(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
2019 年 1 月 31 日 (31.01.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/019287 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2017/100896

(22) 国际申请日: 2017 年 9 月 7 日 (07.09.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710621291.X 2017年7月27日 (27.07.2017) CN

(71) 申请人: 深圳市盛路物联通讯技术有限公司(SHENZHEN SHENGLU IOT COMMUNICATION TECHNOLOGY CO., LTD.) [CN/CN]; 中国广东省深圳市南山区南山街道科技园科技中三路5号国人通信大厦B栋328室, Guangdong 518057 (CN)。

(72) 发明人: 杜光东(DU, Guangdong); 中国广东省深圳市南山区南山街道科技园科技中三路5号国人通信大厦B栋328室, Guangdong 518057 (CN)。

(74) 代理人: 广州三环专利商标代理有限公司(SCIHEAD IP LAW FIRM); 中国广东省广州市越秀区先烈中路80号汇华商贸大厦1508室, Guangdong 510070 (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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL,

WO 2019/019287 A1

(54) **Title:** RANDOM ENCRYPTION METHOD AND APPARATUS FOR INTERNET OF THINGS TERMINAL DATA

(54) 发明名称: 一种物联网终端数据的随机加密方法及装置

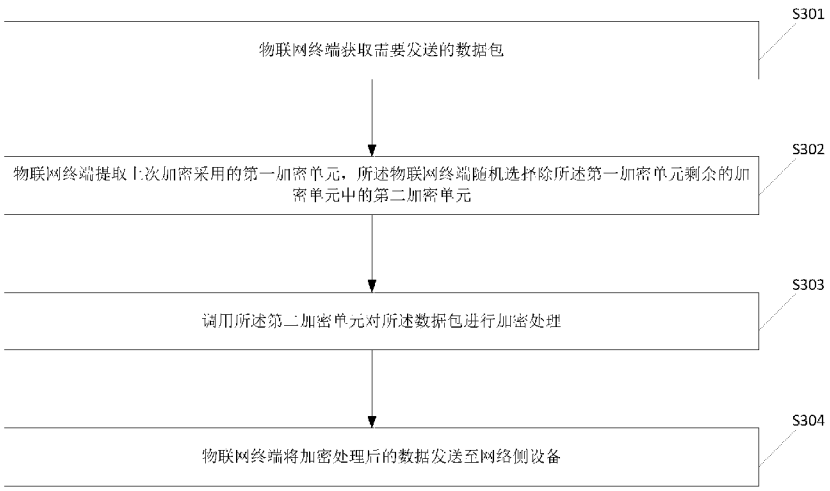

图 3

S301 An Internet of things terminal obtains a data packet that needs to be sent
S302 The Internet of things terminal extracts a first encryption unit adopted during the last encryption, and the Internet of things terminal randomly selects a second encryption unit in the remaining encryption units except the first encryption unit
S303 Invoke the second encryption unit to encrypt the data packet
S304 The Internet of things terminal sends the encrypted data to a network side device

(57) **Abstract:** Disclosed are a random encryption method and apparatus for Internet of things terminal data. The method comprises the following steps: an Internet of things terminal obtains a data packet that needs to be sent; the Internet of things terminal extracts a first encryption unit adopted during the last encryption, and the Internet of things terminal randomly selects a second encryption unit in the remaining encryption units except the first encryption unit; the Internet of things terminal invokes the second encryption unit to encrypt the data packet; and the Internet of things terminal sends the encrypted data and current time to a network side device. The technical solution provided by the present invention has advantages of high security and high user experience.

[见续页]

PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：本申请公开了一种物联网终端数据的随机加密方法及装置，所述方法包括如下步骤：所述物联网终端获取需要发送的数据包；所述物联网终端提取上次加密采用的第一加密单元，物联网终端随机选择除所述第一加密单元剩余的加密单元中的第二加密单元；所述物联网终端调用所述第二加密单元对所述数据包进行加密处理；所述物联网终端将加密处理后的数据以及当前时间向网络侧设备发送。本发明提供的技术方案具有安全性高，用户体验度高的优点。

一种物联网终端数据的随机加密方法及装置

本发明要求 2017 年 7 月 27 日递交的发明名称为“一种物联网终端数据的随机加密方法及装置”的申请号 201710621291.X 的在先申请优先权，上述在先申请的内容以引入的方式并入本文本中。

技术领域

本申请涉及通信领域，尤其涉及一种物联网终端数据的随机加密方法及装置。

背景技术

物联网是新一代信息技术的重要组成部分，也是“信息化”时代的重要发展阶段。其英文名称是：“Internet of things（IoT）”。顾名思义，物联网就是物物相连的互联网。这有两层意思：其一，物联网的核心和基础仍然是互联网，是在互联网基础上的延伸和扩展的网络；其二，其用户端延伸和扩展到了任何物品与物品之间，进行信息交换和通信，也就是物物相息。物联网通过智能感知、识别技术与普适计算等通信感知技术，广泛应用于网络的融合中，也因此被称为继计算机、互联网之后世界信息产业发展的第三次浪潮。物联网是互联网的应用拓展，与其说物联网是网络，不如说物联网是业务和应用。因此，应用创新是物联网发展的核心，以用户体验为核心的创新 2.0 是物联网发展的灵魂。

物联网解决的是物物之间的互联以及物物之间的数据交换，现有的物联网在联网时均基于物联网接入点（英文：access point，AP)来接入互联网，现有的物联网 AP 下有多个物联网终端，物联网 AP（即网络侧设备）与物联网终端之间的数据并不经过加密处理，这样容易出现物联网设备的泄密，导致用户隐私数据泄露，用户体验度不高。

发明内容

本申请提供一种物联网终端数据的随机加密方法。可以提高物联网数据的

安全性，提高用户体验。

第一方面，提供一种物联网终端数据的随机加密方法，所述方法包括如下步骤：

所述物联网终端获取需要发送的数据包；

所述物联网终端提取上次加密采用的第一加密单元，所述物联网终端随机选择除所述第一加密单元剩余的加密单元中的第二加密单元；

所述物联网终端调用所述第二加密单元对所述数据包进行加密处理；

所述物联网终端将加密处理后的数据以及当前时间向网络侧设备发送。

可选的，所述方法在所述物联网终端将加密处理后的数据包以及第二加密单元的标识发送至网关之前还可以包括：

如第二加密单元对所述数据包加密处理失败，则调用第三加密单元的备用加密单元对所述数据包加密处理。

可选的，所述物联网终端调用所述第二加密单元对所述数据包进行加密处理具体包括：

所述物联网终端依据物联网终端的工作时间段对应的提取策略从所述物联网终端媒体接入控制 MAC 地址中提取出 6 位数字，获取物联网终端的信号强度值，将所述 6 位数字与信号强度值连接起来得到一个数字串，将所述数字串除以设定整数得到第一余数的值，从预先存储的多个公钥中提取所述第一余数的值对应的第一公钥，所述第二加密单元采用第一公钥对该数据包进行加密处理。

所述物联网终端调用所述第二加密单元对所述数据包进行加密处理具体包括：

物联网终端提取所述数据包的信号调制方式，依据该信号调制方式从信号调制方式与提取值中得到需要提取的物联网终端 MAC 地址中的位数以及位置，提取该 MAC 地址中的位数值，将该位数值输入预设的算法中计算得到的结果即为秘钥，采用所述秘钥调用第二加密单元对所述数据包进行加密处理可选的，所述方法还包括：物联网终端统计每个加密单元的使用情况，如每个加密单元均使用一次，则物联网终端将每个加密单元的使用情况清零，再次从所有加密单元中随机选取一个加密单元。

第二方面，提供一种物联网终端装置，所述装置包括:

获取单元，用于获取需要发送的数据包;

处理单元，用于提取上次加密采用的第一加密单元，所述物联网终端随机选择除所述第一加密单元剩余的加密单元中的第二加密单元;调用所述第二加密单元对所述数据包进行加密处理;

发送单元，用于将加密处理后的数据以及第二加密单元的标识向网络侧设备发送。

可选的，所述处理单元具体，用于如第二加密单元对所述数据包加密处理失败，则调用第三加密单元的备用加密单元对所述数据包加密处理。

可选的，所述处理单元具体，用于依据物联网终端的工作时间段对应的提取策略从所述物联网终端媒体接入控制 MAC 地址中提取出 6 位数字，获取物联网终端的信号强度值，将所述 6 位数字与信号强度值连接起来得到一个数字串，将所述数字串除以设定整数得到第一余数的值，从预先存储的多个公钥中提取所述第一余数的值对应的第一公钥，所述第二加密单元采用第一公钥对该数据包进行加密处理。

可选的，所述处理单元，具体用于提取所述数据包的信号调制方式，依据该信号调制方式从信号调制方式与提取值中得到需要提取的物联网终端 MAC 地址中的位数以及位置，提取该 MAC 地址中的位数值，将该位数值输入预设的算法中计算得到的结果即为秘钥，采用所述秘钥调用第二加密单元对所述数据包进行加密处理。

可选的，所述处理单元，具体用于统计每个加密单元的使用情况，如每个加密单元均使用一次，则物联网终端将每个加密单元的使用情况清零，再次从所有加密单元中随机选取一个加密单元。

第三方面，提供一种计算机存储介质，其中，该计算机存储介质可存储有程序，该程序执行时包括上述第一方面记载的任何一种物联网终端数据的随机加密方法的部分或全部步骤。

第四方面，提供一种物联网终端设备，所述物联网终端设备包括：一个或多个处理器、存储器、总线系统、收发器以及一个或多个程序，所述处理器、所述存储器和所述收发器通过所述总线系统相连;其中所述一个或多个程序被

存储在所述存储器中，一个或多个程序包括指令，指令当被物联网终端执行时使物联网终端执行上述第一方面及第一方面全部可能设计提供的方法中的任意一种。

本发明提供的技术方案的物联网终端获取需要发送的数据包后，物联网终端提取上次加密采用的第一加密单元，所述物联网终端从剩余加密单元中随机选择一个加密单元即第二加密单元，通过该加密单元对数据进行加密，对于物联网来说，加密设置在物联网终端内，此方式能够对数据进行加密处理，保护了用户的隐私，提高用户的体验。

附图说明

为了更清楚地说明本申请实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本申请的一些实施例，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。

图 1 是一种网络构架示意图；

图 2 是一种物联网终端向网络侧（以中继器为例）发送数据包的传输流程图；

图 3 为物联网终端数据的随机加密方法的流程图

图 4 是本申请一实施例提供的技术场景示意图；

图 5 是本申请一实施例的提供的映射关系示意图；

图 6 是本申请另一实施例提供的物联网终端数据的随机加密方法的流程示意图；

图 7 是本申请提供的一种物联网终端装置的结构示意图；

图 8 为本申请提供的一种物联网终端的硬件结构示意图。

具体实施方式

在更加详细地讨论示例性实施例之前应当提到的是，一些示例性实施例被描述成作为流程图描绘的处理或方法。虽然流程图将各项操作描述成顺序的处

理，但是其中的许多操作可以被并行地、并发地或者同时实施。此外，各项操作的顺序可以被重新安排。当其操作完成时所述处理可以被终止，但是还可以具有未包括在附图中的附加步骤。所述处理可以对应于方法、函数、规程、子例程、子程序等等。

在上下文中所称“计算机设备”，也称为“电脑”，是指可以通过运行预定程序或指令来执行数值计算和/或逻辑计算等预定处理过程的智能电子设备，其可以包括处理器与存储器，由处理器执行在存储器中预存的存续指令来执行预定处理过程，或是由 ASIC、FPGA、DSP 等硬件执行预定处理过程，或是由上述二者组合来实现。计算机设备包括但不限于服务器、个人电脑、笔记本电脑、平板电脑、智能手机等。

后面所讨论的方法（其中一些通过流程图示出）可以通过硬件、软件、固件、中间件、微代码、硬件描述语言或者其任意组合来实施。当用软件、固件、中间件或微代码来实施时，用以实施必要任务的程序代码或代码段可以被存储在机器或计算机可读介质（比如存储介质）中。（一个或多个）处理器可以实施必要的任务。

这里所公开的具体结构和功能细节仅仅是代表性的，并且是用于描述本发明的示例性实施例的目的。但是本发明可以通过许多替换形式来具体实现，并且不应当被解释成仅仅受限于这里所阐述的实施例。

应当理解的是，虽然在这里可能使用了术语“第一”、“第二”等等来描述各个单元，但是这些单元不应当受这些术语限制。使用这些术语仅仅是为了将一个单元与另一个单元进行区分。举例来说，在不背离示例性实施例的范围的情况下，第一单元可以被称为第二单元，并且类似地第二单元可以被称为第一

单元。这里所使用的术语“和/或”包括其中一个或更多所列出的相关联项目的任意和所有组合。

这里所使用的术语仅仅是为了描述具体实施例而不意图限制示例性实施例。除非上下文明确地另有所指，否则这里所使用的单数形式“一个”、“一项”还意图包括复数。还应当理解的是，这里所使用的术语“包括”和/或“包含”规定所陈述的特征、整数、步骤、操作、单元和/或组件的存在，而不排除存在或添加一个或更多其他特征、整数、步骤、操作、单元、组件和/或其组合。

还应当提到的是，在一些替换实现方式中，所提到的功能/动作可以按照不同于附图中标示的顺序发生。举例来说，取决于所涉及的功能/动作，相继示出的两幅图实际上可以基本上同时执行或者有时可以按照相反的顺序来执行。

下面结合附图对本发明作进一步详细描述。

根据本发明的一个方面，提供了一种物联网的数据发送方法。其中，该方法应用在如图 1 所示的物联网络中，如图 1 所示，该物联网络包括：物联网终端 10、物联网接入点 AP20、网关以及中继器 40，上述物联网终端根据不同的情况可以具有不同的表现形式，例如该物联网终端具体可以为：手机、平板电脑、计算机等设备，当然其也可以包含带有联网功能的其他设备，例如智能电视、智能空调、智能水壶或一些物联网的终端设备，上述物联网终端 10 通过无线方式与中继器 40 连接，中继器 40 与 AP 连接，其连接的方式可以为无线方式，也可以为有限方式，上述无线方式包括但不限于：蓝牙、WIFI 等方式，上述网关具体可以为，移动基站、移动中继站、交换机等设备。图 1 中以有线方式为示例，为了方便表示，这里仅以一根实线表示。

上述网关 30 根据物联网的大小可以是一台个人电脑（英文：Personal computer，PC），当然在实际应用中，也可以是多台 PC、服务器或服务器群组，本发明具体实施方式并不局限上述网关 30 的具体表现形式。

上述中继器 40 根据不同的场景可以为多种设备，例如手机、智能手表等等设备。

参阅图 2，图 2 为物联网的数据发送的传输流程图，其中，网络侧设备以中继器为例，如图 2 所示，该流程包括：

步骤 S201、物联网终端 10 将需要发送的数据包通过无线方式发送至中继站 40；

步骤 S202、中继站将数据包转发至物联网接入点；

步骤 S203、物联网接入点将数据包传输至网关。

通过上述图 1 和图 2 的表示，在数据包的实际传输中，如果物联网终端与中继器之间出现泄密，那么对于发送的数据包由于没有经过相应的加密处理，所以很容易导致数据的泄漏，容易出现安全性问题。

参阅图 3，图 3 为本发明提供的一种物联网终端数据的随机加密方法，该方法在如图 4 所示的网络构架下实现，如图 4 所示，一个中继器 40 下可以连接多个物联网终端，该中继器具体可以为开通热点的手机、提供无线连接的个人电脑、转发设备等，该方法如图 3 所示，包括如下步骤：

步骤 S301、物联网终端获取待发送的数据包；

上述步骤 S301 中的物联网终端具体可以为：手机、平板电脑、计算机等设备，当然其也可以包含带有联网功能的其他设备，例如智能电视、智能空调、智能水壶、智能灯、智能开关或一些物联网的智能设备。

步骤 S302、物联网终端提取上次加密采用的第一加密单元，所述物联网

终端随机选择除所述第一加密单元剩余的加密单元中的第二加密单元。

上述步骤 S302 中的物联网终端的类型各个厂家可以根据自行的情况进行设置，例如，该物联网终端具体可以包括：智能电灯、智能电视、智能清扫设备、智能睡眠设备，智能监控设备等，其表现的形式可以为多种多样，例如对于智能电灯，该智能电灯包括但不限于：智能台灯，智能吸顶灯，智能壁灯等设备，例如对于智能电视来说，其可以为三星牌智能电视，当然其也可以为夏普牌智能电视，例如对于智能清扫设备来说，其可以为，智能扫地机器人，当然其还可以包括智能吸尘器、智能垃圾处理器等设备，例如对于智能睡眠设备来说，其可以为：智能床垫、智能沙发等设备，例如对智能监控设备来说或，其可以为，智能血压计，智能温度计等，本发明对上述物联网终端的具体形式以及数量或种类并不限定。

上述步骤中的加密单元可以如图 5 所示。

上述步骤 S302 中的加密单元具体可以为设置在物联网终端的硬件加密单元，其包含厂家预设设置的加密算法，当然在实际应用中，上述加密单元还可以为配置在物联网终端内的软件加密单元，本发明并不限制上述加密单元的具体表现形式。

上述加密算法包括但不限于：3DES、MD5 或 RSA 等加密算法，本发明并不局限具体的加密算法。

步骤 S303、物联网终端调用所述第二加密单元对所述数据包进行加密处理；

上述步骤 S303 的实现方法具体可以为：

例如，第二加密单元为 3DES 加密单元，则物联网终端调用 3DES 加密单元对数据包进行 3DES 加密处理。例如第二加密单元为 RAS 加密单元，则物联网终端调用 RAS 加密单元对数据包进行 RAS 加密处理。例如第二加密单元为 MD5 加密单元，则物联网终端调用 MD5 加密单元对数据包进行 MD5 加密处理。

上述加密算法包括但不限于：三重数据加密算法块密码（英文：riple Data Encryption Algorithm ，3DES）、消息摘要算法（英文：Message Digest Algorithm，MD5）或 RSA（Rivest, Shamir, Adleman）等加密算法，本发明并不局限具体

的加密算法。例如 3DES 是三重数据加密算法块密码的通称。它相当于是对每个数据块应用三次 DES 加密算法。由于计算机运算能力的增强，原版 DES 密码的密钥长度变得容易被暴力破解；3DES 即是设计用来提供一种相对简单的方法，即通过增加 DES 的密钥长度来避免类似的攻击。

上述步骤 S303 的实现方法具体可以为：

物联网终端调用第二加密单元对该数据包进行加密处理，如加密成功，进行后续步骤 S304，如加密不成功，则调用第二加密单元的备用加密单元（即第三加密单元）对该数据包进行加密处理，将采用备用加密单元标识添加到加密处理后的数据包的包头扩展字段。

步骤 S304、物联网终端将加密处理后的数据以及第二加密单元的标识向网络侧设备发送。

上述第二加密单元的标识包括但不限于：编号、码本、名称等等能够标识该第二加密单元的信息。

上述步骤 S304 的实现方法可以为：

上述步骤 S304 中物联网终端向物联网终端发送数据包的方式可以为通过无线连接的方式发送数据包，该无线方式包括但不限于：蓝牙、无线保真（英文：Wireless Fidelity ,WIFI）或 Zigbee 等无线方式，其中，上述 WIFI 需要遵守 IEEE802.11b 的标准。

需要说明的是，这里的物联网以及物联网终端仅仅只是针对无线物联网终端，因为对于物联网来说，其接入的设备数量众多，对于物联网终端来说，如果通过有线连接，首先物联网终端的接入数量会有所限制，并且对于家庭来说，均用有线连接，对于家庭用户的布线来说是无法想象的，另外此有线的成本也非常高，所以本发明的技术方案中的中物联网终端与物联网终端之间的连接仅限无线连接。

依据如图 3 提供的方法，本发明提供的技术方案的物联网终端获取需要发送的数据包后，物联网终端提取上次加密采用的第一加密单元，所述物联网终端从剩余加密单元中随机选择一个加密单元即第二加密单元，通过该加密单元对数据进行加密，对于物联网来说，加密设置在物联网终端内，此方式能够对数据进行加密处理，保护了用户的隐私，提高用户的体验。

参阅图 6，图 6 为本发明提供的一种物联网终端数据的随机加密方法，该方法在如图 4 所示的网络构架下实现，如图 4 所示，一个物联网中继器下可以连接多个物联网终端，该物联网中继器具体可以为开通热点的手机、提供无线连接的个人电脑等设备，该方法如图 6 所示，包括如下步骤：

步骤 S601、物联网终端获取需要发送的数据包；

上述步骤 S601 中的物联网终端具体可以为：手机、平板电脑、计算机等设备，当然其也可以包含带有联网功能的其他设备，例如智能电视、智能空调、智能水壶、智能灯、智能开关或一些物联网的智能设备。

步骤 S602、物联网终端提取上次加密采用的第一加密单元，所述物联网终端随机选择除所述第一加密单元剩余的加密单元中的第二加密单元；调用所述第二加密单元对所述数据包进行加密处理。

上述步骤 S602 中的物联网终端的类型各个厂家可以根据自行的情况进行设置，例如，该物联网终端具体可以包括：智能电灯、智能电视、智能清扫设备、智能睡眠设备，智能监控设备等，其表现的形式可以为多种多样，例如对于智能电灯，该智能电灯包括但不限于：智能台灯，智能吸顶灯，智能壁灯等设备，例如对于智能电视来说，其可以为三星牌智能电视，当然其也可以为夏普牌智能电视，例如对于智能清扫设备来说，其可以为，智能扫地机器人，当然其还可以包括智能吸尘器、智能垃圾处理器等设备，例如对于智能睡眠设备来说，其可以为：智能床垫、智能沙发等设备，例如对智能监控设备来说或，其可以为，智能血压计，智能温度计等，本发明对上述物联网终端的具体形式以及数量或种类并不限定。

上述步骤中的时间段与加密单元映射表如图 5 所示，上述映射可以为一一映射，当然也可以为一对多映射等方式。

上述步骤 S602 中的加密单元具体可以为设置在物联网中继器的硬件加密单元，其包含厂家预设设置的加密算法，当然在实际应用中，上述加密单元还可以为配置在物联网中继器内的软件加密单元，本发明并不限制上述加密单元的具体表现形式。

上述加密算法包括但不限于：3DES、MD5 或 RSA 等加密算法，本发明并不局限具体的加密算法。

步骤 S603、物联网终端依据该物联网终端的工作时间段对应的提取策略从所述物联网终端媒体接入控制 MAC 地址中提取出 6 位数字，获取物联网终端的信号强度值，将所述 6 位数字与信号强度值连接起来得到一个数字串，将所述数字串除以设定整数（具体可以为 6-11 的任意一个整数）得到第一余数的值，从预先存储的多个公钥中提取所述第一余数的值对应的第一公钥，所述第二加密单元采用第一公钥对该数据包进行加密处理；

上述将所述 6 位数字与信号强度值连接起来得到一个数字串具体可以为，将该信号强度值转换成二进制数防止在 6 位数字的前面或后面。

上述步骤 S603 的实现方法具体可以为：

例如，第二加密单元为 3DES 加密单元，则物联网终端调用 3DES 加密单元对数据包进行 3DES 加密处理。例如第二加密单元为 RAS 加密单元，则物联网终端调用 RAS 加密单元对数据包进行 RAS 加密处理。例如第二加密单元为 MD5 加密单元，则物联网终端调用 MD5 加密单元对数据包进行 MD5 加密处理。

上述加密处理的具体方式可以参见 3DES、RSA 以及 MD5 的相关描述，这里不再赘述。

上述步骤 S603 的实现方法具体可以为：

物联网终端调用第二加密单元对该数据包进行加密处理，如加密成功，进行后续步骤 S304，如加密不成功，则调用第二加密单元的备用加密单元对该数据包进行加密处理，将采用备用加密单元标识添加到加密处理后的数据包的包头扩展字段。

步骤 S604、物联网终端将加密处理后的数据包、物联网终端的信号强度值，物联网终端的工作时间段携带在帧的载荷内发送至物联网接入点。

上述步骤 S604 的实现方法可以为：

上述步骤 S604 中物联网终端向物联网中继器（网络侧设备的一种）发送数据包的方式可以为通过无线连接的方式发送数据包，该无线方式包括但不限于：蓝牙、无线保真（英文：Wireless Fidelity ,WIFI）或 Zigbee 等无线方式，

其中，上述 WIFI 需要遵守 IEEE802.11b 的标准。

需要说明的是，这里的物联网以及物联网终端仅仅只是针对无线物联网终端，因为对于物联网来说，其接入的设备数量众多，对于物联网终端来说，如果通过有线连接，首先物联网终端的接入数量会有所限制，并且对于家庭来说，均用有线连接，对于家庭用户的布线来说是无法想象的，另外此有线的成本也非常高，所以本发明的技术方案中的中物联网终端与物联网中继器之间的连接仅限无线连接。

本发明采用的技术方案具有安全性高的优点。

可选的，上述方法在步骤 S604 之前还可以包括:

所述物联网终端调用所述第二加密单元加密不成功，所述物联网终端调用第二加密单元的备用加密单元对所述数据包进行加密处理，将采用备用加密单元标识添加到加密处理后的数据包的包头扩展字段。

可选的，上述方法在步骤 S604 之后还可以包括:

物联网终端统计每个加密单元的使用情况，如每个加密单元均使用一次，则物联网终端将每个加密单元的使用情况清零，再次从所有加密单元中随机选取一个加密单元。

上述使用情况具体可以包括，使用或未使用，其可以通过 1 个 bit 来表示，例如 0 表示未使用，1 表示使用，当然也可以有其他的表现形式，例如 0 表示使用，1 表示未使用。

参阅图 7，图 7 为一种物联网终端装置 700，上述物联网终端装置 700 具体可以为如图 3 或图 6 所示的物联网终端，上述物联网终端装置中的技术术语以及定义可以参见如图 3 或图 6 所示的定义，所述装置包括:

获取单元 701，用于获取需要发送的数据包;

处理单元 702，用于提取上次加密采用的第一加密单元，所述物联网终端随机选择除所述第一加密单元剩余的加密单元中的第二加密单元; 调用所述第二加密单元对所述数据包进行加密处理;

发送单元 703，用于将加密处理后的数据以及当前时间向网络侧设备发送。

可选的，处理单元 702 具体，用于如第二加密单元对所述数据包加密处理

失败，则调用第二加密单元的备用加密单元对所述数据包加密处理。

可选的，处理单元 702 具体，用于依据物联网终端的工作时间段对应的提取策略从所述物联网终端媒体接入控制 MAC 地址中提取出 6 位数字，获取物联网终端的信号强度值，将所述 6 位数字与信号强度值连接起来得到一个数字串，将所述数字串除以设定整数得到第一余数的值，从预先存储的多个公钥中提取所述第一余数的值对应的第一公钥，所述第二加密单元采用第一公钥对该数据包进行加密处理。

可选的，所述处理单元，具体用于提取所述数据包的信号调制方式，依据该信号调制方式从信号调制方式与提取值中得到需要提取的物联网终端 MAC 地址中的位数以及位置，提取该 MAC 地址中的位数值，将该位数值输入预设的算法中计算得到的结果即为秘钥，采用所述秘钥调用第二加密单元对所述数据包进行加密处理。

可选的，所述设定整数为大于等于 6 小于等于 11 的整数。

可选的，处理单元 602，具体用于统计每个加密单元的使用情况，如每个加密单元均使用一次，则物联网终端将每个加密单元的使用情况清零，再次从所有加密单元中随机选取一个加密单元。

本发明还提供一种计算机存储介质，其中，该计算机存储介质可存储有程序，该程序执行时包括上述第一方面记载的任何一种物联网终端数据的随机加密方法的部分或全部步骤。

参阅图 8，图 8 为本发明提供的一种物联网终端 800，该物联网终端可以为部署在互联网系统中的一个节点，互联网系统还可以包括：物联网中继器、物联网接入点和网关，该物联网终端 800 包括但不限于：计算机、服务器等设备，如图 8 所示，该物联网终端 800 包括：处理器 801、存储器 802、收发器 803 和总线 804。收发器 803 用于与外部设备（例如互联系统中的其他设备，包括但不限于：中继器，核心网设备等）之间收发数据。物联网终端 800 中的处理器 801 的数量可以是一个或多个。本申请的一些实施例中，处理器 801、存储器 802 和收发器 803 可通过总线系统或其他方式连接。关于本实施例涉及的术语的含义以及举例，可以参考图 3 或图 6 对应的实施例，此处不再赘述。

其中，存储器 802 中可以存储程序代码。处理器 801 用于调用存储器 802

中存储的程序代码，用于执行以下操作：

收发器 803，用于获取需要发送的数据包；

处理器 801，用于提取上次加密采用的第一加密单元，所述物联网终端随机选择除所述第一加密单元剩余的加密单元中的第二加密单元；调用所述第二加密单元对所述数据包进行加密处理。

收发器 803，还用于将加密处理后的数据包和所述当前时间携带在帧的载荷内发送至物联网接入点。

可选的，处理器 801、收发器 803，还可以用于执行如图 3 或如图 6 所示实施例中的步骤以及步骤的细化方案以及可选方案。

需要说明的是，这里的处理器 801 可以是一个处理元件，也可以是多个处理元件的统称。例如，该处理元件可以是中央处理器（Central Processing Unit，CPU），也可以是特定集成电路（Application Specific Integrated Circuit，ASIC），或者是被配置成实施本申请实施例的一个或多个集成电路，例如：一个或多个微处理器（digital singnal processor，DSP），或，一个或者多个现场可编程门阵列（Field Programmable Gate Array，FPGA）。

存储器 803 可以是一个存储装置，也可以是多个存储元件的统称，且用于存储可执行程序代码或应用程序运行装置运行所需要参数、数据等。且存储器 903 可以包括随机存储器（RAM），也可以包括非易失性存储器（non-volatile memory），例如磁盘存储器，闪存（Flash）等。

总线 804 可以是工业标准体系结构（Industry Standard Architecture，ISA）总线、外部设备互连（Peripheral Component，PCI）总线或扩展工业标准体系结构（Extended Industry Standard Architecture，EISA）总线等。该总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 8 中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

该用户设备还可以包括输入输出装置，连接于总线 804，以通过总线与处理器 801 等其它部分连接。该输入输出装置可以为操作人员提供一输入界面，以便操作人员通过该输入界面选择布控项，还可以是其它接口，可通过该接口外接其它设备。

需要说明的是，对于前述的各个方法实施例，为了简单描述，故将其都表

述为一系列的动作组合，但是本领域技术人员应该知悉，本申请并不受所描述的动作顺序的限制，因为依据本申请，某一些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本申请所必须的。

在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详细描述的部分，可以参见其他实施例的相关描述。

本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：闪存盘、只读存储器（英文：Read-Only Memory，简称：ROM）、随机存取器（英文：Random Access Memory，简称：RAM）、磁盘或光盘等。

以上对本申请实施例所提供的内容下载方法及相关设备、系统进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

权 利 要 求

1、一种物联网终端数据的随机加密方法，其特征在于，所述方法包括如下步骤:

所述物联网终端获取需要发送的数据包;

所述物联网终端提取上次加密采用的第一加密单元，所述物联网终端随机选择除所述第一加密单元剩余的加密单元中的第二加密单元;

所述物联网终端调用所述第二加密单元对所述数据包进行加密处理;

所述物联网终端将加密处理后的数据以及第二加密单元的标识向网络侧设备发送。

2、根据权利要求 1 所述的方法，其特征在于，所述方法在所述物联网终端将加密处理后的数据包发送至网关之前还可以包括:

如第二加密单元对所述数据包加密处理失败，则调用第三加密单元的备用加密单元对所述数据包加密处理。

3、根据权利要求 1 所述的方法，其特征在于，所述物联网终端调用所述第二加密单元对所述数据包进行加密处理具体包括:

所述物联网终端依据物联网终端的工作时间段对应的提取策略从所述物联网终端媒体接入控制 MAC 地址中提取出 6 位数字，获取物联网终端的信号强度值，将所述 6 位数字与信号强度值连接起来得到一个数字串，将所述数字串除以设定整数得到第一余数的值，从预先存储的多个公钥中提取所述第一余数的值对应的第一公钥，所述第二加密单元采用第一公钥对该数据包进行加密处理。

4、根据权利要求 3 所述的方法，其特征在于，所述物联网终端调用所述第二加密单元对所述数据包进行加密处理具体包括:

物联网终端提取所述数据包的信号调制方式，依据该信号调制方式从信号调制方式与提取值中得到需要提取的物联网终端 MAC 地址中的位数以及位置，提取该 MAC 地址中的位数值，将该位数值输入预设的算法中计算得到的结果即为秘钥，采用所述秘钥调用第二加密单元对所述数据包进行加密处理。

5、根据权利要求 1 所述的方法，其特征在于，所述方法还包括:

物联网终端统计每个加密单元的使用情况，如每个加密单元均使用一次，则物联网终端将每个加密单元的使用情况清零，再次从所有加密单元中随机选取一个加密单元。

6、一种物联网终端装置，其特征在于，所述装置包括:

获取单元，用于获取需要发送的数据包;

处理单元，用于提取上次加密采用的第一加密单元，所述物联网终端随机选择除所述第一加密单元剩余的加密单元中的第二加密单元;调用所述第二加密单元对所述数据包进行加密处理;

发送单元，用于将加密处理后的数据以及所述第二加密单元的标识向网络侧设备发送。

7、根据权利要求 6 所述的装置，其特征在于，所述处理单元具体，用于如第二加密单元对所述数据包加密处理失败，则调用第三加密单元的备用加密单元对所述数据包加密处理。

8、根据权利要求 6 所述的装置，其特征在于，所述处理单元具体，用于依据物联网终端的工作时间段对应的提取策略从所述物联网终端媒体接入控制 MAC 地址中提取出 6 位数字，获取物联网终端的信号强度值，将所述 6 位数字与信号强度值连接起来得到一个数字串，将所述数字串除以设定整数得到第一余数的值，从预先存储的多个公钥中提取所述第一余数的值对应的第一公钥，所述第二加密单元采用第一公钥对该数据包进行加密处理。

9、根据权利要求 8 所述的装置，其特征在于，所述处理单元，具体用于提取所述数据包的信号调制方式，依据该信号调制方式从信号调制方式与提取值中得到需要提取的物联网终端 MAC 地址中的位数以及位置，提取该 MAC 地址中的位数值，将该位数值输入预设的算法中计算得到的结果即为秘钥，采用所述秘钥调用第二加密单元对所述数据包进行加密处理。

10、根据权利要求 8 所述的装置，其特征在于，所述处理单元具体，用于统计每个加密单元的使用情况，如每个加密单元均使用一次，则物联网终端将每个加密单元的使用情况清零，再次从所有加密单元中随机选取一个加密单元。

11、一种计算机可读存储介质，其特征在于，其存储用于电子数据交换的

计算机程序，其中，所述计算机程序使得计算机执行如权利要求 1-5 任一项所述的方法。

12、一种计算机程序产品，其特征在于，所述计算机程序产品包括存储了计算机程序的非瞬时性计算机可读存储介质，所述计算机程序可操作来使计算机执行如权利要求 1-5 任一项所述的方法。

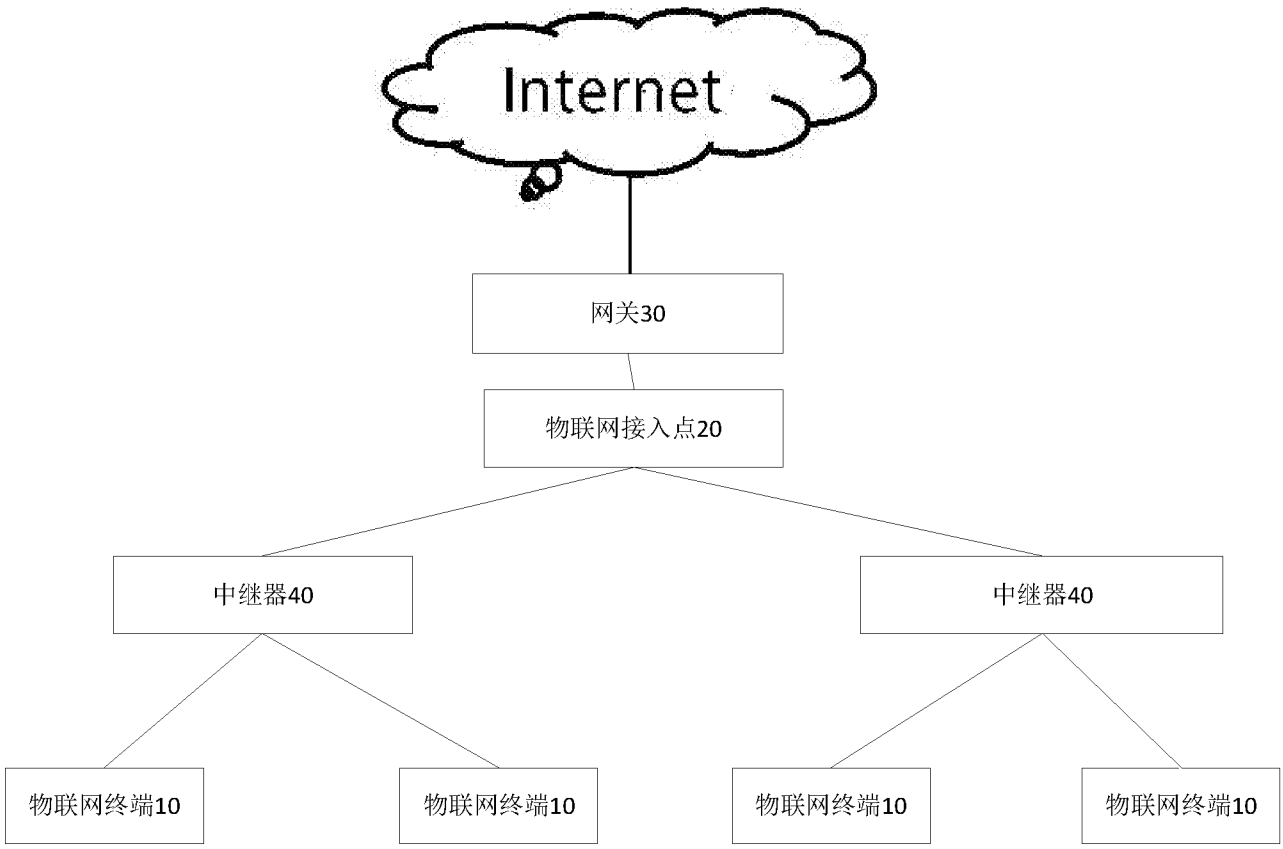
Internet
网关30
物联网接入点20
中继器40
中继器40
物联网终端10
物联网终端10
物联网终端10
物联网终端10

图 1

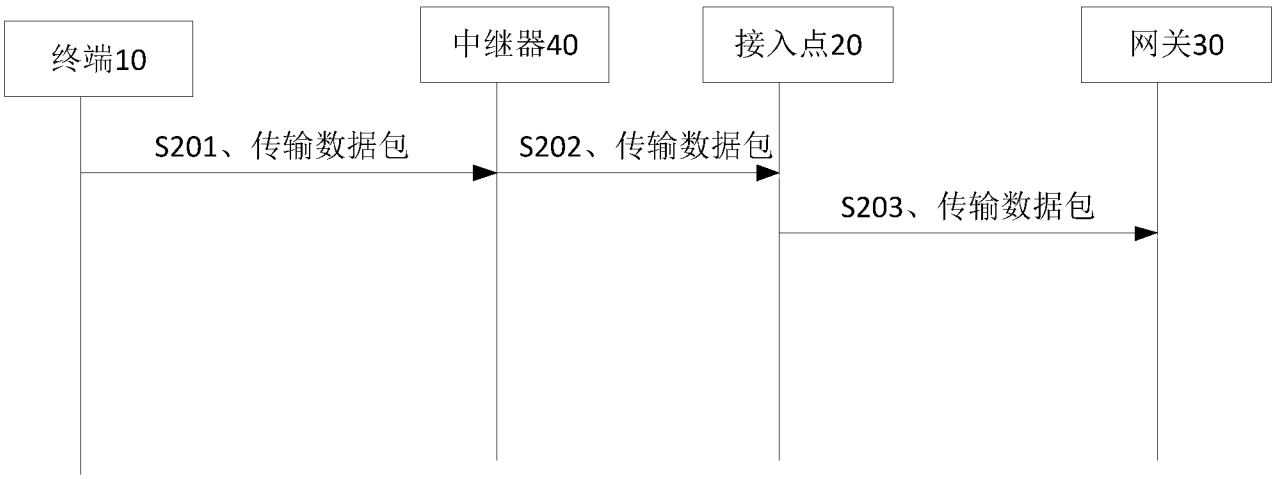
终端10
中继器40
接入点20
网关30
S201、传输数据包
S202、传输数据包
S203、传输数据包

图 2

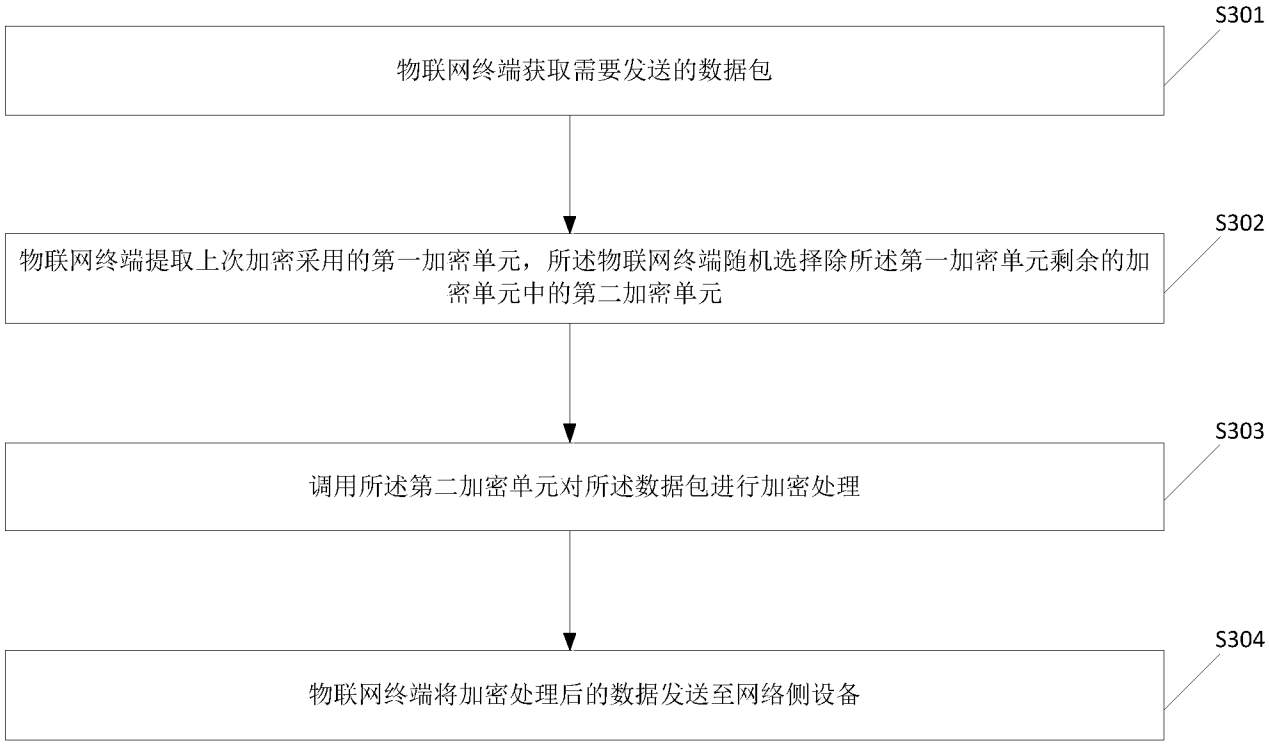
S301
物联网终端获取需要发送的数据包
S302
物联网终端提取上次加密采用的第一加密单元，所述物联网终端随机选择除所述第一加密单元剩余的加密单元中的第二加密单元
S303
调用所述第二加密单元对所述数据包进行加密处理
S304
物联网终端将加密处理后的数据发送至网络侧设备

图 3

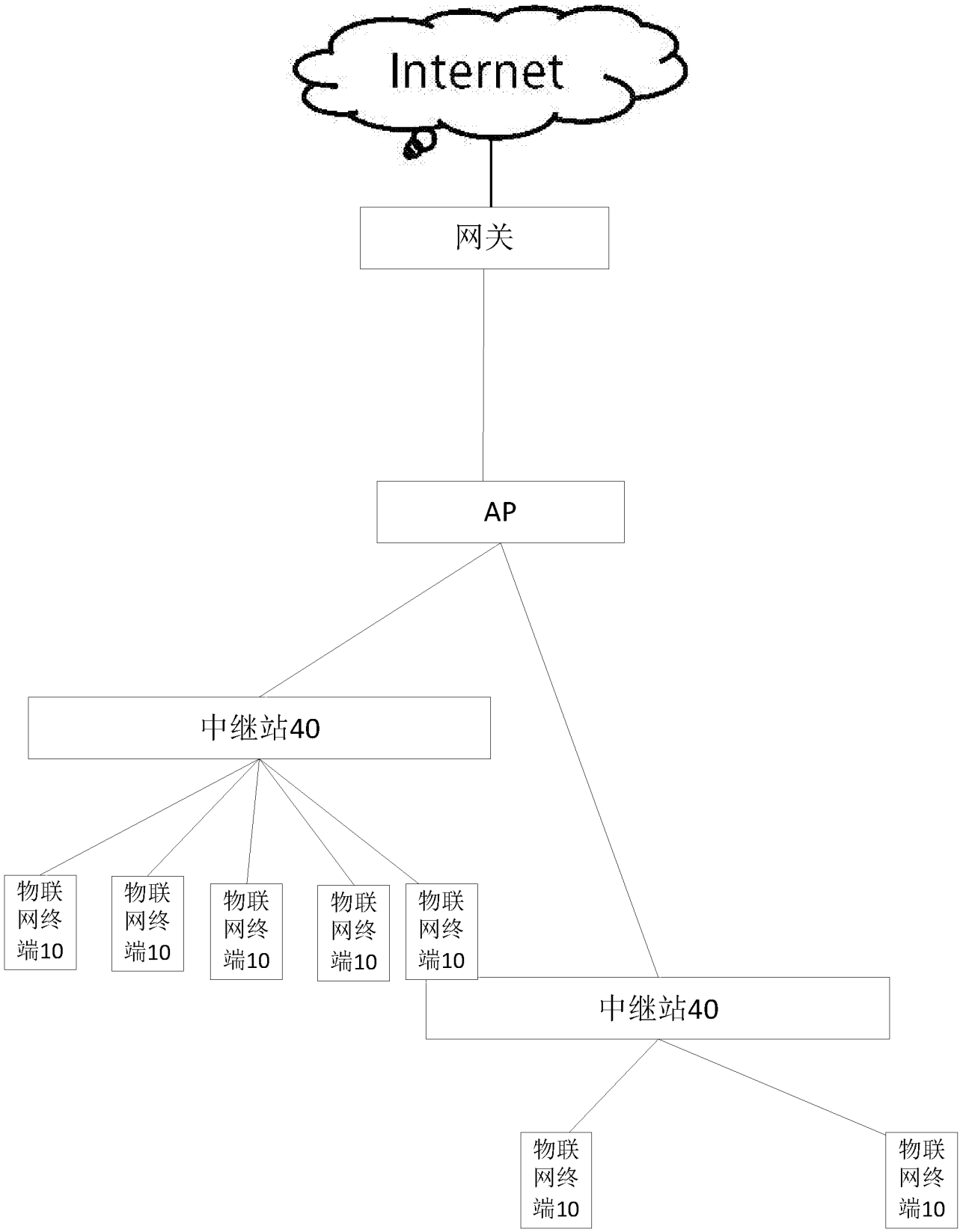
Internet
网关
AP
中继站40
物联网终端10
物联网终端10
物联网终端10
物联网终端10
物联网终端10
中继站40
物联网终端10
物联网终端10

图 4

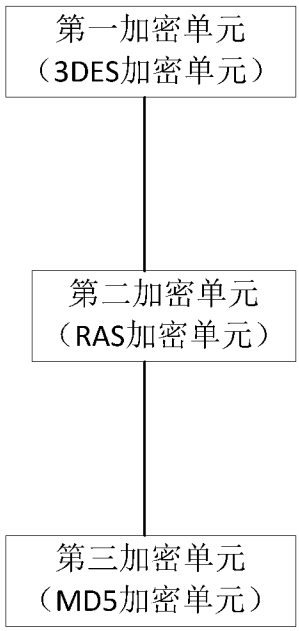
第一加密单元
（3DES加密单元）
第二加密单元
（RAS加密单元）
第三加密单元
（MD5加密单元）

图 5

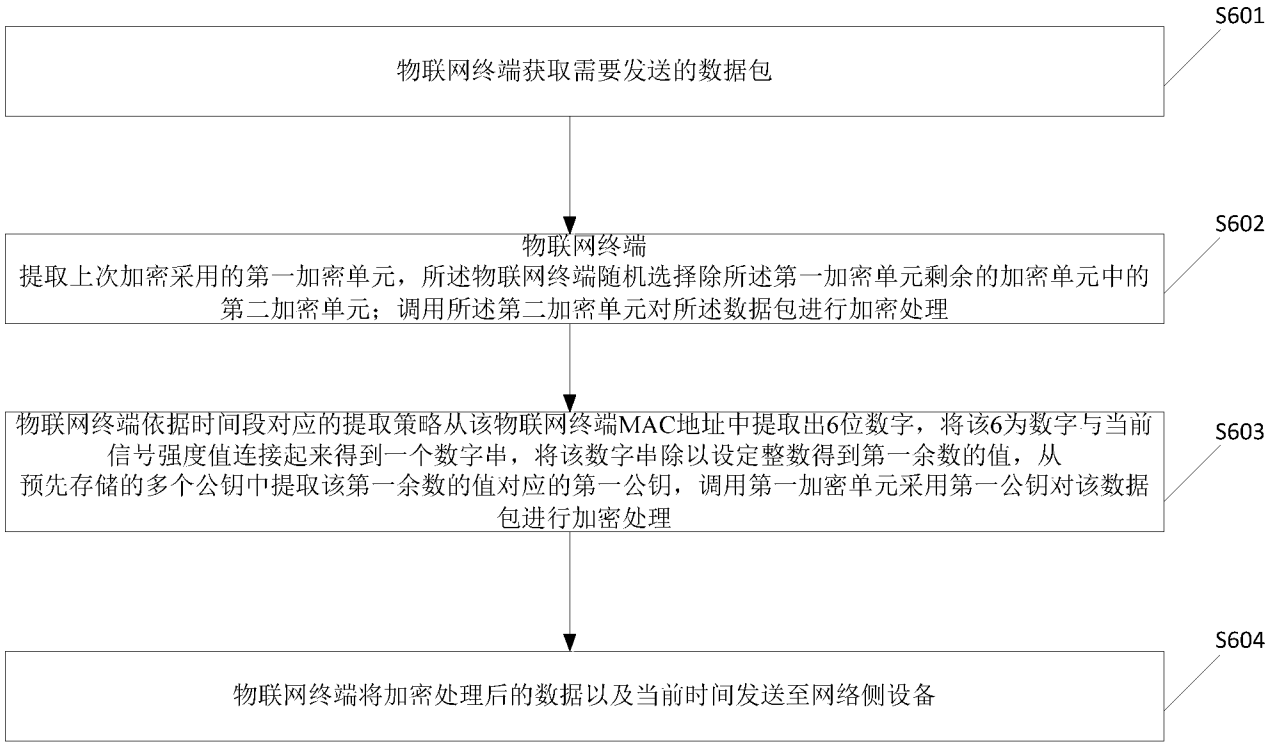
S601
物联网终端获取需要发送的数据包
S602
物联网终端
提取上次加密采用的第一加密单元，所述物联网终端随机选择除所述第一加密单元剩余的加密单元中的第二加密单元；调用所述第二加密单元对所述数据包进行加密处理
S603
物联网终端依据时间段对应的提取策略从该物联网终端MAC地址中提取出6位数字，将该6为数字与当前信号强度值连接起来得到一个数字串，将该数字串除以设定整数得到第一余数的值，从预先存储的多个公钥中提取该第一余数的值对应的第一公钥，调用第一加密单元采用第一公钥对该数据包进行加密处理
S604
物联网终端将加密处理后的数据以及当前时间发送至网络侧设备

图 6

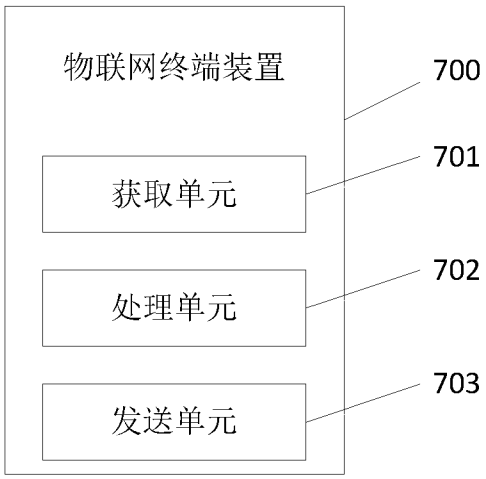
物联网终端装置
700
获取单元
701
处理单元
702
发送单元
703

图 7

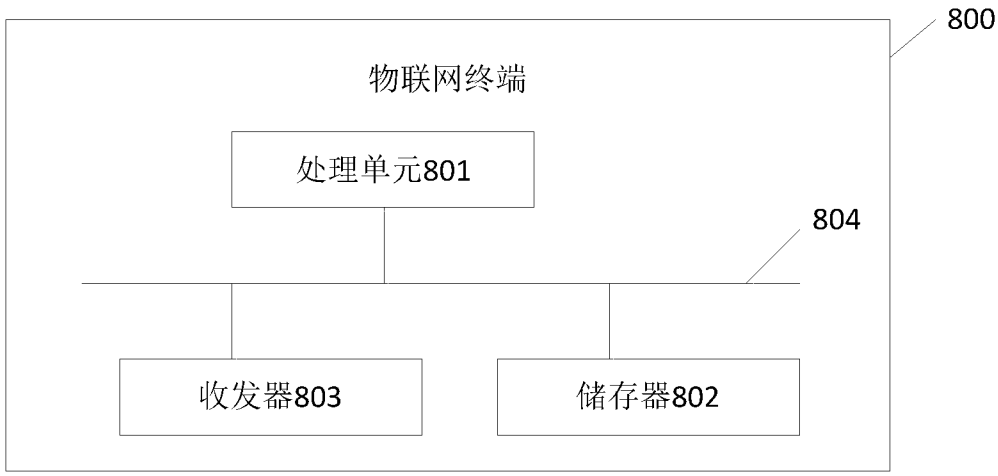
800
物联网终端
处理单元801
804
收发器803
储存器802

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/100896

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) 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)

H04L

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)

CNPAT, CNKI, WPI, EPODOC, IEEE: 物联网, 加密, 密钥, 算法, 顺序, 预设, 设置, 列表, 强度, 对应, 相应, 映射, 等级, iot, key, order, algorithm, preset, set, list, signal, strength

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104935433 A (TENDYRON CORPORATION) 23 September 2015 (23.09.2015), claims	1, 2, 6, 7, 11, 12
A	CN 106850220 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 13 June 2017 (13.06.2017), entire document	1-12
A	CN 101873215 A (DATANG MICROELECTRONICS TECHNOLOGY CO., LTD.) 27 October 2010 (27.10.2010), entire document	1-12
A	CN 101873587 A (DATANG MICROELECTRONICS TECHNOLOGY CO., LTD.) 27 October 2010 (27.10.2010), entire document	1-12

☐ 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	Date of mailing of the international search report
04 April 2018	20 April 2018

Name and mailing address of the ISA	Authorized officer
State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	YANG, Jibin Telephone No. (86-10) 53961580

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/100896

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104935433 A	23 September 2015	None	
CN 106850220 A	13 June 2017	None	
CN 101873215 A	27 October 2010	None	
CN 101873587 A	27 October 2010	None	

国际检索报告

国际申请号 PCT/CN2017/100896

A. 主题的分类

H04L 9/32(2006.01)i

按照国际专利分类(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)

H04L

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）)

CNPAT,CNKI,WPI,EPODOC,IEEE:物联网，加密，密钥，算法，顺序，预设，设置，列表，强度，对应，相应，映射，等级，iot，key，order，algorithm，preset，set，list，signal，strength

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	CN 104935433 A (天地融科技股份有限公司) 2015年 9月 23日 (2015-09-23) 权利要求书	1,2,6,7,11,12
A	CN 106850220 A (腾讯科技深圳有限公司) 2017年 6月 13日 (2017-06-13) 全文	1-12
A	CN 101873215 A (大唐微电子技术有限公司) 2010年 10月 27日 (2010-10-27) 全文	1-12
A	CN 101873587 A (大唐微电子技术有限公司) 2010年 10月 27日 (2010-10-27) 全文	1-12

☐ 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（如具体说明的）

“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	国际检索报告邮寄日期
2018年 4月 4日	2018年 4月 20日
ISA/CN的名称和邮寄地址 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 杨继彬 电话号码 (86-10)53961580

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/100896

检索报告引用的专利文件			公布日（年/月/日）	同族专利	公布日（年/月/日）
CN	104935433	A	2015年 9月 23日	无	
CN	106850220	A	2017年 6月 13日	无	
CN	101873215	A	2010年 10月 27日	无	
CN	101873587	A	2010年 10月 27日	无	