 ECDSA-160 签名，一次 ECDSA-160 解签名。由文献[8]可知，在 8 位 ATmega128L 处理器中，完成一次 ECDSA-160 签名操作须消耗 22.82 mJ 能量，完成一次解签名需 45.05 mJ，而进行一次 SHA-1 只需 5.9 mJ/B，与签名、验证签名运算所耗能量相比可忽略不计。目前，市场上大部分手机已经使用 32 位的 PXA225 处理器。由文献[8]可知，在 32 位 PXA225 处理器中完成一次 ECDSA 签名只需消耗 3.86 mJ 的能量，验证一次 ECDSA 签名要消耗 7.6 mJ。由此可见，本方案的 ME 端大约共须消耗 11.46 mJ 的能量，在无线终端 ME 能量消耗范围内，符合当前移动通信的需求。

另外，ME 端只须存储 AS 分配的公钥/私钥对、ECDSA 签名方案中的系统公共参数 D 和布鲁姆过滤器 p bit 的 $\boldsymbol{v}_B$ 向量，其中，$tN' < p < N'(|PK_{B_j}| + |B_j|)$。

4.2 安全性分析

ME 端和 AP 端在接收到对方的公钥信息后，首先利用布鲁姆过滤器技术验证对方公钥的真实性，然后将签名的身份认证信息发送给对方。ME 收到 (C', D') 后，若能使用通过验证的 PK_{B_j} 验证签名，则该 AP 为可信 AP。同理，AP 通过使用 PK_{U_i} 验证签名 (C, D) 来确定 ME 是否可信。这样通信的双方都向对方表明了自己的合法身份，认证结束，并可利用建立的临时会话密钥进行通信。

该方案建立在 AS 是绝对可信的基础上，欺诈 ME 和欺诈 AP 都不可能获得私钥。在认证过程中，欺诈 ME 和欺诈 AP 可通过窃听网络流量获得公钥，但无法构造正确的签名，因此，ME 和 AP 在用正确的公钥验证签名时必定失败，从而取消连接。

由上述分析可以看出，该协议的安全性依赖于 ECDSA 签名算法的求离散对数困难性、哈希函数的安全性及 ME 和 AP 私钥的保密性。安全假设建立在只有真正的 ME 和 AP 知道私钥的基础上，所以，一旦 ME 或 AP 私钥泄露，协议将失去作用。

5 结束语

本文提出了一种有效、安全的适用于无线移动通信的基于 WAP 的双向认证密钥协商方案。该方案极大地节省了无线移动设备的存储空间、降低了计算量，使低性能的无线设备和高性能的服务器之间能够建立可靠的无线通信。

参考文献

[1] Wong D S, Chan A H. Mutual Authentication and Key Exchange for Low Power Wireless Communications[C]//Proc. of MILCOM'01. Boston, USA: [s. n.], 2001: 39-43.

[2] Shim K. Cryptanalysis of Mutual Authentication and Key Exchange for Low Power Wireless Communications[J]. IEEE Communications Letters, 2003, 7(5): 248-250.

[3] Jan Jinn-Ke, Chen Yi-Hwa. A New Efficient MAKEP for Wireless Communications[C]//Proc. of the 18th International Conference on Advanced Information Networking and Applications. Fukuoka, Japan: [s. n.], 2004: 347-350.

[4] Girluat M. Self-certified Public Key[C]//Proc. of EUROCRYPT'91. New York, USA: Springer, 1991: 490-497.

[5] Yang Fuw-Yi, Jan Jinn-Ke. A Secure and Efficient Key Exchange Protocol for Mobile Communications[EB/OL]. (2007-01-09). http://eprint iacr.org.

[6] Ren Kui, Lou Wenjing, Zhang Yanchao. Multi-user Broadcast Authentication in Wireless Sensor Networks[C]//Proc. of the 4th Annual IEEE Communications Society Conference. San Diego, USA: IEEE Press, 2007: 223-232.

[7] Mitzenmacher M. Compressed Bloom Filters[J]. IEEE/ACM Transactions on Networks, 2002, 10(5): 613-620.

[8] Wander A, Gura N, Eberle H. Energy Analysis of Public-key Cryptography on Small Wireless Devices[C]//Proc. of the 3rd IEEE International Conference on Pervasive Computing and Communications. Kauai Island, Hawaii, USA: IEEE Press, 2005.

编辑 陆燕菲