(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 110808833 B
(45)授权公告日 2021.08.06

(21)申请号 201911100109.1

(22)申请日 2019.11.12

(65)同一申请的已公布的文献号
申请公布号 CN 110808833 A

(43)申请公布日 2020.02.18

(73)专利权人 电子科技大学
地址 611731 四川省成都市成华区建设北路二段4号

(72)发明人 廖永建 梁艺宽 王勇 王栋 吴宇

(74)专利代理机构 成都九鼎天元知识产权代理有限公司 51214
代理人 管高峰

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/06(2006.01)
H04L 9/32(2006.01)
H04L 29/08(2006.01)

(56)对比文件
CN 108122153 A,2018.06.05
CN 103345698 A,2013.10.09
CN 109872787 A,2019.06.11
CN 110299993 A,2019.10.01
US 2016004605 A1,2016.01.07
贾晨军,廖永建,陈抗生.无线传感器网络中高效的基于身份的加密算法.《浙江大学学报(工学版)》.2009,第43卷(第8期),全文.

审查员 李常亮

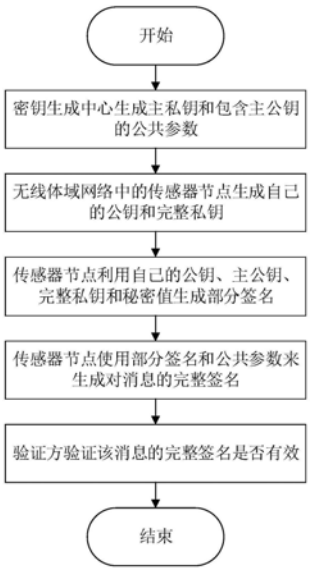
权利要求书2页 说明书5页 附图1页

(54)发明名称

一种轻量级的在线离线无证书签名方法

(57)摘要

本发明公开了一种轻量级的在线离线无证书签名方法,包括如下步骤:(1)初始化阶段,密钥生成中心生成主私钥和包含主公钥的公共参数;(2)密钥生成阶段,无线体域网络中的传感器节点生成自己的公钥和完整私钥;(3)离线签名阶段,在消息已知之前,传感器节点利用自己的公钥、主公钥、完整私钥和秘密值生成部分签名;(4)在线签名阶段,传感器节点使用部分签名和公共参数来生成对消息的完整签名;(5)验证阶段,验证方验证该消息的完整签名是否有效。本发明的在线离线无证书签名方法,能够抵抗伪造攻击和公钥替换攻击,并且,在恶意客户端和恶意密钥生成中心两种攻击下被证明是安全的。



CN 110808833 B

1.一种轻量级的在线离线无证书签名方法，其特征在于，包括如下步骤：

(1)初始化阶段，密钥生成中心生成主私钥和包含主公钥的公共参数；

(2)密钥生成阶段，无线体域网络中的传感器节点生成自己的公钥和完整私钥；

(3)离线签名阶段，在消息已知之前，传感器节点利用自己的公钥、主公钥、完整私钥和秘密值生成部分签名；

(4)在线签名阶段，传感器节点使用部分签名和公共参数来生成对消息的完整签名；

(5)验证阶段，验证方验证该消息的完整签名是否有效。

2.根据权利要求1所述的轻量级的在线离线无证书签名方法，其特征在于，所述步骤(1)包括如下子步骤：

(1.1)选择两个具有相同素数阶p的加法群G_1和乘法群G_2，以及对应的双线性映射$e:G_1 \times G_1 \rightarrow G_2$；

(1.2)选取三个哈希函数$H_1:\{0,1\}^* \rightarrow Z_p^*$，$H_2:G_1^2 \times \{0,1\}^* \rightarrow Z_p^*$以及$H_3:\{0,1\}^n \times G_2 \rightarrow Z_p^*$；

(1.3)从有限域Z_p^*中选取随机数s，从加法群G_1中随机选取P元素并计算$g=e(P,P)$；密钥生成中心把s作为主私钥，然后计算其主公钥$P_{pub}=sP$；

(1.4)发布系统的公共参数$Para=(G_1,G_2,e,p,g,P,H_1,H_2,H_3,P_{pub})$。

3.根据权利要求2所述的轻量级的在线离线无证书签名方法，其特征在于，所述步骤(2)包括：无线体域网络中的传感器节点生成自己的公钥和秘密值；然后密钥生成中心使用所述主私钥和公钥生成传感器节点的部分私钥；最后传感器节点利用秘密值和部分私钥生成完整私钥。

4.根据权利要求3所述的轻量级的在线离线无证书签名方法，其特征在于，所述步骤(2)包括如下子步骤：

(2.1)无线体域网络中用户ID_c的传感器节点从有限域Z_p^*中选取随机值x_c作为自己的秘密值，然后计算自己的公钥$PK_c=H_1(ID_c)x_cP$；

(2.2)该传感器节点发送它的公钥PK_c到密钥生成中心；密钥生成中心计算$x_cP=H_1^{-1}(ID_c)PK_c$和$D_c=(H_2(PK_c,x_c,ID_c)+s)^{-1}P$，并通过安全通道将$D_c$发送到该传感器节点，作为传感器节点的部分私钥；

(2.3)该传感器节点使用秘密值x_c和部分私钥D_c来计算完整私钥$SK_c=x_c^{-1}D_c$。

5.根据权利要求4所述的轻量级的在线离线无证书签名方法，其特征在于，所述步骤(3)包括如下子步骤：

(3.1)传感器节点将自己的公钥PK_c，完整私钥SK_c，用户ID_c，秘密值x_c，主公钥P_{pub}以及公共参数$Para$作为输入，从有限域Z_p^*中选取随机数γ，y，然后计算部分签名σ'如下：

$W_c=x_cP_{pub}$，$Q_c=H_2(PK_c,x_cP,ID_c)x_cP$，$\tau=g^y$，$\mu_c=\gamma^{-1}SK_c$；

(3.2)输出部分签名$\sigma'=(\gamma,y,\tau,\mu_c,Q_c,W_c)$。

6.根据权利要求5所述的轻量级的在线离线无证书签名方法，其特征在于，所述步骤(4)包括如下子步骤：

(4.1)传感器节点将部分签名σ'，公共参数$Para$和消息m作为输入，然后计算完整签名σ_c如下：$h_c=H_3(m,\tau)$，$\beta_c=(y+h_c)\gamma\ modp$；

(4.2)输出对消息m的完整签名$\sigma_c=(h_c,\beta_c,\mu_c)$。

7.根据权利要求6所述的轻量级的在线离线无证书签名方法，其特征在于，所述步骤(5)包括如下子步骤：

(5.1)验证方将部分签名σ'，完整签名σ_c，公共参数$Para$和消息m作为输入，然后计算$S_c=\beta_c\mu_c$；

(5.2)验证下列等式：

等式一，$e(W_c,P)^{H_1(ID_c)}=e\left(PK_c,P_{pub}\right)$；

等式二，$e\left(Q_c,P_{pub}\right)=e(W_c,P)^{H_2(PK_c,x_cP,ID_c)}$；

等式三，$h_c=H_3(m,e(S_c,Q_c+W_c)g^{-h_c})$；

若上述等式成立，则该完整签名有效；否则该完整签名无效。

一种轻量级的在线离线无证书签名方法

技术领域

[0001] 本发明涉及物联网安全技术领域，尤其是一种应用于物联网的轻量级的在线离线无证书签名方法。

背景技术

[0002] 物联网被认为是本世纪最重要的技术革命之一，在当今社会得到了广泛的应用，如智能医疗系统、智能电网、智能交通、智慧城市等。特别是，智能医疗在物联网中的应用越来越受到关注，因为它们有助于为患者远程提供服务。

[0003] 基于物联网的无线体域网络是由部署在人体周围的各种可穿戴传感器组成，这些传感器通过无线通信技术进行连接。传感器收集人体重要的生理和环境信息；然后利用个人终端将信息传输到远程控制中心；最后，远程控制中心对信息进行分析，以提供相应服务。利用可穿戴的生物传感器，智能医疗系统可以提供远程监测、紧急医疗援助和远程医疗等服务。

[0004] 智能医疗系统中交换的信息包含患者身体状况的敏感信息，对患者的隐私非常重要。由于无线体域网络中的可穿戴传感器在存储空间、能量供应、计算能力和通信速率等方面受到资源的限制，针对其他网络提出的安全方案可能并不适用。因此，在智能医疗系统的安全性和隐私方案设计中，必须认真考虑效率、实用性和安全性之间的冲突。其中，适用于资源受限设备的远程匿名认证协议的广泛研究被用于提供智能医疗系统中的匿名性、完整性、不可否认性等安全服务。

[0005] Saeed等人提出的一种在线/离线无证书签名方案(Saeed M E S, Liu Q Y, Tian G, et al. Remote authentication schemes for Wireless Body Area Networks based on the Internet of Things[J]. IEEE Internet of Things Journal, 2018, 5(6): 4926-4944.)被用于构建基于物联网的无线体域网络中的远程匿名认证协议。他们的方案将签名转换成两个阶段：(1)在线阶段和(2)离线阶段。在离线阶段，大多数繁重的工作都是在消息已知之前完成的；在在线阶段，只有轻量级的操作是通过使用离线阶段的预计算和生成签名的信息来完成的。这种技术可以设计出适用于资源受限设备的轻量级安全方案。

[0006] 经过相关研究和证明，Saeed等人提出的无证书签名方案中存在以下问题：

[0007] 1.签名方案易受伪造攻击的影响，该攻击不需要知道除公共系统参数以外的任何信息。

[0008] 2.无线体域网络中的传感器节点在获得其部分私有密钥后，可以生成其他传感器节点的完整私钥和秘密值。

[0009] 上述两个问题都导致了基于物联网的无线体域网络中的远程匿名身份验证协议是不安全的。

发明内容

[0010] 本发明所要解决的技术问题是：针对上述存在的问题，提供一种轻量级的在线离

线无证书签名方法。

[0011] 本发明采用的技术方案如下：

[0012] 一种轻量级的在线离线无证书签名方法，包括如下步骤：

[0013] (1)初始化阶段，密钥生成中心生成主私钥和包含主公钥的公共参数；

[0014] (2)密钥生成阶段，无线体域网络中的传感器节点生成自己的公钥和完整私钥；

[0015] (3)离线签名阶段，在消息已知之前，传感器节点利用自己的公钥、主公钥、完整私钥和秘密值生成部分签名；

[0016] (4)在线签名阶段，传感器节点使用部分签名和公共参数来生成对消息的完整签名；

[0017] (5)验证阶段，验证方验证该消息的完整签名是否有效。

[0018] 进一步，所述步骤(1)包括如下子步骤：

[0019] (1.1)选择两个具有相同素数阶p的加法群G_1和乘法群G_2，以及对应的双线性映射$e:G_1\times G_1\rightarrow G_2$；

[0020] (1.2)选取三个哈希函数$H_1:\{0,1\}^*\rightarrow Z_p^*$，$H_2:G_1^2\times\{0,1\}^*\rightarrow Z_p^*$以及$H_3:\{0,1\}^n\times G_2\rightarrow Z_p^*$；

[0021] (1.3)从有限域Z_p^*中选取随机数s，从加法群G_1中随机选取P元素并计算$g=e(P,P)$；密钥生成中心把s作为主私钥，然后计算其主公钥$P_{pub}=sP$；

[0022] (1.4)发布系统的公共参数$Para=(G_1,G_2,e,p,g,P,H_1,H_2,H_3,P_{pub})$。

[0023] 进一步，所述步骤(2)包括：无线体域网络中的传感器节点生成自己的公钥和秘密值；然后密钥生成中心使用所述主私钥和公钥生成传感器节点的部分私钥；最后传感器节点利用秘密值和部分私钥生成完整私钥。

[0024] 进一步，所述步骤(2)包括如下子步骤：

[0025] (2.1)无线体域网络中用户ID_c的传感器节点从有限域Z_p^*中选取随机值x_c作为自己的秘密值，然后计算自己的公钥$PK_c=H_1(ID_c)x_cP$；

[0026] (2.2)该传感器节点发送它的公钥PK_c到密钥生成中心；密钥生成中心计算$x_cP=H_1^{-1}(ID_c)PK_c$和$D_c=(H_2(PK_c,x_c,ID_c)+s)^{-1}P$，并通过安全通道将$D_c$发送到该传感器节点，作为传感器节点的部分私钥；

[0027] (2.3)该传感器节点使用秘密值x_c和部分私钥D_c来计算完整私钥$SK_c=x_c^{-1}D_c$。

[0028] 进一步，所述步骤(3)包括如下子步骤：

[0029] (3.1)传感器节点将自己的公钥PK_c，完整私钥SK_c，用户ID_c，秘密值x_c，主公钥P_{pub}以及公共参数$Para$作为输入，从有限域Z_p^*中选取随机数γ，y，然后计算部分签名σ'如下：

[0030] $W_c=x_cP_{pub}$，$Q_c=H_2(PK_c,x_cP,ID_c)x_cP$，$\tau=g^y$，$\mu_c=\gamma^{-1}SK_c$；

[0031] (3.2)输出部分签名$\sigma'=(\gamma,y,\tau,\mu_c,Q_c,W_c)$。

[0032] 进一步，所述步骤(4)包括如下子步骤：

[0033] (4.1)传感器节点将部分签名σ'，公共参数$Para$和消息m作为输入，然后计算完整签名σ_c如下：$h_c=H_3(m,\tau)$，$\beta_c=(y+h_c)\gamma\ modp$；

[0034] (4.2)输出对消息m的完整签名$\sigma_c=(h_c,\beta_c,\mu_c)$。

[0035] 进一步，所述步骤(5)包括如下子步骤：

[0036] (5.1)验证方将部分签名σ'，完整签名σ_c，公共参数$Para$和消息m作为输入，然后计算$S_c=\beta_c\mu_c$；

[0037] (5.2)验证下列等式：

[0038] 等式一，$e(W_c,P)^{H_1(ID_c)}=e\left(PK_c,P_{pub}\right)$；

[0039] 等式二，$e\left(Q_c,P_{pub}\right)=e(W_c,P)^{H_2(PK_c,x_cP,ID_c)}$；

[0040] 等式三，$h_c=H_3(m,e(S_c,Q_c+W_c)g^{-h_c})$；

[0041] 若上述等式成立，则该完整签名有效；否则该完整签名无效。

[0042] 综上所述，由于采用了上述技术方案，本发明的有益效果是：

[0043] 1、本发明的在线离线无证书签名方法，能够抵抗伪造攻击和公钥替换攻击，并且，在恶意客户端和恶意密钥生成中心两种攻击下被证明是安全的。

[0044] 2、本发明可用于构建基于物联网的无线体域网络中的远程匿名认证协议来提供智能医疗系统中的匿名性、完整性、不可否认性等安全服务。

附图说明

[0045] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，应当理解，以下附图仅示出了本发明的某些实施例，因此不应被看作是对范围的限定，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他相关的附图。

[0046] 图1为本发明的轻量级的在线离线无证书签名方法的流程框图。

具体实施方式

[0047] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅用以解释本发明，并不用于限定本发明，即所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。通常在此处附图中描述和示出的本发明实施例的组件可以以各种不同的配置来布置和设计。因此，以下对在附图中提供的本发明的实施例的详细描述并非旨在限制要求保护的本发明的范围，而是仅仅表示本发明的选定实施例。基于本发明的实施例，本领域技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0048] 以下结合实施例对本发明的特征和性能作进一步的详细描述。

[0049] 实施例1

[0050] 如图1所示，本实施例提供的一种轻量级的在线离线无证书签名方法，包括如下步骤：

[0051] (1)初始化阶段，密钥生成中心生成主私钥和包含主公钥的公共参数：

[0052] (1.1)选择两个具有相同素数阶p的加法群G_1和乘法群G_2，以及对应的双线性映射$e:G_1\times G_1\rightarrow G_2$；

[0053] (1.2)选取三个哈希函数$H_1:\{0,1\}^*\rightarrow Z_p^*$，$H_2:G_1^2\times\{0,1\}^*\rightarrow Z_p^*$以及$H_3:\{0,1\}^n\times G_2\rightarrow Z_p^*$；

[0054] (1.3)从有限域Z_p^*中选取随机数s，从加法群G_1中随机选取P元素并计算$g=e(P,P)$；密钥生成中心把s作为主私钥，然后计算其主公钥$P_{pub}=sP$；

[0055] (1.4)发布系统的公共参数$Para=(G_1,G_2,e,p,g,P,H_1,H_2,H_3,P_{pub})$。

[0056] (2)密钥生成阶段，无线体域网络中用户的传感器节点生成自己的公钥和完整私

钥;具体地,无线体域网络中用户的传感器节点生成自己的公钥和秘密值;然后密钥生成中心使用所述主私钥和公钥生成传感器节点的部分私钥;最后传感器节点利用秘密值和部分私钥生成完整私钥:

[0057] (2.1)无线体域网络中用户ID_c的传感器节点从有限域Z_p^*中选取随机值x_c作为自己的秘密值,然后计算自己的公钥$PK_c=H_1(ID_c)x_cP$;

[0058] (2.2)该传感器节点发送它的公钥PK_c到密钥生成中心;密钥生成中心计算$x_cP=H_1^{-1}(ID_c)PK_c$和$D_c=(H_2(PK_c,x_c,ID_c)+s)^{-1}P$,并通过安全通道将$D_c$发送到该传感器节点,作为传感器节点的部分私钥;

[0059] (2.3)该传感器节点使用秘密值x_c和部分私钥D_c来计算完整私钥$SK_c=x_c^{-1}D_c$。

[0060] 本发明重新定义了哈希函数H_2来修改传感器节点的部分私钥D_c的生成过程,其中,任何传感器节点的秘密值x_c、公钥PK_c和身份ID_c的更改将导致H_2的哈希值将被更改。同时,传感器节点没有主私钥,因此无法伪造其他传感器节点的公钥和部分私钥。

[0061] (3)离线签名阶段,在消息已知之前,传感器节点利用自己的公钥、主公钥、完整私钥和秘密值生成部分签名:

[0062] (3.1)传感器节点将自己的公钥PK_c,完整私钥SK_c,用户ID_c,秘密值x_c,主公钥P_{pub}以及公共参数$Para$作为输入,从有限域Z_p^*中选取随机数γ,y,然后计算部分签名σ'如下:

[0063] $W_c=x_cP_{pub}$,$Q_c=H_2(PK_c,x_cP,ID_c)x_cP$,$\tau=g^y$,$\mu_c=\gamma^{-1}SK_c$;

[0064] (3.2)输出部分签名$\sigma'=(\gamma,y,\tau,\mu_c,Q_c,W_c)$。

[0065] (4)在线签名阶段,传感器节点使用部分签名和公共参数来生成对消息的完整签名:

[0066] (4.1)传感器节点将部分签名σ',公共参数$Para$和消息m作为输入,然后计算完整签名σ_c如下:$h_c=H_3(m,\tau)$,$\beta_c=(y+h_c)\gamma\ modp$;

[0067] (4.2)输出对消息m的完整签名$\sigma_c=(h_c,\beta_c,\mu_c)$。

[0068] (5)验证阶段,验证方验证该消息的完整签名是否有效。

[0069] (5.1)验证方将部分签名σ',完整签名σ_c,公共参数$Para$和消息m作为输入,然后计算$S_c=\beta_c\mu_c$;

[0070] (5.2)验证下列等式:

[0071] 等式一,$e(W_c,P)^{H_1(ID_c)}=e(PK_c,P_{pub})$;

[0072] 等式二,$e(Q_c,P_{pub})=e(W_c,P)^{H_2(PK_c,x_cP,ID_c)}$;

[0073] 等式三,$h_c=H_3(m,e(S_c,Q_c+W_c)g^{-h_c})$;

[0074] 若上述等式成立,则该完整签名有效;否则该完整签名无效。

[0075] 为了满足验证等式一和二,W_c和Q_c应该同时包含信息x_c,并且W_c和Q_c具有线性关系。如果我们把Q_c+W_c看做公钥,那么通过对基于身份的签名方案的研究,在验证等式三中S_c的计算存在不可伪造性。

[0076] 最后,Q_c+W_c隐藏了私密信息x_c和s,在恶意客户端和恶意密钥生成中心两种攻击下,$x_c^{-1}P$和D_c不能同时恢复,而为了计算S_c需要同时获得x_c和s,因此该方法对恶意客户端和恶意密钥生成中心攻击是安全的。

[0077] 经过上述验证，本发明具有的有益效果如下：

[0078] 1、本发明的在线离线无证书签名方法，能够抵抗伪造攻击和公钥替换攻击，并且，在恶意客户端和恶意密钥生成中心两种攻击下被证明是安全的。

[0079] 2、本发明可用于构建基于物联网的无线体域网络中的远程匿名认证协议来提供智能医疗系统中的匿名性、完整性、不可否认性等安全服务。

[0080] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

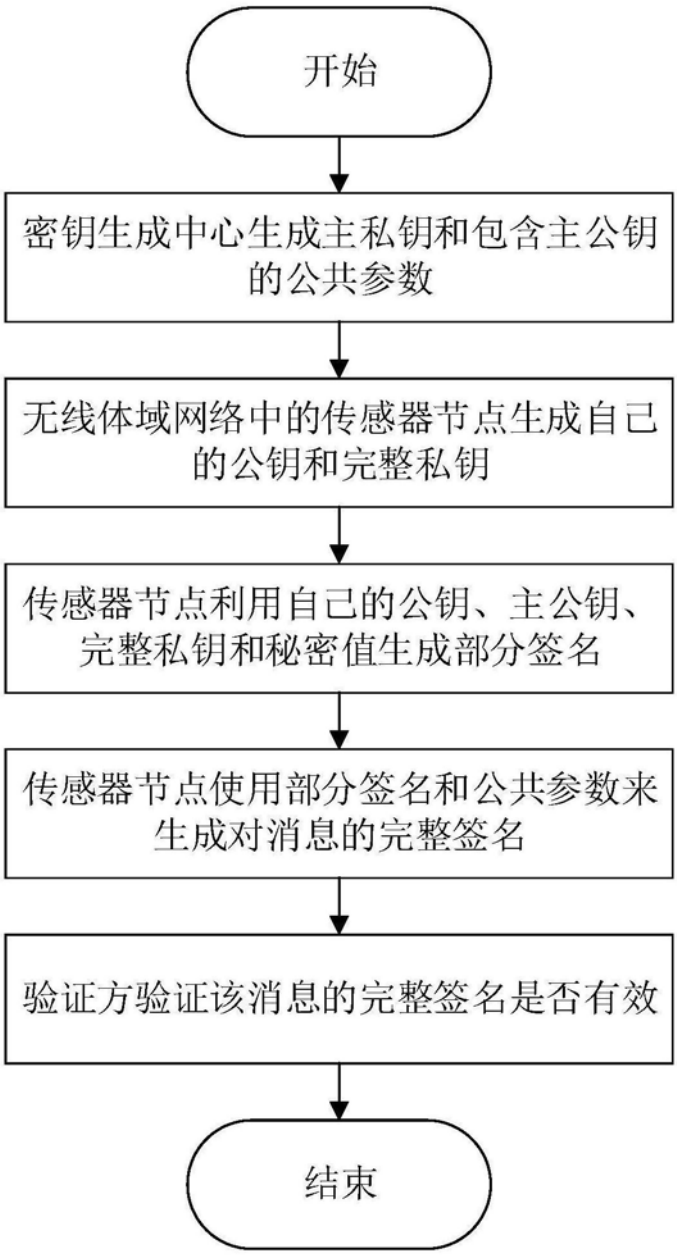

开始
密钥生成中心生成主私钥和包含主公钥的公共参数
无线体域网络中的传感器节点生成自己的公钥和完整私钥
传感器节点利用自己的公钥、主公钥、完整私钥和秘密值生成部分签名
传感器节点使用部分签名和公共参数来生成对消息的完整签名
验证方验证该消息的完整签名是否有效
结束

图1