(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 105119900 A
(43)申请公布日 2015.12.02

(21)申请号 201510424991.0

(22)申请日 2015.07.17

(71)申请人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
申请人 奇智软件(北京)有限公司

(72)发明人 刘敏 叶剑杰

(74)专利代理机构 北京市立方律师事务所 11330
代理人 王增鑫

(51)Int.Cl.
H04L 29/06(2006.01)

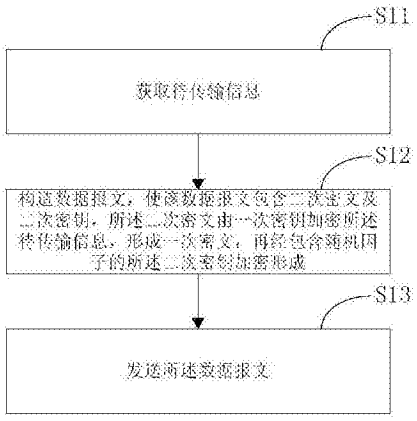
权利要求书1页 说明书23页 附图3页

(54)发明名称

信息安全传输方法、联网接入方法及相应的终端

(57)摘要

本发明的主要目的在于提供一种移动终端及其采用的信息安全传输方法，该方法包括如下步骤：获取待传输信息；构造数据报文，使该数据报文包含二次密文及二次密钥，所述二次密文由一次密钥加密所述待传输信息，形成一次密文，再经包含随机因子的所述二次密钥加密形成；发送所述数据报文。对应的，本发明还提供一种智能终端及其联网接入方法。本发明借助密码技术，通过改进数据报文所加载的内容表达，进一步加强了基于IEEE 802.11协议实现的快连技术的通信安全效果。



CN 105119900 A

1. 一种信息安全传输方法，其特征在于，包括如下步骤：

获取待传输信息；

构造数据报文，使该数据报文包含二次密文及二次密钥，所述二次密文由一次密钥加密所述待传输信息，形成一次密文，再经包含随机因子的所述二次密钥加密形成；

发送所述数据报文。

2. 根据权利要求 1 所述的信息安全传输方法，其特征在于，获取待传输信息的步骤中，通过用户界面接收所述待传输信息及其提交指令，响应于该提交指令而执行后续步骤。

3. 根据权利要求 1 所述的信息安全传输方法，其特征在于，所述待传输信息为用于接入目标网络的配置信息。

4. 根据权利要求 3 所述的信息安全传输方法，其特征在于，所述配置信息包括用于确定所述目标网络的服务集标识以及登录该目标网络的密码。

5. 根据权利要求 1 所述的信息安全传输方法，其特征在于，构造数据报文的步骤包括如下具体步骤：

利用所述一次密钥加密待传输信息获得一次密文；

利用包含随机因子的二次密钥将一次密文加密为二次密文；

组装所述二次密钥与所述的二次密文构成所述数据报文。

6. 根据权利要求 1 所述的信息安全传输方法，其特征在于，所述待传输信息被一次加密前被格式化为包含特定标识的文本。

7. 根据权利要求 1 所述的信息安全传输方法，其特征在于，所述二次密钥包括所述特定标识以用于将所述文本还原为所述待传输信息。

8. 一种移动终端，其特征在于，包括：

获取单元，用于获取待传输信息；

构造单元，用于构造数据报文，使该数据报文包含二次密文及二次密钥，所述二次密文由一次密钥加密所述待传输信息，形成一次密文，再经包含随机因子的所述二次密钥加密形成；

传输单元，用于发送所述数据报文。

9. 一种联网接入方法，其特征在于，包括如下步骤：

接收数据报文；

利用该数据报文所含二次密钥解密所含二次密文以获得一次密文；

利用预存的一次密钥解密所述一次密文以获取其中的配置信息；

以该配置信息配置自身网络设置，接入所述目标网络。

10. 一种智能终端，其特征在于，其包括：

接收单元，用于接收数据报文；

第二解密单元，其利用该数据报文所含二次密钥解密所含二次密文以获得一次密文；

第一解密单元，其利用预存的一次密钥解密所述一次密文以获取其中的配置信息；

接入单元，用于以该配置信息配置自身网络设置，接入所述目标网络。

信息安全传输方法、联网接入方法及相应的终端

技术领域

[0001] 本发明涉及信息安全技术，具体涉及一种移动终端及其所采用的信息安全传输方法，同时涉及一种智能终端及其所联网接入方法。

背景技术

[0002] 智能终端接入目标网络的控制技术，以 IEEE 802.11 协议所规范技术为基础，被大力开发，其应用越来越普遍。最早基于 AD-Hoc、WiFi Direct 技术为基础，使控制端（发送端）与接收端之间建立直连关系，然后开始传输用于接入目标网络的配置信息，具体包括目标网络的服务集标识和登录密码。传统的直连方式由于需要在控制端和接收端以及路由器之间执行复杂的握手和切换过程，因而是低效的。

[0003] 改进的快速连接的技术之一，是利用组播数据帧的目的地址域或其帧本体域的可编辑特性来加载信息，而组播数据帧的接收，不依赖于接收端与控制端之间是否建立直连关系，这样，免除设备间连接的握手过程，免除频繁切换连接关系，因此，快速连接技术的应用范围越来越广泛。

[0004] 由于数据链路层的数据帧能够加载的信息有限，故通常只用于传输容量要求较低的数据，例如所述的配置信息。诚然，也可开拓更为广泛的应用，例如仅仅用于发送一个端到端的需要显示到用户界面的通知，或者仅仅用于发送一个用于驱动接收端的某个部件工作的信号指令等。

[0005] 一方面，无论想要传输的信息是何种类型，均需要考虑到信息安全的问题。目前的上述各种技术中，其通信安全原理，是由接收端和发送端分别持有数学上相同的或者相关的密钥，发送端以其持有的密钥加密待传输信息后，形成数据报文传输到接收端，接收端使用相匹配的密钥解密即可。这种协议方式较为简便，但也更易被破解。究其原因，无论是采用基于对称加密技术实现的私钥加密待，还是采用基于非对称加密技术实现的公钥加密待传输信息，加密待传输信息的密钥总是固定不变，因此，非法用户可以通过截获多次传输时产生的数据包进行暴力破解，或者模拟发送端的数据包，向接收端发起类似 DDOS 的攻击，瘫痪接收端，甚至导致包括 WiFi 路由器在内的其它邻近设备也因为需要识别数据帧而受到同样的影响。

[0006] 另一方面，目前的信息传输过程中，接收与发送双方需要遵守固定的公开或者自定义协议，发送端无法超越既定协议而自由定义待传输信息的格式，接收端同理也无法对应灵活解析所接收的数据报文以获得准确的原始信息，现有信息传输技术不够灵活智能的缺陷由此可见一斑。也正是因为这种不够灵活的缺陷的存在，导致破解者可以通过简单地分析数据报文格式，而以更低的时间成本来从截获的数据报文中获得准确的原始信息，实现其非法窃取信息的目的。

[0007] 有鉴于此，有必要改进现有的数据通信技术，以确保物联网更为安全地进行互联互通。

发明内容

[0008] 本发明的第一目的旨在解决上述至少一个方面的至少部分问题，提供一种移动终端及其所采用的信息安全传输方法，以在源端实现信息安全控制。

[0009] 本发明的第二目的在于解决上述至少一个方面的至少部分问题，提供一种智能终端及其所采用的联网接入方法，以便呼应前一目的使智能终端更为安全地接收配置信息，利用该配置信息接入目标网络。

[0010] 为了实现本发明的第一目的，本发明采取如下技术方案：

[0011] 本发明提供的一种信息安全传输方法，包括如下步骤：

[0012] 获取待传输信息；

[0013] 构造数据报文，使该数据报文包含二次密文及二次密钥，所述二次密文由一次密钥加密所述待传输信息，形成一次密文，再经包含随机因子的所述二次密钥加密形成；

[0014] 发送所述数据报文。

[0015] 进一步，获取待传输信息的步骤中，通过用户界面接收所述待传输信息及其提交指令，响应于该提交指令而执行后续步骤。

[0016] 较佳的，所述待传输信息为用于接入目标网络的配置信息。

[0017] 具体的，所述配置信息包括用于确定所述目标网络的服务集标识以及登录该目标网络的密码。

[0018] 进一步，构造数据报文的步骤包括如下具体步骤：

[0019] 利用所述一次密钥加密待传输信息获得一次密文；

[0020] 利用包含随机因子的二次密钥将一次密文加密为二次密文；

[0021] 组装所述二次密钥与所述的二次密文构成所述数据报文。

[0022] 较佳的，所述待传输信息被一次加密前被格式化为包含特定标识的文本。

[0023] 根据本发明的一个实施例所揭示，所述二次密钥包括所述特定标识以用于将所述文本还原为所述待传输信息。

[0024] 根据本发明另一实施例所揭示，所述二次密钥为随机数。

[0025] 根据本发明的实施例之一所揭示，所述一次密钥为基于非对称加密技术而规范的公钥，适于利用相应的私钥解密该一次密文以获取所述的待传输信息。

[0026] 根据本发明的实施例之一所揭示，所述一次密钥为基于对称加密技术而规范的私钥，适于解密所述的一次密文以获取所述的待传输信息。

[0027] 根据本发明的实施例之一所揭示，所述二次密钥为基于对称加密技术而规范的私钥，适于解密所述的二次密文以获取所述的一次密文。

[0028] 进一步，所述数据报文还包括用于表征整个数据报文长度的校验码。

[0029] 较佳的，发送所述数据报文的步骤中，在数据链路层格式化为多个按序表征的组播数据帧加载该数据报文以便发送。

[0030] 进一步，所述数据报文被加载到所述组播数据帧的目的地址域和/或帧本体域中。

[0031] 具体的，所述组播数据帧符合 IEEE 802.11 协议的规范。

[0032] 本发明提供的一种移动终端，其包括：

[0033] 获取单元，用于获取待传输信息；

[0034] 构造单元，用于构造数据报文，使该数据报文包含二次密文及二次密钥，所述二次密文由一次密钥加密所述待传输信息，形成一次密文，再经包含随机因子的所述二次密钥加密形成；

[0035] 传输单元，用于发送所述数据报文。

[0036] 进一步，所述获取单元被配置为通过用户界面接收所述待传输信息及其提交指令，响应于该提交指令而启动构造单元。

[0037] 较佳的，所述待传输信息为用于接入目标网络的配置信息。

[0038] 具体的，所述配置信息包括用于确定所述目标网络的服务集标识以及登录该目标网络的密码。

[0039] 进一步，所述构造单元包括如下具体模块：

[0040] 一次加密模块，被配置为利用所述一次密钥加密待传输信息获得一次密文；

[0041] 二次加密模块，被配置为利用包含随机因子的二次密钥将一次密文加密为二次密文；

[0042] 结构组装模块，用于组装所述二次密钥与所述的二次密文构成所述数据报文。

[0043] 较佳的，所述待传输信息被一次加密前被格式化为包含特定标识的文本。

[0044] 根据本发明的一个实施例所揭示，所述二次密钥包括所述特定标识以用于将所述文本还原为所述待传输信息。

[0045] 根据本发明另一实施例所揭示，所述二次密钥为随机数。

[0046] 根据本发明的实施例之一所揭示，所述一次密钥为基于非对称加密技术而规范的公钥，适于利用相应的私钥解密该一次密文以获取所述的待传输信息。

[0047] 根据本发明的实施例之一所揭示，所述一次密钥为基于对称加密技术而规范的私钥，适于解密所述的一次密文以获取所述的待传输信息。

[0048] 根据本发明的实施例之一所揭示，所述二次密钥为基于对称加密技术而规范的私钥，适于解密所述的二次密文以获取所述的一次密文。

[0049] 进一步，所述数据报文还包括用于表征整个数据报文长度的校验码。

[0050] 较佳的，所述传输单元，被配置为在数据链路层格式化为多个按序表征的组播数据帧加载该数据报文以便发送。

[0051] 进一步，所述数据报文被加载到所述组播数据帧的目的地址域和 / 或帧本体域中。

[0052] 具体的，所述组播数据帧符合 IEEE 802.11 协议的规范。

[0053] 为实现本发明的第二目的，本发明采用如下技术方案：

[0054] 本发明提供的一种联网接入方法，包括如下步骤：

[0055] 接收数据报文；

[0056] 利用该数据报文所含二次密钥解密所含二次密文以获得一次密文；

[0057] 利用预存的一次密钥解密所述一次密文以获取其中的配置信息；

[0058] 以该配置信息配置自身网络设置，接入所述目标网络。

[0059] 较佳的，接收数据报文的步骤中，获得数据报文之后，利用数据报文所含校验码检验整个数据报文的长度，仅接收校验成功的数据报文。

[0060] 进一步，接收数据报文的步骤包括如下具体步骤：

[0061] 接收具有相同源地址的组播数据帧；

[0062] 按照各组播数据帧提供的顺序码所表征的索引顺序组装各组播数据帧携带的内容码；

[0063] 将按序组装后的内容码转换为所述的数据报文。

[0064] 具体的，所述组播数据帧符合 IEEE 802.11 协议的规范。

[0065] 进一步，所述顺序码及内容码表达于相应的组播数据帧的目的地址域和 / 或帧本体域中。

[0066] 根据本发明的实施例之一所揭示，所述二次密钥为对称加密技术所规范的私钥，所述的二次密文由该私钥加密而得。

[0067] 根据本发明的实施例之一所揭示，所述一次密钥为非对称加密技术所规范的私钥，所述一次密文由对应的公钥加密而得。

[0068] 根据本发明的实施例之一所揭示，所述一次密钥为对称加密技术所规范的私钥，所述一次密文由该私钥加密而得。

[0069] 进一步，利用预存的一次密钥解密所述一次密文以获取其中的配置信息的步骤中，解密完成后获得包含特定格式的文本，利用所述二次密钥所包含的特定标识将该文本解析为所述配置信息。

[0070] 具体的，所述配置信息包括用于确定所述目标网络的服务集标识以及登录该目标网络的密码。

[0071] 本发明提供的一种智能终端，其包括：

[0072] 接收单元，用于接收数据报文；

[0073] 第二解密单元，其利用该数据报文所含二次密钥解密所含二次密文以获得一次密文；

[0074] 第一解密单元，其利用预存的一次密钥解密所述一次密文以获取其中的配置信息；

[0075] 接入单元，用于以该配置信息配置自身网络设置，接入所述目标网络。

[0076] 较佳的，所述接收单元，被配置为获得数据报文之后，利用数据报文所含校验码检验整个数据报文的长度，仅接收校验成功的数据报文。

[0077] 进一步，所述接收单元包括：

[0078] 帧接收模块，用于接收具有相同源地址的组播数据帧；

[0079] 帧组装模块，用于按照各组播数据帧提供的顺序码所表征的索引顺序组装各组播数据帧携带的内容码；

[0080] 转换模块，用于将按序组装后的内容码转换为所述的数据报文。

[0081] 具体的，所述组播数据帧符合 IEEE 802.11 协议的规范。

[0082] 进一步，所述顺序码及内容码表达于相应的组播数据帧的目的地址域和 / 或帧本体域中。

[0083] 根据本发明的实施例之一所揭示，所述二次密钥为对称加密技术所规范的私钥，所述的二次密文由该私钥加密而得。

[0084] 根据本发明的实施例之一所揭示，所述一次密钥为非对称加密技术所规范的私钥，所述一次密文由对应的公钥加密而得。

[0085] 根据本发明的实施例之一所揭示，所述一次密钥为对称加密技术所规范的私钥，所述一次密文由该私钥加密而得。

[0086] 进一步，所述第一解密单元中，被配置为解密完成后获得包含特定格式的文本，利用所述二次密钥中所包含的特定标识将该文本解析为所述配置信息。

[0087] 具体的，所述配置信息包括用于确定所述目标网络的服务集标识以及登录该目标网络的密码。

[0088] 与现有技术相比较，本发明的方案具有以下优点：

[0089] 1、本发明通过对如用于接入目标网络的配置信息之类的待传输信息进行封装，构造出具有特定加密格式的数据报文，在既有的对待传输信息进行一次加密的基础上，施以二次加密，并且将二次加密所用的密钥明文包含到该数据报文中，使得该数据报文无论是以广播还是组播的方式进行传输的过程中，即使被截获，也因为有两重加密而更难被破解。即使被暴力破解，由于所述二次密钥包含有随机因子，每次传输信息时二次密钥都因为随机因子的存在而通常互不相同，因此截获者无法根据多次截获的不同数据包来获得一个确定所述二次密钥的规律，从而无法伪造发送端发送数据报文，由此便于移动终端之类的发送端能够更安全地向接收端传输信息。相应的，在接收端，由于发送端的上述机制使得数据报文呈现了利用其所含二次密钥解密所含的信息内容的规律性，可以依据这一规律提取数据报文所加载的诸如配置信息之类的信息，有效判别数据报文的合法格式，从而确保所获信息的安全性，达到安全接收信息的效果。

[0090] 2、本发明在二次密钥中包括用于解析被传输信息未经加密的格式化文本的特定标识，使二次密钥同时具备加密、解密的功能以及包含了用于解析被传输信息的特定标识，构成解析方案，进一步增加了破解该数据报文的复杂度，使发送端发出数据报文后，传输过程的安全性得以进一步提高。对于接收端而言，则能够依据这一改进规律调用其中的解析方案对被传输信息的未经加密的格式化文本进行解析，利用其中的特定标识识别出所接收信息的内容，最终依然可以获得发送端欲传输表达的原始信息，而其安全性显然得以进一步提高。

[0091] 3、同理，基于数据报文中所述解析方案的存在，使得发送端可以灵活地制定待传输信息的格式化文本的具体格式，而接收端则可依据数据报文的二次密钥所包含的特定标识对格式化的待传输信息进行有效识别，因此，使得发送端与接收端具有了协商细节协议的功能，提高了信息表达及解析的智能化程度。

[0092] 4、本发明基于组播数据帧的特性，在数据链路层将所述数据报文加载到多个按序表述的组播数据帧内部的目的地址域和／或帧本体域中，由于组播数据帧的传播及接收均无需依赖于接收端与发送端之间的直连关系，因而，可以避免连接关系切换、握手等技术环节，便于更快速地传播被传输的信息，也便于接收端更快速地利用所述的信息，特别当所述的信息为用于接入目标网络的配置信息时，可以使接收该配置信息的智能终端更快速地实现目标网络接入。另一方面，由于提高了信息接收的速度，也更能降低传输过程中数据报文被截获的概率，从而进一步体现出本发明无论是其接收方案还是发送方案的安全特性。

[0093] 本发明附加的方面和优点将在下面的描述中部分给出，这些将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[0094] 本发明上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

[0095] 图1为本发明所采用的组播地址的结构示意图；

[0096] 图2为本发明所采用的组播地址与IP地址之间映射关系示意图；

[0097] 图3为本发明的信息安全传输方法的原理示意图；

[0098] 图4为本发明的信息安全传输方法的步骤S12所实现的具体流程的原理示意图；

[0099] 图5为本发明所构造的数据报文的结构示意图；

[0100] 图6为本发明的联网接入方法的原理示意图；

[0101] 图7为本发明的联网接入方法的步骤S21所实现的具体流程的原理示意图；

[0102] 图8为本发明的移动终端的结构示意图；

[0103] 图9为本发明的移动终端的构造单元的内部结构示意图；

[0104] 图10为本发明的智能终端的结构示意图；

[0105] 图11为本发明的智能终端的接收单元的内部结构示意图。

具体实施方式

[0106] 下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，仅用于解释本发明，而不能解释为对本发明的限制。

[0107] 本技术领域技术人员可以理解，除非特意声明，这里使用的单数形式“一”、“一个”、“所述”和“该”也可包括复数形式。应该进一步理解的是，本发明的说明书中使用的措辞“包括”是指存在所述特征、整数、步骤、操作、元件和/或组件，但是并不排除存在或添加一个或多个其他特征、整数、步骤、操作、元件、组件和/或它们的组。应该理解，当我们称元件被“连接”或“耦接”到另一元件时，它可以直接连接或耦接到其他元件，或者也可以存在中间元件。此外，这里使用的“连接”或“耦接”可以包括无线连接或无线耦接。这里使用的措辞“和/或”包括一个或更多个相关联的列出项的全部或任一单元和全部组合。

[0108] 本技术领域技术人员可以理解，除非另外定义，这里使用的所有术语（包括技术术语和科学术语），具有与本发明所属领域中的普通技术人员的一般理解相同的意义。还应该理解的是，诸如通用字典中定义的那些术语，应该被理解为具有与现有技术的上下文中的意义一致的意义，并且除非像这里一样被特定定义，否则不会用理想化或过于正式的含义来解释。

[0109] 本技术领域技术人员可以理解，这里所使用的“终端”、“终端设备”、“智能终端”、“移动终端”既包括无线信号接收器的设备，其仅具备无发射能力的无线信号接收器的设备，又包括接收和发射硬件的设备，其具有能够在双向通信链路上，执行双向通信的接收和发射硬件的设备。这种设备可以包括：蜂窝或其他通信设备，其具有单线路显示器或多线路显示器或没有多线路显示器的蜂窝或其他通信设备；PCS(Personal Communications Service，个人通信系统)，其可以组合语音、数据处理、传真和/或数据通信能力；PDA(Personal Digital Assistant，个人数字助理)，其可以包括射频接收器、寻呼机、互联网/内联网访问、网络浏览器、记事本、日历和/或GPS(Global Positioning System，全球

定位系统）接收器；常规膝上型和/或掌上型计算机或其他设备，其具有和/或包括射频接收器的常规膝上型和/或掌上型计算机或其他设备。这里所使用的各种“终端”可以是便携式、可运输、安装在交通工具（航空、海运和/或陆地）中的，或者适合于和/或配置为在本地运行，和/或以分布形式，运行在地球和/或空间的任何其他位置运行。这里所使用的各种“终端”还可以是通信终端、上网终端、音乐/视频播放终端，例如可以是PDA、MID(Mobile Internet Device，移动互联网设备）和/或具有音乐/视频播放功能的移动电话，也可以是智能电视、机顶盒、智能摄像头、智能遥控器、智能插座等设备。

[0110] 本发明是为了因应物联网的发展而提出的信息安全技术解决方案，使信息从发送到接收的整个传输过程中进一步加强安全性。本发明所适应的应用场景主要体现为以WiFi技术实现的智能终端和移动终端之间的通信，与操作系统无必然关联。以此为基础，本发明不仅在一方面为起中央控制作用的类似手机之类的终端提供了实质上的编码机制，以便为其他智能终端接入目标网络提供自动化接入向导，另一方面，也可以为独立于所述的起中央控制作用的移动终端之外的其他智能终端提供解码机制，从而实现此类智能终端受控接入目标网络。

[0111] 尽管本发明体现安全性能的核心方案既可用于组播也可用于广播的场景中，但出于简洁说明的考虑，仍仅选取在数据链路层以组播技术实现数据报文传输的情况为典型实施例加以说明。具体而言，本发明有关传输数据报文的典型实施例中，以组播数据帧为技术实现载体，实现对数据报文的传输。由此有必要将本发明有关数据链路层的编码和解码两方面所涉基础知识予以揭示，使本领域技术人员依照本说明书即可免经创造性思维实现之。

[0112] 由于本发明以组播技术为例进行说明，涉及对组播数据帧的利用，而本发明的组播数据帧又接受802.11协议的规范，因此，有必要先行了解802.11协议所规范的物理帧(MAC帧）的基础知识。

[0113] 表1：802.11协议族MAC帧结构（首行单位为Bytes字节）：

[0114]

2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration	Address 1	Address 2	Address 3	Seq Ctrl	Address 4	Frame Body	Check Sum

[0115] 以下针对表1涉及的各个域做相应的说明：

[0116] Frame Control，帧控制域；

[0117] Duration/ID，持续时间/标识，表明该帧和它的确认帧将会占用信道多长时间；对于帧控制域子类型为：Power Save-Poll的帧，该域表示了STA的连接身份(AID，Association Indentification)

[0118] Address Fields(1-4)：为地址域，包括4个地址（源地址、目的地址、发送方地址和接收方地址），取决于帧控制字段中的To DS和From DS位。

[0119] Seq Ctrl，即Sequence Control—为序列控制域，用于过滤重复帧。

[0120] Frame Body：帧本体域，或称数据域，用于表示发送或接收的信息。

[0121] Check Sum：校验域，包括 32 位的循环冗余校验 (CRC)。

[0122] 表 2：帧控制 (Frame Control) 结构 (首行单位为比特 (位))：

[0123]

2	2	4	1	1	1	1	1	1	1	1
Version	Type	Subtype	To DS	From DS	MF	Retry	Pwr	More	W	O

[0124] 以下针对表 2 涉及的各个字段做相应的说明：

[0125] Protocol Version－表示 IEEE 802.11 标准的版本。

[0126] Type－表示帧类型：包括管理、控制和数据等类。

[0127] Subtype－表示帧的子类型，如：认证帧 (Authentication Frame)、解除认证帧 (Deauthentication Frame)、连接请求帧 (Association Request Frame)，连接响应帧 (Association Response Frame)、重新连接请求帧 (Reassociation Request Frame)、重新连接响应帧 (Reassociation Response Frame) 解除连接帧 (Disassociation Frame)、信标帧 (Beacon Frame)、Probe 帧 (Probe Frame)、Probe 请求帧 (Probe Request Frame) 或 Probe 响应帧 (Probe Response Frame)。

[0128] To DS- 当帧发送给 Distribution System(DS) 时，该值设置为 1。

[0129] From DS- 当帧从 Distribution System(DS) 处接收到时，该值设置为 1。

[0130] MF-More Fragment 表示当有更多分段属于相同帧时该值设置为 1。

[0131] Retry- 表示该分段是先前传输分段的重发帧。

[0132] Pwr-Power Management，表示传输帧以后，站所采用的电源管理模式。

[0133] More-More Data，表示有很多帧缓存到站中。

[0134] W-WEP，表示根据 WEP(Wired Equivalent Privacy) 算法对帧主体进行加密。

[0135] O-Order1 表示接受者应该严格按照顺序处理该帧。

[0136] 根据表 2 的说明可知，通过 From DS 与 To DS 字段可以确定组播数据帧的目的地址域所在位置。参阅表 3：

[0137] 表 3：地址字段在数据帧中的用法：

[0138]

功能	To DS	From DS	Address1(接收端)	Address2(发送端)	Address3	Address4
IBSS	0	0	DA	SA	BSSID	未使用
To AP(基础结构型)	1	0	BSSID	SA	DA	未使用
From AP(基础结构型)	0	1	DA	BSSID	SA	未使用
WDS(无线分布式系统)	1	1	RA	TA	DA	SA

[0139] 本领域技术人员应当知晓，IP 地址空间被划分为 A、B、C 三类。第四类即 D 类地址被保留用做组播地址。在第四版的 IP 协议 (IPv4) 中，从 224.0.0.0 到 239.255.255.255 间的所有 IP 地址都属于 D 类地址。

[0140] 组播地址中最重要的是第 24 位到 27 位间的这四位，对应到十进制是 224 到 239，

其它 28 位保留用做组播的组标识，如图 1 所示。

[0141] IPv4 的组播地址在网络层要转换成网络物理地址。对一个单播的网络地址，通过 ARP 协议可以获取与 IP 地址对应的物理地址。但在组播方式下 ARP 协议无法完成类似功能，必须得用其它的方法获取物理地址。在下面列出的 RFC 文档中提出了完成这个转换过程的方法：

[0142] RFC1112：Multicast IPv4to Ethernet physical address correspondence

[0143] RFC1390：Correspondence to FDDI

[0144] RFC1469：Correspondence to Token-Ring networks

[0145] 在最大的以太网地址范围内，转换过程是这样的：将以太网地址的前 24 位最固定为 01:00:5E，这几位是重要的标志位。紧接着的一位固定为 0，其它 23 位用 IPv4 组播地址中的低 23 位来填充。该转换过程如图 2 所示。例如，组播地址为 224.0.0.5 其以太网物理地址为 01:00:5E:00:00:05。可以看出，这里的目的地址域的低 23 位（也可更少）便可以作为可编辑比特区，供加载信息。

[0146] 此外，帧本体域，即 Frame Body，这部分内容的长度可变，其具体存储的内容由帧类型（type）和子类型（sub type）决定。

[0147] 可以看出，组播数据帧中的目的地址域与帧本体域是其两个可编辑域，发送端可以设置目的地址域的可编辑比特区即其低 23 位内容，以及控制帧本体域的长度。无论是单独运用目的地址域的可编辑比特区或帧本体域的长度，还是运用两者的结合，均可用于加载需要传输的信息。

[0148] 在智能终端未连接 WiFi 接入点的时候，WiFi 芯片是可以侦测到空间中的射频信号并识别 MAC 帧的，但是此时设备因为经过接入点的认证未有密钥，所以无法进一步解析帧结构中帧本体域的数据，但由于帧本体域的帧长度可知，从而整个组播数据帧的帧长度也可知，因此，这一特性并不影响对组播数据帧的帧长度的利用。故而，本发明通过利用这些字段，使得在智能终端即使不联网的情况下也能接收到移动终端以组播方式发送的信息。实际上，根据 802.11 协议也可知，对于一个组播数据帧而言，其整个帧的长度唯一性地关联并决定于其中的帧本体域的长度。

[0149] 根据上述揭示的知识可以看出，对于组播数据帧而言，其帧结构中的目的地址域和 / 或其帧本体域长度变化均可用于加载配置信息。

[0150] 本发明提供的一种信息安全传输方法，通常是作为主动发起方，或者作为中央控制方的视角来加以描述的，可以通过编程将本方法实现为计算机程序安装在类似手机、平板电脑或者其他移动终端中运行，例如，在运行 Android、IOS、Windows Phone 系统的手机或与平板电脑中安装利用该传输方法实现的 APP（应用程序），由该应用程序执行该传输方法。

[0151] 请参阅图 3，本发明的信息安全传输方法的一个典型实施例，该方法具体包括如下步骤：

[0152] 步骤 S11、获取待传输信息。

[0153] 考虑到本发明主要利用组播或广播技术来实现数据传输，因而所述的待传输信息，尤其适合指数据量不大的信息内容，例如用于接入目标网络的配置信息，通常只包括目标网络的服务集标识和密码，信息量便较小；又如仅仅包含一条用于被接收端执行的指令

语句；再如仅仅包含一条推送给接收端的通知信息。诸如此类，均能最大化程度地发挥本发明的优点。至于信息量大小的量化指标，由于每个数据帧所能表达的数据容量有限，可由本领域技术人员根据实际情况确定。

[0154] 需要指出的是，本发明的各个实施例中，出于说明的简便考虑，常以该传输信息的一个实例即所述的配置信息来指称该待传输信息，但不应理解为是对“待传输信息”这一概念及其变换了说法而又依然指代相同对象的诸如“被传输信息”、“所接收信息”等概念的限制。同理，后续涉及对待传输信息被格式化、加密等操作而引起的不同格式化内容，尽管其表达形式产生变化，但其指向的对象依然是“待传输信息”这一概念所指向的信息。

[0155] 以基于本发明实现的APP为例，当该APP得以运行时，便可通过系统驱动对手机上的硬件设备进行利用。众所周知的，手机上不仅具有WiFi模组、显示器、控制芯片，还具有麦克风、扬声器等部件，这些部件均可通过该APP实现调用。

[0156] 以Android系统为例，手机终端通过其获取单元首先调用并显示一个活动组件(Activity)，或者显示一个利用HTML5实现的页面，在屏幕上显示该用户界面及扫描到的WiFi接入点信息（以服务集标识SSID罗列），请求用户选定目标网络，并要求用户输入相应的密码，从而获取目标网络的SSID和密码。

[0157] 根据WiFi协议的约定，本领域技术人员可以知晓，配置信息通常包括WiFi无线路由器（代表目标网络）所提供的用于确定该目标网络的服务集标识(SSID)与用于登录该目标网络的登录密码，在某些情况下可能还需要包括登录密码的加密方式，而对于开放网络也可不必提供登录密码。尽管WiFi协议存在版本更替的事实，但这些涉及为实现接入网络而必备的配置信息可由本领域技术人员依据协议文件对应确定，因此，对其详情及其等同变化方案恕不加以赘述。

[0158] 作为细节变通，当用户选定了SSID之后，可以向云端服务器查询该SSID所对应的密码，如果密码存在，则直接通过云端下载密码，可省去要求用户输入目标网络密码的过程。

[0159] 步骤S12、构造数据报文，使该数据报文包含二次密文及二次密钥，所述二次密文由一次密钥加密所述待传输信息，形成一次密文，再经包含随机因子的所述二次密钥加密形成。

[0160] 获得所述的配置信息之类的待传输信息之后，便需要为其构造数据报文。构造数据报文的过程，起到了沟通应用层与数据链路层的作用，具体而言，从应用层获取所述配置信息之类的待传输信息，而后续将在数据链路层发送该数据报文，故而，构造数据报文的过程，实质上相当于一个由本发明定义的协议层。因而，本步骤的实现是非常灵活的，以下以若干示例加以说明：

[0161] 参阅图4所示的一种构造所述数据报文的示例过程，包括如下步骤：

[0162] 步骤S121、利用所述一次密钥加密待传输信息获得一次密文。

[0163] 所述的一次密钥，是指目前广为采用的用于对被传输信息进行一次加密的密钥，一般采用公钥加密方式，即非对称加密方式。公钥加密方式中，移动终端作为发送端将待传输信息的原始文本以其持有的公钥进行加密，传输到对端时，作为接收端的智能终端调用预存的私钥，对待传输信息进行解密，从而获得其原始版本。所述的公钥与私钥，在算法上相关，因而可以用于相互解密对方加密的数据。本实施例中，本步骤同理沿用传统技术，利

用所述的一次密钥对原始格式的配置信息进行加密，从而获得一次密文。非对称加密技术体现了较高的安全性，常被用于安全性要求较高的场景中。

[0164] 变通的实施方式中，所述的一次密钥可以利用私钥加密，即对称加密技术实现。这一技术中，移动终端与智能终端分别存有相同的所述一次密钥，移动终端利用一次密钥加密待传输信息，获得一次密文，传输到智能终端，智能终端便可以利用预存的一次密钥将待传输信息解密。对称加密具有算法简单效率更高的特点，因而在某些安全性要求不太高的场景中可被优先选用。

[0165] 步骤 S122、利用包含随机因子的二次密钥将一次密文加密为二次密文。

[0166] 本实施例中，一次密文形成之后，或者某些不依赖于一次加密的实施例中的所述待传输信息，在本步骤中被利用二次密钥进行二次加密形成二次密文。需要指出的是，所述的二次密钥尤其适用于采用对称加密技术所规范的私钥，由此，当智能终端接收到相应的报文后，可以以较低的计算消耗对二次密文进行解密。

[0167] 所述的二次密钥，包括有随机因子，所述的随机因子至少包括在二次密钥中采用随机数以及利用随机的方式选定一个二次密钥两种情况。借助该随机因子的作用，使二次密钥在每次被用于二次加密之前均具有不确定性，也就是即将对一次密文进行二次加密时，才予以确定。由此，二次密钥对每一待传输信息进行二次加密时，均能最大程度地体现出其唯一性。

[0168] 所述的二次密钥的具体实现可以体现为如下几种随意选择的方式：

[0169] 一、采用随机数作为所述的二次密钥。

[0170] 这种方式中，直接调用随机函数，产生一个特定位数如 16 位的随机数，将该随机数确定为所述的二次密钥。这种方式最易实现，更为高效，便于智能终端快速解密。

[0171] 二、随机地从预存的多个密钥中确定所述的二次密钥。

[0172] 这种方式同理可以通过调用随机函数，来确定一个预存的二次密钥，使其内容体现出不确定性。由此而确定的二次密钥，也具有随机性的特点，同理可以起到对截获者制造破译障碍的效果。

[0173] 三、以用于解析未被一次加密前的所述待传输信息的格式化标识的有序集合作为所述的二次密钥。

[0174] 待传输信息，通常包括多个信息元，如前所述的配置信息，在一个应用场景中，可以是包含用于提供 WiFi 接入点的服务集标识 (SSID) 及其密码 (PSW) 的信息。每个信息元中，一般以某种形式予以表征其信息类型及相应的信息内容。当其需要传输时，通常以将这些信息元串接的形式表达成一个字符串，完成对待传输信息的格式化，获得格式化的配置信息。

[0175] 具体而言，以配置信息为例，服务集标识与密码均构成信息元，信息元之间用元素第一格式化标识“|”加以分隔，信息元的信息类型与信息内容之间用第二格式化标识“:”分隔。例如服务集标识是以 SSID 表示其信息类型，密码用 PSW 表示其信息类型，SSID 的信息内容为 MYWiFi，密码的信息内容为 PLZLOGIN，未被一次加密前，对其进行格式化形成的格式化的配置信息的文本形式为：

[0176] SSID:MYWiFi|PSW:PLZLOGIN

[0177] 注意，上述表达的格式化的配置信息中，是按照一定的顺序来组织的，其中 SSID

在前，PSW 在后，这两个信息类型标识符可以供识别相应的信息内容之用，而所述的格式化标识“:|:”则体现出其特质，如果发送端与接收端之间约定从二次密钥的第一字节处获得第一格式化标识，从第二字节处获得第二格式化标识，则发送端无论采用何种符号用于表达所述的格式化标识，对于接收端而言，均可通过从二次密钥的第一字节与第二字节获取具有约定功能的格式化标识，并以其中第一字节的符号分隔各个信息元，而用第二字节的符号分隔信息类型及其信息内容，从而正确解析格式化配置信息，还原出各个信息元的信息内容。因此，这一实例无疑体现出了数据报文具有自带解析方案的功能，使所述的二次密钥不仅适于解密二次密文，而且适于解析未被加密之前的格式化的配置信息，增加了数据报文的复杂度，使截获者更难以破解。

[0178] 显然，作为特定标识，所述的格式化标识适宜按照其在格式化的配置信息中出现的顺序，被同理按序排列在所述的二次密钥中，所述的格式化标识可以随机确定。当需要使用的格式化标识的个数越多，排列越多样化，其能表达的解析功能越强大，密钥的复杂度也将进一步提高，从而使二次密文更难以破译。这种情况下，二次密钥实质上是一个由多个格式化标识构成的特定标识集，该特定标识集内的特定标识串，可以用于解析格式化的配置信息，而作为一个整体，还可用于解密该配置信息的二次密文从而获得一次密文。

[0179] 进一步的一个改进中，所述的配置信息被按照如下方式表达以增加其可读难度：0MYWiFiPLZLOGIN8。可以看出，这种表达方式中，不同信息元未被以任何符号分隔，然而却仍然可以借助格式化标识来加以解析。

[0180] 具体而言，是将信息元的分隔位置表征成格式化标识，使该格式化标识用于指示不同信息元在格式化配置信息中的位置信息。例如，首字符“0”与末字符“8”实际上是非必须的干扰因子，干扰因子的添加，使得破译者即使获得所述格式化的配置信息，也仍然难以直观判断其真实内容。而在二次密钥中，形成的内容为“020815”，其中，“02”用于表征第一个信息元 SSID 的起始位置为顺序第 2 位，“08”用于表征第二个信息元 SSID 的起始位置为第 8 位，而最后两个“15”用于表征整个配置信息的终止位置。根据与上例等效的原理，接收端从二次密钥中读取“020815”这一特定标识串之后，便可通过确定各个信息元的起始位置，从而获取不同的信息元内容。如果传输双方已约定不同顺序的信息元的信息类型，则接收端即可据此理解发送端在格式化配置信息中表达的信息元的确切内容。通过观察这一改进的实例同样可以知晓，由于同一配置信息的各个信息元的信息内容通常长度不一（例如改变了配置信息中的密码），也可能产生变化，导致不同配置信息中各个信息元出现的位置不同，因而，对应形成的特定标识串的内容也并非每次都相同，起到随机因子的作用，因此也使二次密钥体现出了本发明所需的随机特性。

[0181] 可见，二次密钥所包括的所述的特定标识，也即所述的各种格式化标识，可以用于将格式化的配置信息文本还原为原始的具备了识别意义的配置信息，使其各个信息元的信息内容能被顺利识别和利用。

[0182] 按照此处的描述，待传输信息是先以其格式化文本被加密成一次密文之后，再被所述特定标识集加密形成二次密文表述于所述数据报文中的。需要指出的是，考虑到二次密钥具备解析和加密的双重功能的情况下，在一个改进的用于突出特定标识集的解析功能的实例中，也可去除所述一次加密的过程，这种情况下，被表述于数据报文中的配置信息，便可以是由其未加密状态下的格式化文本，以所述的特定标识集对其进行加密形成的密

文。

[0183] 进一步用于强化特定标识集的自解析功能的改进实施例中，进一步忽略加密考虑，不对所述格式化文本进行任何加密，而仅仅将特定标识集的格式化标识串提供到数据报文中，以便接收端利用其中的格式化标识解析包含在所述数据报文中的明文的所述格式化文本。

[0184] 四、在第三种所揭示的两种案例及以此展开的其它变例的基础上，进一步添加随机数构造所述的二次密钥。

[0185] 适应前一种在格式化配置信息中携带自解析方案的多个示例，当然也可以结合所述第一种示例的方式，为前一种示例所述的二次密钥添加一个随机数来加强其安全性。

[0186] 综合上述提供的几种确定包含随机因子的所述二次密钥的示例，程序员可以依照确定的协议在编程时选定任意一种示例方式实现之，进一步便可调用对称加密算法对所述的一次密文进行加密，从而形成所述的二次密文。

[0187] 步骤 S123、组装所述二次密钥与所述的二次密文构成所述数据报文。

[0188] 当所述的二次密文与二次密钥的明文格式得以确定，便可按照发送端与接收端之间的协议，如图 5 所示，将二次密钥前置于所述的二次密文，组装成数据报文。出于校验的考虑，进一步还将数据报文的整体长度用作校验码表达于该数据报文的前端，使接收端能够利用该校验码判定所接收的数据报文是否完整。显然，关于数据报文的结构，也即各个部分的排列是比较灵活的，附图的示例给出的只是较佳的实施方式，使所述的检验码及相继的二次密钥尤其是其特定标识集构成其首部，末尾为其内容部分。本领域技术人员可以参照这一结构灵活调整该数据报文的结构，对数据报文进行组装，而不应受这一结构的影响而限缩对本发明的理解。

[0189] 构造了本发明的数据报文之后，便完成了发送端与接收端在自定义协议层的工作，依照 IEEE 802.11 协议的规范，后续步骤将在数据链路层以下进行处理。

[0190] 步骤 S13、发送所述数据报文。

[0191] 本步骤中，需要进一步将所述的数据报文处理成帧数据。本发明以组播数据帧为例进行说明，现介绍几种利用组播数据帧传输所述的数据报文的示例：

[0192] 一、仅以组播数据帧的目的地址域用于加载所述的数据报文的内容。

[0193] 具体而言，单独对组播数据帧目的地址域的可编辑比特区低 23 位加以利用，利用其中的前 6 位用于表达每个组播数据帧的顺序码，利用余下的 17 位表达要加载的有序分段的内容码，因此共可以通过 $2^6 = 64$ 个组播数据帧来传送一个数据报文。其中顺序码为“000000”的组播数据帧可以用作参考，以利于接收端据此开始接收同源的后续帧，也可不必设置这一参考。以这种方式将所述的数据报文加载到 64 个组播数据帧中，传送给接收端，接收端便可依据相逆原理，按照每个组播数据帧的顺序码所指示的顺序，将各个组播数据帧的内容码按序组装，获得所述的数据报文。

[0194] 二、仅以组播数据帧的帧本体域用于加载所述的数据报文的内容。

[0195] 发送端对组播数据帧的帧本体域的控制，主要体现在对其帧长度的可控利用，但帧长度的利用需要依赖于比较基准，因而，同理可采用上述的参考帧的方式，使该参考帧具有最短的帧长度（唯一性关联于其帧本体域长度），而控制其余各组播数据帧的帧本体域的长度，使不同组播数据帧与所述参考帧的帧长度之间体现出差值，使该差值的二进制格

式比特串用于表达例如 10 位比特内容，其中例如前 4 位用于表达所述顺序码，后 6 位用于表达所述内容码，同理可通过 $2^4 = 16$ 个组播数据帧来加载所述的数据报文。

[0196] 三、同时使用组播数据帧的目的地址域及帧本体域用于加载数据报文。

[0197] 对本实例的理解，请先参照前两例。本实例中，假设按照前述第一实例确定目的地址域低 23 位中的前 6 位用于表达顺序码，余 17 位用于表达内容码，进一步再结合第二实例的方法对帧本体域所决定的帧长度进行利用，使组播数据帧与一个参考帧之间的帧长度的差值的二进制格式比特串为 3 位，则内容码实质上由 17 位加上 3 位共 20 位构成，可以看出，其信息表达能力得以扩展，大大增强。

[0198] 无论采用何种方式对组播数据帧加以利用，利用有序表征的多个组播数据帧实现对所述数据报文的加载，从而将所述的待传输信息在数据链路层完成格式化，均可满足 IEEE 802.11 协议的规范。

[0199] 完成所述在数据链路层的处理工作后，便可以组播数据帧的方式将所述包含待传输信息的数据报文传送给接收端。

[0200] 本发明的信息安全传输方法在传输信息过程中，即使所有组播数据帧均被截获，从而使截获者获得所述的数据报文，由于本发明的方法起到的安全强化作用，截获者依然难以破译本发明的被传输的信息。

[0201] 本发明进一步提供的一种联网接入方法，可以对以前述的信息安全传输方法传输的信息进行利用，请参阅图 6，该联网接入方法包括如下步骤：

[0202] 步骤 S21、接收数据报文。

[0203] 本步骤需要负责完成数据链路层的帧接收以便获得相应的数据报文。接收数据报文的过程与前述发送数据报文的过程具有协议上的相逆关系，可以参考 IEEE 802.11 的规范。以前述采用组播数据帧的实例为基础，可以参照图 7 所示的如下的具体方法对应处理：

[0204] 步骤 S211、接收具有相同源地址的组播数据帧。

[0205] 本步骤通过 WiFi 模组接收具有相同源地址的组播数据帧的技术，为本领域技术人员所知晓，需要指出的是，这里所称的相同源地址，是指所述发送端的源地址，以此识别本方法所需的配置信息的发送方。

[0206] 步骤 S212、按照各组播数据帧提供的顺序码所表征的索引顺序组装各组播数据帧携带的内容码。

[0207] 如前揭示了单独利用组播数据帧的目的地址域的可编辑比特区、单独利用帧本体域长度差值、共同利用所述目的地址域的可编辑比特区以及所述帧本体域的长度差值三个示例，用于实现对所述数据报文的加载。加载数据报文的组播数据帧有多个，均以顺序码予以排序，依据协议上的相逆原理，本步骤可对其所接收的所有组播数据帧进行解码，获得相应的顺序码和内容码，按照顺序码所表征的顺序，将对应的内容码进行串接组装。

[0208] 步骤 S213、将按序组装后的内容码转换为所述的数据报文。

[0209] 按序组装后的编码序列，进一步依据协议上的相逆原理，被转换为本发明自定义协议层所能识别的数据报文，以便进行后续的处理。为确保所述数据报文的完整度，在获得所述的数据报文之后，应利用其前端（具体视数据报文结构而定）的校验码对该数据报文的长度进行校验。对于不相符的数据报文，应予丢弃，仅接收检验成功的数据报文。

[0210] 步骤 S22、利用该数据报文所含二次密钥解密所含二次密文以获得一次密文。

[0211] 根据本发明前述揭示的一个实例，接收端所获得的数据报文中，包含了所述的二次密钥，以及适于以该二次密钥解密的二次密文。由此，从该数据报文中读取其所表达的二次密钥，运用相关算法对该二次密文进行解密，即可获得被传输的配置信息的一次密文。需要理解的是，由于所述的二次密钥接受对称加密技术的规范，因此，不必在本地预存该二次密钥。

[0212] 根据前一方法的揭示，所述二次密钥既可以单纯为随机数，也可以是由格式化标识构成的格式化标识串，即特定标识集，无论二次密钥具有几重意义，在本实例中，只要二次密钥在前用于加密配置信息而使自身具备了解密功能，便必须在本步骤中先行利用二次密钥对二次密文进行解密。如果某些实例中，格式化配置信息未经一次加密，只是经过二次密钥进行简单加密，则经这一解密后便能获得格式化的配置信息，可在此基础上直接解析格式化配置信息。否则，经二次密钥解密后获得的如果是一次密文，则还需要再次进行解密，最后在两次解密的基础上获得格式化配置信息才能加以解析。当然，如果某些实施例中，并未将特定标识集（二次密钥）用于加密配置信息，便无需在此处解密。

[0213] 步骤S23、利用预存的一次密钥解密所述一次密文以获取其中的配置信息。

[0214] 如前所揭示的一个实例中，所述的一次密文，是利用一次密钥（公钥）对格式化的配置信息加密形成的，该一次密钥为非对称加密技术所规范的公钥，因而，作为接收端的智能终端预存有相应的私钥，本步骤中，智能终端调用预存的私钥，也即本方法所称的一次密钥（私钥）对所述的一次密文进行解密。可以看出，本方法所称的一次密钥（私钥）与前一方法所称的一次密钥（公钥）两者是受非对称加密技术所规范，在算法上是相关的，前者为解密密钥，后者为加密密钥，并非具有相同内容的同一密钥，本领域技术人员应当知晓。

[0215] 诚然，如果在发送端采用对称加密技术所规范的一次密钥对格式化的配置信息进行了加密，则智能终端作为接收端便应当预存内容上相同的所述一次密钥，该一次密钥既为发送端的加密密钥，也为接收端的解密密钥。

[0216] 解密所述的一次密文之后，获得相应的格式化的配置信息。然而，依据前述揭示的多种变化实例，无论如何从数据报文中获得所述的格式化的配置信息，作为特定格式的文本形式，这一格式化文本尚未被识别和利用，因而尚未能获得具有识别意义的规范的配置信息。依据协议上的相逆原理，对应于部分实例，应利用所述二次密钥所包含的特定标识将该文本解析为具有识别意义的所述配置信息。对应前述揭示的各个实例，有如下几种对应方式用于处理所述的格式化的配置信息：

[0217] 一、发送端与接收端已协议解析该格式化的配置信息的情况。

[0218] 这种情况下，接收端仅需依照预先的协议而解析所述格式化的配置信息，获得其中各个信息内容即可。

[0219] 二、发送端利用格式化过程中所用的格式化标识形成特定标识集用做二次密钥的情况。

[0220] 这种情况，包括前述揭示的两种细分情况，其中一种是二次密钥即为整个特定标识集，包括特定标识集采用格式化标识用于指示信息内容位置的方式和用于指示分隔字符的方式，另一种是特定标识集只是二次密钥的特定部分。

[0221] 无论何种情况，均不脱离协议上的相逆原理。因而，这类情况下应侧重从所述的二次密钥中获得所述的特定标识集，对应如前各例所揭示的各个具体情况，识别出格式化配

置信息的信息内容。

[0222] 某些实例中，特定标识集中的格式化标识用于指示各个信息内容所处的位置，或者用于指示各个信息内容的分隔符，包括前述的第一格式化标识和第二格式化标识在内，无论如何，均可利用所述的格式化标识的指示，分隔并提取所述格式化配置信息，以获得规范的配置信息，也即具有识别意义的各个信息内容。

[0223] 依据本步骤的处理，最终可以获得规范的配置信息，也即识别到获得发送端传输的信息的原始意义，例如，对于前述的配置信息而言，接收端可以知晓即将要接入的目标网络的服务集标识 SSID 为 MYWiFi，而其对应的登录密码 PSW 则为 PLZLOGIN。

[0224] 需要指出的是，一种仅使所述的特定标识集仅具有解析功能，而不利用其密钥功能的对应实施例中，则不必经过前述的各个解密步骤，而将两个解密步骤替换为一统合步骤，直接在此处利用特定标识集对数据报文所含的格式化的配置信息按照上述原理进行解析即可。这种情况下，尽管格式化的配置信息未经过特殊的一次或两次加密，但由于本发明的特定标识集体现出一定的自协议功能，也即利用其格式化标识的分隔作用而用于识别配置信息所含的各个具体信息内容的功能，因而，这种情况也起到了一定的加密效果。

[0225] 步骤 S24、以该配置信息配置自身网络设置，接入所述目标网络。

[0226] 获得所述配置信息之后，便获得移动终端提供的服务集标识 (SSID) 和相应的密码，智能终端便可以进行自身的网络设置，确定相应的 SSID 为 MYWiFi，并且设置其密码为相应的 PLZLOGIN，启动接入目标网络的过程，进行一系列的握手操作，直至建立与该 SSID 所代表的 WiFi AP 的连接。

[0227] 智能终端连接该 AP 后，便接入了目标网络，理论上可与云端服务器通信，也可通过当前局域网提供的路由功能与网内的所述移动终端进行通信。从而，智能终端可以向该移动终端发送一个表征已经完成网络接入的信号，以便移动终端可以进一步提供操作控制界面给用户做后续操作。

[0228] 可见，本发明的联网接入方法，基于更为安全的加密技术，能够更安全地接收配置信息，避免接收不法用户模拟的配置信息获得更为安全的使用效果。

[0229] 进一步，基于模块化思维，本发明提供一种前述的移动终端和智能终端，较佳的，该移动终端安装了前述相应的 APP 的手机来实现，移动终端与智能终端之间利用计算机程序实现了本发明的技术方案所体现的协议。

[0230] 请参阅图 8，本发明的移动终端的典型实施例中，该智能终端包括获取单元 11、构造单元 12 以及传输单元 13。各单元所执行的功能详细揭示如下：

[0231] 所述的获取单元 11，用于获取待传输信息。

[0232] 考虑到本发明主要利用组播或广播技术来实现数据传输，因而所述的待传输信息，尤其适合指数据量不大的信息内容，例如用于接入目标网络的配置信息，通常只包括目标网络的服务集标识和密码，信息量便较小；又如仅仅包含一条用于被接收端执行的指令语句；再如仅仅包含一条推送给接收端的通知信息。诸如此类，均能最大化程度地发挥本发明的优点。至于信息量大小的量化指标，由于每个数据帧所能表达的数据容量有限，可由本领域技术人员根据实际情况确定。

[0233] 需要指出的是，本发明的各个实施例中，出于说明的简便考虑，常以该传输信息的一个实例即所述的配置信息来指称该待传输信息，但不应理解为是对“待传输信息”这一概

念及其变换了说法而又依然指代相同对象的诸如“被传输信息”、“所接收信息”等概念的限制。同理，后续涉及对待传输信息被格式化、加密等操作而引起的不同格式化内容，尽管其表达形式产生变化，但其指向的对象依然是“待传输信息”这一概念所指向的信息。

[0234] 以基于本发明实现的APP为例，当该APP得以运行时，便可通过系统驱动对手机上的硬件设备进行利用。众所周知的，手机上不仅具有WiFi模组、显示器、控制芯片，还具有麦克风、扬声器等部件，这些部件均可通过该APP实现调用。

[0235] 以Android系统为例，手机终端通过其获取单元11首先调用并显示一个活动组件(Activity)，或者显示一个利用HTML5实现的页面，在屏幕上显示该用户界面及扫描到的WiFi接入点信息（以服务集标识SSID罗列），请求用户选定目标网络，并要求用户输入相应的密码，从而获取目标网络的SSID和密码。

[0236] 根据WiFi协议的约定，本领域技术人员可以知晓，配置信息通常包括WiFi无线路由器（代表目标网络）所提供的用于确定该目标网络的服务集标识(SSID)与用于登录该目标网络的登录密码，在某些情况下可能还需要包括登录密码的加密方式，而对于开放网络也可不必提供登录密码。尽管WiFi协议存在版本更替的事实，但这些涉及为实现接入网络而必备的配置信息可由本领域技术人员依据协议文件对应确定，因此，对其详情及其等同变化方案恕不加以赘述。

[0237] 作为细节变通，当用户选定了SSID之后，可以向云端服务器查询该SSID所对应的密码，如果密码存在，则直接通过云端下载密码，可省去要求用户输入目标网络密码的过程。

[0238] 所述的构造单元12，用于构造数据报文，使该数据报文包含二次密文及二次密钥，所述二次密文由一次密钥加密所述待传输信息，形成一次密文，再经包含随机因子的所述二次密钥加密形成。

[0239] 获得所述的配置信息之类的待传输信息之后，便需要为其构造数据报文。构造数据报文的过程，起到了沟通应用层与数据链路层的作用，具体而言，从应用层获取所述配置信息之类的待传输信息，而后续将在数据链路层发送该数据报文，故而，构造单元12构造数据报文的过程，实质上相当于一个由本发明定义的协议层。因而，构造单元12的实现是非常灵活的，以下以若干示例加以说明：

[0240] 如图9所示的一种用于构造所述数据报文的构造单元12的示例中，该构造单元12包括一次加密模块121、二次加密模块122以及结构组装模块123，各模块的功能说明如下：

[0241] 所述的一次加密模块121，利用所述一次密钥加密待传输信息获得一次密文。

[0242] 所述的一次密钥，是指目前广为采用的用于对被传输信息进行一次加密的密钥，一般采用公钥加密方式，即非对称加密方式。公钥加密方式中，移动终端作为发送端将待传输信息的原始文本以其持有的公钥进行加密，传输到对端时，作为接收端的智能终端调用预存的私钥，对待传输信息进行解密，从而获得其原始版本。所述的公钥与私钥，在算法上相关，因而可以用于相互解密对方加密的数据。本实施例中，所述一次加密模块121同理沿用传统技术，利用所述的一次密钥对原始格式的配置信息进行加密，从而获得一次密文。非对称加密技术体现了较高的安全性，常被用于安全性要求较高的场景中。

[0243] 变通的实施方式中，所述的一次密钥可以利用私钥加密，即对称加密技术实现。这

一技术中，移动终端与智能终端分别存有相同的所述一次密钥，移动终端利用一次密钥加密待传输信息，获得一次密文，传输到智能终端，智能终端便可以利用预存的一次密钥将待传输信息解密。对称加密具有算法简单效率更高的特点，因而在某些安全性要求不太高的场景中可被优先选用。

[0244] 所述的二次加密模块 122，被配置为利用包含随机因子的二次密钥将一次密文加密为二次密文。

[0245] 本实施例中，一次密文形成之后，或者某些不依赖于一次加密的实施例中的所述待传输信息，在二次加密模块 122 中被利用二次密钥进行二次加密形成二次密文。需要指出的是，所述的二次密钥尤其适用于采用对称加密技术所规范的私钥，由此，当智能终端接收到相应的报文后，可以以较低的计算消耗对二次密文进行解密。

[0246] 所述的二次密钥，包括有随机因子，所述的随机因子至少包括在二次密钥中采用随机数以及利用随机的方式选定一个二次密钥两种情况。借助该随机因子的作用，使二次密钥在每次被用于二次加密之前均具有不确定性，也就是即将对一次密文进行二次加密时，才予以确定。由此，二次密钥对每一待传输信息进行二次加密时，均能最大程度地体现出其唯一性。

[0247] 所述的二次密钥的具体实现可以体现为如下几种随意选择的方式：

[0248] 一、采用随机数作为所述的二次密钥。

[0249] 这种方式中，二次加密模块 122 直接调用随机函数，产生一个特定位数如 16 位的随机数，将该随机数确定为所述的二次密钥。这种方式最易实现，更为高效，便于智能终端快速解密。

[0250] 二、随机地从预存的多个密钥中确定所述的二次密钥。

[0251] 这种方式同理可以通过二次加密模块 122 调用随机函数，来确定一个预存的二次密钥，使其内容体现出不确定性。由此而确定的二次密钥，也具有随机性的特点，同理可以起到对截获者制造破译障碍的效果。

[0252] 三、以用于解析未被一次加密前的所述待传输信息的格式化标识的有序集合作为所述的二次密钥。

[0253] 待传输信息，通常包括多个信息元，如前所述的配置信息，在一个应用场景中，可以是包含用于提供 WiFi 接入点的服务集标识 (SSID) 及其密码 (PSW) 的信息。每个信息元中，一般以某种形式予以表征其信息类型及相应的信息内容。当其需要传输时，通常以将这些信息元串接的形式表达成一个字符串，完成对待传输信息的格式化，获得格式化的配置信息。

[0254] 具体而言，以配置信息为例，服务集标识与密码均构成信息元，信息元之间用元素第一格式化标识“|”加以分隔，信息元的信息类型与信息内容之间用第二格式化标识“:”分隔。例如服务集标识是以 SSID 表示其信息类型，密码用 PSW 表示其信息类型，SSID 的信息内容为 MYWiFi，密码的信息内容为 PLZLOGIN，未被一次加密前，对其进行格式化形成的格式化的配置信息的文本形式为：

[0255] SSID:MYWiFi|PSW:PLZLOGIN

[0256] 注意，上述表达的格式化的配置信息中，是按照一定的顺序来组织的，其中 SSID 在前，PSW 在后，这两个信息类型标识符可以供识别相应的信息内容之用，而所述的格式化

标识“:|:”则体现出其特质，如果发送端与接收端之间约定从二次密钥的第一字节处获得第一格式化标识，从第二字节处获得第二格式化标识，则发送端无论采用何种符号用于表达所述的格式化标识，对于接收端而言，均可通过从二次密钥的第一字节与第二字节获取具有约定功能的格式化标识，并以其中第一字节的符号分隔各个信息元，而用第二字节的符号分隔信息类型及其信息内容，从而正确解析格式化配置信息，还原出各个信息元的信息内容。因此，这一实例无疑体现出了数据报文具有自带解析方案的功能，使所述的二次密钥不仅适于解密二次密文，而且适于解析未被加密之前的格式化的配置信息，增加了数据报文的复杂度，使截获者更难以破解。

[0257] 显然，作为特定标识，所述的格式化标识适宜按照其在格式化的配置信息中出现的顺序，被同理按序排列在所述的二次密钥中，所述的格式化标识可以随机确定。当需要使用的格式化标识的个数越多，排列越多样化，其能表达的解析功能越强大，密钥的复杂度也将进一步提高，从而使二次密文更难以破译。这种情况下，二次密钥实质上是一个由多个格式化标识构成的特定标识集，该特定标识集内的特定标识串，可以用于解析格式化的配置信息，而作为一个整体，还可用于解密该配置信息的二次密文从而获得一次密文。

[0258] 进一步的一个改进中，所述的配置信息被按照如下方式表达以增加其可读难度：0MYWiFiPLZLOGIN8。可以看出，这种表达方式中，不同信息元未被以任何符号分隔，然而却仍然可以借助格式化标识来加以解析。

[0259] 具体而言，是将信息元的分隔位置表征成格式化标识，使该格式化标识用于指示不同信息元在格式化配置信息中的位置信息。例如，首字符“0”与末字符“8”实际上是非必须的干扰因子，干扰因子的添加，使得破译者即使获得所述格式化的配置信息，也仍然难以直观判断其真实内容。而在二次密钥中，形成的内容为“020815”，其中，“02”用于表征第一个信息元 SSID 的起始位置为顺序第 2 位，“08”用于表征第二个信息元 SSID 的起始位置为第 8 位，而最后两个“15”用于表征整个配置信息的终止位置。根据与上例等效的原理，接收端从二次密钥中读取“020815”这一特定标识串之后，便可通过确定各个信息元的起始位置，从而获取不同的信息元内容。如果传输双方已约定不同顺序的信息元的信息类型，则接收端即可据此理解发送端在格式化配置信息中表达的信息元的确切内容。通过观察这一改进的实例同样可以知晓，由于同一配置信息的各个信息元的信息内容通常长度不一（例如改变了配置信息中的密码），也可能产生变化，导致不同配置信息中各个信息元出现的位置不同，因而，对应形成的特定标识串的内容也并非每次都相同，起到随机因子的作用，因此也使二次密钥体现出了本发明所需的随机特性。

[0260] 可见，二次密钥所包括的所述的特定标识，也即所述的各种格式化标识，可以用于将格式化的配置信息文本还原为原始的具备了识别意义的配置信息，使其各个信息元的信息内容能被顺利识别和利用。

[0261] 按照此处的描述，待传输信息是先以其格式化文本被加密成一次密文之后，再被所述特定标识集加密形成二次密文表述于所述数据报文中的。需要指出的是，考虑到二次密钥具备解析和加密的双重功能的情况下，在一个改进的用于突出特定标识集的解析功能的实例中，也可去除所述一次加密的过程，这种情况下，被表述于数据报文中的配置信息，便可以是由其未加密状态下的格式化文本，以所述的特定标识集对其进行加密形成的密文。

[0262] 进一步用于强化特定标识集的自解析功能的改进实施例中，进一步忽略加密考虑，不对所述格式化文本进行任何加密，而仅仅将特定标识集的格式化标识串提供到数据报文中，以便接收端利用其中的格式化标识解析包含在所述数据报文中的明文的所述格式化文本。

[0263] 四、在第三种所揭示的两种案例及以此展开的其它变例的基础上，进一步添加随机数构造所述的二次密钥。

[0264] 适应前一种在格式化配置信息中携带自解析方案的多个示例，当然也可以结合所述第一种示例的方式，为前一种示例所述的二次密钥添加一个随机数来加强其安全性。

[0265] 综合上述提供的几种确定包含随机因子的所述二次密钥的示例，程序员可以依照确定的协议在编程时选定任意一种示例方式实现之，进一步便可通过二次加密模块 122 调用对称加密算法对所述的一次密文进行加密，从而形成所述的二次密文。

[0266] 所述的结构组装模块 123，用于组装所述二次密钥与所述的二次密文构成所述数据报文。

[0267] 当所述的二次密文与二次密钥的明文格式得以确定，便可按照发送端与接收端之间的协议，如图 5 所示，将二次密钥前置于所述的二次密文，组装成数据报文。出于校验的考虑，进一步还将数据报文的整体长度用作校验码，表达于该数据报文的前端，使接收端能够利用该校验码判定所接收的数据报文是否完整。显然，关于数据报文的结构，也即各个部分的排列是比较灵活的，附图的示例给出的只是较佳的实施方式，使所述的检验码及相继的二次密钥尤其是其特定标识集构成其首部，末尾为其内容部分。本领域技术人员可以参照这一结构灵活调整该数据报文的结构，对数据报文进行组装，而不应受这一结构的影响而限缩对本发明的理解。

[0268] 构造单元 12 构造了本发明的数据报文之后，便完成了发送端与接收端在自定义协议层的工作，依照 IEEE 802.11 协议的规范，调用传输单元 13 在数据链路层对数据报文进行处理。

[0269] 所述的传输单元 13，用于发送所述数据报文。

[0270] 所述的传输单元 13，需要进一步将所述的数据报文处理成帧数据。本发明以组播数据帧为例进行说明，现介绍几种利用组播数据帧传输所述的数据报文的示例：

[0271] 一、仅以组播数据帧的目的地址域用于加载所述的数据报文的内容。

[0272] 具体而言，单独对组播数据帧目的地址域的可编辑比特区低 23 位加以利用，利用其中的前 6 位用于表达每个组播数据帧的顺序码，利用余下的 17 位表达要加载的有序分段的内容码，因此共可以通过 $2^6 = 64$ 个组播数据帧来传送一个数据报文。其中顺序码为“000000”的组播数据帧可以用作参考，以利于接收端据此开始接收同源的后续帧，也可不必设置这一参考。以这种方式将所述的数据报文加载到 64 个组播数据帧中，传送给接收端，接收端便可依据相逆原理，按照每个组播数据帧的顺序码所指示的顺序，将各个组播数据帧的内容码按序组装，获得所述的数据报文。

[0273] 二、仅以组播数据帧的帧本体域用于加载所述的数据报文的内容。

[0274] 发送端对组播数据帧的帧本体域的控制，主要体现在对其帧长度的可控利用，但帧长度的利用需要依赖于比较基准，因而，同理可采用上述的参考帧的方式，使该参考帧具有最短的帧长度（唯一性关联于其帧本体域长度），而控制其余各组播数据帧的帧本体域

的长度，使不同组播数据帧与所述参考帧的帧长度之间体现出差值，使该差值的二进制格式比特串用于表达例如 10 位比特内容，其中例如前 4 位用于表达所述顺序码，后 6 位用于表达所述内容码，同理可通过 $2^4=16$ 个组播数据帧来加载所述的数据报文。

[0275] 三、同时使用组播数据帧的目的地址域及帧本体域用于加载数据报文。

[0276] 对本实例的理解，请先参照前两例。本实例中，假设按照前述第一实例确定目的地址域低 23 位中的前 6 位用于表达顺序码，余 17 位用于表达内容码，进一步再结合第二实例的原理对帧本体域所决定的帧长度进行利用，使组播数据帧与一个参考帧之间的帧长度的差值的二进制格式比特串为 3 位，则内容码实质上由 17 位加上 3 位共 20 位构成，可以看出，其信息表达能力得以扩展，大大增强。

[0277] 可以看出，无论采用何种方式对组播数据帧加以利用，利用有序表征的多个组播数据帧实现对所述数据报文的加载，从而将所述的待传输信息在数据链路层完成格式化，均可满足 IEEE 802.11 协议的规范。

[0278] 传输单元 13 完成所述在数据链路层的处理工作后，便可以组播数据帧的方式将所述包含待传输信息的数据报文传送给接收端。

[0279] 本发明的移动终端在传输信息的过程中，即使所有组播数据帧均被截获，从而使截获者获得所述的数据报文，由于移动终端起到的安全强化作用，截获者依然难以破译本发明的被传输的信息。

[0280] 请参阅图 10，本发明进一步提供的一种智能终端，可以对移动终端传输的信息进行利用，其包括接收单元 21、第二解密单元 22、第一解密单元 23 以及接入单元 24，各单元的功能揭示如下：

[0281] 所述的接收单元 21，用于接收数据报文。

[0282] 接收单元 21 需要负责完成数据链路层的帧接收以便获得相应的数据报文。接收数据报文的过程与前述发送数据报文的过程具有协议上的相逆关系，可以参考 IEEE 802.11 的规范。以前述采用组播数据帧的实例为基础，利用该接收单元 21 的构造模块实现接收功能，请参阅图 11，接收单元 21 具体包括帧接收模块 211、帧组装模块 212 以及转换模块 213，各模块实现的功能如下：

[0283] 所述的帧接收模块 211，用于接收具有相同源地址的组播数据帧。

[0284] 帧接收模块 211 通过 WiFi 模组接收具有相同源地址的组播数据帧的技术，为本领域技术人员所知晓，需要指出的是，这里所称的相同源地址，是指所述发送端的源地址，以此识别智能终端所需的配置信息的发送方。

[0285] 所述的帧组装模块 212，用于按照各组播数据帧提供的顺序码所表征的索引顺序组装各组播数据帧携带的内容码。

[0286] 如前揭示了单独利用组播数据帧的目的地址域的可编辑比特区、单独利用帧本体域长度差值、共同利用所述目的地址域的可编辑比特区以及所述帧本体域的长度差值三个示例，用于实现对所述数据报文的加载。加载数据报文的组播数据帧有多个，均以顺序码予以排序，依据协议上的相逆原理，帧组装模块 212 可对其所接收的所有组播数据帧进行解码，获得相应的顺序码和内容码，按照顺序码所表征的顺序，将对应的内容码进行串接组装。

[0287] 所述的转换模块 213，用于将按序组装后的内容码转换为所述的数据报文。

[0288] 按序组装后的编码序列，进一步依据协议上的相逆原理，被转换为本发明自定义协议层所能识别的数据报文，以便进行后续的处理。为确保所述数据报文的完整度，在获得所述的数据报文之后，应利用其前端（具体视数据报文结构而定）的校验码对该数据报文的长度进行校验。对于不相符的数据报文，应予丢弃，仅接收检验成功的数据报文。

[0289] 所述的第二解密单元 22，其利用该数据报文所含二次密钥解密所含二次密文以获得一次密文。

[0290] 根据本发明前述揭示的一个实例，接收端所获得的数据报文中，包含了所述的二次密钥，以及适于以该二次密钥解密的二次密文。由此，第二解密单元 22 从该数据报文中读取其所表达的二次密钥，运用相关算法对该二次密文进行解密，即可获得被传输的配置信息的一次密文。需要理解的是，由于所述的二次密钥接受对称加密技术的规范，因此，不必在本地预存该二次密钥。

[0291] 根据移动终端的揭示，所述二次密钥既可以单纯为随机数，也可以是由格式化标识构成的格式化标识串，即特定标识集，无论二次密钥具有几重意义，在本实例中，只要二次密钥在前用于加密配置信息而使自身具备了解密功能，便必须在第二解密单元 22 先行利用二次密钥对二次密文进行解密。如果某些实例中，格式化配置信息未经一次加密，只是经过二次密钥进行简单加密，则经这一解密后便能获得格式化的配置信息，可在此基础上直接解析格式化配置信息。否则，经二次密钥解密后获得的如果是一次密文，则还需要再次进行解密，最后在两次解密的基础上获得格式化配置信息才能加以解析。当然，如果某些实施例中，并未将特定标识集（二次密钥）用于加密配置信息，便无需在此处解密。

[0292] 所述的第一解密单元 23，其利用预存的一次密钥解密所述一次密文以获取其中的配置信息。

[0293] 如前所揭示的一个实例中，所述的一次密文，是利用一次密钥（公钥）对格式化的配置信息加密形成的，该一次密钥为非对称加密技术所规范的公钥，因而，作为接收端的智能终端预存有相应的私钥，在第一解密单元 23 的作用下，调用预存的私钥，也即本智能终端所称的一次密钥（私钥）对所述的一次密文进行解密。可以看出，本智能终端所称的一次密钥（私钥）与移动终端（公钥）所称的一次密钥两者是受非对称加密技术所规范，在算法上是相关的，前者为解密密钥，后者为加密密钥，并非具有相同内容的同一密钥，本领域技术人员应当知晓。

[0294] 诚然，如果在发送端采用对称加密技术所规范的一次密钥对格式化的配置信息进行了加密，则智能终端作为接收端便应当预存内容上相同的所述一次密钥，该一次密钥既为发送端的加密密钥，也为接收端的解密密钥。

[0295] 第一解密单元 23 解密所述的一次密文之后，获得相应的格式化的配置信息。然而，依据前述揭示的多种变化实例，无论如何从数据报文中获得所述的格式化的配置信息，作为特定格式的文本形式，这一格式化文本尚未被识别和利用，因而尚未能获得具有识别意义的规范的配置信息。依据协议上的相逆原理，对应于部分实例，应利用所述二次密钥所包含的特定标识将该文本解析为具有识别意义的所述配置信息。对应前述揭示的各个实例，有如下几种对应方式用于处理所述的格式化的配置信息：

[0296] 一、发送端与接收端已协议解析该格式化的配置信息的情况。

[0297] 这种情况下，接收端仅需依照预先的协议而解析所述格式化的配置信息，获得其

中各个信息内容即可。

[0298] 二、发送端利用格式化过程中所用的格式化标识形成特定标识集用做二次密钥的情况。

[0299] 这种情况，包括前述揭示的两种细分情况，其中一种是二次密钥即为整个特定标识集，包括特定标识集采用格式化标识用于指示信息内容位置的方式和用于指示分隔字符的方式，另一种是特定标识集只是二次密钥的特定部分。

[0300] 无论何种情况，均不脱离协议上的相逆原理。因而，这类情况下应侧重从所述的二次密钥中获得所述的特定标识集，对应如前各例所揭示的各个具体情况，识别出格式化配置信息的信息内容。

[0301] 某些实例中，特定标识集中的格式化标识用于指示各个信息内容所处的位置，或者用于指示各个信息内容的分隔符，包括前述的第一格式化标识和第二格式化标识在内，无论如何，均可利用所述的格式化标识的指示，分隔并提取所述格式化配置信息，以获得规范的配置信息，也即具有识别意义的各个信息内容。

[0302] 依据本单元的处理，最终可以获得规范的配置信息，也即识别到获得发送端传输的信息的原始意义，例如，对于前述的配置信息而言，接收端可以知晓即将要接入的目标网络的服务集标识 SSID 为 MYWiFi，而其对应的登录密码 PSW 则为 PLZLOGIN。

[0303] 需要指出的是，一种仅使所述的特定标识集仅具有解析功能，而不利用其密钥功能的对应实施例中，则不必经过前述的解密，而将第一解密单元 23 和第二解密单元 22 替换为一解析单元，在此处利用特定标识集对数据报文所含的格式化的配置信息按照上述原理进行解析即可。这种情况下，应当看到，尽管格式化的配置信息未经过特殊的一次或两次加密，但由于本发明的特定标识集体现出一定的自协议功能，也即利用其格式化标识的分隔作用而用于识别配置信息所含的各个具体信息内容的功能，因而，这种情况也起到了一定的加密效果。

[0304] 所述的接入单元 24，用于以该配置信息配置自身网络设置，接入所述目标网络。

[0305] 获得所述配置信息之后，便获得移动终端提供的服务集标识 (SSID) 和相应的密码，智能终端便可以进行自身的网络设置，确定相应的 SSID 为 MYWiFi，并且设置其密码为相应的 PLZLOGIN，启动接入目标网络的过程，进行一系列的握手操作，直至建立与该 SSID 所代表的 WiFi AP 的连接。

[0306] 智能终端连接该 AP 后，便接入了目标网络，理论上可与云端服务器通信，也可通过当前局域网提供的路由功能与网内的所述移动终端进行通信。从而，智能终端可以向该移动终端发送一个表征已经完成网络接入的信号，以便移动终端可以进一步提供操作控制界面给用户做后续操作。

[0307] 可见，本发明的智能终端，基于更为安全的加密技术，能够更安全地接收配置信息，避免接收不法用户模拟的配置信息获得更为安全的使用效果。

[0308] 综上所述，本发明借助密码技术，通过改进数据报文所加载的内容表达，进一步加强了基于 IEEE 802.11 协议实现的快连技术的通信安全效果。

[0309] 以上所述仅是本发明的部分实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

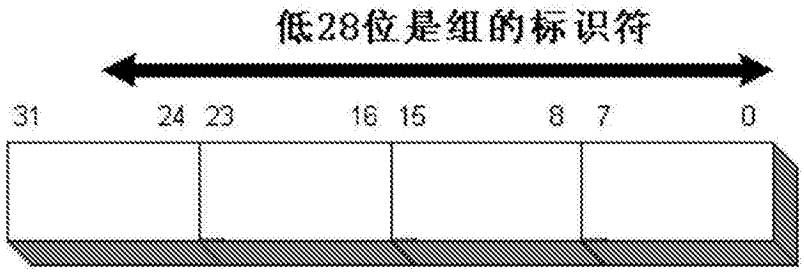

低28位是组的标识符
31
24 23
16 15
8 7
0

图 1

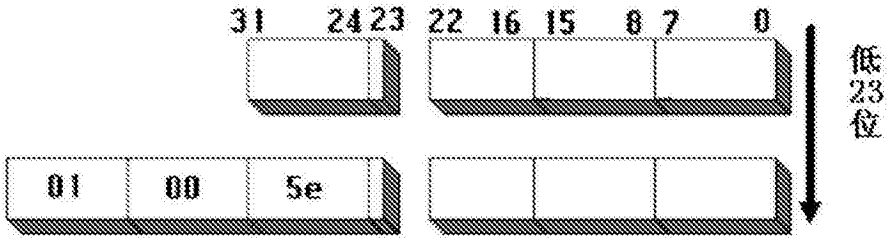

31 24 23 22 16 15 8 7 0
低23位
01
00
5e

图 2

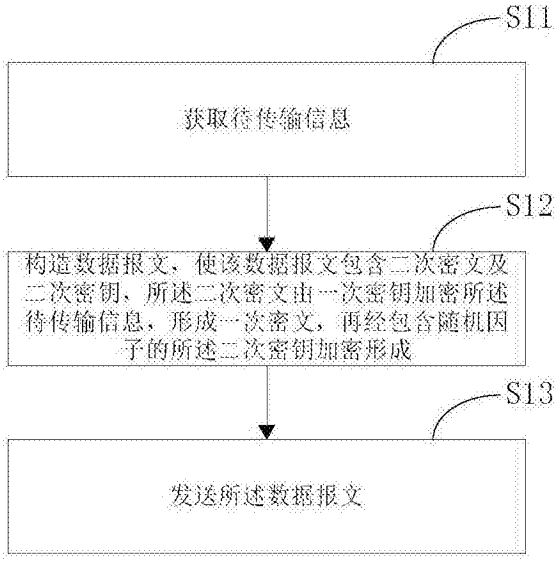

S11
获取待传输信息
S12
构造数据报文，使该数据报文包含二次密文及二次密钥，所述二次密文由一次密钥加密所述待传输信息，形成一次密文，再经包含随机因子的所述二次密钥加密形成
S13
发送所述数据报文

图 3

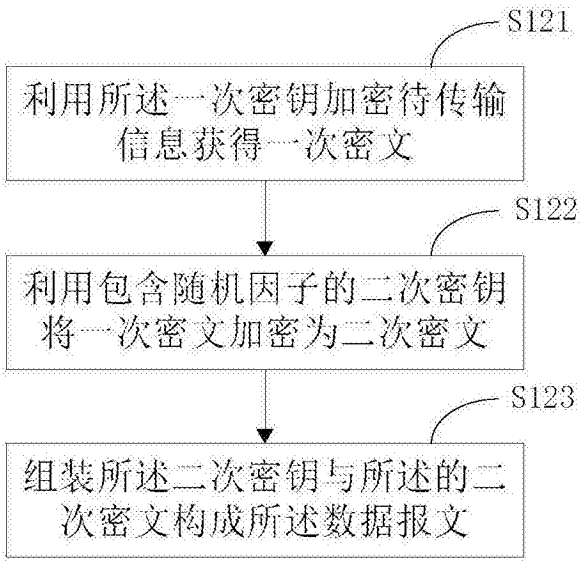

S121
利用所述一次密钥加密待传输信息获得一次密文
S122
利用包含随机因子的二次密钥将一次密文加密为二次密文
S123
组装所述二次密钥与所述的二次密文构成所述数据报文

图 4


长度
二次密钥
二次密文

图 5

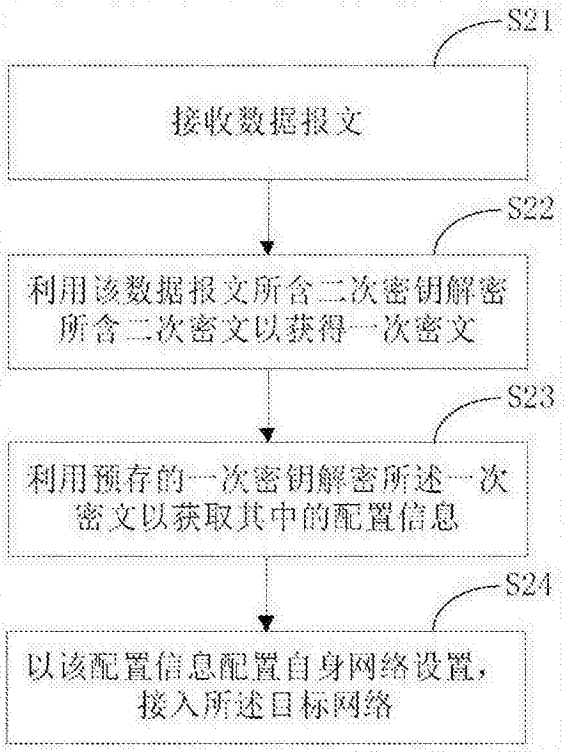

S21
接收数据报文
S22
利用该数据报文所含二次密钥解密所含二次密文以获得一次密文
S23
利用预存的一次密钥解密所述一次密文以获取其中的配置信息
S24
以该配置信息配置自身网络设置，接入所述目标网络

图 6

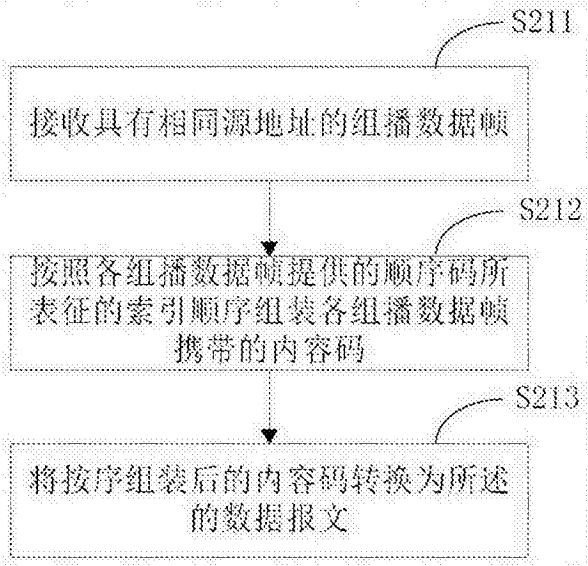

S211
接收具有相同源地址的组播数据帧
S212
按照各组播数据帧提供的顺序码所表征的索引顺序组装各组播数据帧携带的内容码
S213
将按序组装后的内容码转换为所述的数据报文

图 7

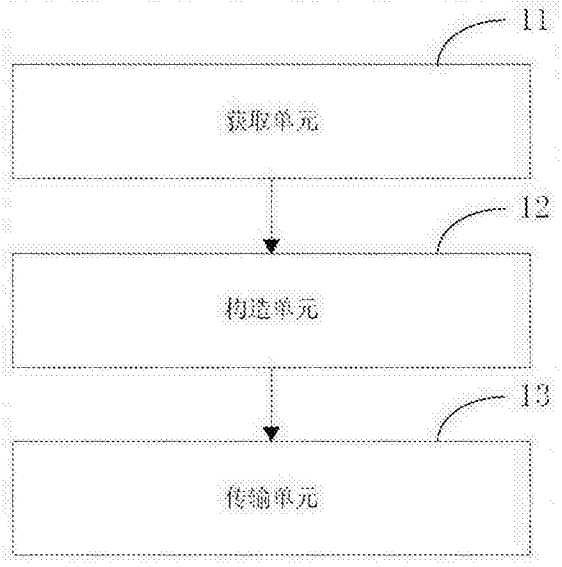

11
获取单元
12
构造单元
13
传输单元

图 8

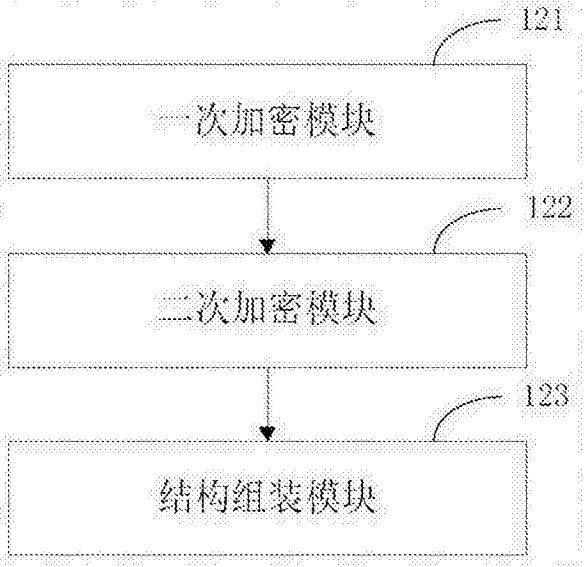

121
一次加密模块
122
二次加密模块
123
结构组装模块

图 9

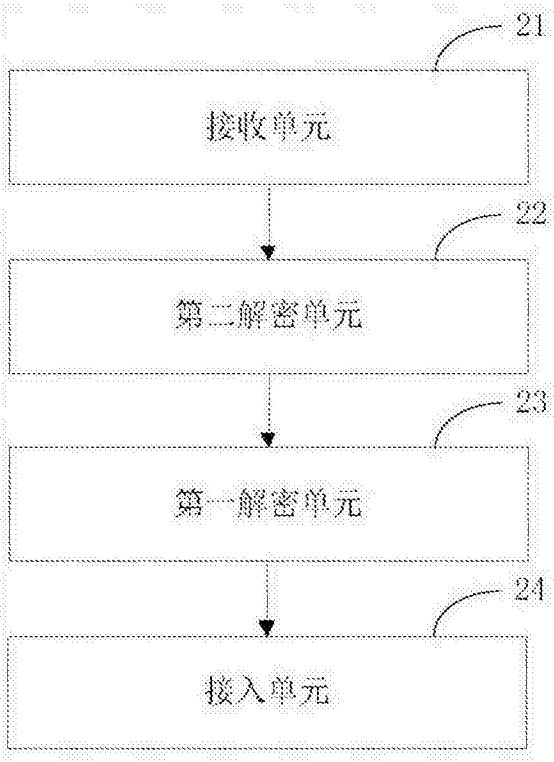

21
接收单元
22
第二解密单元
23
第一解密单元
24
接入单元

图 10

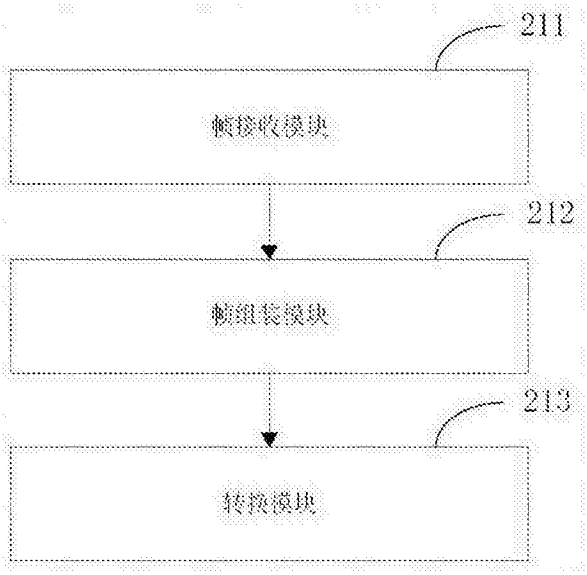

211
帧接收模块
212
帧组装模块
213
转换模块

图 11