

(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



(10) 国际公布号

WO 2018/233044 A1

(43) 国际公布日

2018 年 12 月 27 日 (27.12.2018)

WIPO | PCT

(51) 国际专利分类号:

H04L 9/08 (2006.01)

H04L 29/06 (2006.01)

H04L 12/66 (2006.01)

(21) 国际申请号:

PCT/CN2017/100007

(22) 国际申请日:

2017 年 8 月 31 日 (31.08.2017)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

201710473278.4

2017年6月21日

(21.06.2017) 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: 广州德科知识产权代理有限公司 (GUANGZHOU DEKE INTELLECTUAL PROPERTY); 中国广东省广州市黄埔区科学城科学大道162号创意大厦B2栋10层1001室 万振雄, Guangdong 510663 (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,

(54) Title: FILTER GATEWAY BASED INTERNET OF THINGS DATA FILTERING METHOD AND SYSTEM

(54) 发明名称: 一种基于过滤网关的物联网数据过滤方法及系统



图 2

(57) Abstract: The invention discloses a filtering method and system for The invention discloses a data filtering method and system for Internet of things based on a filter gateway. The method comprises: a terminal device sends an authorization request to the filter gateway through an access node; the filter gateway sends the authorization request to a convergence unit, and sends a response message returned by the convergence unit to the access node; the access node sends the response message to the terminal device; the terminal device collects data when an acquisition time point reaches, and generates signature encryption information to sign the collected data

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, 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))。

on the basis of a signature generation algorithm and a device ID number, so as to obtain a data message and send the same to the access node; the access node forwards the data message to the filter gateway; and the filter gateway generates the signature verification information on the basis of the built-in signature generation algorithm according to the device ID number to verify whether the signature of the data message is correct or not, and if the signature of the data message is correct, forwards the data message to the convergence unit. The invention is used for filtering the data message sent by an unauthorized terminal device, so as to improve the security of data transmission.

(57) 摘要: 本发明公开一种基于过滤网关的物联网数据过滤方法及系统, 该方法包括: 终端设备通过接入节点向过滤网关发送授权请求; 过滤网关将授权请求发送给汇聚单元, 并将汇聚单元返回的响应消息发送给接入节点; 接入节点将响应消息发送给终端设备; 终端设备在采集时间点到达时采集数据, 并以设备ID号为依据, 基于签名生成算法生成签名加密信息以对采集的数据进行签名, 以获得数据报文并发送给接入节点; 接入节点将数据报文转发给过滤网关; 过滤网关以设备ID号为依据, 基于内置的签名生成算法生成签名验证信息, 以验证数据报文的签名是否正确, 如果正确, 将数据报文转发给汇聚单元; 用于过滤非授权终端设备发送的数据报文, 提高数据传输的安全性。

一种基于过滤网关的物联网数据过滤方法及系统

技术领域

本发明涉及物联网技术领域，具体涉及一种基于过滤网关的物联网数据过滤方法及系统。

背景技术

将物联网环境下各个节点的设备分类，分别包括：终端设备、接入节点和汇聚单元，其中，在一些应用环境下还包括过滤网关，终端设备可以是湿敏元件、照明灯、状态监控器、烤箱等等。终端设备采集的数据通过无线网络发送给接入节点，接入节点通过互联网发送给汇聚单元，汇聚单元完成数据分析、终端设备监控等。由于数据在多个环节中传输，容易造成数据泄漏，攻击者也可以轻易伪装授权终端设备进行数据传输，造成物联网数据传输的安全隐患。

发明内容

本发明实施例公开了一种基于过滤网关的物联网数据过滤方法及系统，用于解决现有物联网数据传输的安全隐患，以提高数据传输的安全性。

本发明第一方面公开了一种基于过滤网关的物联网数据过滤方法，可包括：

终端设备通过接入节点向过滤网关发送授权请求，所述授权请求携带所述终端设备的设备身份标识（Identity，简称 ID）号、设备类型和互联网协议地址（Internet Protocol，简称 IP）；

所述过滤网关将所述授权请求发送给所述汇聚单元，以及接收所述汇聚单元返回的用于授权所述终端设备的响应消息并发送给所述接入节点，所述响应消息包括所述签名生成算法和采集时间点；

所述接入节点将所述响应消息发送给所述终端设备；

所述终端设备在所述采集时间点到达时采集数据，获取所述终端设备的设备 ID 号，以所述设备 ID 号为依据，基于所述签名生成算法生成签名加密

信息，并根据所述签名加密信息对采集的数据进行签名，以获得数据报文，并将所述数据报文发送给接入节点，所述数据报文携带所述设备 ID 号；

所述接入节点将所述数据报文转发给所述过滤网关；

所述过滤网关从所述数据报文中获取所述设备 ID 号，以所述设备 ID 号为依据，基于内置的所述签名生成算法生成签名验证信息；

所述过滤网关根据所述签名验证信息验证所述数据报文的签名是否正确；

所述过滤网关在验证所述数据报文的签名正确时，将所述数据报文转发给所述汇聚单元。

作为一种可选的实施方式，在本发明第一方面中，所述过滤网关将所述授权请求发送给所述汇聚单元，以及接收所述汇聚单元返回的用于授权所述终端设备的响应消息并发送给所述接入节点，包括：

所述过滤网关将所述授权请求发送给所述汇聚单元，以及接收所述汇聚单元在确定所述授权请求携带的设备类型属于其感兴趣的设备类型时、返回的用于授权所述终端设备的响应消息，并将所述响应消息发送给所述接入节点。

作为一种可选的实施方式，在本发明第一方面中，所述接入节点将所述响应消息发送给所述终端设备包括：

所述接入节点将所述响应消息的所述签名生成算法和所述采集时间点，写入所述终端设备。

作为一种可选的实施方式，在本发明第一方面中，其特征在于，所述接入节点将所述数据报文转发给所述过滤网关包括：

所述接入节点通过跳频方式从目标传输频段中确定用于发送所述数据报文的物理资源块的频域位置；

所述接入节点在确定的物理资源块的频域位置所对应的时频资源上，向所述过滤网关发送所述数据报文。

作为一种可选的实施方式，在本发明第一方面中，所述响应消息还包括所述采集时间点对应的工作状态，所述终端设备在所述采集时间点到达时采集数据，包括：

所述终端设备实时监控所述终端设备的系统时间，在监控到所述系统时间到达所述采集时间点时，将所述终端设备的工作状态切换至所述采集时间点对应的工作状态，并采集数据。

本发明第二方面公开了一种基于过滤网关的物联网数据过滤系统，可包括：

终端设备，用于通过接入节点向过滤网关发送授权请求，所述授权请求携带所述终端设备的设备身份标识 ID 号、设备类型和互联网协议地址 IP；

所述过滤网关，用于将所述授权请求发送给所述汇聚单元，以及接收所述汇聚单元返回的用于授权所述终端设备的响应消息并发送给所述接入节点，所述响应消息包括所述签名生成算法和采集时间点；

所述接入节点，用于将所述响应消息发送给所述终端设备；

所述终端设备还用于在所述采集时间点到达时采集数据，获取所述终端设备的设备 ID 号，以所述设备 ID 号为依据，基于所述签名生成算法生成签名加密信息，并根据所述签名加密信息对采集的数据进行签名，以获得数据报文，并将所述数据报文发送给接入节点，所述数据报文携带所述设备 ID 号；

所述接入节点还用于将所述数据报文转发给所述过滤网关；

所述过滤网关还用于从所述数据报文中获取所述设备 ID 号，以所述设备 ID 号为依据，基于内置的所述签名生成算法生成签名验证信息；

所述过滤网关还用于根据所述签名验证信息验证所述数据报文的签名是否正确；

所述过滤网关还用于在验证所述数据报文的签名正确时，将所述数据报文转发给所述汇聚单元。

作为一种可选的实施方式，在本发明第二方面中，所述过滤网关用于将所述授权请求发送给所述汇聚单元，以及接收所述汇聚单元返回的用于授权所述终端设备的响应消息并发送给所述接入节点的方式具体为：

所述过滤网关用于将所述授权请求发送给所述汇聚单元，以及接收所述汇聚单元在确定所述授权请求携带的设备类型属于其感兴趣的设备类型时、返回的用于授权所述终端设备的响应消息，并将所述响应消息发送给所述接

入节点。

作为一种可选的实施方式，在本发明第二方面中，所述接入节点用于将所述响应消息发送给所述终端设备的方式具体为：

所述接入节点用于将所述响应消息的所述签名生成算法和所述采集时间点，写入所述终端设备。

作为一种可选的实施方式，在本发明第二方面中，所述接入节点还用于将所述数据报文转发给所述过滤网关的方式具体为：

所述接入节点还用于通过跳频方式从目标传输频段中确定用于发送所述数据报文的物理资源块的频域位置，在确定的物理资源块的频域位置所对应的时频资源上，向所述过滤网关发送所述数据报文。

作为一种可选的实施方式，在本发明第二方面中，所述响应消息还包括所述采集时间点对应的工作状态，所述终端设备还用于在所述采集时间点到达时采集数据的方式具体为：

所述终端设备还用于实时监控所述终端设备的系统时间，在监控到所述系统时间到达所述采集时间点时，将所述终端设备的工作状态切换至所述采集时间点对应的工作状态，并采集数据。

与现有技术相比，本发明实施例具有以下有益效果：

在本发明实施例中，终端设备经过接入节点、过滤网关向汇聚单元发送授权请求，该授权请求携带设备ID号、设备类型和IP地址；在汇聚单元授权该终端设备时，将返回响应消息，该响应消息包括签名生成算法和采集时间点。终端设备在该采集时间点到达时采集数据，获取设备ID号，以该设备ID号为依据，基于签名生成算法生成签名加密信息，然后对采集的数据进行签名，获得数据报文，并将该数据报文发送给接入节点。接入节点在接收到数据报文后，将数据报文转发给过滤网关，过滤网关从数据报文中获取设备ID号，以该设备ID号为依据，基于内置在过滤网关中的该签名生成算法生成签名验证信息，根据该签名验证信息验证数据报文中的签名是否正确，如果正确，将数据报文发送给汇聚单元。可以看出，实施本发明实施例，过滤网关能够先一步对终端设备发送的数据报文进行签名验证，以过滤非授权终端设备发送的数据报文，以提高数据传输的安全性；进一步地，也能减轻汇聚单

元的处理负担。

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例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。

图1为本发明一些实施例公开的物联网架构示意图；

图2为本发明实施例公开的基于过滤网关的物联网数据过滤方法的流程图示意图；

图3为本发明实施例公开的基于过滤网关的物联网数据过滤方法的另一流程图示意图；

图4为本发明实施例公开的基于过滤网关的物联网数据过滤系统的结构示意图。

具体实施方式

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，本发明实施例的术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

本发明实施例公开了一种基于过滤网关的物联网数据过滤方法，用于过滤非授权终端设备发送的数据报文，以提高数据传输的安全性；进一步地，也能减轻汇聚单元的处理负担。本发明实施例还相应地公开了一种基于过滤网关的物联网数据过滤系统。

在介绍本发明技术方案之前，先简单介绍本发明一些实施例公开的物联网架构，图1为本发明一些实施例公开的物联网架构示意图，需要说明的是，图1仅为本发明一些实施例公开的物联网架构示意图，其它在图1基础上进行优化或者变形得到的示意图均属于本发明的保护范围，在此不再一一举例。图1所示的物联网架构按照功能划分可以包括终端设备层、接入节点层以及汇聚层三个层。其中，终端设备层可以包括海量规模的终端设备，例如湿度计、烟感器、通风设备、雨量传感器、灌溉阀等等；接入节点层可以包括网络连接的大量的接入节点，接入节点可以包括路由器、中继器、接入点等设备，本发明实施例不作限定；接入节点可以使用任何标准的组网协议，而且接入节点可以在不同的网络制式之间实现数据解析；汇聚层可以包括过滤网关和汇聚单元，其中，过滤网关可以通过互联网与转发节点层的各个转发节点直接或间接通讯连接（在图中未全部示出）；汇聚单元可以通过过滤网关对转发节点层的各个转发节点进行高层管理，从而实现数据传输频率、网络拓扑以及其他组网功能的控制；汇聚单元不仅可以对海量终端设备产生的物联网数据进行分析决策，还可以通过发指令去获取信息或者配置终端设备参数（此时数据的传输指向终端设备）；汇聚单元还可以引入各种业务，从大数据到社交网络、甚至从社交工具“点赞”到天气分享等。在图1所示的物联网架构中，每一个转发节点可以为其自身无线网络覆盖范围内的海量终端设备提供物联网数据收发服务，其中，每一个转发节点自身无线网络覆盖范围内的每一个终端设备可以内置有无线通讯模块，这使得每一转发节点可以通过无线网络通讯方式与自身无线网络覆盖范围内的每一个终端设备进行无线通讯。在图1所示的物联网架构中，终端设备内置的无线通讯模块在生产时，可以输入上频点470MHz，下频点510MHz，这样无线通讯模块可以自动将通讯频段定义为470MHz~510MHz，以符合中国SRRC标准的规定；或者，也可以输入上频点868MHz，下频点908MHz，这样无线通讯模块可以自动将通讯频段定义为868MHz~908MHz，以符合欧洲ETSI标准的规定；或者，可以输入上频点918MHz，下频点928MHz，这样无线通讯模块可以自动将通讯频段定义为918MHz~928MHz，以符合美国FCC标准的规定；或者，无线通讯模块的通讯频段也可以定义为符合日本ARIB标准或加拿大IC标准的规定，本发明实施

例不作限定。在图1所示的物联网架构中，终端设备可以采用频分复用（Frequency Division Multiple Access, FDMA）、跳频（Frequency-Hopping Spread Spectrum, FHSS）、动态时分复用（Dynamic Time Division Multiple Access, DTDMA）、退避复用（CSMA）相结合的方法来解决干扰问题。

基于图1所示的物联网架构，下面将结合具体实施例，对本发明技术方案进行详细说明。

请参阅图2，图2为本发明实施例公开的基于过滤网关的物联网数据过滤方法的流程示意图；如图2所示，一种基于过滤网关的物联网数据过滤方法可包括：

201、终端设备通过接入节点向过滤网关发送授权请求，该授权请求携带终端设备的设备ID号、设备类型和IP地址。

其中，终端设备在首次开启并接入无线网络时或者在重新启动后或者在授权内容（包括下面的签名生成算法有效期到达后），终端设备可以向汇聚单元发送授权请求，以获得授权。

作为一种可选的实施方式，接入节点在其无线网络覆盖范围内实时侦听，在侦听到新的终端设备接入时，触发该终端设备发送授权请求。

进一步地，接入节点在其无线网络覆盖范围内实时广播侦听消息，其无线网络覆盖范围内的终端设备在接收到侦听消息时，对该侦听消息进行响应，以发送响应消息，该响应消息携带设备类型、设备ID号和IP地址等，接入节点在接收到响应消息后，根据设备ID号或者IP地址等确定有新的终端设备接入。通过该实施方式，能够实现终端设备在接入网络时发送授权请求。

202、过滤网关将授权请求发送给汇聚单元，以及接收该汇聚单元返回的用于授权终端设备的响应消息并发送给接入节点，响应消息包括签名生成算法和采集时间点。

作为一种可选的实施方式，该过滤网关将授权请求发送给汇聚单元，以及接收该汇聚单元返回的用于授权终端设备的响应消息并发送给接入节点，包括：

该过滤网关将授权请求发送给汇聚单元，以及接收汇聚单元在确定授权请求携带的设备类型属于其感兴趣的设备类型时、返回的用于授权终端设备

的响应消息，并将响应消息发送给接入节点。

具体地，汇聚单元在接收到授权请求时，从授权请求中提取该终端设备的设备类型，判断该设备类型是否为自己感兴趣的设备类型，如果是自己感兴趣的设备类型时，进一步对其设备 ID 号和 ID 地址进行确认，在确认后成功，返回响应消息。在该实施方式中，汇聚单元可以针对其感兴趣的终端设备进行设置，以提供这些设备用于传输数据时的签名生成算法，提高数据传输的安全性。

203、接入节点将响应消息发送给终端设备。

作为一种可选的实施方式，接入节点在将响应消息发送给终端设备后，实时监控响应消息中的签名生成算法的有效期，在签名生成算法的有效期到达时，将通知终端设备，以触发终端设备再次向汇聚单元发送授权请求，以获得再次授权。通过该实施方式，实现在签名生成算法有效期到达后，再次触发终端设备去获取授权。

作为一种可选的实施方式，接入节点将响应消息发送给终端设备具体包括：接入节点获取目标传输频段，然后确定目标传输频段所对应的时频资源，在时频资源上向终端设备发送该响应消息。在该实施方式中，采用时分方式向终端设备发送响应消息，能够减少干扰，提高传输效率。

204、终端设备在采集时间点到达时采集数据，获取终端设备的设备 ID 号，以设备 ID 号为依据，基于签名生成算法生成签名加密信息，并根据签名加密信息对采集的数据进行签名，以获得数据报文，并将数据报文发送给接入节点，数据报文携带设备 ID 号。

205、接入节点将数据报文转发给过滤网关。

作为一种可选的实施方式，接入节点将数据报文转发给过滤网关具体包括：接入节点通过跳频方式从目标传输频段中确定用于发送数据报文的物理资源块的频域位置；该接入节点在确定的物理资源块的频域位置所对应的时频资源上，向过滤网关发送数据报文。在该实施方式中，接入节点和过滤网关通信时，采用频分方式，能够减少干扰，提高传输效率。

206、过滤网关从数据报文中获取设备 ID 号，以设备 ID 号为依据，基于内置的签名生成算法生成签名验证信息。

作为一种可选的实施方式，在执行本发明步骤 201 之前，汇聚单元下发签名生成算法给过滤网关，过滤网关接收签名生成算法并保存。

207、过滤网关根据签名验证信息验证数据报文的签名是否正确。其中，在验证正确时，转向步骤208；在验证失败时，则丢弃该数据报文，结束流程。

其中，签名验证信息与用于数据报文签名的签名加密信息若匹配，则验证正确，若不匹配，则验证失败。

208、过滤网关将数据报文转发给汇聚单元。

在本发明实施例中，终端设备经过接入节点、过滤网关向汇聚单元发送授权请求，该授权请求携带设备ID号、设备类型和IP地址；在汇聚单元授权该终端设备时，将返回响应消息，该响应消息包括签名生成算法和采集时间点。终端设备在该采集时间点到达时采集数据，获取设备ID号，以该设备ID号为依据，基于签名生成算法生成签名加密信息，然后对采集的数据进行签名，获得数据报文，并将该数据报文发送给接入节点。接入节点在接收到数据报文后，将数据报文转发给过滤网关，过滤网关从数据报文中获取设备ID号，以该设备ID号为依据，基于内置在过滤网关中的该签名生成算法生成签名验证信息，根据该签名验证信息验证数据报文中的签名是否正确，如果正确，将数据报文发送给汇聚单元。可以看出，实施本发明实施例，过滤网关能够先一步对终端设备发送的数据报文进行签名验证，以过滤非授权终端设备发送的数据报文，以提高数据传输的安全性；进一步地，也能减轻汇聚单元的处理负担。

实施例二

请参阅图3，图3为本发明实施例公开的基于过滤网关的物联网数据过滤方法的另一流程示意图；如图3所示，一种基于过滤网关的物联网数据过滤方法可包括：

301、终端设备通过接入节点向过滤网关发送授权请求，该授权请求携带终端设备的设备ID号、设备类型和IP地址。

其中，汇聚单元针对其感兴趣的设备类型（可以设置了用于采集重要数据的终端设备的设备类型），需要加强这类终端设备发出的数据的安全。进而，在本发明实施例中，汇聚单元可以针对这些终端设备，设置相应的签名

生成算法，该签名生成算法采用设备类型作为因子，生成签名加密信息。

作为另一种可选的实施方式，授权请求还可以携带有位置信息，汇聚单元针对其感兴趣的位置信息（可以设置了用于采集重要数据的终端设备的位置信息），需要加强这类终端设备发出的数据的安全。进而，在本发明实施例中，汇聚单元可以针对这些终端设备，设置相应的签名生成算法，该签名生成算法采用设备类型作为因子，生成签名加密信息。

302、过滤网关将授权请求发送给汇聚单元，以及接收汇聚单元返回的用于授权终端设备的响应消息并发送给接入节点，该响应消息包括签名生成算法、采集时间点和该采集时间点对应的工作状态。

作为一种可选的实施方式，汇聚单元可以对终端设备指定采集数据的采集时间点，并在响应消息中将采集时间点一起发送给终端设备，以便终端设备能够设置其采集时间点。

进一步地，汇聚单元还将指定终端设备在采集时间点采集数据时的工作状态，本发明实施例提供的工作状态可以包括终端设备的工作状态可以包括休眠状态（终端设备未被激活，且无线网络也处于关闭状态）、激活状态且关闭无线网络、激活状态且开启无线网络。通常情况下，终端设备处于休眠状态，能够释放无线网络资源，也能够让终端设备得到休整，提高其使用寿命，而且在休眠状态下，终端设备对电池能量的消耗也比较小，从而能够提高电池的续航能力。在本发明实施例中，可以将终端设备的“激活状态且关闭无线网络”设置为采集数据时的工作状态。

作为一种可选的实施方式，过滤网关在将响应消息发送给接入节点之后，过滤网关实时监测该响应消息的签名生成算法的有效期，在该签名生成算法的有效期到达时，向汇聚单元发送请求消息，以请求有效的签名生成算法，并将请求到的有效的签名生成算法发送给接入节点。

303、接入节点将响应消息发送给终端设备。

其中，接入节点在接收汇聚单元下发的签名生成算法和采集时间点之后，将签名生成算法写入该终端设备。

作为一种可选的实施方式，接入节点还将在其无线网络覆盖范围内广播侦听消息，以实时侦听长时间不在线的终端设备，以实时更新路由表。

304、终端设备实时监控终端设备的系统时间，在监控到系统时间到达采集时间点时，将终端设备的工作状态切换至采集时间点对应的工作状态，并采集数据。

在本发明实施例中，终端设备在系统时间到达采集时间点时，将工作状态切换至采集时间点对应的工作状态，开始采集数据，直至采集完数据。终端设备在采集完数据后，将工作状态从采集时间点对应的工作状态切换至休眠状态，以再次进入休整、释放无线网络资源。

305、终端设备获取终端设备的设备ID号，以设备ID号为依据，基于签名生成算法生成签名加密信息，并根据签名加密信息对采集的数据进行签名，以获得数据报文，并将数据报文发送给接入节点，数据报文携带设备ID号。

306、接入节点将数据报文转发给过滤网关。

307、过滤网关从数据报文中获取设备ID号，以设备ID号为依据，基于内置的签名生成算法生成签名验证信息。

作为一种可选的实施方式，数据报文还携带有设备类型或者位置信息，过滤网关从数据报文中提取该设备类型或者位置信息，在确定出设备类型或者位置信息匹配汇聚单元感兴趣的设备类型或者位置信息时，进一步获取设备ID号，以设备ID号为依据，基于内置的签名生成算法生成签名验证信息，对签名进行验证。

308、过滤网关根据签名验证信息验证数据报文的签名是否正确。其中，在验证正确时，转向步骤308；在验证失败时，则丢弃该数据报文，结束流程。

309、过滤网关将数据报文转发给汇聚单元。

在本发明实施例中，汇聚单元指定终端设备用于生成签名加密信息的签名生成算法、采集数据的采集时间点、以及采集时间点对应的工作状态，终端设备在采集时间点到达时，切换到指定工作状态进行工作，然后以设备ID号为依据，基于签名生成算法生成签名加密信息，对采集到的数据进行签名，获得数据报文，然后上报到过滤网关，过滤网关以该设备ID号为依据，基于内置在过滤网关中的该签名生成算法生成签名验证信息，根据该签名验证信息验证数据报文中的签名是否正确，如果正确，将数据报文发送给汇聚单元。

可以看出，实施本发明实施例，过滤网关能够先一步对终端设备发送的数据报文进行签名验证，以过滤非授权终端设备发送的数据报文，以提高数据传输的安全性；进一步地，也能减轻汇聚单元的处理负担。

实施例三

请参阅图4，图4为本发明实施例公开的基于过滤网关的物联网数据过滤系统的结构示意图；如图4所示，一种基于过滤网关的物联网数据过滤系统可包括：

终端设备 410，用于通过接入节点 420 向过滤网关 430 发送授权请求，授权请求携带终端设备 410 的设备身份标识 ID 号、设备类型和互联网协议地址 IP；

过滤网关 430，用于将授权请求发送给汇聚单元 440，以及接收汇聚单元 440 返回的用于授权终端设备 410 的响应消息并发送给接入节点 420，响应消息包括签名生成算法和采集时间点；

接入节点 420，用于将响应消息发送给终端设备 410；

终端设备 410 还用于在采集时间点到达时采集数据，获取终端设备 410 的设备 ID 号，以设备 ID 号为依据，基于签名生成算法生成签名加密信息，并根据签名加密信息对采集的数据进行签名，以获得数据报文，并将数据报文发送给接入节点 420，数据报文携带设备 ID 号；

接入节点 420 还用于将数据报文转发给过滤网关 430；

过滤网关 430 还用于从数据报文中获取设备 ID 号，以设备 ID 号为依据，基于内置的签名生成算法生成签名验证信息；

过滤网关 430 还用于根据签名验证信息验证数据报文的签名是否正确；

过滤网关 430 还用于在验证数据报文的签名正确时，将数据报文转发给汇聚单元 440。

作为一种可选的实施方式，终端设备 410 在首次开启并接入无线网络时或者在重新启动后或者在授权内容（包括下面的签名生成算法有效期到达后），终端设备 410 可以向汇聚单元 440 发送授权请求，以获得授权。

作为一种可选的实施方式，接入节点 420 在其无线网络覆盖范围内实时侦听，在侦听到新的终端设备 410 接入时，触发该终端设备 410 发送授权请

求。

进一步地，接入节点 420 在其无线网络覆盖范围内实时广播侦听消息，其无线网络覆盖范围内的终端设备 410 在接收到侦听消息时，对该侦听消息进行响应，以发送响应消息，该响应消息携带设备类型、设备 ID 号和 IP 地址等，接入节点 420 在接收到响应消息后，根据设备 ID 号或者 IP 地址等确定有新的终端设备接入。通过该实施方式，能够实现终端设备 410 在接入网络时发送授权请求。

作为一种可选的实施方式，过滤网关 430 用于将授权请求发送给汇聚单元 440，以及接收汇聚单元 440 返回的用于授权终端设备 410 的响应消息并发送给接入节点 420 的方式具体为：

过滤网关 430 用于将授权请求发送给汇聚单元 440，以及接收汇聚单元 440 在确定授权请求携带的设备类型属于其感兴趣的设备类型时、返回的用于授权终端设备 410 的响应消息，并将响应消息发送给接入节点 420。

汇聚单元 440 在接收到授权请求时，从授权请求中提取该终端设备 410 的设备类型，判断该设备类型是否为自己感兴趣的设备类型，如果是自己感兴趣的设备类型时，进一步对其设备 ID 号和 ID 地址进行确认，在确认后，返回响应消息。在该实施方式中，汇聚单元 440 可以针对其感兴趣的终端设备 410 进行设置，以提供这些设备用于传输数据时的签名生成算法，提高数据传输的安全性。

作为一种可选的实施方式，接入节点 420 用于将响应消息发送给终端设备 410 的方式具体为：

接入节点 420 用于将响应消息的签名生成算法和采集时间点，写入终端设备 410。

作为一种可选的实施方式，接入节点 420 在将响应消息发送给终端设备 410 后，实时监控响应消息中的签名生成算法的有效期，在签名生成算法的有效期到达时，将通知终端设备 410，以触发终端设备 410 再次向汇聚单元 440 发送授权请求，以获得再次授权。通过该实施方式，实现在签名生成算法有效期到达后，再次触发终端设备 410 去获取授权。

作为一种可选的实施方式，接入节点 420 还用于将数据报文转发给过滤

网关 430 的方式具体为：

接入节点 420 还用于通过跳频方式从目标传输频段中确定用于发送数据报文的物理资源块的频域位置，在确定的物理资源块的频域位置所对应的时频资源上，向过滤网关 430 发送数据报文。

作为一种可选的实施方式，上述响应消息还包括采集时间点对应的工作状态，终端设备 410 还用于在采集时间点到达时采集数据的方式具体为：

终端设备 410 还用于实时监控终端设备 410 的系统时间，在监控到系统时间到达采集时间点时，将终端设备 410 的工作状态切换至采集时间点对应的工作状态，并采集数据。

作为一种可选的实施方式，过滤网关 430 在将响应消息发送给接入节点 420 之后，过滤网关 430 实时监测该响应消息的签名生成算法的有效期，在该签名生成算法的有效期到达时，向汇聚单元 440 发送请求消息，以请求有效的签名生成算法，并将请求到的有效的签名生成算法发送给接入节点 420。

实施上述实施方式，过滤网关 430 能够先一步对终端设备 410 发送的数据报文进行签名验证，以过滤非授权终端设备发送的数据报文，以提高数据传输的安全性；进一步地，也能减轻汇聚单元 440 的处理负担。

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，存储介质包括只读存储器（Read-Only Memory, ROM）、随机存储器（Random Access Memory, RAM）、可编程只读存储器（Programmable Read-only Memory, PROM）、可擦除可编程只读存储器（Erasable Programmable Read Only Memory, EPROM）、一次可编程只读存储器（One-time Programmable Read-Only Memory, OTPROM）、电子抹除式可复写只读存储器（Electrically-Erasable Programmable Read-Only Memory, EEPROM）、只读光盘（Compact Disc Read-Only Memory, CD-ROM）或其他光盘存储器、磁盘存储器、磁带存储器、或者能够用于携带或存储数据的计算机可读的任何其他介质。

以上对本发明实施例公开的一种基于过滤网关的物联网数据过滤方法及系统进行了详细介绍，本文中应用了具体个例对本发明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发明的方法及其核心思想;同时,对于本领域的一般技术人员,依据本发明的思想,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发明的限制。

权 利 要 求 书

1、一种基于过滤网关的物联网数据过滤方法，其特征在于，包括：

终端设备通过接入节点向过滤网关发送授权请求，所述授权请求携带所述终端设备的设备身份标识 ID 号、设备类型和互联网协议地址 IP；

所述过滤网关将所述授权请求发送给所述汇聚单元，以及接收所述汇聚单元返回的用于授权所述终端设备的响应消息并发送给所述接入节点，所述响应消息包括所述签名生成算法和采集时间点；

所述接入节点将所述响应消息发送给所述终端设备；

所述终端设备在所述采集时间点到达时采集数据，获取所述终端设备的设备 ID 号，以所述设备 ID 号为依据，基于所述签名生成算法生成签名加密信息，并根据所述签名加密信息对采集的数据进行签名，以获得数据报文，并将所述数据报文发送给接入节点，所述数据报文携带所述设备 ID 号；

所述接入节点将所述数据报文转发给所述过滤网关；

所述过滤网关从所述数据报文中获取所述设备 ID 号，以所述设备 ID 号为依据，基于内置的所述签名生成算法生成签名验证信息；

所述过滤网关根据所述签名验证信息验证所述数据报文的签名是否正确；

所述过滤网关在验证所述数据报文的签名正确时，将所述数据报文转发给所述汇聚单元。

2、根据权利要求 1 所述的方法，其特征在于，所述过滤网关将所述授权请求发送给所述汇聚单元，以及接收所述汇聚单元返回的用于授权所述终端设备的响应消息并发送给所述接入节点，包括：

所述过滤网关将所述授权请求发送给所述汇聚单元，以及接收所述汇聚单元在确定所述授权请求携带的设备类型属于其感兴趣的设备类型时、返回的用于授权所述终端设备的响应消息，并将所述响应消息发送给所述接入节点。

3、根据权利要求 1 所述的方法，其特征在于，所述接入节点将所述响应消息发送给所述终端设备包括：

所述接入节点将所述响应消息的所述签名生成算法和所述采集时间点，写入所述终端设备。

4、根据权利要求 1~3 任一项所述的方法，其特征在于，所述接入节点将所述数据报文转发给所述过滤网关包括：

所述接入节点通过跳频方式从目标传输频段中确定用于发送所述数据报文的物理资源块的频域位置；

所述接入节点在确定的物理资源块的频域位置所对应的时频资源上，向所述过滤网关发送所述数据报文。

5、根据权利要求 1 所述的方法，其特征在于，所述响应消息还包括所述采集时间点对应的工作状态，所述终端设备在所述采集时间点到达时采集数据，包括：

所述终端设备实时监控所述终端设备的系统时间，在监控到所述系统时间到达所述采集时间点时，将所述终端设备的工作状态切换至所述采集时间点对应的工作状态，并采集数据。

6、一种基于过滤网关的物联网数据过滤系统，其特征在于，包括：

终端设备，用于通过接入节点向过滤网关发送授权请求，所述授权请求携带所述终端设备的设备身份标识 ID 号、设备类型和互联网协议地址 IP；

所述过滤网关，用于将所述授权请求发送给所述汇聚单元，以及接收所述汇聚单元返回的用于授权所述终端设备的响应消息并发送给所述接入节点，所述响应消息包括所述签名生成算法和采集时间点；

所述接入节点，用于将所述响应消息发送给所述终端设备；

所述终端设备还用于在所述采集时间点到达时采集数据，获取所述终端设备的设备 ID 号，以所述设备 ID 号为依据，基于所述签名生成算法生成签名加密信息，并根据所述签名加密信息对采集的数据进行签名，以获得数据报文，并将所述数据报文发送给接入节点，所述数据报文携带所述设备 ID 号；

所述接入节点还用于将所述数据报文转发给所述过滤网关；

所述过滤网关还用于从所述数据报文中获取所述设备 ID 号，以所述设备 ID 号为依据，基于内置的所述签名生成算法生成签名验证信息；

所述过滤网关还用于根据所述签名验证信息验证所述数据报文的签名是否正确；

所述过滤网关还用于在验证所述数据报文的签名正确时，将所述数据报文转发给所述汇聚单元。

7、根据权利要求6所述的系统，其特征在于，所述过滤网关用于将所述授权请求发送给所述汇聚单元，以及接收所述汇聚单元返回的用于授权所述终端设备的响应消息并发送给所述接入节点的方式具体为：

所述过滤网关用于将所述授权请求发送给所述汇聚单元，以及接收所述汇聚单元在确定所述授权请求携带的设备类型属于其感兴趣的设备类型时、返回的用于授权所述终端设备的响应消息，并将所述响应消息发送给所述接入节点。

8、根据权利要求6所述的系统，其特征在于，所述接入节点用于将所述响应消息发送给所述终端设备的方式具体为：

所述接入节点用于将所述响应消息的所述签名生成算法和所述采集时间点，写入所述终端设备。

9、根据权利要求6~8任一项所述的系统，其特征在于，所述接入节点还用于将所述数据报文转发给所述过滤网关的方式具体为：

所述接入节点还用于通过跳频方式从目标传输频段中确定用于发送所述数据报文的物理资源块的频域位置，在确定的物理资源块的频域位置所对应的时频资源上，向所述过滤网关发送所述数据报文。

10、根据权利要求6所述的系统，其特征在于，所述响应消息还包括所述采集时间点对应的工作状态，所述终端设备还用于在所述采集时间点到达时采集数据的方式具体为：

所述终端设备还用于实时监控所述终端设备的系统时间，在监控到所述系统时间到达所述采集时间点时，将所述终端设备的工作状态切换至所述采集时间点对应的工作状态，并采集数据。

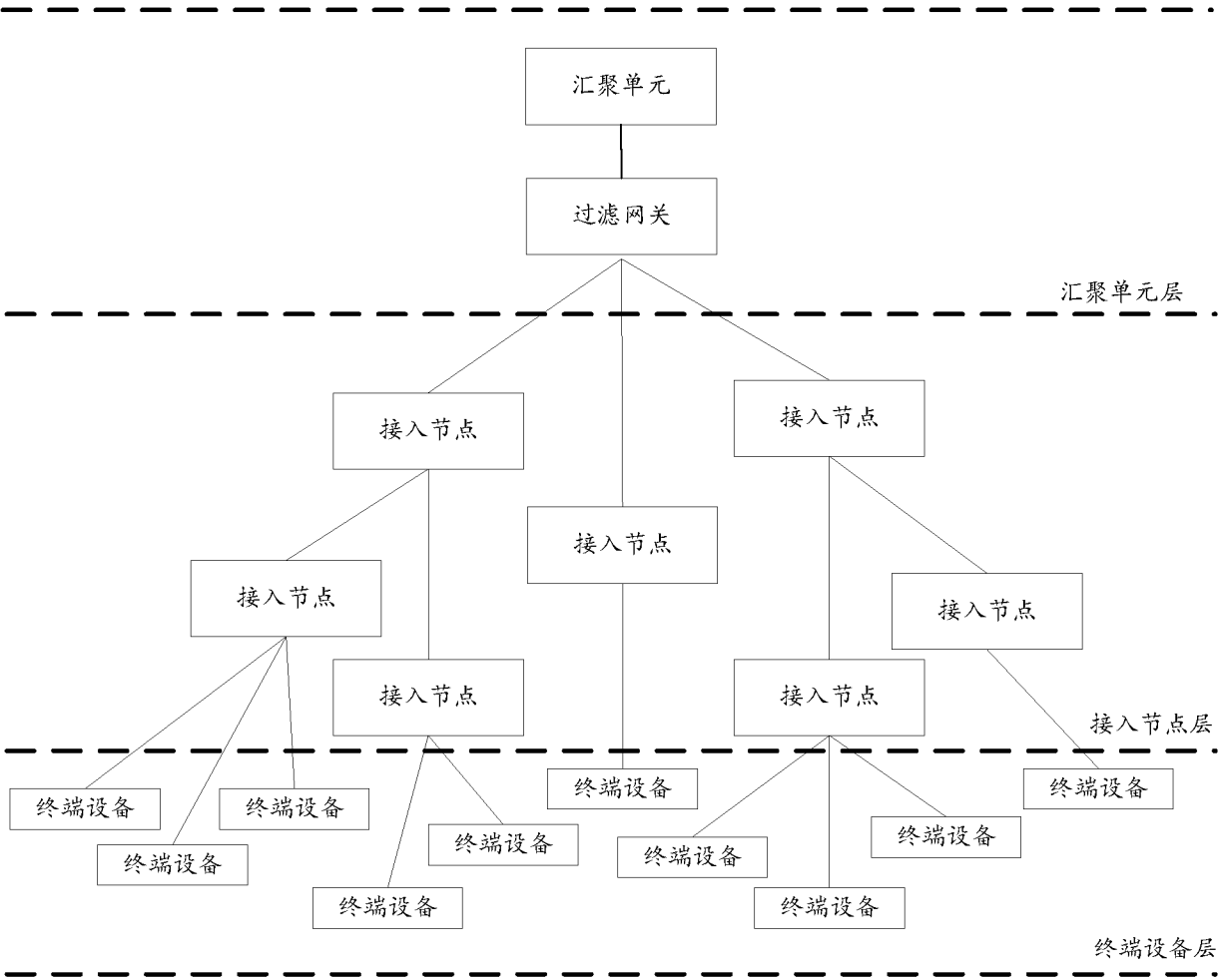


图 1

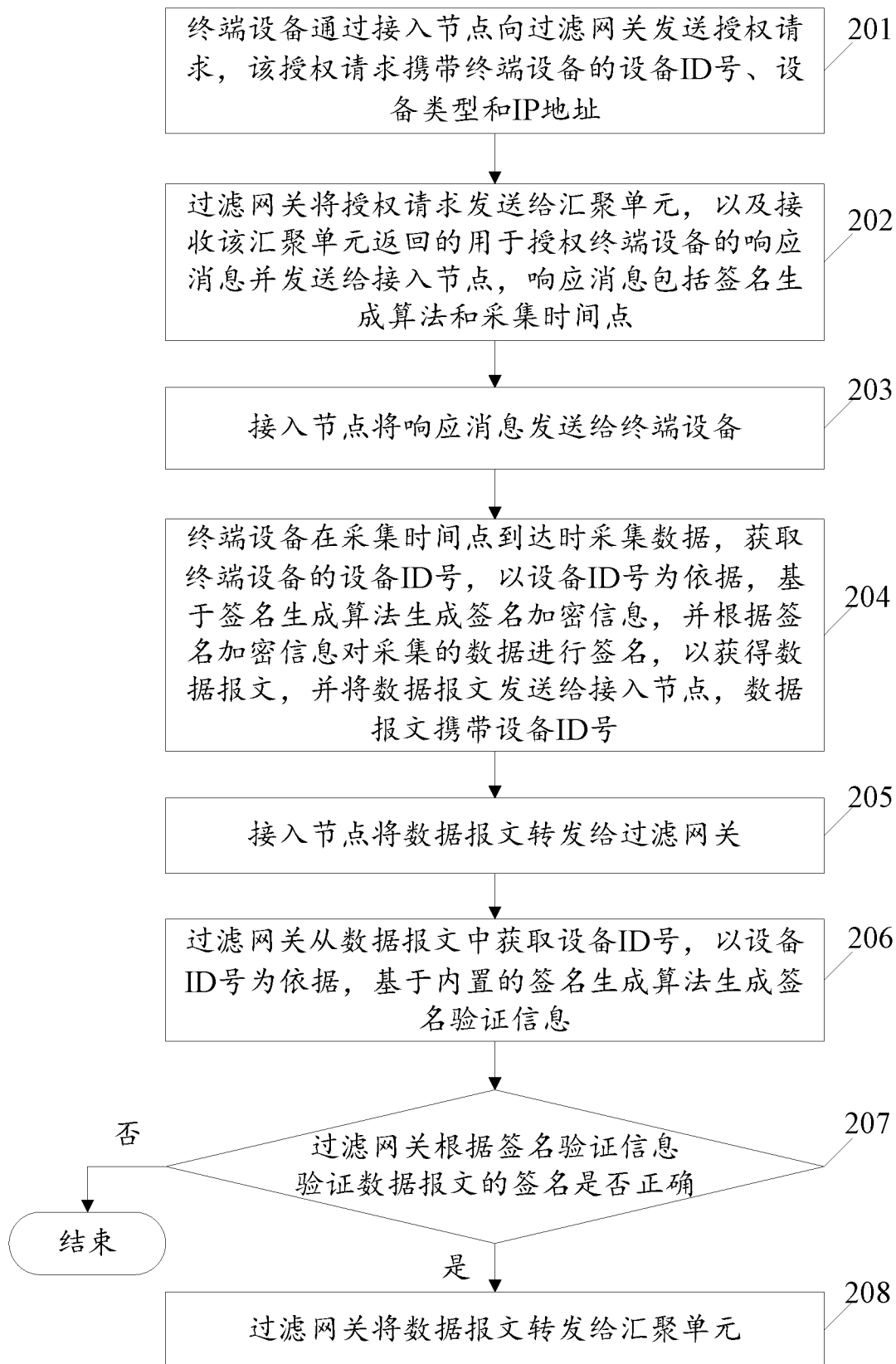


图 2

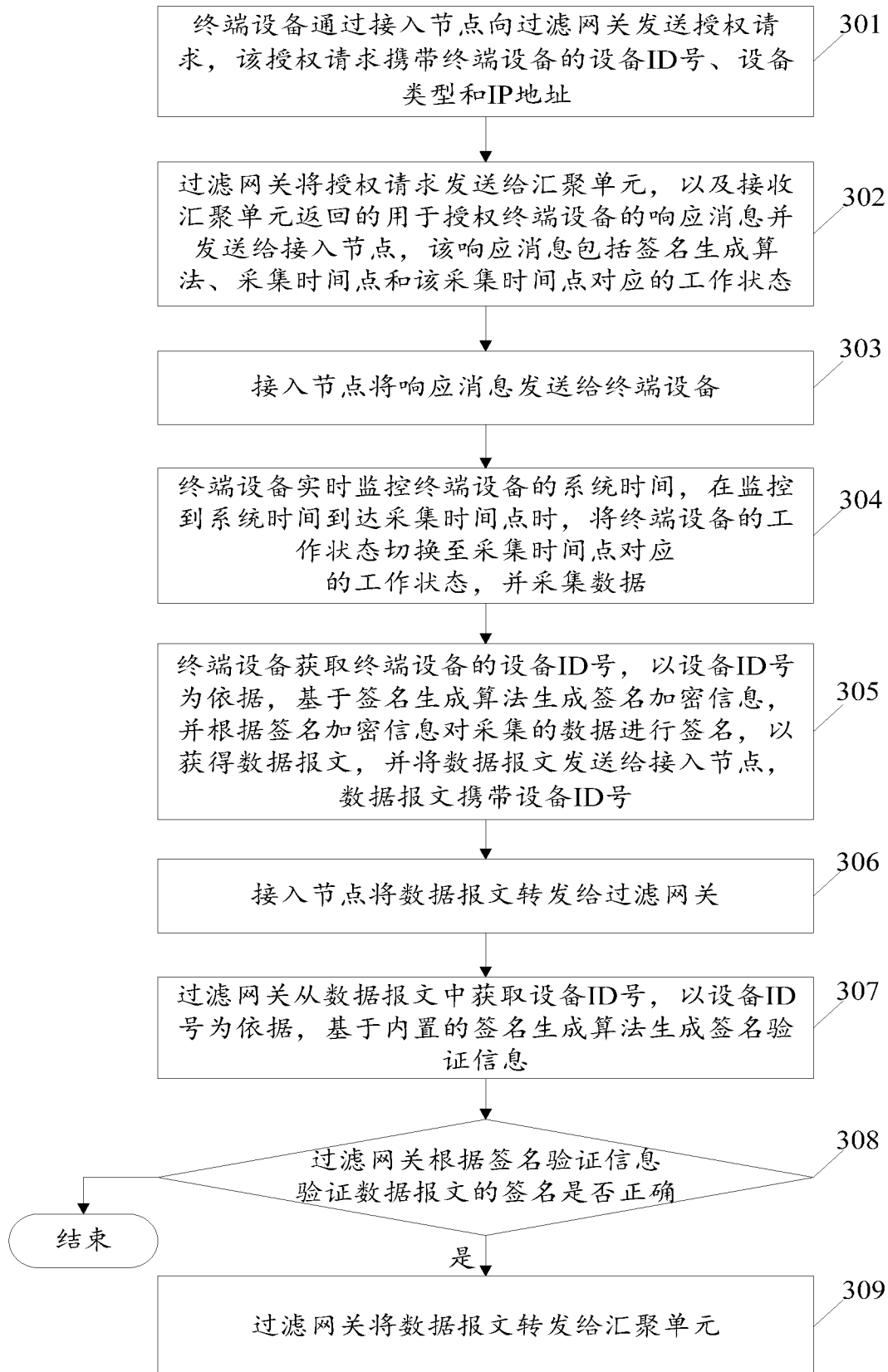


图 3

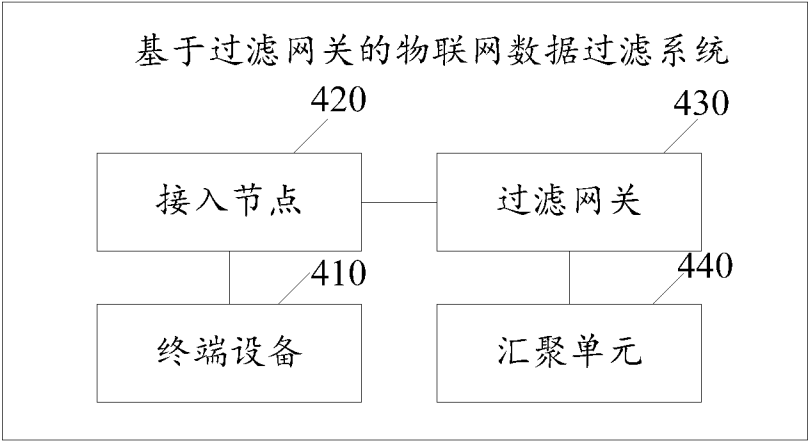


图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/100007

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08 (2006.01) i; H04L 12/66 (2006.01) i; H04L 29/06 (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, H04W

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)

CNABS, VEN, CNKI: 物联网, 传感器, 请求, 签名, 密钥, 验证, 授权, 鉴权, 时间, 认证, 采集, 安全, internet of things, sensor, request, signature, key, authenticat+, verif+, time, collect+, security, secure

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103401687 A (GUANGZHOU UNIVERSITY) 20 November 2013 (20.11.2013), description, paragraphs [0041]-[0062]	1-10
A	CN 103945378 A (ZTE CORPORATION) 23 July 2014 (23.07.2014), entire document	1-10
A	CN 101895888 A (CHINA MOBILE COMMUNICATION GROUP CHONGQIN CO., LTD.) 24 November 2010 (24.11.2010), entire document	1-10
A	CN 106793005 A (SHENZHEN WINEXT TECHNOLOGY CO., LTD.) 31 May 2017 (31.05.2017), entire document	1-10
A	KR 20130005726 A (NAT UNIV CHONBUK IND COOP FOUN) 16 January 2013 (16.01.2013), the abstract	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 06 March 2018	Date of mailing of the international search report 12 March 2018
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer PENG, Yuan Telephone No. (86-10) 62411268

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/CN2017/100007

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103401687 A	20 November 2013	CN 103401687 B	28 December 2016
CN 103945378 A	23 July 2014	WO 2013167070 A2	14 November 2013
		WO 2013167070 A3	03 January 2014
CN 101895888 A	24 November 2010	None	
CN 106793005 A	31 May 2017	None	
KR 20130005726 A	16 January 2013	KR 101238637 B1	04 March 2013

国际检索报告

国际申请号

PCT/CN2017/100007

A. 主题的分类

H04L 9/08(2006.01)i; H04L 12/66(2006.01)i; H04L 29/06(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, H04W

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))

CNABS, VEN, CNKI:物联网, 传感器, 请求, 签名, 密钥, 验证, 授权, 鉴权, 时间, 认证, 采集, 安全, internet of things, sensor, request, signature, key, authenticat+, verif+, time, collect+, security, secure

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 103401687 A (广州大学) 2013年 11月 20日 (2013 - 11 - 20) 说明书第[0041]-[0062]段	1-10
A	CN 103945378 A (中兴通讯股份有限公司) 2014年 7月 23日 (2014 - 07 - 23) 全文	1-10
A	CN 101895888 A (中国移动通信集团重庆有限公司) 2010年 11月 24日 (2010 - 11 - 24) 全文	1-10
A	CN 106793005 A (深圳市唯传科技有限公司) 2017年 5月 31日 (2017 - 05 - 31) 全文	1-10
A	KR 20130005726 A (NAT UNIV CHONBUK IND COOP FOUN) 2013年 1月 16日 (2013 - 01 - 16) 摘要	1-10

☐ 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

2018年 3月 6日

国际检索报告邮寄日期

2018年 3月 12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

彭媛

电话号码 (86-10)62411268

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/100007

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	103401687	A	2013年 11月 20日	CN	103401687	B	2016年 12月 28日
CN	103945378	A	2014年 7月 23日	WO	2013167070	A2	2013年 11月 14日
				WO	2013167070	A3	2014年 1月 3日
CN	101895888	A	2010年 11月 24日	无			
CN	106793005	A	2017年 5月 31日	无			
KR	20130005726	A	2013年 1月 16日	KR	101238637	B1	2013年 3月 4日

表 PCT/ISA/210 (同族专利附件) (2009年7月)