(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106603508 A
(43)申请公布日 2017.04.26

(21)申请号 201611076164.8

(22)申请日 2016.11.30

(71)申请人 青岛海尔科技有限公司
地址 266101 山东省青岛市崂山区海尔路1号海尔工业园

(72)发明人 崔伟

(74)专利代理机构 北京名华博信知识产权代理有限公司 11453
代理人 李冬梅 苗源

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/06(2006.01)
H04W 12/02(2009.01)
H04W 76/02(2009.01)

权利要求书2页 说明书6页 附图3页

(54)发明名称

一种无线加密通信方法及智能家电、服务器及终端

(57)摘要

本发明公开了一种无线加密通信方法及智能家电、服务器及终端，此方法包括：智能家电通过局域网将所述智能家电的wifi模块的标识信息发送至终端；通过所述局域网从所述终端接收服务器的连接地址和所述服务器根据所述wifi模块的标识信息生成的加密工具信息；根据所述连接地址与所述服务器连接成功后，使用所述加密工具信息根据默认加密算法对上传数据进行加密后发送至所述服务器以及对从所述服务器接收到数据进行解密。本发明可以对不同的智能家电进行定制化的加密通信，能够有效保证不同智能家电的数据传输的安全性。

CN 106603508 A

1.一种无线加密通信方法,其特征在于,包括:

智能家电通过局域网将所述智能家电的wifi模块的标识信息发送至终端;

通过所述局域网从所述终端接收服务器的连接地址和所述服务器根据所述wifi模块的标识信息生成的加密工具信息;

根据所述连接地址与所述服务器连接成功后,使用所述加密工具信息根据默认加密算法对上传数据进行加密后发送至所述服务器以及对从所述服务器接收到数据进行解密。

2.如权利要求1所述的无线加密通信方法,其特征在于,

所述智能家电对从所述服务器接收到的数据进行解密,解密失败时,断开与所述服务器的连接。

3.如权利要求1或2所述的无线加密通信方法,其特征在于,

所述默认加密算法为高级加密标准ASE加密算法;

所述加密工具信息包括加密密钥和初始化向量。

4.一种智能家电,其特征在于,包括:wifi模块、记录模块、数据处理模块;

所述wifi模块,用于通过局域网将所述智能家电的wifi模块的标识信息发送至终端;还用于通过所述局域网从所述终端接收服务器的连接地址和所述服务器根据所述嵌入式wifi模块的标识信息生成的加密工具信息,根据所述连接地址与所述服务器进行连接;还用于将从处理模块收到的数据发送至服务器以及将从所述服务器收到的数据发送至所述处理模块;

所述记录模块,用于记录所述wifi模块接收到的所述加密工具信息;

所述数据处理模块,用于使用所述记录模块所记录的加密工具信息根据默认加密算法对需发送至服务器的数据进行加密后发送至所述wifi模块,还用于使用所述记录模块所记录的加密工具信息根据默认加密算法对从所述wifi模块接收到的数据进行解密。

5.一种无线加密通信方法,其特征在于,包括:

服务器从终端接收智能家电的wifi模块标识信息,根据所述智能家电的wifi模块标识信息生成加密工具信息,将所述加密工具信息和所述服务器的连接地址反馈至所述终端;

与所述智能家电连接成功后,查找与所述智能家电的wifi模块标识信息所对应的加密工具信息,使用此加密工具信息根据默认加密算法对从所述智能家电接收到的数据进行解密以及对向所述智能家电发送的数据进行加密。

6.如权利要求5所述的无线加密通信方法,其特征在于,

所述服务器对从智能家电接收到的数据进行解密,解密失败时,断开与所述智能家电的连接。

7.如权利要求5所述的无线加密通信方法,其特征在于,

所述默认加密算法为高级加密标准ASE加密算法;

所述加密工具信息包括加密密钥和初始化向量。

8.一种服务器,其特征在于,包括:通信模块、加密工具信息生成模块、记录模块、数据处理模块;

所述通信模块,用于从终端接收智能家电的wifi模块标识信息并发送至所述加密工具信息生成模块,将所述加密工具信息生成模块返回的加密工具信息和从所述数据处理模块接收到的所述服务器的连接地址反馈至所述终端;还用于与所述智能家电建立连接,从所

述智能家电接收数据并发送至所述数据处理模块，还用于从所述数据处理模块接收数据后发送至所述智能家电；

所述加密工具信息生成模块，用于根据从所述通信模块接收到的智能家电的wifi模块标识信息生成加密工具信息；还用于将智能家电的wifi模块标识信息和相应的加密工具信息存储至所述记录模块；

所述数据处理模块，用于将所述服务器的连接地址发送至所述通信模块；还用于在所述通信模块与智能家电连接成功后，从所述通信模块接收到智能家电发送的数据后，从所述记录模块查询与所述智能家电的wifi模块标识信息所对应的加密工具信息，使用此加密工具信息根据默认加密算法对所述数据进行解密；还用于从所述记录模块查询与目标智能家电的wifi模块标识信息所对应的加密工具信息，使用此加密工具信息根据默认加密算法对所述数据进行加密后发送至所述通信模块。

9.一种无线加密通信方法，其特征在于，包括：

终端将局域网的配置信息发送至智能家电，通过所述局域网接收所述智能家电发送的所述智能家电的wifi模块的标识信息，将所述智能家电的wifi模块的标识信息发送至服务器，

所述终端从服务器接收服务器的连接地址和所述服务器根据所述wifi模块的标识信息生成的加密工具信息，并将所述服务器的连接地址和所述加密工具信息发送至所述智能家电，以使所述智能家电根据所述连接地址与所述服务器连接成功后，使用所述加密工具信息根据默认加密算法对上传数据进行加密后发送至所述服务器以及对从所述服务器接收到数据进行解密。

10.一种终端，其特征在于，包括：

配置模块，用于将局域网的配置信息发送至智能家电；

第一通信模块，用于通过所述局域网接收所述智能家电发送的所述智能家电的wifi模块的标识信息；还用于将所述服务器的连接地址和所述加密工具信息发送至所述智能家电；

第二通信模块，用于将所述智能家电的wifi模块的标识信息发送至服务器，还用于从服务器接收服务器的连接地址和所述服务器根据所述wifi模块的标识信息生成的加密工具信息。

一种无线加密通信方法及智能家电、服务器及终端

技术领域

[0001] 本发明涉及移动通信控制技术领域，尤其涉及一种无线加密通信方法及智能家电、服务器及终端。

背景技术

[0002] 伴随物联网时代迅猛发展，市场上wifi(Wireless Fidelity)物联产品种类和存量也在急剧增加。通过网络终端进行本地或远程控制wifi物联产品的技术已经非常成熟。包括智能医疗仪表、智能家电、智能家居及其他惠及人民生活的许多智能数码产品都已经配备了wifi网络接入功能。

[0003] 对于wifi物联产品，远程控制的应用场景通常是移动终端的应用程序(APP)通过网络将控制数据传送到服务器(也称云端)，服务器再与wifi设备进行数据通信，以实现控制wifi设备的目的。为实现此功能，首先需要将wifi设备接入无线网络中，其次将智能家电的信息提交到云端，这两个步骤分别称为wifi设备的配置和绑定。目前家电产品大都有便捷化、无屏化的特点，因此一般是通过移动终端将家庭网络中路由器的用户名和密码发给设备，同时将设备的各种信息发给云端；然后wifi设备接入网络并与云端进行通信，实现APP的控制操作。

[0004] 由于wifi设备与云端通过网络进行数据通信，二者之间数据通信链路的安全尤为重要。目前，对于嵌入式wifi设备和服务器的通信大都是通过安全套接层(Secure Sockets Layer，SSL)证书进行数据加密。

[0005] 现有的wifi设备与云端数据通信加密主要有SSL证书加密方法，其主要流程包括：

[0006] (1)首先付费借助专业机构或开发工具，根据某些加密算法和特定信息(比如厂家信息等)，生成云端证书和设备证书。

[0007] (2)云端证书存储在云端服务器，设备证书通常是设备出厂前将证书烧录到wifi模块内存中。

[0008] (3)APP操作设备配置到wifi网络中，并将设备信息提交到云端中，即完成设备的配置和绑定。

[0009] (4)wifi设备通过网络与云端建立网络连接，之后进行SSL证书认证，认证通过，则继续进行数据通过，否则断开与云端之前的网络连接。

[0010] 这种方式的主要缺点有：

[0011] 1、针对不同的智能家电的证书都是使用同一的加密算法，安全性能不足。

[0012] 2、需要专门制作SSL证书，会产生费用；服务器和WiFi设备端都需要存储证书，特别是对于WiFi设备出厂前需要增加专门存贮证书的工序。

[0013] 3、SSL证书需要占用设备的内存空间，对WiFi设备内存的大小有要求；且部分WiFi设备软件系统不支持SSL认证。

[0014] 4、服务器和模块进行SSL链接或验证时，需要消耗较大的系统资源；特别是对于设备接入数量巨大的情况，对服务器的性能配置要求非常高。

发明内容

[0015] 为了解决现有技术中的上述缺点，本发明提供了一种无线加密通信方法及智能家电、服务器及终端。

[0016] 本发明提供了一种无线加密通信方法，包括：

[0017] 智能家电通过局域网将所述智能家电的wifi模块的标识信息发送至终端；

[0018] 通过所述局域网从所述终端接收服务器的连接地址和所述服务器根据所述wifi模块的标识信息生成的加密工具信息；

[0019] 根据所述连接地址与所述服务器连接成功后，使用所述加密工具信息根据默认加密算法对上传数据进行加密后发送至所述服务器以及对从所述服务器接收到数据进行解密。

[0020] 上述无线加密通信方法还具有以下特点：

[0021] 所述智能家电对从所述服务器接收到的数据进行解密，解密失败时，断开与所述服务器的连接。

[0022] 上述无线加密通信方法还具有以下特点：

[0023] 所述默认加密算法为高级加密标准ASE加密算法；

[0024] 所述加密工具信息包括加密密钥和初始化向量。

[0025] 本发明还提供了一种智能家电，包括：wifi模块、记录模块、数据处理模块；

[0026] 所述wifi模块，用于通过局域网将所述智能家电的wifi模块的标识信息发送至终端；还用于通过所述局域网从所述终端接收服务器的连接地址和所述服务器根据所述嵌入式wifi模块的标识信息生成的加密工具信息，根据所述连接地址与所述服务器进行连接；还用于将从处理模块收到的数据发送至服务器以及将从所述服务器收到的数据发送至所述处理模块；

[0027] 所述记录模块，用于记录所述wifi模块接收到的所述加密工具信息；

[0028] 所述数据处理模块，用于使用所述记录模块所记录的加密工具信息根据默认加密算法对需发送至服务器的数据进行加密后发送至所述wifi模块，还用于使用所述记录模块所记录的加密工具信息根据默认加密算法对从所述wifi模块接收到的数据进行解密。

[0029] 本发明还提供了一种无线加密通信方法，包括：

[0030] 服务器从终端接收智能家电的wifi模块标识信息，根据所述智能家电的wifi模块标识信息生成加密工具信息，将所述加密工具信息和所述服务器的连接地址反馈至所述终端；

[0031] 与所述智能家电连接成功后，查找与所述智能家电的wifi模块标识信息所对应的加密工具信息，使用此加密工具信息根据默认加密算法对从所述智能家电接收到的数据进行解密以及对向所述智能家电发送的数据进行加密。

[0032] 上述无线加密通信方法还具有以下特点：

[0033] 所述服务器对从智能家电接收到的数据进行解密，解密失败时，断开与所述智能家电的连接。

[0034] 上述无线加密通信方法还具有以下特点：

[0035] 所述默认加密算法为高级加密标准ASE加密算法；

[0036] 所述加密工具信息包括加密密钥和初始化向量。

[0037] 本发明还提供了一种服务器，包括：通信模块、加密工具信息生成模块、记录模块、数据处理模块；

[0038] 所述通信模块，用于从终端接收智能家电的wifi模块标识信息并发送至所述加密工具信息生成模块，将所述加密工具信息生成模块返回的加密工具信息和从所述数据处理模块接收到的所述服务器的连接地址反馈至所述终端；还用于与所述智能家电建立连接，从所述智能家电接收数据并发送至所述数据处理模块，还用于从所述数据处理模块接收数据后发送至所述智能家电；

[0039] 所述加密工具信息生成模块，用于根据从所述通信模块接收到的智能家电的wifi模块标识信息生成加密工具信息；还用于将智能家电的wifi模块标识信息和相应的加密工具信息存储至所述记录模块；

[0040] 所述数据处理模块，用于将所述服务器的连接地址发送至所述通信模块；还用于在所述通信模块与智能家电连接成功后，从所述通信模块接收到智能家电发送的数据后，从所述记录模块查询与所述智能家电的wifi模块标识信息所对应的加密工具信息，使用此加密工具信息根据默认加密算法对所述数据进行解密；还用于从所述记录模块查询与目标智能家电的wifi模块标识信息所对应的加密工具信息，使用此加密工具信息根据默认加密算法对所述数据进行加密后发送至所述通信模块。

[0041] 本发明还提供了一种无线加密通信方法，包括：

[0042] 终端将局域网的配置信息发送至智能家电，通过所述局域网接收所述智能家电发送的所述智能家电的wifi模块的标识信息，将所述智能家电的wifi模块的标识信息发送至服务器，

[0043] 所述终端从服务器接收服务器的连接地址和所述服务器根据所述wifi模块的标识信息生成的加密工具信息，并将所述服务器的连接地址和所述加密工具信息发送至所述智能家电，以使所述智能家电根据所述连接地址与所述服务器连接成功后，使用所述加密工具信息根据默认加密算法对上传数据进行加密后发送至所述服务器以及对从所述服务器接收到数据进行解密。

[0044] 本发明还提供了一种终端，包括：

[0045] 配置模块，用于将局域网的配置信息发送至智能家电；

[0046] 第一通信模块，用于通过所述局域网接收所述智能家电发送的所述智能家电的wifi模块的标识信息；还用于将所述服务器的连接地址和所述加密工具信息发送至所述智能家电；

[0047] 第二通信模块，用于将所述智能家电的wifi模块的标识信息发送至服务器，还用于从服务器接收服务器的连接地址和所述服务器根据所述wifi模块的标识信息生成的加密工具信息。

[0048] 本发明提出的结合wifi模块信息的加密方式通信方法，可以对不同的智能家电进行定制化的加密通信，能够有效保证不同智能家电的数据传输的安全性，并且将加密方法与现有APP与智能家电的WiFi模块的配置绑定流程结合一起，实现简单，操作便捷。

附图说明

[0049] 构成本发明的一部分的附图用来提供对本发明的进一步理解，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0050] 图1是实施例一中无线加密通信方法的流程图；

[0051] 图2是实施例一中智能家电的结构图；

[0052] 图3是实施例二中无线加密通信方法的流程图；

[0053] 图4是实施例二中服务器的结构图；

[0054] 图5是实施例三中无线加密通信方法的流程图；

[0055] 图6是实施例三中终端的结构图。

具体实施方式

[0056] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动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。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

[0057] 实施例一

[0058] 图1是实施例一中无线加密通信方法的流程图；此方法的执行主体为智能家电，如图1所示，此方法包括：

[0059] 步骤101，智能家电通过局域网将智能家电的wifi模块的标识信息发送至终端；

[0060] 步骤102，智能家电通过局域网从终端接收服务器的连接地址和服务器根据wifi模块的标识信息生成的加密工具信息；

[0061] 步骤103，智能家电根据连接地址与服务器连接成功后，使用加密工具信息根据默认加密算法对上传数据进行加密后发送至服务器以及对从服务器接收到数据进行解密。

[0062] 其中，

[0063] 步骤103中，智能家电对从服务器接收到的数据进行解密，解密失败时，断开与服务器的连接。

[0064] 本方法中，默认加密算法为高级加密标准AES加密算法，加密工具信息包括加密密钥和初始化向量。AES加密算法是当前对密钥加密中最流行的算法之一，其实现原理是：根据一组初始化向量(iv)、密钥(key)和AES加密算法(数据矩阵)对于数据进行一系列计算或反运算，从而得出加密或解密的数据。AES方法运算速度快，对设备的系统软件及资源等要求低。本方法中除了AES加密算法，还可以使用其它加密算法。

[0065] 图2是实施例一中智能家电的结构图；如图2所示，智能家电包括：wifi模块、记录模块、数据处理模块。

[0066] wifi模块，用于通过局域网将智能家电的wifi模块的标识信息发送至终端；还用于通过局域网从终端接收服务器的连接地址和服务器根据嵌入式wifi模块的标识信息生成的加密工具信息，根据连接地址与服务器进行连接；还用于将从处理模块收到的数据发送至服务器以及将从服务器收到的数据发送至处理模块；

[0067] 记录模块，用于记录wifi模块接收到的加密工具信息；

[0068] 数据处理模块，用于使用记录模块所记录的加密工具信息根据默认加密算法对需

发送至服务器的数据进行加密后发送至wifi模块，还用于使用记录模块所记录的加密工具信息根据默认加密算法对从wifi模块接收到的数据进行解密。

[0069] 实施例二

[0070] 图3是实施例二中无线加密通信方法的流程图；此方法的执行主体为服务器，如图3所示，此方法包括：

[0071] 步骤301，服务器从终端接收智能家电的wifi模块标识信息，根据智能家电的wifi模块标识信息生成加密工具信息，将加密工具信息和服务器的连接地址反馈至终端；

[0072] 步骤302，与智能家电连接成功后，查找与所述智能家电的wifi模块标识信息所对应的加密工具信息，使用此加密工具信息根据默认加密算法对从智能家电接收到的数据进行解密以及对向智能家电发送的数据进行加密。

[0073] 其中，步骤302中服务器对从智能家电接收到的数据进行解密，解密失败时，断开与智能家电的连接。

[0074] 本方法中，默认加密算法为高级加密标准ASE加密算法；加密工具信息包括加密密钥和初始化向量。除了AES加密算法，还可以使用其它加密算法。

[0075] 图4是实施例二中智能家电的结构图；如图4所示，服务器包括：通信模块、加密工具信息生成模块、记录模块、数据处理模块；

[0076] 通信模块，用于从终端接收智能家电的wifi模块标识信息并发送至加密工具信息生成模块，将加密工具信息生成模块返回的加密工具信息和从数据处理模块接收到的服务器的连接地址反馈至终端；还用于与智能家电建立连接，从智能家电接收数据并发送至数据处理模块，还用于从数据处理模块接收数据后发送至智能家电；

[0077] 加密工具信息生成模块，用于根据从通信模块接收到的智能家电的wifi模块标识信息生成加密工具信息；还用于将智能家电的wifi模块标识信息和相应的加密工具信息存储至记录模块；

[0078] 数据处理模块，用于将服务器的连接地址发送至通信模块；还用于在通信模块与智能家电连接成功后，从通信模块接收到智能家电发送的数据后，从记录模块查询与智能家电的wifi模块标识信息所对应的加密工具信息，使用此加密工具信息根据默认加密算法对数据进行解密；还用于从记录模块查询与目标智能家电的wifi模块标识信息所对应的加密工具信息，使用此加密工具信息根据默认加密算法对数据进行加密后发送至通信模块。

[0079] 本方法中，智能家电与服务器建立网络连接之前，需要经由终端进行信息转发，具体包括：终端通过广播的方式发送局域网内路由器的配置信息(包括用户名和密码)，智能家电根据此配置信息接入局域网，通过局域网将wifi模块的标识信息发送至终端，终端将智能家电的标识、wifi模块的标识信息发送至服务器，完成智能家电的绑定。终端从服务器收到针对智能家电的加密工具信息和服务器的连接地址后，发送至相应的智能家电。

[0080] 实施例三

[0081] 图5是实施例三中无线加密通信方法的流程图；此方法的执行主体为终端，如图5所示，此方法包括：

[0082] 步骤501，终端将局域网的配置信息发送至智能家电；

[0083] 步骤502，通过所述局域网接收所述智能家电发送的所述智能家电的wifi模块的标识信息，将所述智能家电的wifi模块的标识信息发送至服务器，

[0084] 步骤503，终端从服务器接收服务器的连接地址和所述服务器根据所述wifi模块的标识信息生成的加密工具信息，并将所述服务器的连接地址和所述加密工具信息发送至所述智能家电，以使所述智能家电根据所述连接地址与所述服务器连接成功后，使用所述加密工具信息根据默认加密算法对上传数据进行加密后发送至所述服务器以及对从所述服务器接收到数据进行解密。

[0085] 图6是实施例三中终端的结构图，此终端包括：

[0086] 配置模块，用于将局域网的配置信息发送至智能家电；

[0087] 第一通信模块，用于通过所述局域网接收所述智能家电发送的所述智能家电的wifi模块的标识信息；还用于将所述服务器的连接地址和所述加密工具信息发送至所述智能家电；

[0088] 第二通信模块，用于将所述智能家电的wifi模块的标识信息发送至服务器，还用于从服务器接收服务器的连接地址和所述服务器根据所述wifi模块的标识信息生成的加密工具信息。本发明提出的结合wifi模块信息的加密方式通信方法，可以对不同的智能家电进行定制化的加密通信，能够有效保证不同智能家电的数据传输的安全性，并且将加密方法与现有APP与智能家电的WiFi模块的配置绑定流程结合一起，实现简单，操作便捷。

[0089] 上面描述的内容可以单独地或者以各种方式组合起来实施，而这些变型方式都在本发明的保护范围之内。

[0090] 本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件完成，程序可以存储于计算机可读存储介质中，如只读存储器、磁盘或光盘等。可选地，上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现，相应地，上述实施例中的各模块/单元可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。本发明不限制于任何特定形式的硬件和软件的结合。

[0091] 需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括……”限定的要素，并不排除在包括所述要素的物品或者设备中还存在另外的相同要素。

[0092] 以上实施例仅用以说明本发明的技术方案而非限制，仅仅参照较佳实施例对本发明进行了详细说明。本领域的普通技术人员应当理解，可以对本发明的技术方案进行修改或者等同替换，而不脱离本发明技术方案的精神和范围，均应涵盖在本发明的权利要求范围当中。

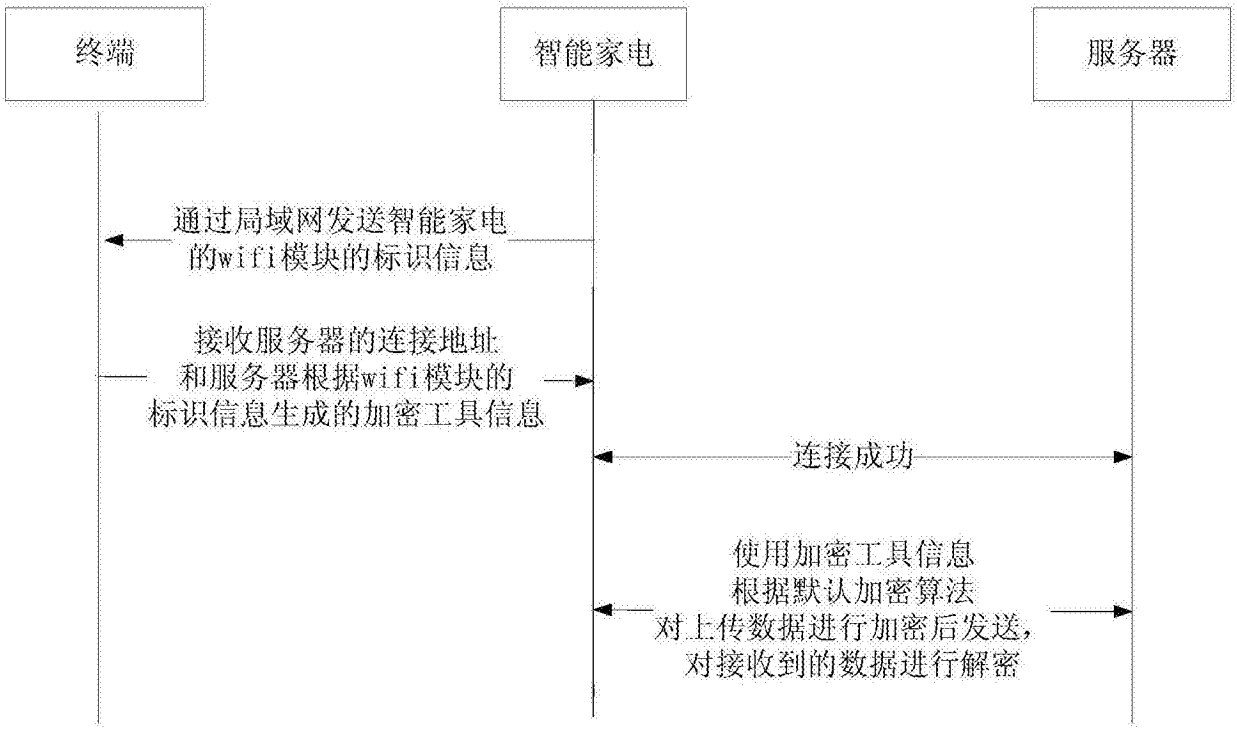
终端
智能家电
服务器
通过局域网发送智能家电
的wifi模块的标识信息
接收服务器的连接地址
和服务器根据wifi模块的
标识信息生成的加密工具信息
连接成功
使用加密工具信息
根据默认加密算法
对上传数据进行加密后发送，
对接收到的数据进行解密

图1

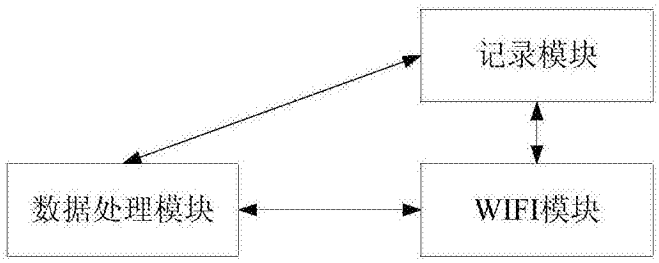
记录模块
数据处理模块
WIFI模块

图2

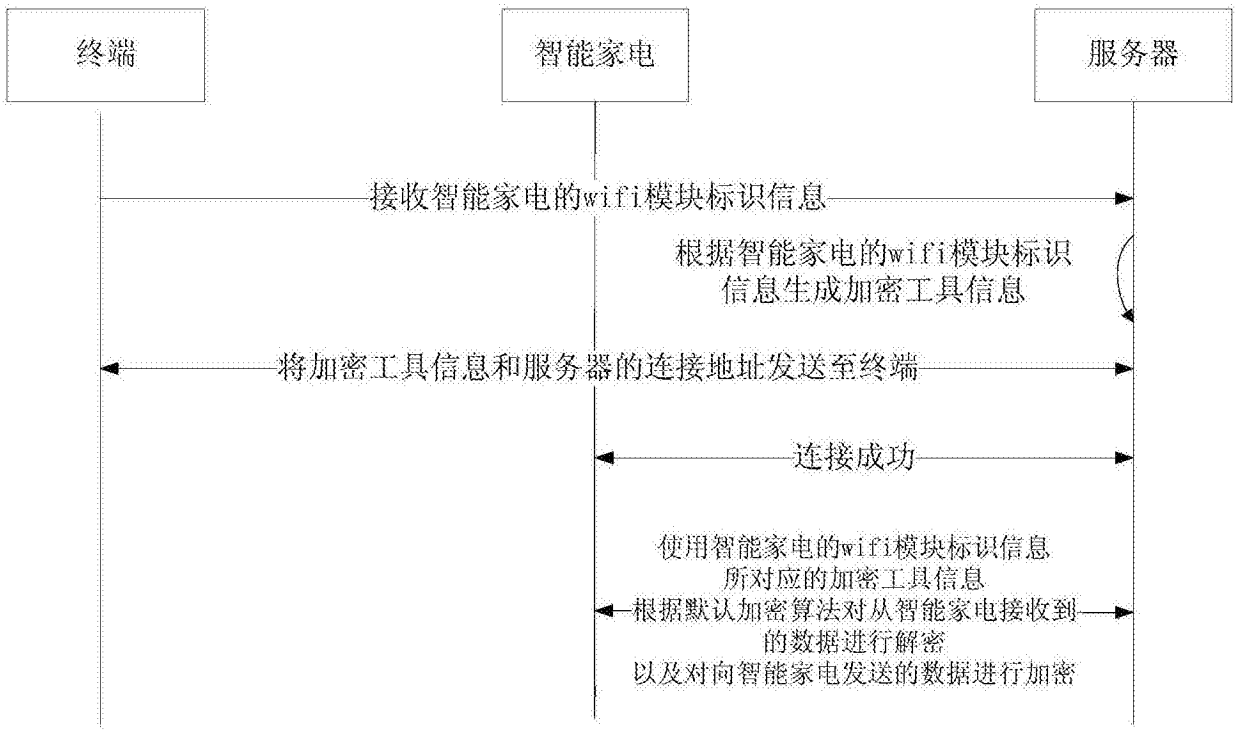
终端
智能家电
服务器
接收智能家电的wifi模块标识信息
根据智能家电的wifi模块标识信息生成加密工具信息
将加密工具信息和服务器的连接地址发送至终端
连接成功
使用智能家电的wifi模块标识信息所对应的加密工具信息
根据默认加密算法对从智能家电接收到的数据进行解密
以及对向智能家电发送的数据进行加密

图3

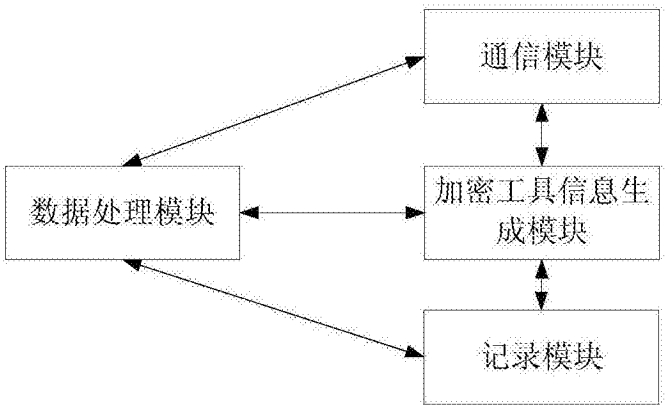
通信模块
数据处理模块
加密工具信息生成模块
记录模块

图4

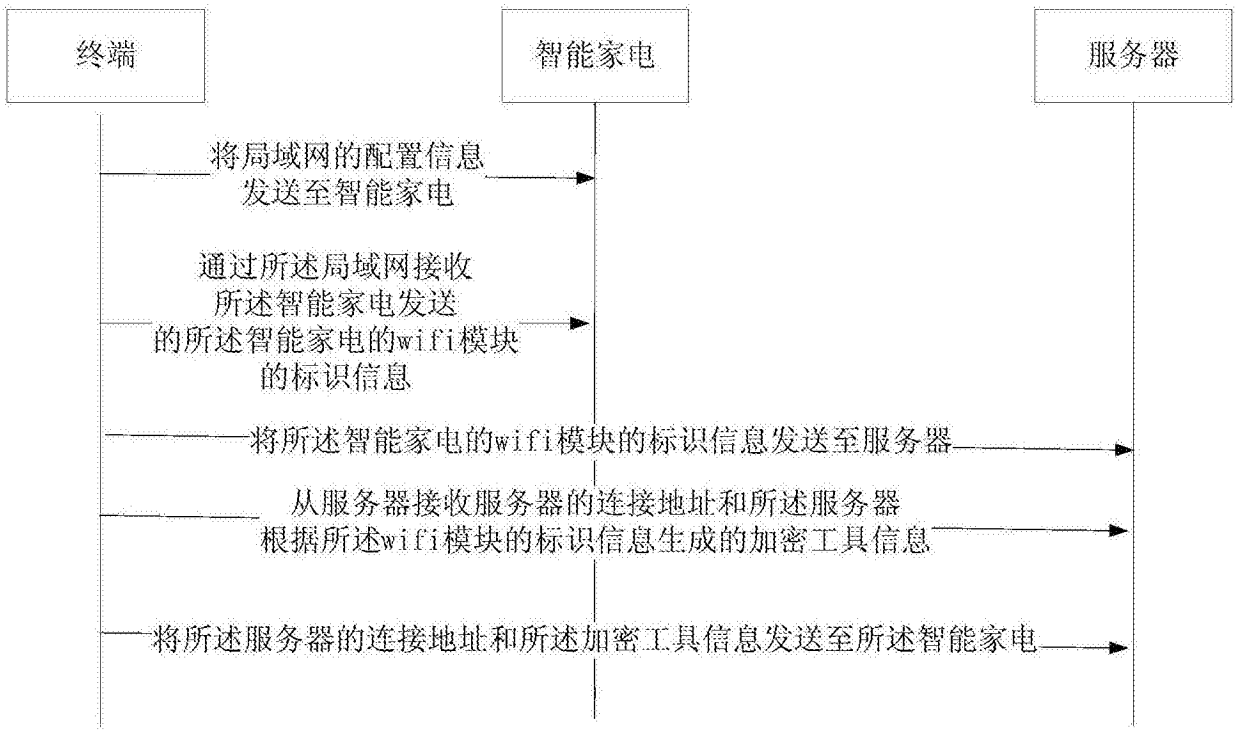
终端
智能家电
服务器
将局域网的配置信息
发送至智能家电
通过所述局域网接收
所述智能家电发送
的所述智能家电的wifi模块
的标识信息
将所述智能家电的wifi模块的标识信息发送至服务器
从服务器接收服务器的连接地址和所述服务器
根据所述wifi模块的标识信息生成的加密工具信息
将所述服务器的连接地址和所述加密工具信息发送至所述智能家电

图5

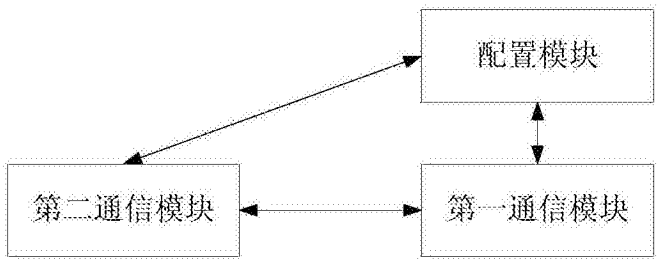
配置模块
第二通信模块
第一通信模块

图6