



(12)发明专利申请

(10)申请公布号 CN 110582084 A
(43)申请公布日 2019.12.17

(21)申请号 201910999575.1

(22)申请日 2019.10.21

(71)申请人 长虹美菱股份有限公司

地址 230000 安徽省合肥市经济技术开发
区莲花路2163号

(72)发明人 李帅明

(74)专利代理机构 上海精晟知识产权代理有限
公司 31253

代理人 孙永智

(51) Int. Cl.

H04W 12/04(2009.01)

H04W 12/06(2009.01)

H04L 9/08(2006.01)

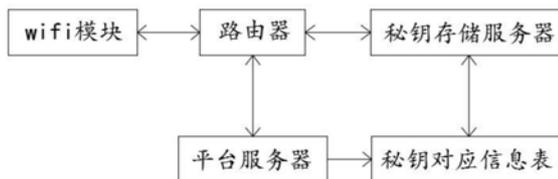
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种云端烧写wifi设备认证密钥的系统及其方法

(57)摘要

本发明公开一种云端烧写wifi设备认证密钥的系统,包括wifi模块、路由器、平台服务器以及密钥存储服务器;所述wifi模块与路由器连接,路由器分别与平台服务器和密钥存储服务器连接。本发明提供的一种云端烧写wifi设备认证密钥的系统,通过在云端烧写设备密钥信息的方式,既实现了一机一密的双向认证方案在wifi设备端的写入,有效提升了终端接入服务器的安全可靠,避免服务器被攻击,也避免了对原有生产环境做出较大改动,以至于影响实际的生产进程和效率,且将密钥与wifi模块的MAC地址的对应信息在云端存储,便于信息的更新维护与wifi获取下载。



1. 一种云端烧写wifi设备认证密钥的系统,其特征在于:包括wifi模块、路由器、平台服务器以及密钥存储服务器;

所述wifi模块与路由器连接,路由器分别与平台服务器和密钥存储服务器连接;

所述wifi模块用于接入密钥服务器和平台服务器,完成产品密钥认证和实现产品与终端的互联互通;

所述路由器用于为wifi模块接入平台服务器和密钥存储服务器提供网络;

所述平台服务器可根据密钥生成算法生成并存储wifi模块的MAC地址的对应认证密钥信息,并对需要接入的wifi模块进行密钥认证;

所述密钥服务器用于存储wifi模块的MAC地址和产品认证密钥信息的对应关系表,并为请求的wifi模块提供对应的认证密钥信息。

2. 根据权利要求1所述的一种云端烧写wifi设备认证密钥的方法,其特征在于:包括以下步骤:

S1、为每一个wifi模块的MAC地址生成对应的认证密钥信息,汇总成为一张wifi模块的MAC地址和产品密钥对应的信息表;

S2、将生成的wifi模块的MAC地址和产品密钥对应的信息表事先存储在密钥存储服务器;

S3、具有wifi的智能产品正常生产销售,在用户配网时,wifi模块会首先连接到路由器;

S4、wifi模块在首次连接到路由器后,通过路由器发送携带MAC地址的信息请求到密钥存储服务器,密钥存储服务器在接收到wifi模块的请求信息后,查询所存储的wifi MAC和产品密钥对应的信息表,以获取对应MAC的产品密钥信息,然后携带密钥信息通过路由器回送给wifi模块;

S5、wifi模块从路由器接收到密钥存储服务器回送的信息后,提取相关密钥信息,并写入自身模块;

S6、wifi模块在自己包含密钥信息的状态下,再通过路由器连接平台服务器进行接入请求。

3. 根据权利要求2所述的一种云端烧写wifi设备认证密钥的方法,,其特征在于:还包括步骤S7,所述步骤S7为wifi模块复位不清除自身的密钥信息,在后续连接路由器后,不再连接密钥存储服务器。

一种云端烧写wifi设备认证密钥的系统及其方法

技术领域

[0001] 本发明属于wifi设备认证技术领域,涉及到一种云端烧写wifi设备认证密钥的系统及其方法。

背景技术

[0002] 当前家电产品中,智能带wifi产品越来越多,服务器对于接入的wifi模块的安全性的要求越来越高,在这个过程中,不同的认证加密方式层出不穷,目前一种一机一密的双向认证方式可以有效的保证产品和服务器的安全性,避免终端及服务器被恶意攻击或密钥泄露,进而影响其他终端;既在服务器和wifi模块都提前写入对应的密钥信息,每台产品一个密钥,wifi模块在接入服务器时会进行密钥双向认证,密钥认证通过则才可接入服务器,但该认证方案要求提前将产品密钥写入wifi模块中,目前常规手段是在生产时写入,要完成一机一密的产品密钥信息在生产写入,需要对产品生产过程进行较大的改动,对生产的影响很大,且生产环境过于复杂,所以实际实施起来很困难。

发明内容

[0003] 本发明的目的在于提供的一种云端烧写wifi设备认证密钥的系统及其方法,解决了现有产品密钥信息写入的过程中,存在复杂程度大以及难度大的问题,提到了生产进程和效率。

[0004] 本发明的目的可以通过以下技术方案实现:

[0005] 一种云端烧写wifi设备认证密钥的系统,包括wifi模块、路由器、平台服务器以及密钥存储服务器;

[0006] 所述wifi模块与路由器连接,路由器分别与平台服务器和密钥存储服务器连接;

[0007] 所述wifi模块用于接入密钥服务器和平台服务器,完成产品密钥认证和实现产品与终端的互联互通;

[0008] 所述路由器用于为wifi模块接入平台服务器和密钥存储服务器提供网络;

[0009] 所述平台服务器可根据密钥生成算法生成并存储wifi模块的MAC地址的对应认证密钥信息,并对需要接入的wifi模块进行认证;

[0010] 其中,所述密钥生成算法为将每个wifi模块的MAC码以标准ASCII码规则转换为十六进制数据,将转换后的十六进制数据每一位都加1,F+1后用0表示,最后将数据转化为8进制数据作为对应wifi模块的密钥信息;

[0011] 特别的,本发明对所述密钥算法不做限定,只是举例一个算法,目前可以想到的密钥生成算法都包括在本发明的内容中;

[0012] 所述密钥服务器用于存储wifi模块的MAC地址和产品认证密钥信息的对应关系表,并为请求的wifi模块提供对应的认证密钥信息。

[0013] 一种云端烧写wifi设备认证密钥的方法,包括以下步骤:

[0014] S1、为每一个wifi模块的MAC地址生成对应的认证密钥信息,汇总成为一张wifi模

块的MAC地址和产品密钥对应的信息表；

[0015] S2、将生成的wifi模块的MAC地址和产品密钥对应的信息表事先存储在密钥存储服务器；

[0016] S3、具有wifi的智能产品正常生产销售,在用户配网时,wifi模块会首先连接到路由器；

[0017] S4、wifi模块在首次连接到路由器后,通过路由器发送携带MAC地址的信息请求到密钥存储服务器,密钥存储服务器在接收到wifi模块的请求信息后,查询所存储的wifi MAC和产品密钥对应的信息表,以获取对应MAC的产品密钥信息,然后携带密钥信息通过路由器回送给wifi模块；

[0018] S5、wifi模块从路由器接收到密钥存储服务器回送的信息后,提取相关密钥信息,并写入自身模块；

[0019] S6、wifi模块在自己包含密钥信息的状态下,再通过路由器连接平台服务器进行接入请求。

[0020] 进一步地,还包括步骤S7,所述步骤S7为wifi模块复位不删除自身的密钥信息,在后续连接路由器后,不再连接密钥存储服务器。

[0021] 本发明的有益效果：

[0022] 本发明提供了一种云端烧写wifi设备认证密钥的系统及其方法,通过在云端烧写设备密钥信息的方式,既实现了一机一密的双向认证方案在wifi设备端的写入,有效提升了终端接入服务器的安全可靠,避免服务器被攻击,也避免了对原有生产环境做出较大改动,以至于影响实际的生产进程和效率,且将密钥与wifi模块的MAC地址的对应信息在云端存储,便于信息的更新维护与wifi获取下载。

附图说明

[0023] 为了更清楚地说明本发明实施例的技术方案,下面将对实施例描述所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,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的附图。

[0024] 图1为本发明中一种云端烧写wifi设备认证密钥的系统的示意图。

具体实施方式

[0025] 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,所描述的实施例仅仅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作出创造性劳动前提下所获得的所有其它实施例,都属于本发明保护的范围。

[0026] 请参阅图1所示,一种云端烧写wifi设备认证密钥的系统,包括wifi模块、路由器、平台服务器以及密钥存储服务器；

[0027] wifi模块与路由器连接,路由器分别与平台服务器和密钥存储服务器连接；

[0028] 所述wifi模块用于接入密钥服务器和平台服务器,完成产品密钥认证和实现产品与终端的互联互通；

- [0029] 路由器用于为wifi模块接入平台服务器和密钥存储服务器提供网络；
- [0030] 平台服务器可根据密钥生成算法生成并存储wifi模块的MAC地址的对应认证密钥信息,并对需要接入的wifi模块进行认证；
- [0031] 密钥服务器用于存储wifi模块的MAC地址和产品认证密钥信息的对应关系表,并为请求的wifi模块提供对应的认证密钥信息。
- [0032] 一种云端烧写wifi设备认证密钥的方法,包括以下步骤:
- [0033] S1、为每一个wifi模块的MAC地址生成对应的认证密钥信息,汇总成为一张wifi模块的MAC地址和产品密钥信息表,其中,所述密钥信息表由平台服务器根据wifi模块MAC生成并分别存储于平台服务器和密钥服务器；
- [0034] S2、将生成的wifi模块的MAC地址和产品密钥对应的信息表事先存储在密钥存储服务器；
- [0035] S3、具有wifi的智能产品正常生产销售,在用户配网时,wifi模块会首先连接到路由器；
- [0036] S4、wifi模块在首次连接到路由器后,通过路由器发送携带MAC地址的信息请求到密钥存储服务器,密钥存储服务器在接收到wifi模块的请求信息后,查询所存储的wifi MAC和产品密钥对应的信息表,以获取对应MAC的产品密钥信息,然后携带密钥信息通过路由器回送给wifi模块；
- [0037] S5、wifi模块从路由器接收到密钥存储服务器回送的信息后,提取相关密钥信息,并写入自身模块；
- [0038] S6、wifi模块在自己包含密钥信息的状态下,再通过路由器连接平台服务器进行接入请求；
- [0039] S7、wifi模块复位为不清除自身的密钥信息,在后续连接路由器后,不再连接密钥存储服务器。
- [0040] 以上内容仅仅是对本发明的构思所作的举例和说明,所属本技术领域的技术人员对所描述的具体实施例做各种各样的修改或补充或采用类似的方式替代,只要不偏离发明的构思或者超越本权利要求书所定义的范围,均应属于本发明的保护范围。

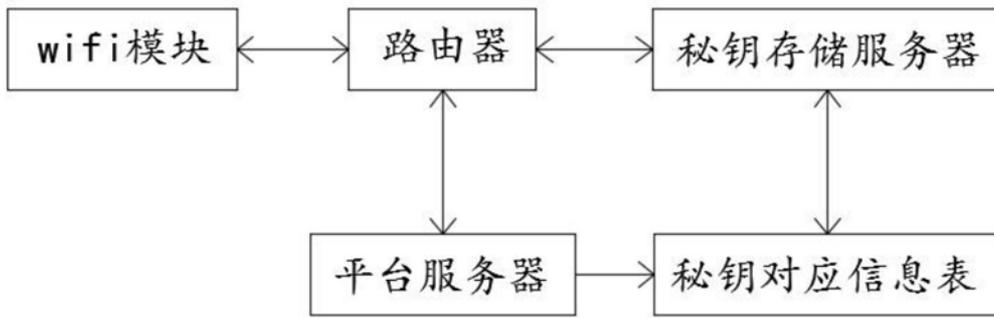


图1