

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(43) 国际公布日
2009 年 8 月 6 日 (06.08.2009)

PCT

(10) 国际公布号
WO 2009/094938 A1

- (51) 国际专利分类号:
H04W 12/04 (2009.01)
- (21) 国际申请号: PCT/CN2009/070255
- (22) 国际申请日: 2009 年 1 月 21 日 (21.01.2009)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
200810017387.6
2008 年 1 月 23 日 (23.01.2008) CN
- (71) 申请人 (对除美国外的所有指定国): 西安西电捷通
无线网络通信有限公司 (CHINA IWNCOMM CO.,
LTD) [CN/CN]; 中国陕西省西安市高新区科技二路
68 号西安软件园秦风阁 A201, Shaanxi 710075 (CN)。
- (72) 发明人; 及
- (75) 发明人/申请人 (仅对美国): 肖跃雷 (XIAO, Yuelei)

- [CN/CN]; 中国陕西省西安市高新区科技二路 68 号
西安软件园秦风阁 A201, Shaanxi 710075 (CN)。曹
军 (CAO, Jun) [CN/CN]; 中国陕西省西安市高新
区科技二路 68 号西安软件园秦风阁 A201, Shaanxi
710075 (CN)。赖晓龙 (LAI, Xiaolong) [CN/CN]; 中
国陕西省西安市高新区科技二路 68 号西安软件园秦
风阁 A201, Shaanxi 710075 (CN)。黄振海 (HUANG,
Zhenhai) [CN/CN]; 中国陕西省西安市高新区科技
二路 68 号西安软件园秦风阁 A201, Shaanxi 710075
(CN)。
- (74) 代理人: 北京集佳知识产权代理有限公司 (UNI-
TALEN ATTORNEYS AT LAW); 中国北京市朝阳区
建国门外大街 22 号赛特广场 7 层, Beijing 100004
(CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保
护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG,
BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,
DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD,
GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE,

[见续页]

(54) Title: METHOD FOR MANAGING WIRELESS MULTI-HOP NETWORK KEY

(54) 发明名称: 一种无线多跳网络密钥管理方法

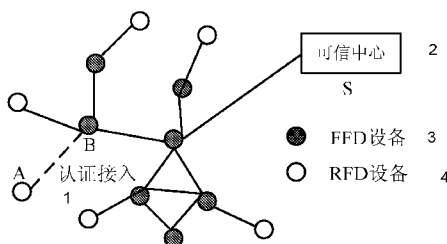


图 5 / Fig 5

- 1 AUTHENTICATION ACCESS
2 CREDITABLE CENTRE
3 FFD EQUIPMENT
4 RFD EQUIPMENT

(57) Abstract: A method for managing wireless multi-hop network key is applicable to a security application protocol when a WAPI frame method (TePA, an access control method based on the ternary peer-to-peer identification) is applied in a concrete network containing a Wireless Local Area Network, a Wireless Metropolitan Area Network AN and a Wireless Personal Area Network. The key management method of the present invention includes the steps of key generation, key distribution, key storage, key modification and key revocation. The present invention solves the technical problems that the prior pre-share-key based key management method is not suitable for larger networks and the PKI-based key management method is not suitable for wireless multi-hop networks; the public-key system and the ternary structure are adopted, thereby the security and the performance of the wireless multi-hop networks are improved.

[见续页]

WO 2009/094938 A1



KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA,

本国际公布:

— 包括国际检索报告。

(57) 摘要:

一种无线多跳网络密钥管理方法, 适用于 WAPI 框架方法 (TePA, 基于三元对等鉴别的访问控制方法) 在包括无线局域网、无线城域网和无线个域网在内的具体网络上应用时的安全应用协议。本发明密钥管理方法包括密钥产生、密钥分发、密钥存储、密钥更改和密钥撤销的步骤。本发明解决了现有基于预共享密钥的密钥管理方法不适合于规模较大的网络以及基于 PKI 的密钥管理方法不适合无线多跳网络的技术问题, 由于采用了公钥体制以及三元结构, 从而可提高了无线多跳网络的安全性和性能。

一种无线多跳网络密钥管理方法

本申请要求于 2008 年 01 月 23 日提交中国专利局、申请号为 200810017387.6、发明名称为“一种基于 ID 的无线多跳网络密钥管理方法”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5 技术领域

本发明涉及网络信息安全技术领域，尤其涉及一种无线多跳网络密钥管理方法。

背景技术

随着计算机网络和全球移动通信技术的发展，便携的数字处理终端设备已经成为人们日常生活和办公的必需品，这些终端设备包括笔记本电脑、个人数字助理（PDA）、计算机外设、移动电话、寻呼机和家用电子产品等。它们都具有较强的处理能力和较大的存储空间，从而形成了一个个人操作空间（POS）。但是目前这些终端设备之间的信息交换大都还依赖于电缆的连接，使用非常不方便，人们越来越需要一种无线技术将个人操作空间内的这些终端设备连接起来，真正实现终端设备之间可移动的、自动的互联，这就是无线多跳网络技术。在无线多跳网络中，非相邻终端设备之间的通信数据需要以多跳路由的方式传输。

在无线多跳网络中存在着四种角色的设备：终端设备、路由协调器、网络协调器和可信中心。终端设备可与该网络中的其他设备进行通信，但在该网络中不能为其他设备转发数据，即不能完成路由功能。路由协调器除了完成终端设备的功能外还负责为该网络中的其他设备转发数据，即能完成路由功能。网络协调器负责发送网络信标、建立一个网络、管理网络节点、存储网络节点信息、寻找一对节点间的路由消息和不断地接收信息，也能为该网络中的其他设备转发数据，即能完成路由功能。网络协调器和路由协调器可统称为协调器。可信中心是该网络的密钥管理中心，负责为该网络中的所有设备配置密钥信息。可信中心可以由网络协调器充当，也可以由网络协调器在该网络中指定的其他设备充当。无线多跳网络支持两种网络拓扑结构：星

-2-

型网络和点到点网络,点到点网络的网络拓扑结构又可分为网状结构和簇型结构,如图1-图3所示。

对于无线多跳网络,目前采用的密钥管理方法通常为基于预共享密钥的密钥管理方法和基于PKI的密钥管理方法。

- 5 对于第一种密钥管理方法,由于预共享密钥不便于管理,一般不适合于规模较大的网络。对于第二种密钥管理方法,由于证书的管理以及通信量较大,所以也不适合无线多跳网络。

发明内容

- 10 本发明提供一种无线多跳网络的密钥管理方法,基于每个设备自身ID产生公私钥,以对无线多跳网络中设备进行加密认证,提高了无线多跳网络的安全性和性能,解决了现有基于预共享密钥的密钥管理方法不适合于规模较大的网络以及基于PKI的密钥管理方法不适合无线多跳网络的技术问题。

本发明实施例提供的一种无线多跳网络密钥管理方法,包括:

密钥产生步骤:

- 15 可信中心根据注册设备的身份标识构造基于ID的公钥;
可信中心利用所述公钥和主密钥产生该注册设备的基于ID的私钥;

密钥分发步骤:

注册设备向无线多跳网络的可信中心提交自身的身份标识;
注册设备从该无线多跳网络的可信中心安全获得基于ID的公私钥对;

- 20 密钥存储步骤:

存储用于产生注册设备基于ID的私钥的主密钥及基于ID的公私钥对。
存储注册设备的基于ID的公私钥对。

- 25 综上所述,本发明提出的密钥管理方案,采用基于ID的公钥体制,每个设备利用基于自身ID的公私钥可以在无线多跳网络中进行安全通信,从而提高了无线多跳网络的安全性和性能。由于基于ID的公钥本身具有撤销特性且基于ID的公钥长度较短,这样不仅可以减少了公钥有效性查询的次数,而且还减少了传输的负荷,从而提高了无线多跳网络的性能。而且采用了类似于中国无线局域网标准中所述的三元结构,在认证接入过程中设备和

-3-

协调器都可以根据可信中心的公钥撤销表知道其基于 ID 的公钥有效性，从而提高了无线多跳网络认证接入的安全性；利用基于 ID 的公私钥对，可以非交互式地进行密钥协商，从而提高了无线多跳网络的性能。

附图说明

- 5 图 1 为现有的星型无线多跳网络拓扑结构图；
图 2 为现有的网状网络拓扑结构图；
图 3 为现有的簇型网络拓扑结构图；
图 4 是本发明实施方案中的无线多跳网密钥管理方法流程图；
图 5 是本发明实施方案中的无线多跳网络的认证接入系统结构示意图。
- 10 附图中：
“●”协调器，“○”为终端设备，“ $\leftrightarrow$ ”为通信信道。

A 为请求认证接入的终端设备，B 是 A 所关联的协调器，S 是该无线多跳网络的可信中心。

具体实施方式

- 15 本发明提供的技术方案适用于 WAPI 框架方法（TePA，基于三元对等鉴别的访问控制方法）在包括无线局域网、无线城域网在内的具体网络上应用时的安全应用协议。

无线多跳网络包括低速率无线个域网、高速率无线个域网和无线传感器网等，这种密钥管理方法可适用于这些网络。

- 20 本发明提供的无线多跳网络密钥管理主要包括基于 ID 的密钥的产生、分发、存储、更改和撤销。

参照图 4，基于 ID 的无线多跳网密钥管理方法的具体实现如下：

S01、密钥产生：

- 25 在基于 ID 的密码体制中，由于基于 ID 的私钥等于主密钥和基于 ID 的公钥的标量乘，所以主密钥的安全非常重要，可采取多个可信中心共同分享，即：每一个可信中心拥有该主密钥的一部分，可称为部分主密钥。类似地，公钥的每一个部分可称为部分公钥，私钥的每一个部分可称为部分私钥。

当用于产生本发明实施例中注册设备基于 ID 的私钥的主密钥由上一层

-4-

可信中心群共同分享时,该无线多跳网络中的可信中心首先根据注册设备的身份标识构造注册设备基于 ID 的公钥,然后采用密码学中的门限机制向上一层可信中心群的 k 个可信中心提交注册设备的基于 ID 的公钥,接着该 k 个可信中心利用所拥有的部分主密钥产生注册设备基于 ID 的部分私钥并发送
5 送给该无线多跳网络中的可信中心,最后该可信中心利用注册设备基于 ID 的部分私钥合成为该注册设备基于 ID 的私钥。

本发明实施例中,参照如图 5 所示的系统,当用于产生注册设备基于 ID 的私钥的主密钥存储于该无线多跳网络的可信中心时,该无线多跳网络中的可信中心根据注册设备的身份标识构造注册设备基于 ID 的公钥,然后利用
10 存储于本地的主密钥产生该注册设备基于 ID 的私钥。

注册设备基于 ID 的公钥可为无线多跳网络中可信中心的 CA 证书身份、无线多跳网络标识、注册设备的身份标识和公钥的时限的级联值。

密钥产生,具体包括以下步骤:

步骤 11,无线多跳网络中的可信中心根据注册设备的身份标识构造基于
15 ID 的公钥,如:注册设备基于 ID 的公钥为注册设备的身份标识和公钥的时限的级联值;

步骤 12,无线多跳网络中的可信中心产生注册设备的基于 ID 的私钥。

S02、密钥分发:

注册设备在向该无线多跳网络的可信中心提交注册设备的身份标识之
20 后,从该可信中心获得注册设备基于 ID 的公私钥对。其中,基于 ID 的私钥需要采用加密措施传输给注册设备,以保证私钥的安全。

密钥分发,具体包括以下步骤:

步骤 21,注册设备向无线多跳网络的可信中心提交自身的身份标识,如
设备 ID;

25 步骤 22,注册设备从该无线多跳网络的可信中心安全获得基于 ID 的公私钥对。

S03、密钥存储:

当用于产生注册设备基于 ID 的私钥的主密钥由上一层可信中心群共同

-5-

分享时,该主密钥经多项式函数分成 n 个部分后,将该 n 个部分存储于上一层可信中心群的 n 个可信中心中。每个可信中心存储主密钥的一部分。

用于产生注册设备基于 ID 的私钥的主密钥也可存储于该无线多跳网络的可信中心。

- 5 无线多跳网络的可信中心完成注册设备基于 ID 的公私钥对分发后就删除注册设备基于 ID 的公私钥对,仅存储自身的基于 ID 的公私钥对。注册设备存储从无线多跳网络的可信中心获得的注册设备基于 ID 的公私钥对。其中,基于 ID 的私钥需要进行安全存储。

密钥存储,具体包括以下步骤:

- 10 步骤 31,获取并存储用于产生注册设备基于 ID 的私钥的主密钥;
步骤 32,存储注册设备的基于 ID 的公私钥对。

S04、密钥撤销:

为便于管理公钥,无线多跳网络的可信中心中维护一个公钥撤销表,用于记录被撤销的公钥,使注册设备可以查询基于 ID 公钥是否被撤销。

- 15 当注册设备基于 ID 的私钥发生泄漏时,该注册设备以离线形式向该无线多跳网络中的可信中心申请撤销注册设备基于 ID 的公钥,可信中心收到该申请后,将该注册设备基于 ID 的公钥加入公钥撤销表;

- 当注册设备基于 ID 的私钥不再使用时,该注册设备利用与该无线多跳网络中可信中心之间的会话密钥的安全保护向该可信中心申请撤销注册设备基于 ID 的公钥,可信中心收到该申请后将该注册设备基于 ID 的公钥加入公钥撤销表。
- 20

S05、密钥更改:

- 当注册设备基于 ID 的公私钥对需要更改时,该注册设备利用与该无线多跳网络中可信中心之间的会话密钥向该可信中心申请更改注册设备基于 ID 的公私钥对,可信中心收到该申请后重新构造该注册设备基于 ID 的公钥,然后从上层可信中心群获得(或本地产生)该注册设备基于 ID 的公钥对应的注册设备基于 ID 的私钥,最后该可信中心利用与该注册设备之间的会话密钥传输重新产生的注册设备基于 ID 的公私钥对,同时将原来的注册设备
- 25

基于 ID 的公钥加入公钥撤销表。

综上所述，本发明提出的密钥管理方案，采用基于 ID 的公钥体制，每个设备利用基于自身 ID 的公私钥可以在无线多跳网络中进行安全通信，从而提高了无线多跳网络的安全性和性能。由于基于 ID 的公钥本身具有撤销特性且基于 ID 的公钥长度较短，这样不仅可以减少了公钥有效性查询的次数，而且还减少了传输的负荷，从而提高了无线多跳网络的性能。而且采用了类似于中国无线局域网标准中所述的三元结构，在认证接入过程中设备和协调器都可以根据可信中心的公钥撤销表知道其基于 ID 的公钥有效性，从而提高了无线多跳网络认证接入的安全性；利用基于 ID 的公私钥对，可以非交互式地进行密钥协商，从而提高了无线多跳网络的性能。

以上举较佳实施例，对本发明的目的、技术方案和优点进行了进一步详细说明，所应理解的是，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、改进等，均应包含在本发明的保护范围之内。

-7-

权 利 要 求

1、一种无线多跳网络密钥管理方法，其特征在于，包括：

密钥产生步骤：

可信中心根据注册设备的身份标识构造基于 ID 的公钥；

5 可信中心利用所述公钥和主密钥产生该注册设备的基于 ID 的私钥；

密钥分发步骤：

注册设备向无线多跳网络的可信中心提交自身的身份标识；

注册设备从该无线多跳网络的可信中心安全获得基于 ID 的公私钥对；

密钥存储步骤：

10 存储用于产生注册设备基于 ID 的私钥的主密钥及基于 ID 的公私钥对。

存储注册设备的基于 ID 的公私钥对。

2、根据权利要求1所述的密钥管理方法，其特征在于，当用于产生注册设备基于ID的私钥的主密钥由至少两个上一层可信中心共同分享时，密钥产生的步骤具体包括：

15 无线多跳网络中的可信中心向所述至少两个上一层可信中心提交注册设备的基于 ID 的公钥，获得该注册设备基于 ID 的私钥的部分私钥；

利用所获得的注册设备基于 ID 的部分私钥构成注册设备基于 ID 的私钥。

20 3、根据权利要求 1 所述的密钥管理方法，其特征在于，当用于产生注册设备基于 ID 的私钥的主密钥由至少两个上一层可信中心共同分享时，密钥存储步骤具体包括：

无线多跳网络的可信中心完成注册设备基于 ID 的公私钥对分发后，删除该注册设备基于 ID 的公私钥对，存储自身基于 ID 的公私钥对；将从无线多跳网络的可信中心获得的基于 ID 的公私钥对保存在所述注册设备。

25 4、根据权利要求1所述的密钥管理方法，其特征在于，

当所述主密钥存储于该无线多跳网络的可信中心时，

密钥存储步骤具体包括：

无线多跳网络的可信中心完成注册设备基于 ID 的公私钥对分发后，删

—8—

除该注册设备基于 ID 的公私钥对，保存自身基于 ID 的公私钥对；

将从所述可信中心获得的基于 ID 的公私钥对保存在所述注册设备。

5、根据权利要求1至4中任一项所述的密钥管理方法，其特征在于，还包括：

5 更改密钥的步骤：

若需要更改注册设备基于ID的公私钥对，则注册设备利用与该无线多跳网络的可信中心之间的会话密钥的安全保护向该可信中心申请更改注册设备基于ID的公私钥对；

可信中心收到所述注册设备发送的申请后，构造注册设备新的基于ID的
10 公钥；

利用所述注册设备新的基于ID的公钥，可信中心生成注册设备新的基于ID的私钥，得到注册设备新的基于ID公私钥对；

可信中心利用与注册设备之间的会话密钥的安全保护传输新的基于ID的公私钥对，并将原来的基于ID的公钥加入公钥撤销表。

15 6、根据权利要求 1 至 4 中任一项所述的密钥管理方法，其特征在于，还包括

撤销密钥的步骤：

接收注册设备向无线多跳网络中的可信中心发送撤销申请；

将注册设备基于 ID 的公钥添加到公钥撤销表。

20 7、根据权利要求 6 所述的密钥管理方法，其特征在于，所述撤销密钥的步骤还包括：

当注册设备基于 ID 的私钥发生泄漏时，注册设备以离线形式向无线多跳网络中的可信中心申请撤销注册设备基于 ID 的公钥；

当注册设备基于 ID 的私钥不再使用时，注册设备向该可信中心申请撤
25 销注册设备基于 ID 的公钥。

8、根据权利要求 1 至 4 中任一项所述的密钥管理方法，其特征在于，还包括：

密钥撤销步骤：

—9—

若需要撤销注册设备基于 ID 的公钥，则注册设备向无线多跳网络中的可信中心申请撤销注册设备基于 ID 的公钥；

可信中心收到注册设备发送的申请后将注册设备基于 ID 的公钥加入公钥撤销表。

5 9、根据权利要求 8 所述的密钥管理方法，其特征在于，

当注册设备基于 ID 的私钥发生泄漏时，注册设备以离线形式向无线多跳网络中的可信中心申请撤销注册设备基于 ID 的公钥。

10 10、根据权利要求 8 所述的密钥管理方法，其特征在于，当注册设备基于 ID 的私钥没有被泄漏但不再使用时，注册设备利用与无线多跳网络中可信中心之间的会话密钥的安全保护向该可信中心申请撤销注册设备基于 ID 的公钥。

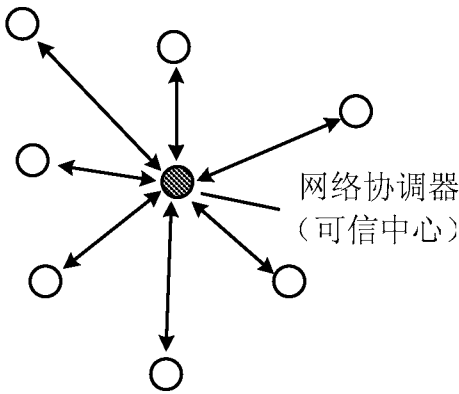


图 1

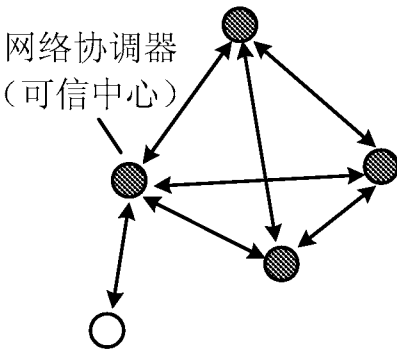


图 2

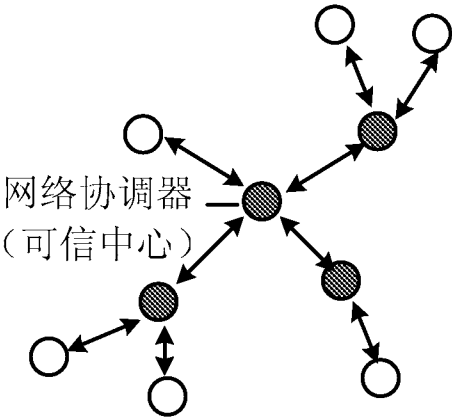


图 3

-2/2-

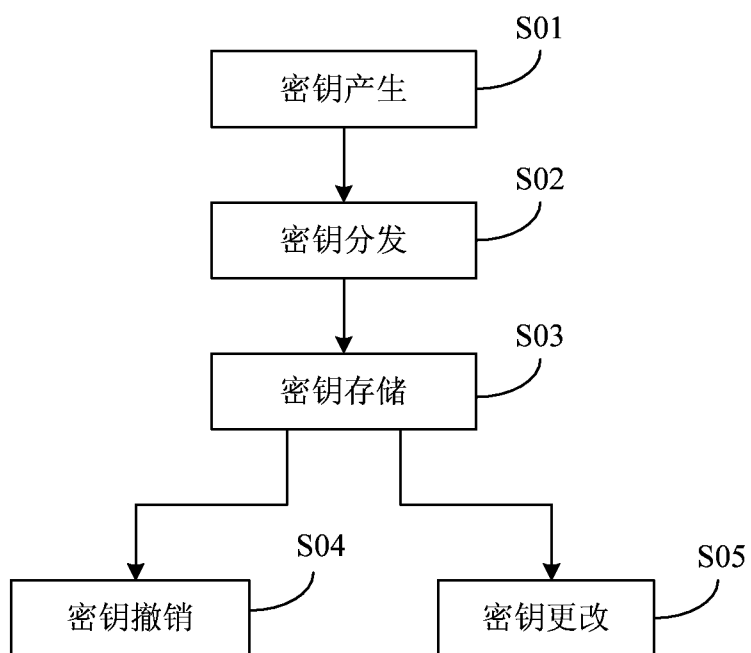


图 4

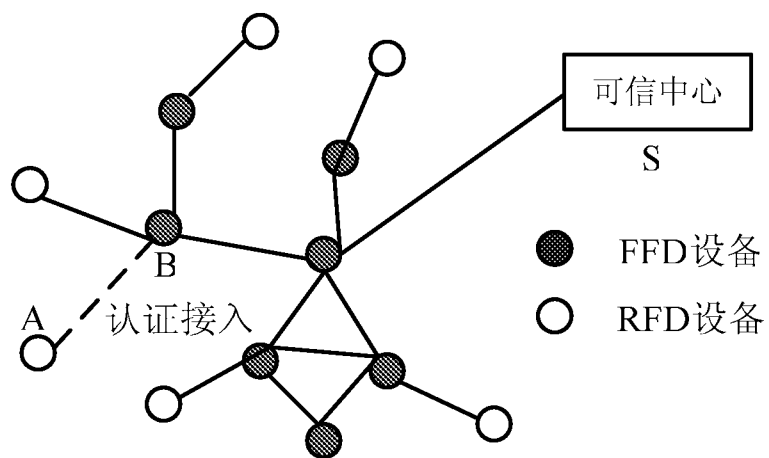


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2009/070255

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/04 (2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L, H04Q, H04B, H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, PAJ, CPRS, CNKI, IEEE: identi+ id ibe encrypt+ pubile private key multi hop adhoc base? 2d id

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN101039182A (GUANGDONG SOUTH INFORMATION SAFETY IND BASE CO LTD) 19 Sept. 2007 (19.09.2007) Page 5 lines 5-14 of the description	1
A		2-10
PX	CN101222325A (XIAN XIDIAN JIETONG WIRELESS NETWORK COM) 16 Jul. 2008 (16.07.2008) Claims 1-10	1-10
A	US2006023887A1 (AGRAWAL, dharma p. et al.) 02 Feb. 2006 (02.02.2006) The whole document	1-10
A	JP2007208410A (HITACHI LTD) 16 Aug. 2007 (16.08.2007) The whole document	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search
15 Apr. 2009 (15.04.2009)

Date of mailing of the international search report
30 Apr. 2009 (30.04.2009)

Name and mailing address of the ISA/CN
The State Intellectual Property Office, the P.R.China
6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China
100088
Facsimile No. 86-10-62019451

Authorized officer
WANG, Xiaoli
Telephone No. (86-10)62411389

Information on patent family members

PCT/CN2009/070255

None

国际检索报告

国际申请号
PCT/CN2009/070255**A. 主题的分类**

H04W 12/04 (2009.01)i

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: H04L, H04Q, H04B, H04W

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CPRS, CNKI: 标识 ID 身份 识别 IBE 密钥 公钥 私钥 加密 多跳 自组织 adhoc

WPI, EPODOC, PAJ, IEEE: identi+ id ibe encrypt+ pubile private key multi hop adhoc base? 2d id

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN101039182A (广东南方信息安全产业基地有限公司) 19.9 月 2007 (19.09.2007) 说明书第 5 页第 5-14 行	1
A		2-10
PX	CN101222325A (西安西电捷通无线网络通信有限公司) 16.7 月 2008 (16.07.2008) 权利要求 1-10	1-10
A	US2006023887A1 (AGRAWAL, dharmap 等) 02.2 月 2006 (02.02.2006) 全文	1-10
A	JP2007208410A (株式会社日立制作所) 16.8 月 2007 (16.08.2007) 全文	1-10

☐ 其余文件在 C 栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇
引用文件的公布日而引用的或者因其他特殊理由而引
用的文件

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了
理解发明之理论或原理的在后文件“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的
发明不是新颖的或不具有创造性“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件
结合并且这种结合对于本领域技术人员为显而易见时,
要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

15.4 月 2009 (15.04.2009)

国际检索报告邮寄日期

30.4 月 2009 (30.04.2009)

中华人民共和国国家知识产权局(ISA/CN)

中国北京市海淀区蓟门桥西土城路 6 号 100088

传真号: (86-10)62019451

受权官员

王晓丽电话号码: (86-10) **62411389**

关于同族专利的信息

PCT/CN2009/070255

PCT/ISA/210 表(同族专利附件) (2008 年 7 月)