(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 112291066 B
(45)授权公告日 2022.02.01

(21)申请号 202011181333.0
(22)申请日 2020.10.29
(65)同一申请的已公布的文献号
申请公布号 CN 112291066 A
(43)申请公布日 2021.01.29
(73)专利权人 中国科学院信息工程研究所
地址 100093 北京市海淀区闵庄路甲89号
(72)发明人 孟丹 孟慧石 贾晓启 黄庆佳 武希耀 孙慧琪 杜海超 王睿怡 谢静
(74)专利代理机构 北京新知远方知识产权代理事务所(普通合伙) 11397
代理人 马军芳 张艳
(51)Int.Cl.
H04L 9/32(2006.01)
H04W 12/069(2021.01)

(56)对比文件
CN 111262693 A,2020.06.09
CN 101594229 A,2009.12.02
CN 1859291 A,2006.11.08
CN 102065423 A,2011.05.18
CN 101304407 A,2008.11.12
US 2017264600 A1,2017.09.14
US 2004193880 A1,2004.09.30
US 10129228 B1,2018.11.13
US 2010169645 A1,2010.07.01

审查员 陈君

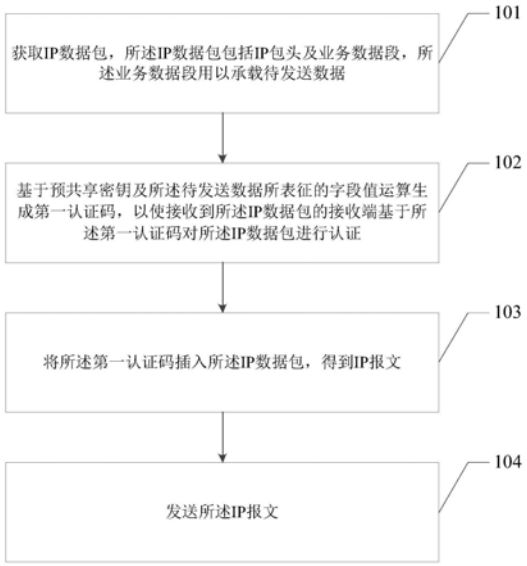
权利要求书2页 说明书10页 附图3页

(54)发明名称

一种数据发送方法、接收方法、终端设备及电子设备

(57)摘要

本申请实施例中提供了一种数据发送方法、接收方法、终端设备及电子设备，在发送数据时，首先封装生成IP数据包，然后基于预共享密钥以及所述IP数据包中的业务数据段运算生成第一认证码，以使接收到所述IP数据包的接收端基于所述第一认证码对所述IP数据包进行认证；再将所述第一认证码插入所述IP数据包，生成并发送IP报文；从而在预设群体用户范围内，通过设置相同的预共享密钥，实现信息安全认证，因此，本申请实施例技术方案具有提高信息传播安全性的技术效果。



CN 112291066 B

1.一种数据发送方法,其特征在于,包括:

获取IP数据包,所述IP数据包包括IP包头及业务数据段,所述业务数据段用以承载待发送数据,其中包括:通用操作模块封装生成所述IP数据包,并将所述IP数据包发送至实时操作模块,所述通用操作模块包括应用处理芯片和通用操作系统的系统处理环境,所述实时操作模块包括基带处理芯片和实时操作系统的系统处理环境;

基于预共享密钥及所述待发送数据所表征的字段值运算生成第一认证码,以使接收到所述IP数据包的接收端基于所述第一认证码对所述IP数据包进行认证,其中包括:所述实时操作模块基于所述预共享密钥以及所述字段值,采用HMAC算法运算生成所述第一认证码;

将所述第一认证码插入所述IP数据包,得到IP报文,其中包括:所述实时操作模块将所述第一认证码插入所述IP数据包,获得IP报文;

发送所述IP报文,其中包括:通过所述实时操作模块发送所述IP报文。

2.根据权利要求1所述的数据发送方法,其特征在于,所述实时操作模块基于所述预共享密钥以及所述字段值,采用HMAC算法运算生成所述第一认证码,包括:

所述实时操作模块从终端设备的SIM卡中获取所述预共享密钥。

3.根据权利要求1所述的数据发送方法,其特征在于,所述实时操作模块将所述第一认证码插入所述IP数据包,获得IP报文,包括:

将所述第一认证码插入所述IP包头。

4.一种数据接收方法,其特征在于,包括:

接收IP报文并发送至实时操作模块;

基于预共享密钥及所述IP报文的业务数据段所表征的字段值运算生成第二认证码,其中包括:实时操作模块基于所述预共享密钥以及所述字段值,采用HMAC算法运算生成所述第二认证码;

提取所述IP报文中的第一认证码,其中包括:实时操作模块提取所述第一认证码,其中,生成所述第一认证码和生成所述第二认证码的算法相同;

将所述第一认证码及所述第二认证码进行匹配处理,获得匹配结果;

在所述匹配结果表征为匹配通过时,解析并转发所述IP报文,其中包括:所述实时操作模块将所述IP报文发送至通用操作模块以进行解析并转发,其中,所述通用操作模块包括应用处理芯片和通用操作系统的系统处理环境,所述实时操作模块包括基带处理芯片和实时操作系统的系统处理环境。

5.根据权利要求4所述的数据接收方法,其特征在于,所述实时操作模块提取所述第一认证码,包括:

所述实时操作模块从所述IP报文的IP包头提取所述第一认证码。

6.根据权利要求4所述的数据接收方法,其特征在于,在所述将所述第一认证码及所述第二认证码进行匹配处理,获得匹配结果之后,所述方法还包括:

在所述匹配结果表征为不匹配时,将所述IP报文丢弃。

7.一种终端设备,其特征在于,包括:

IP包封装模块,用以封装生成IP数据包,并将所述IP数据包发送至实时操作模块;所述IP数据包包括IP包头及业务数据段,所述业务数据段用以承载待发送数据;

IP认证模块，用以基于预共享密钥及所述待发送数据所表征的字段值采用HMAC算法运算生成第一认证码，以使接收到所述IP数据包的接收端基于所述第一认证码对所述IP数据包进行认证；

IP加载模块，用以将所述第一认证码插入所述IP数据包，得到IP报文；

数据发送模块，用以发送所述IP报文；

其中，通用操作模块包括所述IP包封装模块、应用处理芯片和通用操作系统的系统处理环境；实时操作模块包括所述IP认证模块、所述IP加载模块、所述数据发送模块、基带处理芯片和实时操作系统的系统处理环境。

8.根据权利要求7所述的终端设备，其特征在于，所述IP认证模块，用以从所述终端设备的SIM卡中获取所述预共享密钥。

9.根据权利要求7所述的终端设备，其特征在于，所述IP加载模块，用以将所述第一认证码插入所述IP包头。

10.一种终端设备，其特征在于，包括：

数据接收模块，用以接收IP报文并发送至实时操作模块；

IP认证模块，用以基于预共享密钥及所述IP报文的业务数据段所表征的字段值采用HMAC算法运算生成第二认证码；

认证码提取模块，用以提取所述IP报文中的第一认证码；

IP过滤模块，用以将所述第一认证码及所述第二认证码进行匹配处理，获得匹配结果；

第一处理模块，用以在所述匹配结果表征为匹配通过时，将所述IP报文发送至通用操作模块以进行解析并转发；

其中，通用操作模块包括数据接收模块、应用处理芯片和通用操作系统的系统处理环境，实时操作模块包括所述IP认证模块、所述认证码提取模块、所述IP过滤模块、所述第一处理模块、基带处理芯片、以及实时操作系统的系统处理环境；生成所述第一认证码和生成所述第二认证码的算法相同。

11.根据权利要求10所述的终端设备，其特征在于，所述认证码提取模块，用以从所述IP报文的IP包头提取所述第一认证码。

12.根据权利要求10所述的终端设备，其特征在于，所述实时操作模块还包括：

第二处理模块，用以在所述匹配结果表征为不匹配时，将所述IP报文丢弃。

13.一种终端设备，包括存储装置、处理装置及存储在所述存储装置上并可在所述处理装置上运行的计算机程序，其特征在于，所述处理装置执行所述计算机程序时实现如权利要求1-3任一权利要求所述的数据发送方法中的步骤。

14.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求1-3任一权利要求所述的数据发送方法中的步骤。

15.一种电子设备，包括存储装置、处理装置及存储在所述存储装置上并可在所述处理装置上运行的计算机程序，其特征在于，所述处理装置执行所述计算机程序时实现如权利要求4-6任一权利要求所述的数据接收方法中的步骤。

16.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求4-6任一权利要求所述的数据接收方法中的步骤。

一种数据发送方法、接收方法、终端设备及电子设备

技术领域

[0001] 本申请涉及网络安全技术，具体地，涉及一种数据发送方法、接收方法、终端设备及电子设备。

背景技术

[0002] 目前，市场上主流的智能移动终端的功能通常采用AP(应用处理器，Application Processor)和CP(基带处理器，Communication Processor)两种方式来实现。AP运行在通用操作系统中，如Android、IOS等，AP主要用来处理智能终端上各种应用，如游戏、新闻、视频类应用；而CP运行在实时操作系统，以进行快速、低时延的语音、数据的通信处理。AP和通用操作系统算力要强于CP和实时操作系统，同时也具有合理、高效的应用软件框架，因此，目前绝大多数的信息安全解决方案均运行于通用操作系统。然而，装有大量应用程序的通用操作系统的运行环境相对复杂，通用操作系统往往存在较大的安全漏洞风险，采用通用操作系统处理运行信息安全解决方案往往会让传播各类恶意非法信息者有可趁之机，对用户的信息安全造成严重影响。

[0003] 可见，现有技术中存在着不法分子可利用移动终端通用操作系统中的安全漏洞以攻破信息安全屏障，实现网络信息窃取或传播各类恶意非法信息的技术问题。

发明内容

[0004] 本申请实施例中提供了一种数据发送方法、接收方法、终端设备及电子设备。

[0005] 根据本申请实施例的第一个方面，提供了一种数据发送方法，包括：

[0006] 获取IP数据包，所述IP数据包包括IP包头及业务数据段，所述业务数据段用以承载待发送数据；

[0007] 基于预共享密钥及所述待发送数据所表征的字段值运算生成第一认证码，以使接收到所述IP数据包的接收端基于所述第一认证码对所述IP数据包进行认证；

[0008] 将所述第一认证码插入所述IP数据包，得到IP报文；

[0009] 发送所述IP报文。

[0010] 可选地，所述获取IP数据包包括：

[0011] 通用操作模块封装生成所述IP数据包，并将所述IP数据包发送至实时操作模块；

[0012] 所述基于预共享密钥及所述待发送数据所表征的字段值运算生成第一认证码，包括：

[0013] 实时操作模块基于所述预共享密钥以及所述字段值，采用HMAC算法运算生成所述第一认证码；

[0014] 所述将所述第一认证码插入所述IP数据包，得到IP报文，包括：

[0015] 所述实时操作模块将所述第一认证码插入所述IP数据包，获得IP报文；

[0016] 所述发送所述IP报文，包括：

[0017] 通过所述实时操作模块发送所述IP报文。

[0018] 可选地，所述实时操作模块基于所述预共享密钥以及所述字段值，采用HMAC算法运算生成所述第一认证码，包括：

[0019] 所述实时操作模块从所述终端设备的SIM卡中获取所述预共享密钥。

[0020] 可选地，所述实时操作模块将所述第一认证码插入所述IP数据包，获得IP报文，包括：

[0021] 将所述第一认证码插入所述IP包头。

[0022] 根据本申请实施例的第二方面，提供了一种数据接收方法，包括：

[0023] 接收IP报文；

[0024] 基于预共享密钥及所述IP报文的业务数据段所表征的字段值运算生成第二认证码；

[0025] 提取所述IP报文中的第一认证码；

[0026] 将所述第一认证码及所述第二认证码进行匹配处理，获得匹配结果；

[0027] 在所述匹配结果表征为匹配通过时，解析并转发所述IP报文。

[0028] 可选地，所述基于预共享密钥及所述IP报文的业务数据段所表征的字段值运算生成第二认证码，包括：

[0029] 实时操作模块基于所述预共享密钥以及所述字段值，采用HMAC算法运算生成所述第二认证码；

[0030] 所述提取所述IP报文中的第一认证码，包括：

[0031] 实时操作模块提取所述第一认证码；

[0032] 所述在所述匹配结果表征为匹配通过时，解析并转发所述IP报文，包括：

[0033] 将所述IP报文发送至所述通用操作模块以进行解析并转发。

[0034] 可选地，所述实时操作模块提取所述第一认证码，包括：

[0035] 所述实时操作模块从所述IP报文的IP包头提取所述第一认证码。

[0036] 可选地，在所述将所述第一认证码及所述第二认证码进行匹配处理，获得匹配结果之后，所述方法还包括：

[0037] 在所述匹配结果表征为不匹配时，将所述IP报文丢弃。

[0038] 根据本申请实施例的第三个方面，提供了一种终端设备，包括：

[0039] 数据接收模块，用以获取IP数据包，所述IP数据包包括IP包头及业务数据段，所述业务数据段用以承载待发送数据；

[0040] IP认证模块，用以基于预共享密钥及所述待发送数据所表征的字段值运算生成第一认证码，以使接收到所述IP数据包的接收端基于所述第一认证码对所述IP数据包进行认证；

[0041] IP加载模块，用以将所述第一认证码插入所述IP数据包，得到IP报文；

[0042] 数据发送模块，用以发送所述IP报文。

[0043] 可选地，所述通用操作模块包括：

[0044] 应用处理芯片和通用操作系统；

[0045] IP包封装模块，用以封装生成所述IP数据包，并将所述IP数据包发送至所述实时操作模块；

[0046] 所述实时操作模块包括：

[0047] 基带处理芯片和实时操作系统；

[0048] 所述数据接收模块、所述IP认证模块、所述IP加载模块、及所述数据发送模块。

[0049] 可选地，所述IP认证模块，用以从所述终端设备的SIM卡中获取所述预共享密钥。

[0050] 可选地，所述IP加载模块，用以将所述第一认证码插入所述IP包头。

[0051] 根据本申请实施例的第四个方面，提供了一种终端设备，包括：

[0052] 数据接收模块，用以接收IP报文；

[0053] IP认证模块，用以基于预共享密钥及所述IP报文的业务数据段所表征的字段值运算生成第二认证码；

[0054] 认证码提取模块，用以提取所述IP报文中的第一认证码；

[0055] IP过滤模块，用以将所述第一认证码及所述第二认证码进行匹配处理，获得匹配结果；

[0056] 第一处理模块，用以在所述匹配结果表征为匹配通过时，解析并转发所述IP报文。

[0057] 可选地，所述通用操作模块包括：

[0058] 应用处理芯片和通用操作系统；

[0059] 所述实时操作模块包括：

[0060] 基带处理芯片和实时操作系统；

[0061] 所述IP认证模块，用以基于所述预共享密钥以及所述字段值，采用HMAC算法运算生成所述第二认证码；

[0062] 所述第一处理模块，用以将所述IP报文发送至所述通用操作模块以进行解析并转发。

[0063] 可选地，所述认证码提取模块，用以从所述IP报文的IP包头提取所述第一认证码。

[0064] 可选地，所述实时操作模块还包括：

[0065] 第二处理模块，用以在所述匹配结果表征为不匹配时，将所述IP报文丢弃。

[0066] 根据本申请实施例的第五个方面，提供了一种终端设备，包括存储装置、处理装置及存储在所述存储装置上并可在所述处理装置上运行的计算机程序，所述处理装置执行所述计算机程序时实现如第一方面所述的数据发送方法中的步骤。

[0067] 根据本申请实施例的第六个方面，提供了一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现如第一方面所述的数据发送方法中的步骤。

[0068] 根据本申请实施例的第七个方面，提供了一种电子设备，包括存储装置、处理装置及存储在所述存储装置上并可在所述处理装置上运行的计算机程序，所述处理装置执行所述计算机程序时实现如第二方面所述的数据接收方法中的步骤。

[0069] 根据本申请实施例的第八个方面，提供了一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现如第二方面所述的数据接收方法中的步骤。

[0070] 本申请实施例中提供一种数据发送方法、接收方法、终端设备及电子设备，在发送数据时，首先封装生成IP数据包，然后基于预共享密钥以及所述IP数据包中的业务数据段运算生成第一认证码，以使接收到所述IP数据包的接收端基于所述第一认证码对所述IP数据包进行认证；再将所述第一认证码插入所述IP数据包，生成并发送IP报文；从而在预设群

体用户范围内，通过设置相同的预共享密钥，实现信息安全认证，因此，本申请实施例技术方案具有提高信息传播安全性的技术效果。

[0071] 本申请实施例至少还具有如下技术效果或优点：

[0072] 进一步地，本申请实施例中的技术方案还可以将认证码的生成、提取、封装、解析、匹配工作均放置在实时操作模块中处理，实现将非法信息阻挡在通用操作系统之外，阻止非法信息进入用户应用程序，因此还具有进一步提升终端系统安全性的技术效果。

[0073] 进一步地，本申请实施例中的技术方案还可以通过将预共享密钥存储于SIM卡中而实现进一步提升数据信息安全性的技术效果。

附图说明

[0074] 此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

[0075] 图1为本申请实施例提供的一种数据发送方法的流程图；

[0076] 图2为本申请实施例提供的一种数据接收方法的流程图；

[0077] 图3为本申请实施例提供的一种终端设备的结构图；

[0078] 图4为本申请实施例提供的另一种终端设备的结构图。

具体实施方式

[0079] 在实现本申请的过程中，发明人发现现有技术中存在着不法分子可利用移动终端通用操作系统中的安全漏洞以攻破信息安全屏障，实现网络信息窃取或传播各类恶意非法信息的技术问题。

[0080] 针对上述问题，提供了一种数据发送方法、接收方法、终端设备及电子设备，在发送数据时，首先封装生成IP数据包，然后基于预共享密钥以及所述IP数据包中的业务数据段运算生成第一认证码，以使接收到所述IP数据包的接收端基于所述第一认证码对所述IP数据包进行认证；再将所述第一认证码插入所述IP数据包，生成并发送IP报文；从而在预设群体用户范围内，通过设置相同的预共享密钥，实现信息安全认证，因此，本申请实施例技术方案具有提高信息传播安全性的技术效果。

[0081] 为了使本申请实施例中的技术方案及优点更加清楚明白，以下结合附图对本申请的示例性实施例进行进一步详细的说明，显然，所描述的实施例仅是本申请的一部分实施例，而不是所有实施例的穷举。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组合。

[0082] 本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

[0083] 实施例一

[0084] 请参考图1，本申请实施例一提供一种数据发送方法，包括：

[0085] 步骤101：获取IP数据包，所述IP数据包包括IP包头及业务数据段，所述业务数据段用以承载待发送数据。

[0086] 所述IP数据包可以为包括IP包头和业务数据段的IP协议包，所述业务数据段可以

承载所述待发送数据，也就是业务数据，也可以为空载。

[0087] 步骤102：基于预共享密钥及所述待发送数据所表征的字段值运算生成第一认证码，以使接收到所述IP数据包的接收端基于所述第一认证码对所述IP数据包进行认证。

[0088] 所述业务数据段可以是指：承载业务数据(也就是所述待发送数据)的预设数量字段；

[0089] 所述字段值可以是指：由所述业务数据段中的部分或所有字段所表征、映射的参数值。

[0090] 所述预共享密钥可以通过多种方式获取，例如，可以从云端获取、从本地存储器获取、从用户输入的指令参数中获取、从密钥程序计算获取，等等。在获得了预共享密钥后，进一步可基于所述预共享密钥结合所述业务数据段所表征的参数值，采用多种算法运算生成第一认证码。

[0091] 步骤103：将所述第一认证码插入所述IP数据包，得到IP报文。

[0092] 作为一种优选，可将所述第一认证码插入所述IP数据包的包头字段；当然，在一些特殊情况下，也可以将所述第一认证码插入在所述IP数据包的其它预设字段位置，在解析时只需按照既定算法或顺序对应提取出所述第一认证码即可，本领域普通技术人员可根据需要而设置所述第一认证码的插入字段位置。

[0093] 步骤104：发送所述IP报文。

[0094] 进一步地，所述获取IP数据包包括：

[0095] 通用操作模块封装生成所述IP数据包，并将所述IP数据包发送至实时操作模块；

[0096] 所述基于预共享密钥及所述待发送数据所表征的字段值运算生成第一认证码，包括：

[0097] 实时操作模块基于所述预共享密钥以及所述字段值，采用HMAC算法运算生成所述第一认证码；

[0098] 所述将所述第一认证码插入所述IP数据包，得到IP报文，包括：

[0099] 所述实时操作模块将所述第一认证码插入所述IP数据包，获得IP报文；

[0100] 所述发送所述IP报文，包括：

[0101] 通过所述实时操作模块发送所述IP报文。

[0102] 所述通用操作模块可以是指：包括AP应用处理芯片和通用操作系统的系统处理环境，以及通过该系统处理环境实现功能应用或执行各运行指令的软件程序；

[0103] 所述实时操作模块可以是指：包括CP基带处理芯片和实时操作系统的系统处理环境，以及通过该系统处理环境实现功能应用或执行各运行指令的软件程序；

[0104] 需要指出的是，在本申请实施例中，通过所述通用操作模块或通过所述实时操作模块执行的各方法步骤，可以是指：通过对应操作模块中的应用程序或处理芯片所对应执行的功能步骤。

[0105] 也就是说，在本申请实施例技术方案中，封装IP数据包的工作可放置于包括AP应用处理芯片和通用操作系统的处理环境中完成；而运算生成第一认证码、插入第一认证码、生成并发送IP报文的工作可放置于包括CP基带处理芯片和实时操作系统的处理环境中完成；由此可以在数据发送过程中，避免环境复杂的通用操作系统涉及认证码的生成和加载工作，实现提升系统信息安全性的技术效果。

[0106] 由于实时操作系统具有时延低、响应快的特点，因此通过实时操作模块发送报文可以有效提升通信数据发送效率。

[0107] 另一方面，作为一种可选方式，本申请实施例技术方案具体采用HMAC算法计算生成所述第一认证码，所述HMAC算法的公式可表示为如下：

[0108] $$HMAC(K, M)=H((K' \oplus opad) \mid H((K' \oplus ipad) \mid M))$$

[0109] 其中，K为所述预共享密钥，M为所述业务数据段所表征的参数值，通过HMAC运算，可生成固定长度的第一认证码。

[0110] 进一步地，所述实时操作模块基于所述预共享密钥以及所述字段值，采用HMAC算法运算生成所述第一认证码，包括：

[0111] 所述实时操作模块从所述终端设备的SIM卡中获取所述预共享密钥。

[0112] 也就是说，本申请实施例技术方案将所述预共享密钥存储在终端设备的SIM卡中，通过该项设置，即使终端丢失，用户也可以通过向运营商申请挂失而将该SIM卡报废，拒绝终端从SIM卡中读取共享密钥，即可使丢失终端的认证功能失效，使该丢失终端上的应用无法获取相关机密信息。

[0113] 可见，本申请实施例中的技术方案还可以通过将预共享密钥存储于SIM卡中而实现进一步提升数据信息安全性的技术效果。

[0114] 再进一步地，所述实时操作模块将所述第一认证码插入所述IP数据包，获得IP报文，包括：

[0115] 将所述第一认证码插入所述IP包头。

[0116] 也就是说，本申请实施例技术方案中的IP数据包其包头字段可用以承载认证码数据，当然，所述包头字段也可承载其它预设数据，例如IP数据包的校验码，当在IP数据包中插入第一认证码后可同时更新或插入校验码，以实现对IP数据包的版本标识或其它信息标识。进一步地，所述IP数据包的非包头字段的其它预设字段位置可用来承载业务数据，而该非包头字段的预设字段位置也就是所述业务数据段。

[0117] 实施例二

[0118] 请参考图2，本申请实施例二提供一种数据接收方法，包括：

[0119] 步骤201：接收IP报文。

[0120] 步骤202：基于预共享密钥及所述IP报文的业务数据段所表征的字段值运算生成第二认证码。

[0121] 同理，所述预共享密钥可以通过多种方式获取，进一步可基于所述预共享密钥结合所述业务数据段所表征的参数值，采用预定算法运算生成第二认证码。所述预共享密钥以及所述HMAC算法可以为与生成所述第二IP报文时，所采用的预共享密钥和HMAC算法相同。

[0122] 本步骤中的预共享密钥以及所述预定算法可以为与生成所述IP报文时，所采用的预共享密钥和算法相同。

[0123] 步骤203：提取所述IP报文中的第一认证码；

[0124] 在本步骤的执行过程中，可以通过所述终端设备中的微型TCP/IP协议栈解析获得所述IP报文中的第一认证码。也就是说，所述微型TCP/IP协议栈只用以解析IP报文的预定字段范围的信息即可，而无需解析得到IP报文中的业务数据段所承载的业务数据信息。而

在本申请实施例中，该预定字段范围可以为所述IP报文的包头字段。

[0125] 步骤204：将所述第一认证码及所述第二认证码进行匹配处理，获得匹配结果；

[0126] 步骤205：在所述匹配结果表征为匹配通过时，解析并转发所述IP报文。

[0127] 在本步骤中，可以对所述IP报文的业务数据段所承载的业务数据信息进行解析，在解析完成后，可将业务数据信息转发给相应应用程序。

[0128] 进一步地，所述基于预共享密钥及所述IP报文的业务数据段所表征的字段值运算生成第二认证码，包括：

[0129] 实时操作模块基于所述预共享密钥以及所述字段值，采用HMAC算法运算生成所述第二认证码；

[0130] 所述提取所述IP报文中的第一认证码，包括：

[0131] 实时操作模块提取所述第一认证码；

[0132] 所述在所述匹配结果表征为匹配通过时，解析并转发所述IP报文，包括：

[0133] 将所述IP报文发送至所述通用操作模块以进行解析并转发。

[0134] 也就是说，运算生成第二认证码、提取第一认证码、将第一认证码和第二认证码进行匹配处理、基于匹配结果对IP报文进行相应转发或处理的工作可放置于包括CP基带处理芯片和实时操作系统的处理环境中完成；而在认证通过后，可将IP报文的业务数据段解析工作放置于包括AP应用处理芯片和通用操作系统的处理环境中完成，通过框架更合理高效、算力更强大的通用操作模块实现对完整的业务数据信息解析；一方面可在数据接收过程中，避免环境复杂的通用操作系统涉及认证码的计算和认证工作，另一方面也可保证终端设备对业务数据信息的解析处理能力，提升终端设备的系统资源利用效率。

[0135] 进一步地，所述实时操作模块提取所述第一认证码，包括：

[0136] 所述实时操作模块从所述IP报文的IP包头提取所述第一认证码。

[0137] 进一步地，在所述将所述第一认证码及所述第二认证码进行匹配处理，获得匹配结果之后，所述方法还包括：

[0138] 在所述匹配结果表征为不匹配时，将所述IP报文丢弃。

[0139] 将所述IP报文丢弃可以包括将所述IP报文删除或隔离。

[0140] 由此可见，本申请实施例技术方案在发送数据时，首先封装生成IP数据包，然后基于预共享密钥以及所述IP数据包中的业务数据段运算生成第一认证码，再将所述第一认证码插入所述IP数据包，生成并发送IP报文；在接收数据时基于同样的预共享密钥以及接收IP报文中的业务数据段，采用相同的算法运算生成第二认证码；如果第二认证码与接收IP报文中的第一认证码匹配，则将IP报文进行解析并转发；如果不匹配则将接收IP报文丢弃。可见，本申请技术方案可以使预定群体范围内的用户通过设置相同的预共享密钥，而将非法信息阻挡在通用操作系统之外，阻止非法信息进入用户应用程序，因此，本申请实施例技术方案具有提高信息传播安全性的技术效果。

[0141] 实施例三

[0142] 请参考图3，本申请实施例三提供了一种终端设备，包括：

[0143] 数据接收模块301，用以获取IP数据包，所述IP数据包包括IP包头及业务数据段，所述业务数据段用以承载待发送数据；

[0144] IP认证模块302，用以基于预共享密钥及所述待发送数据所表征的字段值运算生

成第一认证码，以使接收到所述IP数据包的接收端基于所述第一认证码对所述IP数据包进行认证；

[0145] IP加载模块303，用以将所述第一认证码插入所述IP数据包，得到IP报文；

[0146] 数据发送模块304，用以发送所述IP报文。

[0147] 可选地，所述通用操作模块包括：

[0148] 应用处理芯片和通用操作系统；

[0149] IP包封装模块，用以封装生成所述IP数据包，并将所述IP数据包发送至所述实时操作模块；

[0150] 所述实时操作模块包括：

[0151] 基带处理芯片和实时操作系统；

[0152] 所述数据接收模块、所述IP认证模块、所述IP加载模块、及所述数据发送模块。

[0153] 可选地，所述IP认证模块，用以从所述终端设备的SIM卡中获取所述预共享密钥。

[0154] 可选地，所述IP加载模块，用以将所述第一认证码插入所述IP包头。

[0155] 前述图1实施例中的数据发送方法中的各种变化方式和具体实例同样适用于本实施例的终端设备，通过前述对数据发送方法的详细描述，本领域技术人员可以清楚的知道本实施例中的终端设备的实施方法，所以为了说明书的简洁，在此不再详述。

[0156] 实施例四

[0157] 请参考图4，本申请实施例四提供了一种终端设备，包括：

[0158] 数据接收模块401，用以接收IP报文；

[0159] IP认证模块402，用以基于预共享密钥及所述IP报文的业务数据段所表征的字段值运算生成第二认证码；

[0160] 认证码提取模块403，用以提取所述IP报文中的第一认证码；

[0161] IP过滤模块404，用以将所述第一认证码及所述第二认证码进行匹配处理，获得匹配结果；

[0162] 第一处理模块405，用以在所述匹配结果表征为匹配通过时，解析并转发所述IP报文。

[0163] 可选地，在所述终端设备包括通用操作模块和实时操作模块时，所述通用操作模块包括：

[0164] 应用处理芯片和通用操作系统；

[0165] 所述实时操作模块包括：

[0166] 基带处理芯片和实时操作系统；

[0167] 所述IP认证模块，用以基于所述预共享密钥以及所述字段值，采用HMAC算法运算生成所述第二认证码；

[0168] 所述第一处理模块，用以将所述IP报文发送至所述通用操作模块以进行解析并转发。

[0169] 可选地，所述认证码提取模块，用以从所述IP报文的IP包头提取所述第一认证码。

[0170] 可选地，所述实时操作模块还包括：

[0171] 第二处理模块，用以在所述匹配结果表征为不匹配时，将所述IP报文丢弃。

[0172] 前述图2实施例中的数据接收方法中的各种变化方式和具体实例同样适用于本实

施例的终端设备，通过前述对数据接收方法的详细描述，本领域技术人员可以清楚的知道本实施例中终端设备的实施方法，所以为了说明书的简洁，在此不再详述。

[0173] 本申请实施例还提供一种终端设备，包括存储装置、处理装置及存储在所述存储装置上并可在所述处理装置上运行的计算机程序，所述处理装置执行所述计算机程序时实现如第一方面所述的数据发送方法中的步骤。

[0174] 本申请实施例还提供一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现如第一方面所述的数据发送方法中的步骤。

[0175] 本申请实施例还提供一种电子设备，包括存储装置、处理装置及存储在所述存储装置上并可在所述处理装置上运行的计算机程序，所述处理装置执行所述计算机程序时实现如第二方面所述的数据接收方法中的步骤。

[0176] 本申请实施例还提供一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现如第二方面所述的数据接收方法中的步骤。

[0177] 由此可见，本申请实施例中提供一种数据发送方法、接收方法、终端设备及电子设备，在发送数据时，首先封装生成IP数据包，然后基于预共享密钥以及所述IP数据包中的业务数据段运算生成第一认证码，以使接收到所述IP数据包的接收端基于所述第一认证码对所述IP数据包进行认证；再将所述第一认证码插入所述IP数据包，生成并发送IP报文；从而在预设群体用户范围内，通过设置相同的预共享密钥，实现信息安全认证，因此，本申请实施例技术方案具有提高信息传播安全性的技术效果。

[0178] 本申请实施例至少还具有如下技术效果或优点：

[0179] 进一步地，本申请实施例中的技术方案还可以将认证码的生成、提取、封装、解析、匹配工作均放置在实时操作模块中处理，实现将非法信息阻挡在通用操作系统之外，阻止非法信息进入用户应用程序，因此还具有进一步提升终端系统安全性的技术效果。

[0180] 进一步地，本申请实施例中的技术方案还可以通过将预共享密钥存储于SIM卡中而实现进一步提升数据信息安全性的技术效果。

[0181] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0182] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0183] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0184] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0185] 尽管已描述了本申请的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请范围的所有变更和修改。

[0186] 显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

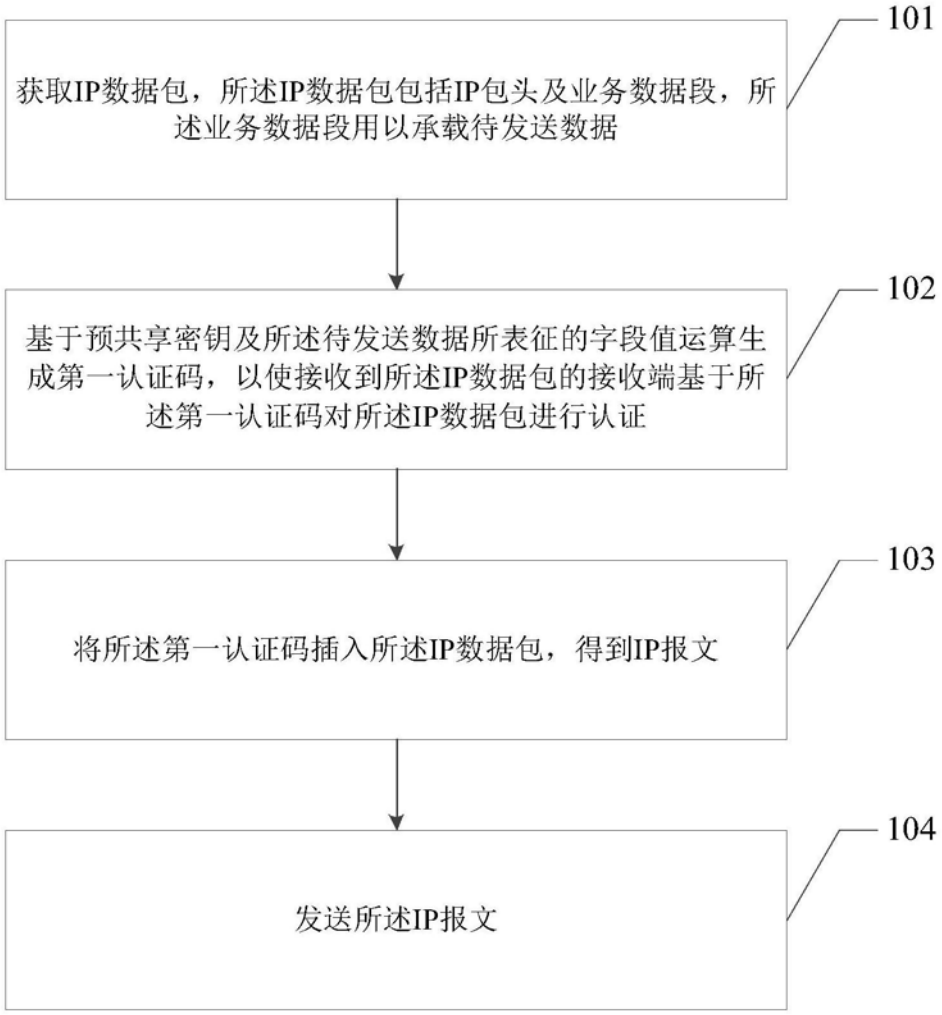

101
获取IP数据包，所述IP数据包包括IP包头及业务数据段，所述业务数据段用以承载待发送数据
102
基于预共享密钥及所述待发送数据所表征的字段值运算生成第一认证码，以使接收到所述IP数据包的接收端基于所述第一认证码对所述IP数据包进行认证
103
将所述第一认证码插入所述IP数据包，得到IP报文
104
发送所述IP报文

图1

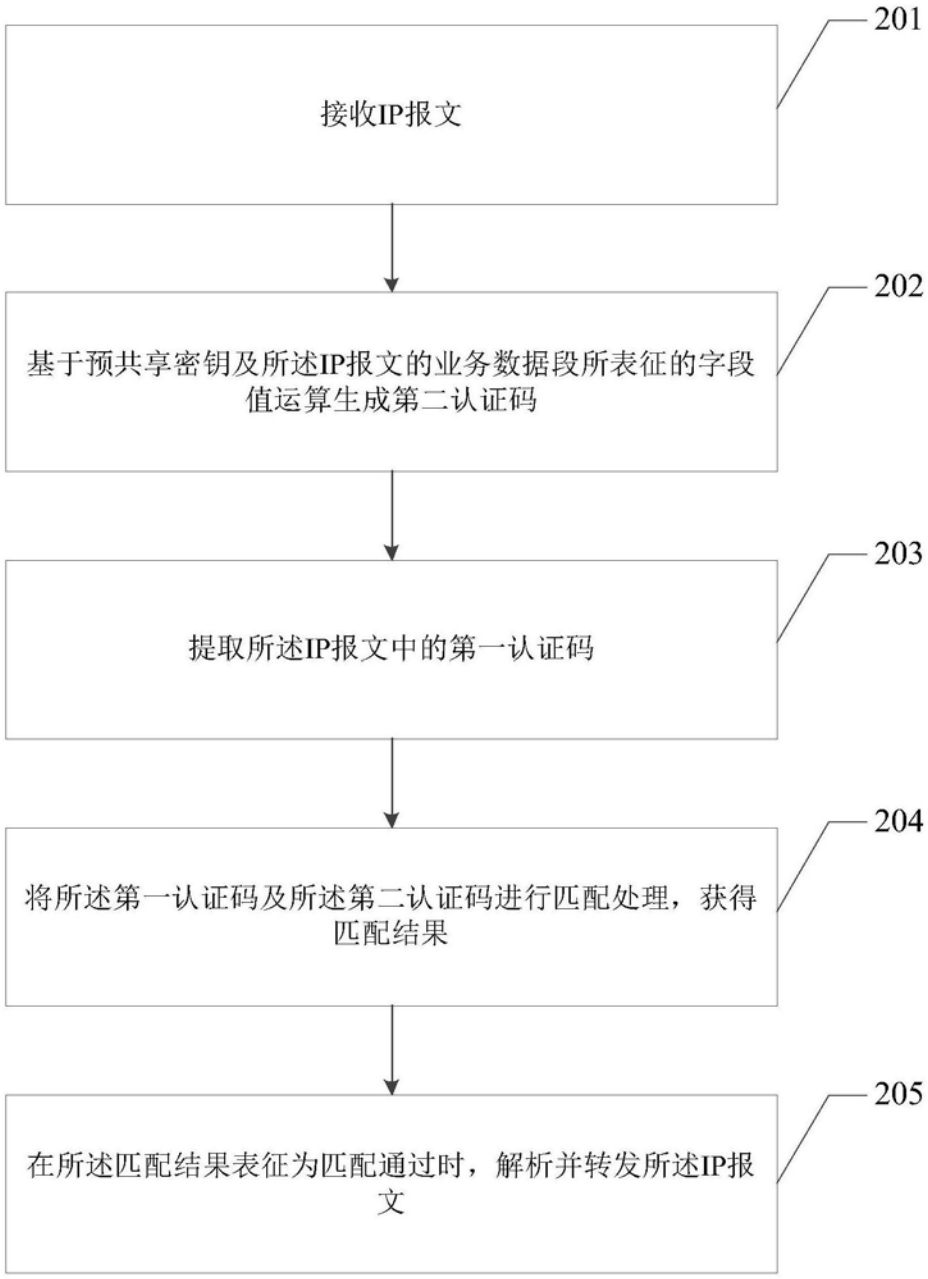

201
接收IP报文
202
基于预共享密钥及所述IP报文的业务数据段所表征的字段值运算生成第二认证码
203
提取所述IP报文中的第一认证码
204
将所述第一认证码及所述第二认证码进行匹配处理，获得匹配结果
205
在所述匹配结果表征为匹配通过时，解析并转发所述IP报文

图2

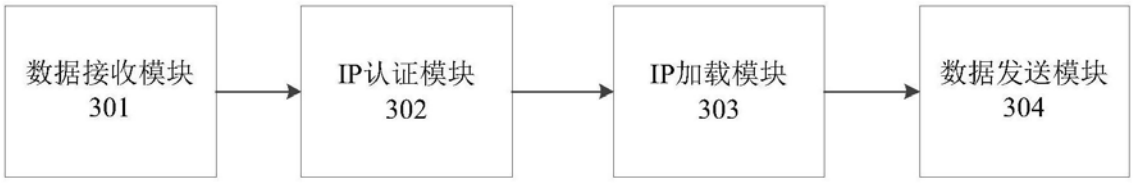

数据接收模块
301
IP认证模块
302
IP加载模块
303
数据发送模块
304

图3

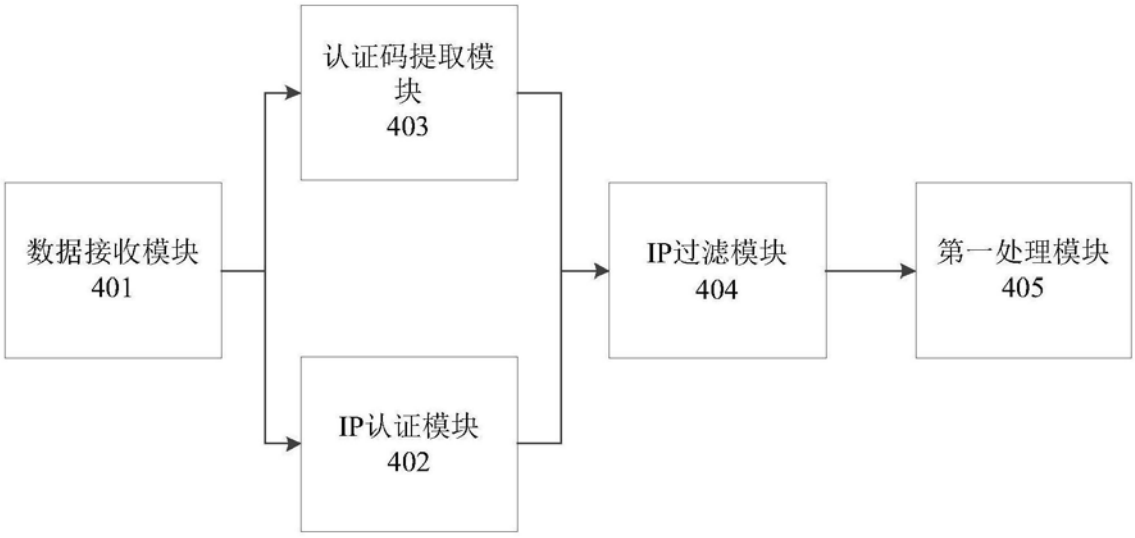


图4