(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101820626 B
(45)授权公告日 2013.04.10

(21)申请号 200910117524.8

(22)申请日 2009.10.19

(73)专利权人 兰州理工大学
地址 730050 甘肃省兰州市兰工坪 287 号

(72)发明人 冯涛 彭伟

(74)专利代理机构 兰州振华专利代理有限责任公司 62102
代理人 董斌

(51)Int.Cl.
H04W 12/06(2009.01)
H04W 84/18(2009.01)
H04L 9/32(2006.01)

(56)对比文件
CN 101471776 A,2009.07.01,
CN 101383707 A,2009.03.11,
CN 1633774 A,2005.06.29,
CN 1633776 A,2005.06.29,

审查员 徐静文

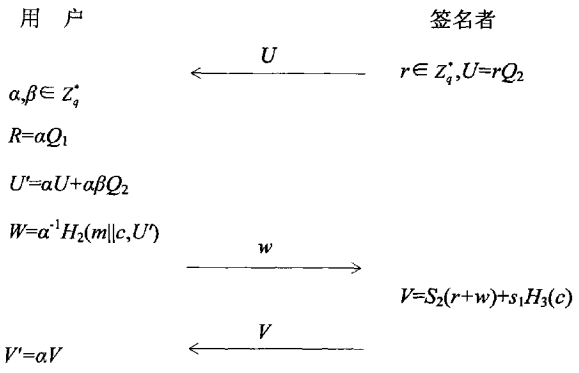
权利要求书 1 页 说明书 4 页 附图 1 页

(54)发明名称

基于无线MESH网络身份的无可信PKG的部分盲签名方法

(57)摘要

基于无线MESH网络身份的无可信PKG的部分盲签名方法，PKG随机选取一个整数，计算出系统公钥，PKG将其作为系统私钥保存，并且公开系统参数；签名者任意选取第一部分私钥，然后计算$Q_1 = s_1P$，并发送Q_1给PKG；PKG计算出S_2，并将S_2发送给签名者，于是签名者得到其私钥对(s_1, S_2)和公钥对(Q_1, Q_2)；签名者选取一个随机数，计算$U = rQ_2$，并把U发送给请求用户；用户随机选取$\alpha,\beta \in Z_q^*$，计算U'_2，w以及$R = \alpha Q_1$，将w发送给签名人；签名者计算V，将V发送给用户；用户收到V后计算$V' = \alpha V$，则(U', V', R)为签名人对消息(m, c)的部分盲签名；验证者收到身份为id的签名者对(m, c)的签名(U', V', R)，验证$e(V', P)$成立，若该式成立则通过验证，否则失败。



CN 101820626 B

1. 基于无线 MESH 网络身份的无可信 PKG 的部分盲签名方法，其步骤为：

(1)PKG 随机选取整数$s_{PKG} \in Z_q^*$，计算出系统公钥 $Q_{PKG} = s_{PKG}P$，并选择以下强无碰撞杂凑函数$H_1:\{0,1\}^* \rightarrow G_1$，$H_2:\{0,1\}^* \times G_1 \rightarrow Z_q^*$和 $H_3:\{0,1\}^* \rightarrow G_1$；PKG 将 s_{PKG} 作为系统私钥保存，并且公开系统参数 $\{G_1, G_2, e, P, q, Q_{PKG}, H_1, H_2, H_3\}$，其中$Z_q^*$为除 0 元素以外且小于素数 q 的整数集合，$G_1$ 为 q 阶的 Gap Diffie-Hellman 群，P 为 G_1 的生成元；G_2 为 q 阶的循环乘法群，$e: G_1 \times G_1 \rightarrow G_2$ 是一个双线性对；

(2) 签名者 $id \in ID$ 随机选取整数$s_1 \in Z_q^*$作为其第一部分私钥，然后计算 $Q_1 = s_1P$，并发送 Q_1 给 PKG，其中 ID 是所有参与者的身份信息集合；

(3)PKG 计算出 $S_2 = s_{PKG}Q_2$，其中 $Q_2 = H_1(id, Q_1)$ 并将 S_2 发送给签名者，于是签名者得到其私钥对 (s_1, S_2) 和公钥对 (Q_1, Q_2)；

(4) 签名者随机选取整数$r \in Z_q^*$，计算 $U = rQ_2$，并把 U 发送给用户；

(5) 用户随机选取整数$\alpha, \beta \in Z_q^*$，计算 $U' = \alpha U + \alpha \beta Q_2$，$w = \alpha^{-1} H_2(m||c, U') + \beta$ 以及 $R = \alpha Q_1$，将 w 发送给签名者；其中 m 表示用户待签名消息，c 为公共信息；

(6) 签名者计算 $V = S_2(r+w) + s_1 H_3(c)$，将 V 发送给用户；

(7) 用户收到 V 后计算 $V' = \alpha V$，则 (U', V', R) 为签名者对消息 (m,c) 的部分盲签名；

(8) 验证者收到身份为 id 的签名者对 (m, c) 的签名 (U', V', R)，验证 $e(V', P) = e(U' + H_2(m||c, U')Q_2, QPKG)e(H_3(c), R)$ 是否成立，若该式成立则通过验证，否则失败。

基于无线 MESH 网络身份的无可信 PKG 的部分盲签名方法

技术领域

[0001] 本发明涉及无线 Mesh 网络 (Wireless Mesh Network, WMN) 安全数据通信技术领域。

背景技术

[0002] 无线 Mesh 网络作为一种近年来新兴的无线网络，融合了无线局域网 WLAN 和移动 Ad Hoc 网络的优势。由于其组网快速灵活、接入速率高、覆盖范围广、投资成本较小、技术相对成熟、网络建设时间短、便于升级等优点，受到研究者越来越多的重视。无线 Mesh 网络既是 WLAN 的延伸，又可以作为 3G 的补充，也可以与 Wi MAX 相辅相成。无线 Mesh 网络不仅在战场、救灾等特殊领域有着不可替代的作用；同时在日常公共通信服务中也有着巨大的应用潜力。

[0003] WMN 是一种基于 IEEE 802.11 的无线分布系统，由两个以上通过 IEEE802.11 链路进行互联并使用 WMN 服务进行通信的 MP(Mesh Point) 组成。一个 WMN 可能还支持若干个 MPP(Mesh Portal Point)，以提供与其他分布系统或非 802.11 网络的互联能力；同时支持若干个 MAP(Mesh Access Point)，提供普通 802.11STA(Station) 与 Mesh 网络的互联。其中 MP 是核心节点，MP 的主要功能是传输、路由及数据转发等。

[0004] WMN 体系结构可以分为基于客户机的 Mesh 网络、基于基础设施的 Mesh 网络和混合型的 Mesh 网络 3 种。无线 Mesh 网络是动态移动网络，移动节点需要周围节点提供路由和转发，网络拓扑动态变化，每个节点经常接触新的节点，因而移动节点间的身份认证非常频繁，安全的无线 Mesh 网络认证必须适应移动网络的需求。目前，对 Mesh 网络安全认证问题的研究还很不成熟，基本的安全认证机制并没有很好的定义或规范。

[0005] 基于身份的签名体制 (IBS) 简化了传统的 PKI 系统中复杂的证书管理过程，在 IBS 系统中用户的公钥是直接从其身份信息（如姓名、身份证号、Email 地址等）得到，而私钥则是由一个称为私钥生成中心 (PKG, private key generator) 的可信方生成。但是 PKG 利用系统范围内的主密钥为用户生成私钥不可避免地导致了 IBC 系统所固有的密钥托管问题，即 PKG 知道所有用户的私钥。由于无线 Mesh 网络结构可以动态变化，所以在 WMN 中一个可被小组所有成员信任的可信中心很难找到，或者 PKG 被攻陷后会给系统带来严重的后果。

发明内容

[0006] 本发明的目的是提供一种基于无线 MESH 网络身份的无可信 PKG 的部分盲签名方法。

[0007] 本发明是基于无线 MESH 网络身份的无可信 PKG 的部分盲签名方法，其步骤为：

[0008] (1)PKG 随机选取整数$s_{PKG} \in Z_q^*$，计算出系统公钥 $Q_{PKG} = s_{PKG}P$，并选择以下强无碰撞杂凑函数$H_1:\{0,1\}^* \rightarrow G_1$，$H_2:\{0,1\}^* \times G_1 \rightarrow Z_q^*$和 $H_3:\{0,1\}^* \rightarrow G_1$；PKG 将 s_{PKG} 作为系统私钥保存，并且公开系统参数 $\{G_1, G_2, e, P, q, Q_{PKG}, H_1, H_2, H_3\}$，其中$Z_q^*$为除 0 元素以外且小于素数 q 的整数集合，G1 为 q 阶的 GDH(Gap Diffie-Hellman) 群，P 为 G_1 的生成元；G_2 为 q 阶

的循环乘法群，e：$G_1 \times G_1 \rightarrow G_2$ 是一个双线性对；

[0009] (2) 签名者 id ∈ ID 随机选取整数$s_1 \in Z_q^*$作为其第一部分私钥，然后计算 $Q_1 = s_1P$，并发送 Q_1 给 PKG，其中 ID 是所有参与者的身份信息集合；

[0010] (3)PKG 计算出 $S_2 = s_{PKG}Q_2$，其中 $Q_2 = H_1(id, Q_1)$ 并将 S_2 发送给签名者，于是签名者得到其私钥对 (s_1, S_2) 和公钥对 (Q_1, Q_2)；

[0011] (4) 签名者选取随机选取整数$r \in Z_q^*$，计算 $U = rQ_2$，并把 U 发送给用户；

[0012] (5) 用户随机选取整数 $\alpha, \beta \in Z_q^*$，计算 $U' = \alpha U + \alpha \beta Q_2$，$w = \alpha^{-1} H_2(m||c, U') + \beta$ 以及 $R = \alpha Q_1$，将 w 发送给签名者；其中 m 表示用户待签名消息，c 为公共信息；

[0013] (6) 签名者计算 $V = S_2(r+w) + s_1 H_3(c)$，将 V 发送给用户；

[0014] (7) 用户收到 V 后计算 $V' = \alpha V$，则 (U', V', R) 为签名者对消息 (m,c) 的部分盲签名；

[0015] (8) 验证者收到身份为 id 的签名者对 (m,c) 的签名 (U', V', R)，验证 $e(V', P) = e(U' + H_2(m||c, U')Q_2, Q_{PKG}) e(H_3(c), R)$ 是否成立，若该式成立则通过验证，否则失败。

[0016] 本发明具有以下优点：

[0017] 本发明在站点 STA、MP 和 MAP 之间进行数据通信时，设计了一个安全、有效的基于身份无可信 PKG 的部分盲签名，该签名方法具有以下优点：

[0018] (1) 交互次数少

[0019] 本发明的部分盲签名方法涉及了较少的交互次数，协议交互次数仅为 3 次。因此，在无线 MESH 网络中各类节点用户如需生成盲签名，则其只需要和签名者之间用 3 次交互即可生成所需的签名。

[0020] (2) 计算量小

[0021] 本发明中，基于身份的部分盲签名方法不但需要进行群 G_1 中的加法运算 G_1A，G_1 中的点乘运算 G_1M，还有Z_q^*中的乘法 Z_qM 和Z_q^*中的除法 Z_qd 运算。所需要的计算量 $3G_1A+8G_1M+2Z_qM+1Z_qd+3Pa$，其中，Pa 表示双线性对运算。使用哈希函数来构造的签名方法，表明本发明是切实可行的并且是高效的。

[0022] (3) 协议是安全的

[0023] 本发明的基于身份的无可信 PKG 的部分盲签名是安全的，可以在随机预言模型下将将该方法的安全性归约到的在 GDH 群上 CDH(Computational Diffie-Hellman) 困难问题。CDH 问题的难解性为本发明提供了安全保证。

附图说明

[0024] 图 1 为基于无线 MESH 网络无可信 PKG 的部分盲签名交互过程图。

具体实施方式

[0025] 本发明是基于无线 MESH 网络身份的无可信 PKG 的部分盲签名方法，其步骤为：

[0026] (1)PKG 随机选取整数$s_{PKG} \in Z_q^*$，计算出系统公钥 $Q_{PKG} = s_{PKG}P$，并选择以下强无碰撞杂凑函数$H_1: \{0,1\}^* \rightarrow G_1$，$H_2: \{0,1\}^* \times G_1 \rightarrow Z_q^*$和 $H_3: \{0,1\}^* \rightarrow G_1$；PKG 将 sPKG 作为系统私钥保存，并且公开系统参数 $\{G_1, G_2, e, P, q, Q_{PKG}, H_1, H_2, H_3\}$，其中$Z_q^*$为除 0 元素以外且

小于素数 q 的整数集合，G_1 为 q 阶的 GDH 群，P 为 G_1 的生成元；G_2 为 q 阶的循环乘法群，e：$G_1 \times G_1 \rightarrow G_2$ 是一个双线性对；

[0027] (2) 签名者 id ∈ ID 随机选取整数 $s_1 \in Z_q^*$ 作为其第一部分私钥，然后计算 $Q_1 = s_1P$，并发送 Q1 给 PKG，其中 ID 是所有参与者的身份信息集合；

[0028] (3)PKG 计算出 $S_2 = s_{PKG}Q_2$，其中 $Q_2 = H_1(id, Q_1)$ 并将 S_2 发送给签名者，于是签名者得到其私钥对 (s_1, S_2) 和公钥对 (Q_1, Q_2)；

[0029] (4) 签名者随机选取整数 $r \in Z_q^*$，计算 $U = rQ_2$，并把 U 发送给用户；

[0030] (5) 用户随机选取整数 $\alpha, \beta \in Z_q^*$，计算 $U' = \alpha U + \alpha \beta Q_2$，$w = \alpha^{-1} H_2(m||c, U') + \beta$ 以及 $R = \alpha Q_1$，将 w 发送给签名者；其中 m 表示用户待签名消息，c 为公共信息；

[0031] (6) 签名者计算 $V = S_2(r+w) + s_1 H_3(c)$，将 V 发送给用户；

[0032] (7) 用户收到 V 后计算 $V' = \alpha V$，则 (U′，V′，R) 为签名者对消息 (m,c) 的部分盲签名；

[0033] (8) 验证者收到身份为 id 的签名者对 (m,c) 的签名 (U′，V′，R)，验证 $e(V', P) = e(U' + H_2(m||c, U')Q_2, Q_{PKG}) e(H_3(c), R)$ 是否成立，若该式成立则通过验证，否则失败。

[0034] 结合基于身份的无可信中心签名机制和部分盲签名机制，通过利用 Gap Diffie-Hellman(GDH) 群，提出了一种有效的基于身份的无可信 PKG 的部分盲签名方法。该方法通过给合法签名者赋予一对私钥，该对私钥分别由签名者和 PKG 计算生成从而解决了密钥托管问题，其安全性依赖于 CDHP(Computational Diffie-Hellman Problem)。

[0035] 符号说明：

[0036] M：$M = \{M_1, M_2\}$。M 表示明文空间；M_1 表示用户待签名消息的集合而 M_2 表示用户和签名者协商后的消息集合。

[0037] ID：所有可能的参与者的身份的集合。

[0038] Δ：$\Delta = \{\Delta_1, \Delta_2\}$。Δ 表示签名空间；$\Delta_1$ 表示签名者对盲化之后的消息所有可能的签名组成的集合；Δ_2 表示用户对签名者所作的签名脱盲之后所有可能的签名组成的集合。

[0039] X：$X = \{X_1, X_2\}$。X 表示签名私有密钥空间；X_1 是由签名者生成的可能的部分私钥集合；X_2 是由 PKG 生成的可能的部分私钥集合。

[0040] Y：$Y = \{Y_1, Y_2\}$。Y 表示验证公开密钥空间；Y_1 是由签名者生成的可能的部分公钥集合；Y_2 是由 PKG 生成的可能的部分公钥集合。

[0041] 下面结合无可信 PKG 的部分盲签名交互过程附图对本发明进行详细的描述：

[0042] 设 G_1 为 q 阶的 Gap Diffie-Hellman 群，P 为 G_1 的生成元；G_2 为 q 阶的循环乘法群，e：$G_1 \times G_1 \rightarrow G_2$ 是一个双线性对。

[0043] Setup：PKG 随机选取整数 $s_{PKG} \in Z_q^*$，计算出系统公钥 $Q_{PKG} = s_{PKG}P$，并选择以下强无碰撞杂凑函数 $H_1: \{0,1\}^* \rightarrow G_1$，$H_2: \{0,1\}^* \times G_1 \rightarrow Z_q^*$ 和 $H_3: \{0,1\}^* \rightarrow G_1$。然后 PKG 将 s_{PKG} 作为系统私钥保存，并且公开系统参数 parameters = $\{G_1, G_2, e, P, q, Q_{PKG}, H_1, H_2, H_3\}$；

[0044] Extract：假定 id 表示签名者的惟一可识别的身份，PKG 对其进行物理鉴定确信 id 具有惟一性。签名者随机选取整数 $s_1 \in Z_q^*$ 作为其第一部分私钥，然后计算 $Q_1 = s_1P$，并发送 Q_1 给 PKG。PKG 计算出 $S_2 = s_{PKG}Q_2$，其中 $Q_2 = H_1(id, Q_1)$，并将 S_2 发送给签名者，于是签名者

得到其私钥对 (s_1, S_2) 和公钥对 (Q_1, Q_2)。

[0045] Issue：假设用户需要得到消息 m 的部分盲签名，c 为用户和签名者事先协商的公共信息。基于身份的无可信 PKG 部分盲签名由以下步骤组成：

[0046] (1) 签名者随机选取整数 $r \in Z_q^*$，计算 $U = rQ_2$，并把 U 发送给用户。

[0047] (2) 用户随机选取整数 $\alpha, \beta \in Z_q^*$，计算 $U' = \alpha U + \alpha \beta Q_2$，$w = \alpha^{-1} H_2(m||c, U') + \beta$ 以及 $R = \alpha Q_1$；将 w 发送给签名者。

[0048] (3) 签名者计算 $V = S_2(r+w) + s_1 H_3(c)$，将 V 发送给用户。

[0049] (4) 用户收到 V 后计算 $V' = \alpha V$，则 (U', V', R) 为签名者对消息 (m,c) 的部分盲签名，其中 c 为公共信息。

[0050] Verify：验证者收到身份为 id 的签名者对 (m,c) 的签名 (U', V', R)，验证如下：

[0051] 验证 $e(V', P) = e(U' + H_2(m||c, U')Q_2, Q_{PKG}) e(H_3(c), R)$ 是否成立，若该式成立则通过验证，否则失败。

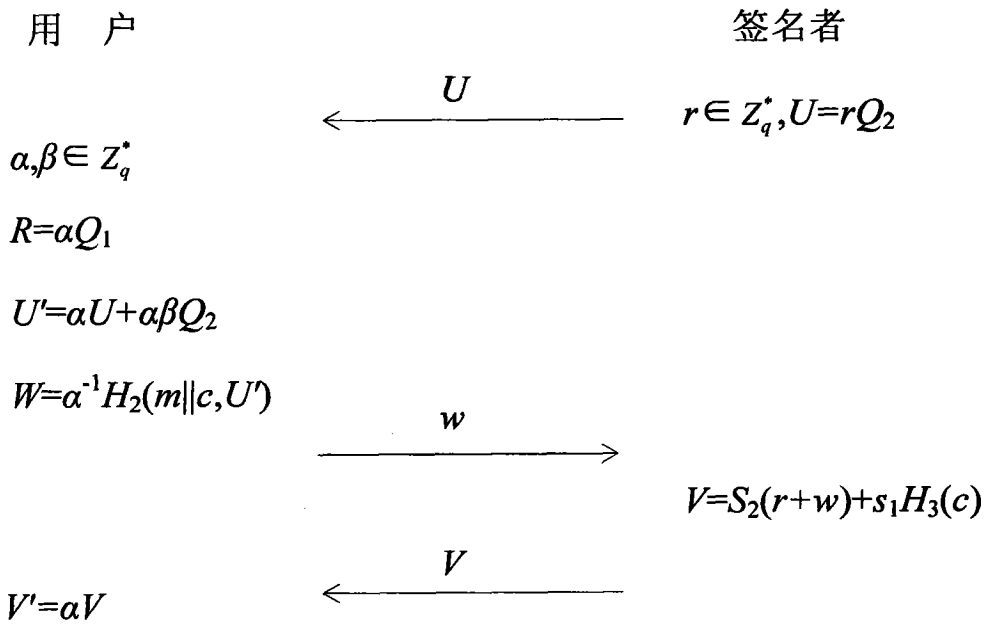

用 户
签名者
U
$r \in Z_q^*, U=rQ_2$
$\alpha,\beta \in Z_q^*$
$R=\alpha Q_1$
$U'=\alpha U+\alpha\beta Q_2$
$W=\alpha^{-1}H_2(m\|c,U')$
w
$V=S_2(r+w)+s_1H_3(c)$
V
$V'=\alpha V$

图 1