

(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
2020 年 3 月 5 日 (05.03.2020)



(10) 国际公布号
WO 2020/043098 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2019/102852

(22) 国际申请日: 2019 年 8 月 27 日 (27.08.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810996397.2 2018年8月29日 (29.08.2018) CN

(71) 申请人: 新华三技术有限公司 (NEW H3C TECHNOLOGIES CO., LTD.) [CN/CN]; 中国浙江省杭州市滨江区长河路 466 号, Zhejiang 310052 (CN)。

(72) 发明人: 赵赞 (ZHAO, Yun); 中国北京市朝阳区广顺南大街8号院1号楼利星行中心A座640室, Beijing 100102 (CN)。 张友和 (ZHANG, Youhe); 中国北京市朝阳区广顺南大街8号院1号楼利星行中心A座640室, Beijing 100102 (CN)。

(74) 代理人: 北京柏杉松知识产权代理事务所 (普通合伙) (PATENTSINO IP FIRM); 中国北京市西城区北三环中路 27 号 商 房 大 厦 413 室, Beijing 100029 (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: DEVICE ENTRY ESTABLISHMENT

(54) 发明名称: 建立设备表项

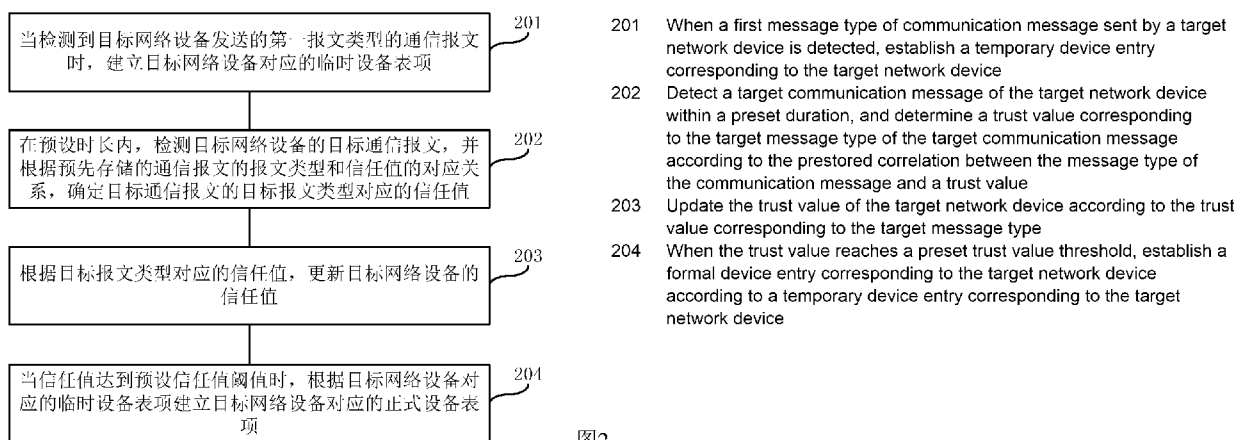


图2

(57) Abstract: When an AP detects a first message type of communication message sent by a target network device, establishing a temporary device entry corresponding to the target network device; detecting a target communication message of the target network device within a preset duration, and determining a trust value corresponding to the target message type of the target communication message according to the prestored correlation between the message type of the communication message and a trust value; updating the trust value of the target network device according to the trust value corresponding to the target message type; and when the trust value reaches a preset trust value threshold, establishing a formal device entry corresponding to the target network device according to a temporary device entry corresponding to the target network device. By means of the present application, the accuracy of a learning device can be improved.

(57) 摘要: 当AP检测到目标网络设备发送的第一报文类型的通信报文时, 建立所述目标网络设备对应的临时设备表项; 在预设时长内, 检测所述目标网络设备的目标通信报文, 并根据预先存储的通信报文的报文类型和信任值的对应关系, 确定所述目标通信报文的目标报文类型对应的信任值; 根据所述目标报文类型对应的信任值, 更新所述目标网络设备的信任值; 当所述信任值达到预设信任值阈值时, 根据所述目标网络设备对应的临时设备表项建立所述目标网络设备对应的正式设备表项。采用本申请可以提高学习设备的准确度。

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))。

建立设备表项

相关申请的交叉引用

本申请要求于 2018 年 8 月 29 日提交中国专利局、申请号为 201810996397.2 发明名称为“一种建立设备表项的方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

背景技术

随着通信技术的发展，无线通信网络的应用越来越广泛。为了提高无线通信网络的安全性，人们需要对无线通信网络中的网络设备进行监测，以识别无线通信网络中是否存在恶意设备，并在识别出非法设备时，对非法设备进行反制处理，从而防止非法设备入侵无线通信网络。

无线通信网络通常包括接入控制器（英文：Access Controller，简称：AC）、接入点（英文：Access Point，简称：AP）和用户终端。AP可以是启用无线入侵防护系统（英文：Wireless Intrusion Prevention System，简称：WIPS）功能的AP，基于WIPS，该AP可以扫描其扫描射频范围内的各网络设备发送和接收的报文，进而根据扫描到的报文，判断网络设备是否为恶意设备。具体的处理过程为：针对未启用WIPS功能的AP，当检测到该AP发送的beacon报文和probe response报文时，判定该AP为合法AP，然后建立该AP对应的设备表项，该设备表项中可以存储有该AP的媒体访问控制（英文：Media Access Control，简称：MAC）地址、信号强度、服务集标识（英文：Service Set Identifier，简称：SSID）等信息，如果未检测到该AP发送的beacon报文或probe response（探测响应）报文，不建立该AP对应的设备表项；针对用户终端，当检测到该用户终端发送的probe request（探测请求）报文和数据报文时，建立该用户终端对应的设备表项，该设备表项中可以存储有该用户终端的媒体访问控制（英文：Media Access Control，简称：MAC）地址、信号强度、与其他网络设备的关联关系等信息，如果未检测到该用户终端发送的probe request报文或数据报文，则不建立该用户终端对应的表项。

附图简要说明

图 1 为本申请实施例提供的系统框架图；

-2-

图 2 为本申请实施例提供的一种建立设备表项的方法的流程图；

图 3 为本申请实施例提供的一种建立设备表项的方法示例的流程图；

图 4 为本申请实施例提供的又一种建立设备表项的方法示例的流程图；

图 5 为本申请实施例提供的建立设备表项的装置的结构示意图；

5 图 6 为本申请实施例提供的建立设备表项的装置的结构示意图；

图 7 为本申请实施例提供的建立设备表项的装置的结构示意图；

图 8 为本申请实施例提供的建立设备表项的装置的结构示意图；

图 9 为本申请实施例提供的 AP 的结构示意图。

具体实施方式

10 为使本申请的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本申请作进一步详细的说明。

在现有技术中，部分非法设备会采用变源报文攻击的方式进行网络攻击，例如，某非法用户终端会通过不同的源MAC地址发送大量的probe request报文和数据报文，AC则会确定该用户终端为合法用户终端。由于各报文携带的
15 MAC地址不同，因此AC会认为存在多个合法用户终端，建立多个无效的设备表项。因此，相关技术中，启用WIPS功能的AP学习设备的准确度较低。

本申请实施例提供了一种建立设备表项的方法，该方法可以应用于无线网络中的AP。无线网络中通常还包括AC以及通过AP接入网络的用户终端。其中，该方法所应用的AP可以是启用WIPS功能的AP。技术人员可
20 可以根据无线网络中各AP的覆盖范围，选择若干个AP，并通过AC向这些AP下发启动WIPS功能的配置信息，使其成为监测设备。为了便于区分，本申请实施例中将启用WIPS功能的AP称为监测设备。AC与多个AP、以及多个监测设备连接，其中，每个AP对应一个预先分配的信道，终端可以接入某AP，并通过该AP的信道访问网络。如图1所示，为本申请实施例提供的系统框架图，
25 包括AC、多个AP、多个监测设备和多个终端。其中，AC连接AP1、AP2、监测设备1和监测设备2；终端1和终端2通过AP1接入至无线网络中，终端3和终端4通过AP2接入至无线网络中。

—3—

本方案提供的建立设备表项的方法，可以应用于上述监测设备中。当监测设备检测到目标网络设备发送的第一报文类型的通信报文时，监测设备可以建立目标网络设备对应的临时设备表项，然后在预设时长内，继续检测目标网络设备的目标通信报文，并根据预先存储的通信报文的报文类型和信任值的对应关系，确定目标通信报文的目标报文类型对应的信任值，进而根据目标报文类型对应的信任值，更新目标网络设备的信任值。只有当信任值达到预设信任值阈值时，监测设备才会根据目标网络设备对应的临时设备表项建立目标网络设备对应的正式设备表项。由于在变源报文攻击的方式中，非法网络设备通常不会进行正常的业务流程，发送的通信报文的种类比较单一，因此，本方案能够有效的识别出合法网络设备，并且只针对合法网络设备建立正式设备表项，提高了监测设备学习设备的准确度。

可选的，技术人员可以在AC中预先配置本方案所提供的建立设备表项的策略，AC将这些策略下发给监测设备，以使各监测设备能够实现本申请实施例提出的建立设备表项的方法。

下面将结合具体实施方式，对本申请实施例提供的一种建立设备表项的方法进行详细的说明，如图2所示，具体步骤如下：

步骤201，当检测到目标网络设备发送的第一报文类型的通信报文时，建立目标网络设备对应的临时设备表项。

在本申请实施例中，监测设备可以监测其射频范围之内的各网络设备发送和接收的报文。例如，针对AP，监测设备可以监测到该AP发送的beacon报文、probe response报文（即探测响应报文）、以及该AP向用户终端发送的数据报文（即AP数据报文）等；针对用户终端，监测设备可以监测到该用户终端发送的probe request（探测请求）报文、关联请求报文和该用户终端向AP发送的数据报文（即用户数据报文）等。

另外，监测设备还可以获取其监测范围内的各网络设备的设备信息，设备信息至少包括网络设备的设备标识和所占信道。其中，设备标识可以是MAC地址。设备信息还可以包括设备关联信息、网络设备的信号强度、以及网络设备发送通信报文的频率等信息。设备关联信息可以包括该网络设备接入的AP的标识、以及该网络设备发送的通信报文中的目的地址等。针对AP，设

备关联信息还可以包括 SSID 等信息。

当监测设备检测到某网络设备（即目标网络设备）发送的特定类型（即第一报文类型）的通信报文时，该监测设备可以判断本地是否已建立该目标网络设备对应的设备表项，如果未建立该目标网络设备对应的设备表项（该设备表项包括临时设备表项和正式设备表项），则建立该目标网络设备对应的临时设备表项。其中，临时设备表项中可以包括目标网络设备的MAC地址、信号强度、所占信道等信息。当目标网络设备为未启用WIPS功能的AP时，临时设备表项中还可以包括SSID；当目标网络设备为用户终端时，临时设备表项中还可以包括设备关联信息。

另外，如果本地已建立该目标网络设备对应的正式设备表项，则监测设备不进行后续处理；如果本地未建立该目标网络设备对应的临时设备表项，则可以按照步骤 202 的处理过程，更新目标网络设备对应的信任值，具体的处理过程后续会进行详细说明。

可选的，当目标网络设备为未启用WIPS功能的AP时，第一报文类型可以为beacon报文类型；当目标网络设备为用户终端时，第一报文类型可以为探测请求报文类型。

步骤202，在预设时长内，检测目标网络设备的目标通信报文，并根据预先存储的通信报文的报文类型和信任值的对应关系，确定目标通信报文的目标报文类型对应的信任值。

在本申请实施例中，监测设备中可以预先存储有通信报文的报文类型和信任值的对应关系，该对应关系可以由技术人员进行设置，该对应关系可以以对应关系表的形式进行存储。其中，针对不同类型的网络设备，设置的对应关系的内容可以是不同的。

在一种可能的实现方式中，当目标网络设备为未启用WIPS功能的AP时，该对应关系中的报文类型包括beacon报文类型、探测响应报文（即probe response报文）类型、认证响应报文（即authentication response报文）类型、关联响应报文（即association response报文）类型、用户数据报文类型和AP数据报文类型中的一种或多种。

-5-

其中，不同报文类型对应的信任值可以是不同的，例如，beacon报文是AP周期性广播的报文，beacon报文类型可以对应较小的信任值，比如2；probe response报文是AP在接收到用户终端发送的probe request报文后发送的，而AP响应probe request报文属于AP通常具备的业务功能，因此，probe response报文类型可以对应较大的信任值，比如20；同理，authentication response报文类型和association response报文类型也可以对应较大的信任值，比如20。AP数据报文对于识别非法AP的有效度较低，AP数据报文类型可以对应较低信任值，比如10；同理，对于AP来说，用户数据报文对于识别非法AP的有效度也较低，用户数据报文类型对应的信任值可以低于AP数据报文类型对应的信任值，比如5。

在一种可能的实现方式中，当目标网络设备为用户终端时，该对应关系中的报文类型包括探测请求报文（即probe request报文）类型、认证响应报文（即authentication response报文）类型、关联响应报文（即association response报文）类型、认证请求报文（即authentication request报文）类型、关联请求报文（即association request报文）类型、用户数据报文类型、AP数据报文类型中的一种或多种。

其中，不同报文类型对应的信任值可以是不同的，例如，probe request报文是用户终端周期性广播的报文，probe request报文类型可以对应较小的信任值，比如2；authentication request报文、association request报文和用户数据报文，是用户终端发送的用于进行业务的报文，可以对应较大的信任值，比如10。authentication response报文、association response报文和AP数据报文是AP响应该用户终端的报文，由于AP具有一定的识别能力，并且，AP通常只针对合法用户终端进行响应，因此，这三种类型的报文对应的信任值可以较大，比如20。

监测设备建立目标网络设备对应的临时设备表项之后，可以启动计时器开始计时，并且，可以继续检测目标网络设备的通信报文。当检测到目标网络设备接收或发送的通信报文（即目标通信报文）时，监测设备可以根据目标网络设备的设备类型，查询相应的对应关系表，进而确定目标通信报文的目标报文类型对应的信任值。其中，如果该对应关系表中不存在目标报文类型，则可以认为目标报文类型对应的信任值为0，即不更新目标网络设备对应

的信任值。

步骤203, 根据目标报文类型对应的信任值, 更新目标网络设备的信任值。

在本申请实施例中, 监测设备中可以预先存储有网络设备的信任值的更新策略, 该更新策略可以由技术人员进行设置。

- 5 在一种可能的实现方式中, 由于第一报文类型是AP或用户终端周期性发送的报文, 因此, 针对第一报文类型, 可以多次增加目标网络设备的信任值, 而对于其他报文类型, 可以仅增加一次目标网络设备的信任值, 具体的处理过程可以如下: 判断目标报文类型是否为第一报文类型; 如果目标报文类型为第一报文类型, 则获取上一次根据第一报文类型对应的信任值更新目标网络设备的信任值的更新时间; 如果更新时间与当前时间的时间间隔超过预设时长阈值, 则执行根据目标报文类型对应的信任值, 更新目标网络设备的信任值步骤; 如果目标报文类型不为第一报文类型, 则判断在检测到目标通信报文之前, 是否已根据目标报文类型更新目标网络设备的信任值; 如果未根据目标报文类型根据目标网络设备的信任值, 则执行根据目标报文类型对应的信任值, 更新目标网络设备的信任值步骤。
- 10
- 15

在本申请实施例中, 针对目标AP, 监测设备可以判断目标报文类型是否为beacon报文类型, 如果目标报文类型为beacon报文类型, 则获取上一次根据beacon报文的信任值更新目标AP的信任值的更新时间, 进而判断该更新时间与当前时间的的时间间隔是否超过预设时长阈值。如果更新时间与当前时间的的时间间隔超过预设时长阈值, 则执行步骤203; 如果更新时间与当前时间的的时间间隔未超过预设时长阈值, 则不更新目标AP的信任值。

20

如果目标报文类型不为beacon报文类型, 则监测设备判断在检测到目标通信报文之前, 是否已根据目标报文类型更新目标AP的信任值。如果未根据目标报文类型根据目标AP的信任值, 则执行步骤203; 如果已根据目标报文类型根据目标AP的信任值, 则不更新目标AP的信任值。

25

针对目标用户终端, 监测设备可以判断目标报文类型是否为探测请求报文类型。如果目标报文类型为探测请求报文类型, 则获取上一次根据探测请求报文的信任值更新目标用户终端的信任值的更新时间, 然后判断该更新时

-7-

间与当前时间的时间间隔是否超过预设时长阈值。如果更新时间与当前时间的
时间间隔超过预设时长阈值，则执行步骤203；如果更新时间与当前时间的
时间间隔未超过预设时长阈值，则不更新目标用户终端的信任值。

5 如果目标报文类型不为探测请求报文类型，则判断在检测到目标通信报
文之前，是否已根据目标报文类型更新目标用户终端的信任值。如果未根据
目标报文类型根据目标用户终端的信任值，则执行步骤203；如果已根据目标
报文类型根据目标用户终端的信任值，则不更新目标用户终端的信任值。

10 可选的，目标网络设备对应的信任值的计算方式具体可以如下：在建立
目标网络设备对应的临时设备表项之后，将预设初始值作为目标网络设备当
前的信任值；监测设备确定目标报文类型对应的信任值后，计算目标通信报
文的报文类型对应的信任值与目标网络设备当前的信任值的和值，将目标网
络设备的信任值更新为和值。

15 在本申请实施例中，监测设备在建立目标网络设备对应的临时设备表项
之后，将预设初始值作为目标网络设备当前的信任值；当监测设备更新目标
网络设备对应的信任值时，监测设备可以计算目标通信报文的报文类型对应
的信任值与该目标网络设备当前的信任值的和值，然后将目标网络设备的信
任值更新为和值。

20 例如，目标网络设备为AP，当检测到该AP发送的beacon报文时，建立该
AP对应的临时设备表项，并设置该AP当前的信任值为初始值10；然后，检测
到该AP发送的probe response报文，确定probe response报文类型对应的信任值
为20，则该AP的信任值更新为 $10+20=30$ ；之后，检测到该AP发送的
authentication response报文，确定authentication response报文类型对应的信任值
为20，则该AP的信任值更新为 $30+20=50$ ；另外，在建立该AP对应的临时设备
表项后，监测设备每达到预设时间间隔后检测到该AP发送的beacon报文时，
25 可以将该AP的信任值加2，比如，该AP当前的信任值为50，且已达到预设时
间间隔5s，则检测到该AP发送的beacon报文后，将信任值更新为 $50+2=52$ 。

又如，目标网络设备为用户终端，当检测到该用户终端发送的probe
request报文时，建立该用户终端对应的临时设备表项，并设置该用户终端当前
的信任值为初始值10；然后，检测到该用户终端发送的authentication request

—8—

报文，确定authentication request报文类型对应的信任值为10，则该用户终端的信任值更新为 $10+10=20$ ；之后，检测到AP向该用户终端发送的authentication response报文，确定authentication response报文类型对应的信任值为20，则该用户终端的信任值更新为 $20+20=40$ ；同时，建立该用户终端对应的临时设备表项后，监测设备每达到预设时间间隔后检测到该用户终端发送的probe request报文时，可以将该用户终端的信任值加2，比如，该用户终端当前的信任值为40，且已达到预设时间间隔5s，则检测到该用户终端发送的probe request报文后，将信任值更新为 $40+2=42$ 。

步骤204，当信任值达到预设信任值阈值时，根据目标网络设备对应的临时设备表项建立目标网络设备对应的正式设备表项。

在本申请实施例中，如果在预设时长内，监测设备判定目标网络设备的信任值达到预设信任值阈值，则监测设备可以根据该目标网络设备对应的临时设备表项，建立该目标网络设备对应的正式设备表项。其中，临时设备表项包含的内容可以与正式设备表项所包含的内容相同，二者的区别在于，临时设备表项具有监测设备分配的临时标识，并且，临时设备表项对技术人员是不可见的；而正式设备表项没有临时标识，并且，正式设备表项对技术人员是可见的。监测设备可以删除临时设备表项的临时标识，并且，将该设备表项添加到用户可见的表项中，以得到该临时设备表项对应的正式设备表项。

在另一种可能的实现方式中，临时设备表项包含的内容可以少于正式设备表项所包含的内容，例如，临时设备表项中可以仅包含目标网络设备的MAC地址等预设的重要参数，相应的，监测设备判定目标网络设备的信任值达到预设信任值阈值时，除了需要删除临时设备表项的临时标识，并将该设备表项添加到用户可见的表项中，还需要获取目标网络设备的其他信息，比如信号强度、所占信道、SSID或设备关联信息等，并将这些信息添加到目标网络设备对应的表项中，以建立目标网络设备对应的正式设备表项。

可选的，如果在预设时长内，目标网络设备的信任值未达到预设信任值阈值，则监测设备可以删除目标网络设备对应的临时设备表项，并将目标网络设备对应的信任值置为0。

本申请实施例中，当AP检测到目标网络设备发送的第一报文类型的通信

报文时, AP可以建立目标网络设备对应的临时设备表项, 然后在预设时长内, 继续检测目标网络设备的目标通信报文, 并根据预先存储的通信报文的报文类型和信任值的对应关系, 确定目标通信报文的目标报文类型对应的信任值, 进而根据目标报文类型对应的信任值, 更新目标网络设备的信任值。只有当

5 信任值达到预设信任值阈值时, AP才会根据目标网络设备对应的临时设备表项建立目标网络设备对应的正式设备表项。由于在变源报文攻击的方式中, 非法网络设备通常不会进行正常的业务流程, 发送的通信报文的种类比较单一, 因此, 本方案能够有效的识别出合法网络设备, 并且只针对合法网络设备建立正式设备表项, 提高了AP学习设备的准确度。

10

以针对AP的设备学习过程为例, 本申请实施例还提供了一种建立设备表项的方法示例, 如图3所示, 具体包括以下步骤。

步骤301, 当检测到目标AP的发送的beacon报文时, 建立目标AP对应的临时设备表项, 并设置目标AP当前的信任值为预设初始值。

15 步骤302, 检测目标AP的目标通信报文, 确定目标通信报文的报文类型(即目标报文类型)。

步骤303, 根据预先存储的通信报文的报文类型和信任值的对应关系, 确定目标通信报文的目标报文类型对应的信任值。

其中, 该对应关系中的报文类型包括beacon报文类型、探测响应报文类型、

20 认证响应报文类型、关联响应报文类型和用户数据报文类型。

步骤304, 判断目标报文类型是否为beacon报文类型。

如果目标报文类型为beacon报文类型, 则执行步骤305~步骤306; 如果目标报文类型不为beacon报文类型, 则执行步骤307。

步骤305, 获取上一次根据beacon报文的信任值更新目标AP的信任值的更

25 新时间。

步骤306, 判断该更新时间与当前时间的时间间隔是否超过预设时长阈值。

如果更新时间与当前时间的的时间间隔超过预设时长阈值, 则执行步骤308;

如果更新时间与当前时间的时间间隔未超过预设时长阈值，则不更新目标AP的信任值。

步骤307，判断在检测到目标通信报文之前，是否已根据目标报文类型更新目标AP的信任值。

- 5 如果未根据目标报文类型根据目标AP的信任值，则执行步骤308；如果已根据目标报文类型根据目标AP的信任值，则不更新目标AP的信任值。

步骤308，计算目标通信报文的报文类型对应的信任值与目标AP当前的信任值的和值，将目标AP的信任值更新为该和值。

步骤309，判断目标AP的信任值是否达到预设信任值阈值。

- 10 如果目标AP的信任值达到预设信任值阈值，则执行步骤310，如果目标AP的信任值未达到预设信任值阈值，则执行步骤311。

步骤310，根据目标AP对应的临时设备表项建立目标AP对应的正式设备表项。

步骤311，判断计时器是否达到预设时长。

- 15 如果计时器未达到预设时长，则返回步骤302；如果计时器已达到预设时长，则执行步骤312。

步骤312，删除目标AP对应的临时设备表项，并将目标AP对应的信任值置为0。

- 20 以针对用户终端的设备学习过程为例，本申请实施例还提供了一种建立设备表项的方法示例，如图4所示，具体包括以下步骤。

步骤401，当检测到目标用户终端的发送的探测请求报文时，建立目标用户终端对应的临时设备表项，并设置目标用户终端当前的信任值为预设初始值。

- 25 步骤402，检测目标用户终端的目标通信报文，确定目标通信报文的报文类型（即目标报文类型）。

- 11 -

步骤403, 根据预先存储的通信报文的报文类型和信任值的对应关系, 确定目标通信报文的目标报文类型对应的信任值。

其中, 该对应关系中的报文类型包括探测请求报文类型、认证响应报文类型、关联响应报文类型、认证请求报文类型、关联请求报文类型、用户数据报文类型、AP数据报文类型。

步骤404, 判断目标报文类型是否为探测请求报文类型。

如果目标报文类型为探测请求报文类型, 则执行步骤405~步骤406; 如果目标报文类型不为探测请求报文类型, 则执行步骤407。

步骤405, 获取上一次根据探测请求报文的信任值更新目标用户终端的信任值的更新时间。

步骤406, 判断该更新时间与当前时间的时间间隔是否超过预设时长阈值。

如果更新时间与当前时间的时间间隔超过预设时长阈值, 则执行步骤408; 如果更新时间与当前时间的时间间隔未超过预设时长阈值, 则不更新目标用户终端的信任值。

步骤407, 判断在检测到目标通信报文之前, 是否已根据目标报文类型更新目标用户终端的信任值。

如果未根据目标报文类型根据目标用户终端的信任值, 则执行步骤408; 如果已根据目标报文类型根据目标用户终端的信任值, 则不更新目标用户终端的信任值。

步骤408, 计算目标通信报文的报文类型对应的信任值与目标用户终端当前的信任值的和值, 将目标用户终端的信任值更新为该和值。

步骤409, 判断目标用户终端的信任值是否达到预设信任值阈值。

如果目标用户终端的信任值达到预设信任值阈值, 则执行步骤410, 如果目标用户终端的信任值未达到预设信任值阈值, 则执行步骤411。

步骤410, 根据目标用户终端对应的临时设备表项建立目标用户终端对应的正式设备表项。

— 12 —

步骤411，判断计时器是否达到预设时长。

如果计时器未达到预设时长，则返回步骤402；如果计时器已达到预设时长，则执行步骤412。

5 步骤412，删除目标用户终端对应的临时设备表项，并将目标用户终端对应的信任值置为0。

基于相同的技术构思，如图 5 所示，本申请实施例还提供了一种建立设备表项的装置，该装置应用于启用无线入侵防护系统 WIPS 功能的接入点 AP，该装置包括：

10 第一建立模块510，用于当检测到目标网络设备发送的第一报文类型的通信报文时，建立目标网络设备对应的临时设备表项；

确定模块520，用于在预设时长内，检测目标网络设备的目标通信报文，并根据预先存储的通信报文的报文类型和信任值的对应关系，确定目标通信报文的目标报文类型对应的信任值；

15 更新模块530，用于根据目标报文类型对应的信任值，更新目标网络设备的信任值；

第二建立模块540，用于当信任值达到预设信任值阈值时，根据目标网络设备对应的临时设备表项建立目标网络设备对应的正式设备表项。

20 可选的，当目标网络设备为未启用WIPS功能的AP时，第一报文类型为 beacon报文类型；

对应关系中的报文类型包括beacon报文类型、探测响应报文类型、认证响应报文类型、关联响应报文类型和用户数据报文类型中的一种或多种。

可选的，当目标网络设备为用户终端时，第一报文类型为探测请求报文类型；

25 对应关系中的报文类型包括探测请求报文类型、认证响应报文类型、关联响应报文类型、认证请求报文类型、关联请求报文类型、用户数据报文类

型、AP数据报文类型中的一种或多种。

可选的，如图6所示，该装置还包括：

第一判断模块550，用于判断目标报文类型是否为第一报文类型；

5 获取模块560，用于如果目标报文类型为第一报文类型，则获取上一次根据第一报文类型对应的信任值更新目标网络设备的信任值的更新时间；如果更新时间与当前时间的时间间隔超过预设时长阈值，则触发更新模块530执行根据目标报文类型对应的信任值，更新目标网络设备的信任值步骤；

10 第二判断模块570，用于如果目标报文类型不为第一报文类型，则判断在检测到目标通信报文之前，是否已根据目标报文类型更新目标网络设备的信任值；如果未根据目标报文类型根据目标网络设备的信任值，则触发更新模块530执行根据目标报文类型对应的信任值，更新目标网络设备的信任值步骤。

可选的，如图7所示，该装置还包括：

设置模块580，用于将预设初始值作为目标网络设备当前的信任值；

更新模块530，具体用于：

15 计算目标通信报文的报文类型对应的信任值与目标网络设备当前的信任值的和值，将目标网络设备的信任值更新为和值。

可选的，如图8所示，该装置还包括：

20 删除模块590，用于如果在预设时长内，信任值未达到预设信任值阈值，则删除目标网络设备对应的临时设备表项，并将目标网络设备对应的信任值置为0。

25 本申请实施例中，当AP检测到目标网络设备发送的第一报文类型的通信报文时，AP可以建立目标网络设备对应的临时设备表项，然后在预设时长内，继续检测目标网络设备的目标通信报文，并根据预先存储的通信报文的报文类型和信任值的对应关系，确定目标通信报文的目标报文类型对应的信任值，进而根据目标报文类型对应的信任值，更新目标网络设备的信任值。只有当信任值达到预设信任值阈值时，AP才会根据目标网络设备对应的临时设备表项建立目标网络设备对应的正式设备表项。由于在变源报文攻击的方式中，

非法网络设备通常不会进行正常的业务流程，发送的通信报文的种类比较单一，因此，本方案能够有效的识别出合法网络设备，并且只针对合法网络设备建立正式设备表项，提高了AP学习设备的准确度。

5 基于相同的技术构思，如图9所示，本申请实施例还提供了一种AP，该AP为启用WIPS功能的AP，该AP包括：处理器901和机器可读存储介质902，所述机器可读存储介质902存储有能够被所述处理器901执行的机器可执行指令，所述机器可执行指令促使所述处理器901：

10 当检测到目标网络设备发送的第一报文类型的通信报文时，建立所述目标网络设备对应的临时设备表项；

在预设时长内，检测所述目标网络设备的目标通信报文，并根据预先存储的通信报文的报文类型和信任值的对应关系，确定所述目标通信报文的目标报文类型对应的信任值；

根据所述目标报文类型对应的信任值，更新所述目标网络设备的信任值；

15 当所述信任值达到预设信任值阈值时，根据所述目标网络设备对应的临时设备表项建立所述目标网络设备对应的正式设备表项。

在本申请的一个可选实施例中，当所述目标网络设备为未启用WIPS功能的AP时，所述第一报文类型为beacon报文类型；

20 所述对应关系中的报文类型包括beacon报文类型、探测响应报文类型、认证响应报文类型、关联响应报文类型和用户数据报文类型中的一种或多种。

在本申请的一个可选实施例中，当所述目标网络设备为用户终端时，所述第一报文类型为探测请求报文类型；

25 所述对应关系中的报文类型包括探测请求报文类型、认证响应报文类型、关联响应报文类型、认证请求报文类型、关联请求报文类型、用户数据报文类型、AP数据报文类型中的一种或多种。

在本申请的一个可选实施例中，所述机器可执行指令还促使所述处理器901：

-15-

判断所述目标报文类型是否为所述第一报文类型；

如果所述目标报文类型为所述第一报文类型，则获取上一次根据所述第一报文类型对应的信任值更新所述目标网络设备的信任值的更新时间；如果所述更新时间与当前时间的时间间隔超过预设时长阈值，则执行所述根据所述目标报文类型对应的信任值，更新所述目标网络设备的信任值步骤；

如果所述目标报文类型不为所述第一报文类型，则判断在检测到所述目标通信报文之前，是否已根据所述目标报文类型更新所述目标网络设备的信任值；如果未根据所述目标报文类型更新所述目标网络设备的信任值，则执行所述根据所述目标报文类型对应的信任值，更新所述目标网络设备的信任值步骤。

在本申请的一个可选实施例中，所述机器可执行指令还促使所述处理器 901：

将预设初始值作为所述目标网络设备当前的信任值；

所述根据所述目标报文类型对应的信任值，更新所述目标网络设备的信任值，包括：

计算所述目标通信报文的报文类型对应的信任值与所述目标网络设备当前的信任值的和值，将所述目标网络设备的信任值更新为所述和值。

在本申请的一个可选实施例中，所述机器可执行指令还促使所述处理器 901：

如果在所述预设时长内，所述信任值未达到所述预设信任值阈值，则删除所述目标网络设备对应的临时设备表项，并将所述目标网络设备对应的信任值置为 0。

如图 9 所示，网络设备还可以包括通信总线 903。通过通信总线 903，处理器 901、机器可读存储介质 902 之间完成通信交互。通信总线 903 可以是外设部件互连标准（英文：Peripheral Component Interconnect，简称：PCI）总线或扩展工业标准结构（英文：Extended Industry Standard Architecture，简称：EISA）总线等。该通信总线 903 可以分为地址总线、数据总线、控制总线等。

机器可读存储介质 902 可以包括随机存取存储器（英文：Random Access Memory，简称：RAM），也可以包括非易失性存储器（英文：Non-Volatile Memory，简称：NVM），例如至少一个磁盘存储器。另外，机器可读存储介质 902 还可以是至少一个位于远离前述处理器 901 的存储装置。

- 5 处理器901可以是通用处理器901，包括中央处理器901（英文：Central Processing Unit，简称：CPU）、网络处理器901（英文：Network Processor，简称：NP）等；还可以是数字信号处理器901（英文：Digital Signal Processing，简称：DSP）、专用集成电路（英文：Application Specific Integrated Circuit，简称：ASIC）、现场可编程门阵列（英文：Field-Programmable Gate Array，简称：FPGA）或其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。
- 10

在本申请提供的又一实施例中，还提供了一种计算机可读存储介质，该计算机可读存储介质内存储有计算机程序，所述计算机程序被处理器执行时实现上述任一建立设备表项的方法的步骤。

- 15 在本申请提供的又一实施例中，还提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行上述实施例中任一建立设备表项的方法。

- 在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁
- 20
- 25

性介质，(例如，软盘、硬盘、磁带)、光介质(例如，DVD)、或者半导体介质（例如固态硬盘Solid State Disk (SSD)）等。

需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示
5 这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除
10 在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

本说明书中的各个实施例均采用相关的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于装置实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

15 以上所述仅为本申请的较佳实施例而已，并非用于限定本申请的保护范围。凡在本申请的精神和原则之内所作的任何修改、等同替换、改进等，均包含在本申请的保护范围内。

权 利 要 求

1、一种建立设备表项的方法，其特征在于，所述方法应用于启用无线入侵防护系统 WIPS 功能的接入点 AP，所述方法包括：

5 当检测到目标网络设备发送的第一报文类型的通信报文时，建立所述目标网络设备对应的临时设备表项；

在预设时长内，检测所述目标网络设备的目标通信报文，并根据预先存储的通信报文的报文类型和信任值的对应关系，确定所述目标通信报文的目標报文类型对应的信任值；

根据所述目标报文类型对应的信任值，更新所述目标网络设备的信任值；

10 当所述信任值达到预设信任值阈值时，根据所述目标网络设备对应的临时设备表项建立所述目标网络设备对应的正式设备表项。

2、根据权利要求1所述的方法，其特征在于，当所述目标网络设备为未启用WIPS功能的AP时，所述第一报文类型为beacon报文类型；

15 所述对应关系中的报文类型包括beacon报文类型、探测响应报文类型、认证响应报文类型、关联响应报文类型和用户数据报文类型中的一种或多种。

3、根据权利要求1所述的方法，其特征在于，当所述目标网络设备为用户终端时，所述第一报文类型为探测请求报文类型；

20 所述对应关系中的报文类型包括探测请求报文类型、认证响应报文类型、关联响应报文类型、认证请求报文类型、关联请求报文类型、用户数据报文类型、AP数据报文类型中的一种或多种。

4、根据权利要求1所述的方法，其特征在于，所述根据所述目标报文类型对应的信任值，更新所述目标网络设备的信任值之前，所述方法还包括：

判断所述目标报文类型是否为所述第一报文类型；

25 如果所述目标报文类型为所述第一报文类型，则获取上一次根据所述第一报文类型对应的信任值更新所述目标网络设备的信任值的更新时间；如果所述更新时间与当前时间的时间间隔超过预设时长阈值，则执行所述根据所述目标报文类型对应的信任值，更新所述目标网络设备的信任值步骤；

如果所述目标报文类型不为所述第一报文类型，则判断在检测到所述目标通信报文之前，是否已根据所述目标报文类型更新所述目标网络设备的信任值；如果未根据所述目标报文类型更新所述目标网络设备的信任值，则执行所述根据所述目标报文类型对应的信任值，更新所述目标网络设备的信任值步骤。

5、根据权利要求1~4任一所述的方法，其特征在于，所述建立所述目标网络设备对应的临时设备表项之后，所述方法还包括：

将预设初始值作为所述目标网络设备当前的信任值；

10 所述根据所述目标报文类型对应的信任值，更新所述目标网络设备的信任值，包括：

计算所述目标通信报文的报文类型对应的信任值与所述目标网络设备当前的信任值的和值，将所述目标网络设备的信任值更新为所述和值。

6、根据权利要求5所述的方法，其特征在于，所述方法还包括：

15 如果在所述预设时长内，所述信任值未达到所述预设信任值阈值，则删除所述目标网络设备对应的临时设备表项，并将所述目标网络设备对应的信任值置为0。

20 7、一种接入点 AP，其特征在于，所述 AP 启用无线入侵防护系统 WIPS 功能的接入点 AP，所述 AP 包括：处理器和机器可读存储介质，所述机器可读存储介质存储有能够被所述处理器执行的机器可执行指令，所述机器可执行指令促使所述处理器：

当检测到目标网络设备发送的第一报文类型的通信报文时，建立所述目标网络设备对应的临时设备表项；

25 在预设时长内，检测所述目标网络设备的目标通信报文，并根据预先存储的通信报文的报文类型和信任值的对应关系，确定所述目标通信报文的报文类型对应的信任值；

根据所述目标报文类型对应的信任值，更新所述目标网络设备的信任值；

—20—

当所述信任值达到预设信任值阈值时，根据所述目标网络设备对应的临时设备表项建立所述目标网络设备对应的正式设备表项。

8、根据权利要求7所述的AP，其特征在于，当所述目标网络设备为未启用WIPS功能的AP时，所述第一报文类型为beacon报文类型；

5 所述对应关系中的报文类型包括beacon报文类型、探测响应报文类型、认证响应报文类型、关联响应报文类型和用户数据报文类型中的一种或多种。

9、根据权利要求7所述的AP，其特征在于，当所述目标网络设备为用户终端时，所述第一报文类型为探测请求报文类型；

10 所述对应关系中的报文类型包括探测请求报文类型、认证响应报文类型、关联响应报文类型、认证请求报文类型、关联请求报文类型、用户数据报文类型、AP数据报文类型中的一种或多种。

10、根据权利要求7所述的AP，其特征在于，所述机器可执行指令还促使所述处理器：

判断所述目标报文类型是否为所述第一报文类型；

15 如果所述目标报文类型为所述第一报文类型，则获取上一次根据所述第一报文类型对应的信任值更新所述目标网络设备的信任值的更新时间；如果所述更新时间与当前时间的时间间隔超过预设时长阈值，则执行所述根据所述目标报文类型对应的信任值，更新所述目标网络设备的信任值步骤；

20 如果所述目标报文类型不为所述第一报文类型，则判断在检测到所述目标通信报文之前，是否已根据所述目标报文类型更新所述目标网络设备的信任值；如果未根据所述目标报文类型更新所述目标网络设备的信任值，则执行所述根据所述目标报文类型对应的信任值，更新所述目标网络设备的信任值步骤。

25 11、根据权利要求7~10任一所述的AP，其特征在于，所述机器可执行指令还促使所述处理器：

将预设初始值作为所述目标网络设备当前的信任值；

所述根据所述目标报文类型对应的信任值，更新所述目标网络设备的信

任值，包括：

计算所述目标通信报文的报文类型对应的信任值与所述目标网络设备当前的信任值的和值，将所述目标网络设备的信任值更新为所述和值。

12、根据权利要求11所述的AP，其特征在于，所述机器可执行指令还促使所述处理器：

如果在所述预设时长内，所述信任值未达到所述预设信任值阈值，则删除所述目标网络设备对应的临时设备表项，并将所述目标网络设备对应的信任值置为0。

13、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质内存储有计算机程序，所述计算机程序被处理器执行时实现权利要求 1-6 任一所述的方法步骤。

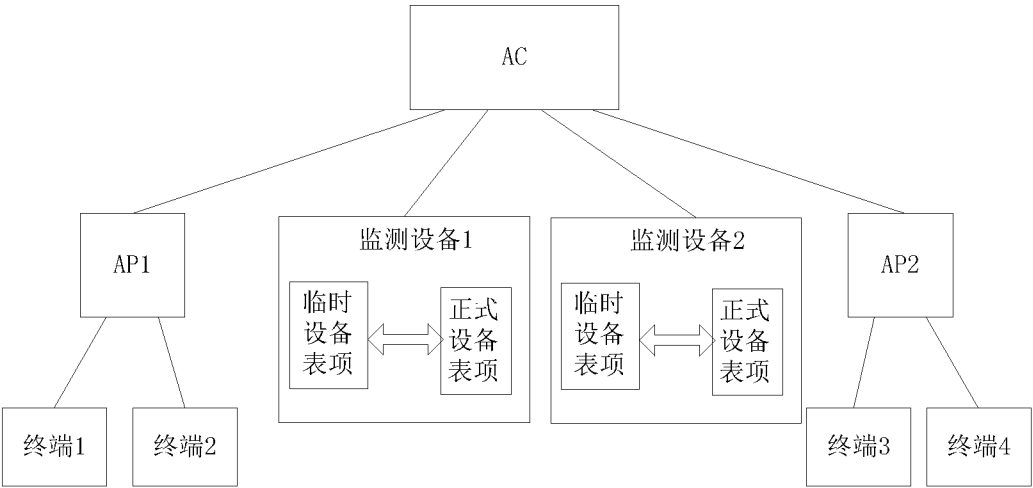


图1

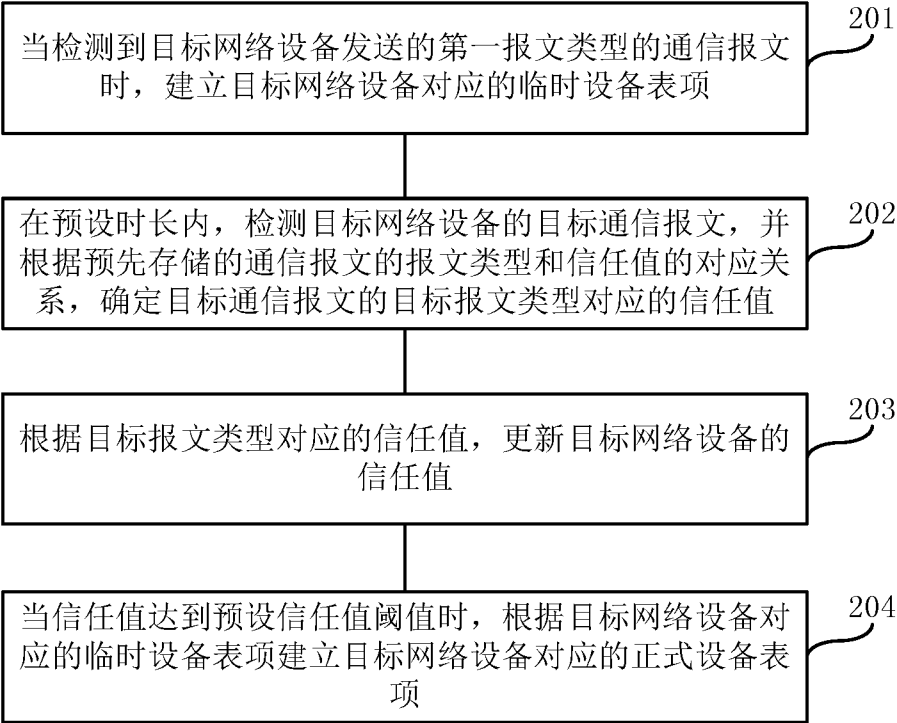


图2

— 2/5 —

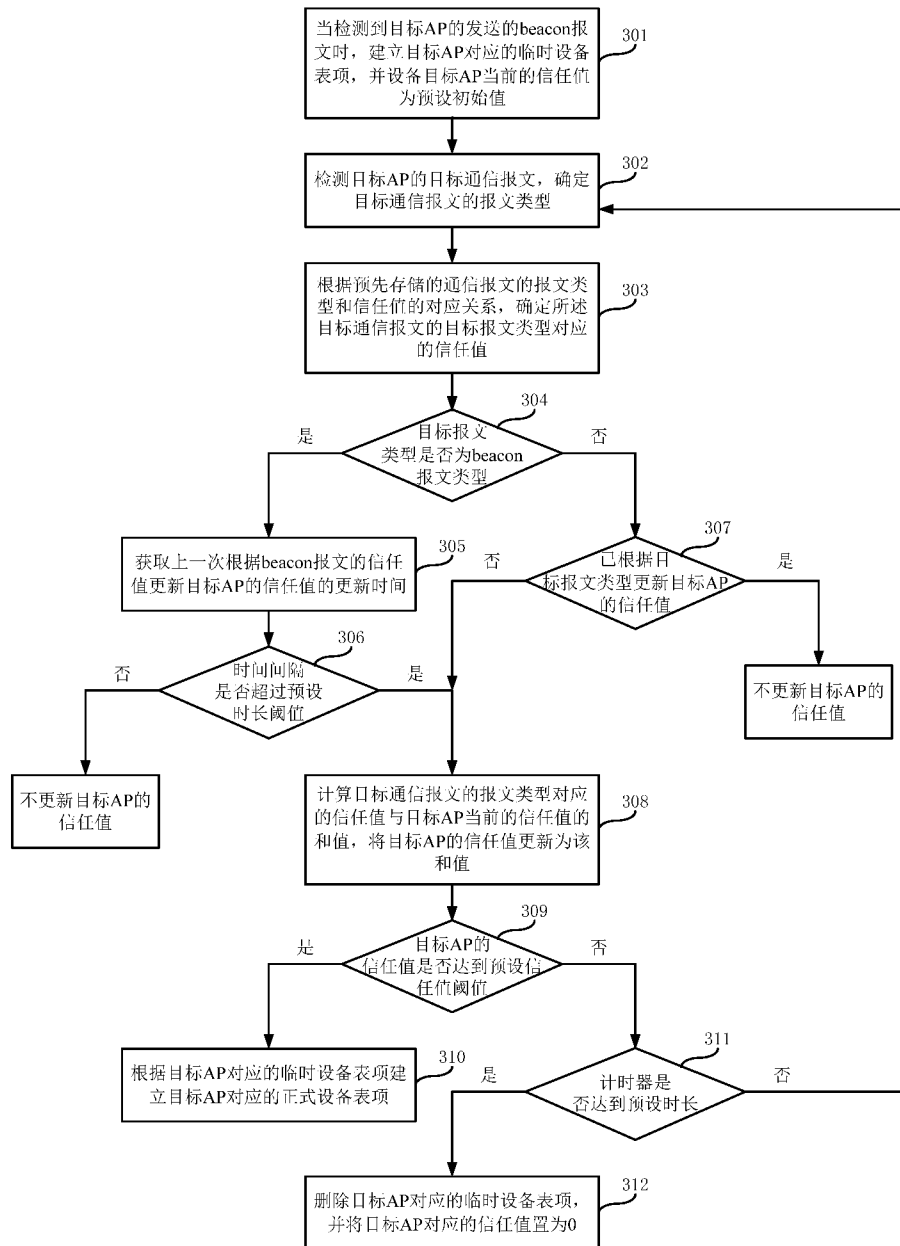


图3

— 3/5 —

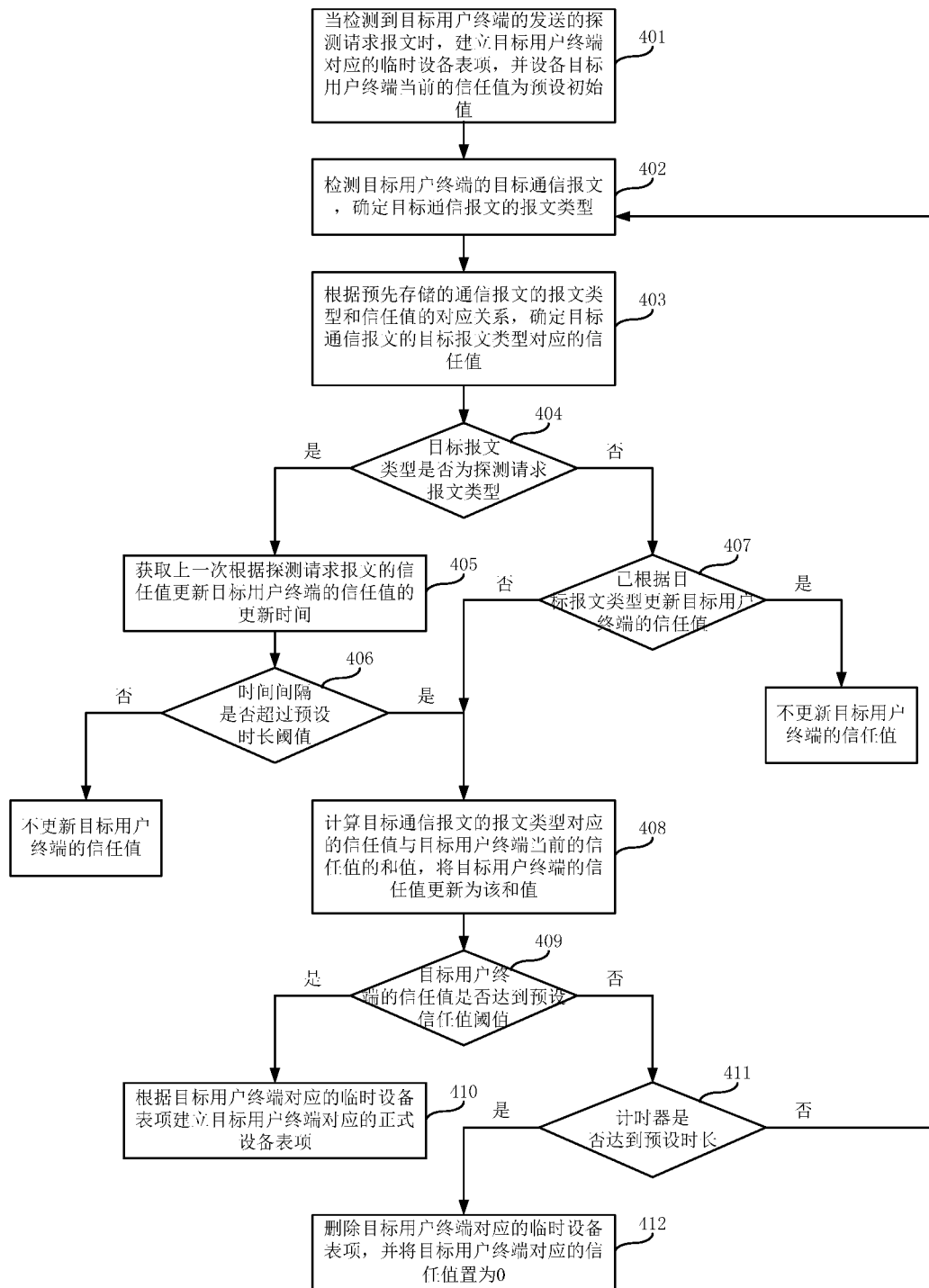


图4

—4/5—

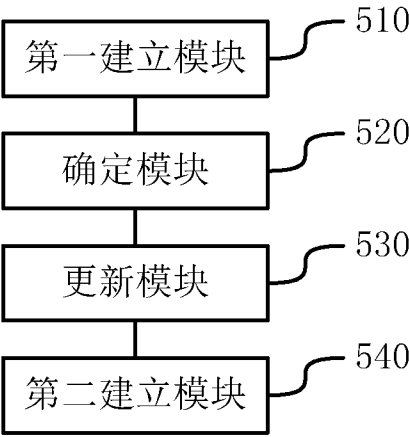


图5

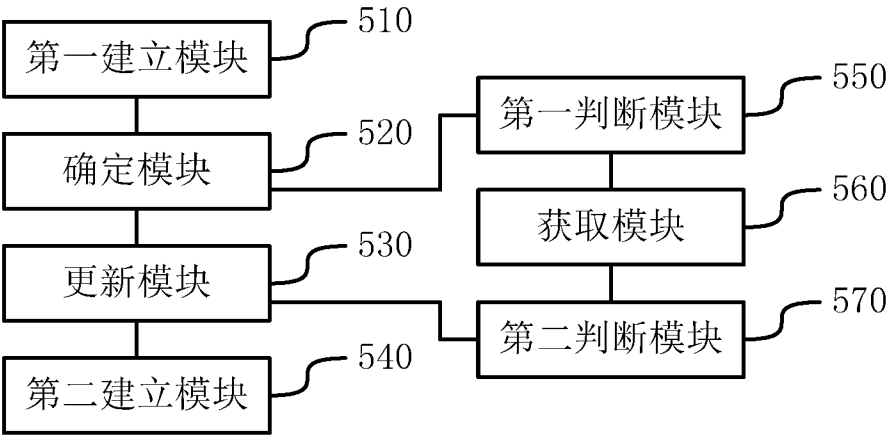


图6

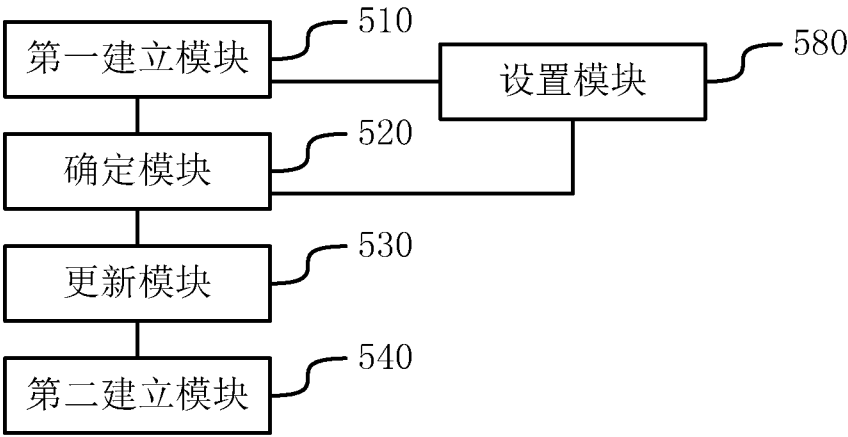


图7

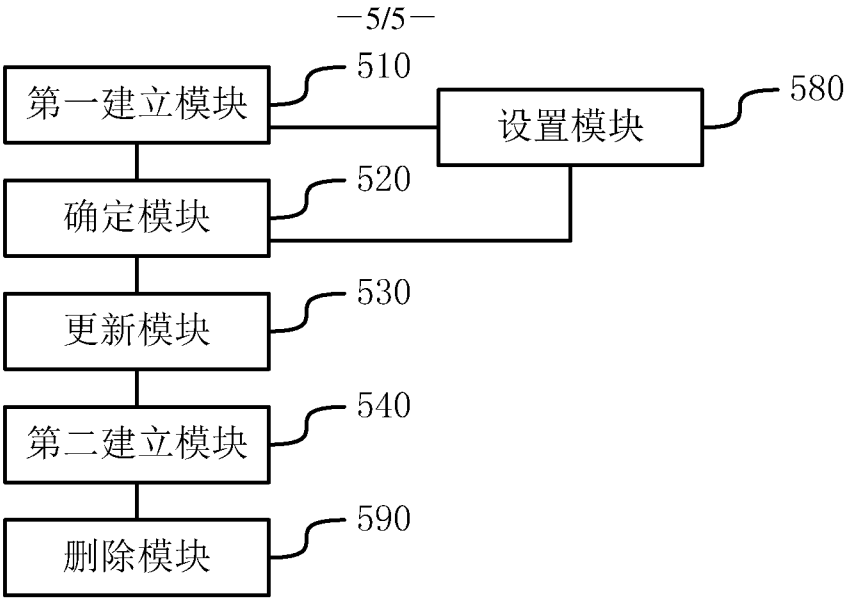


图8

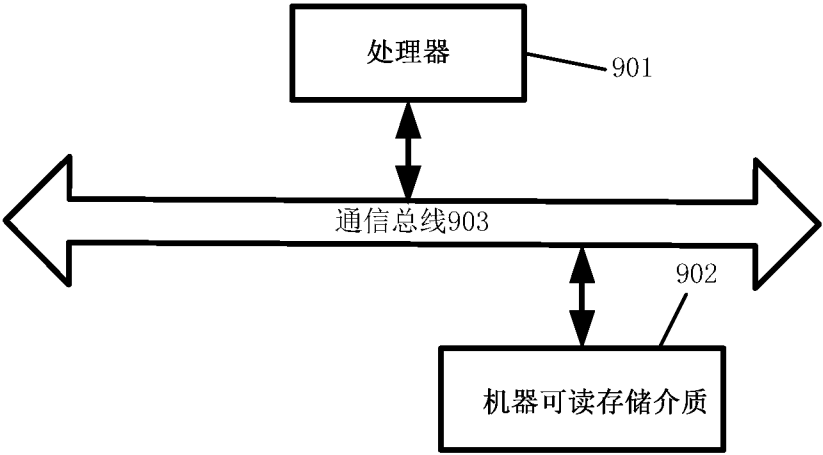


图9

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/102852

A. CLASSIFICATION OF SUBJECT MATTER

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; H04Q

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: 接入点, AP, 入侵防护, WIPS, 报文, 表项, 表, 临时, 关联, 信任, 安全, 可信, 终端, STA, 合法, 恶意, 类型, 阈值, access point, wireless intrusion prevention system, message, list, temporary, associate, trust, safe, terminal, legal, spite, type, threshold

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109067764 A (NEW H3C TECHNOLOGIES CO., LTD.) 21 December 2018 (2018-12-21) claims 1-14	1-13
A	CN 101068179 A (H3C TECHNOLOGIES CO., LIMITED) 07 November 2007 (2007-11-07) description, page 7, paragraph 1 to page 12, paragraph 5	1-13
A	CN 107548065 A (NEW H3C TECHNOLOGIES CO., LTD.) 05 January 2018 (2018-01-05) entire document	1-13
A	CN 106376003 A (CHINA MOBILE HANGZHOU INFORMATION TECHNOLOGY CO., LTD. et al.) 01 February 2017 (2017-02-01) entire document	1-13
A	CN 102802236 A (H3C TECHNOLOGIES CO., LIMITED) 28 November 2012 (2012-11-28) entire document	1-13
A	CN 104378369 A (PHICOMM (SHANGHAI) CO., LTD.) 25 February 2015 (2015-02-25) entire document	1-13



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

“D” document cited by the applicant in the international application

“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

01 November 2019

Date of mailing of the international search report

27 November 2019

Name and mailing address of the ISA/CN

China National Intellectual Property Administration
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/102852

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2010135085 A1 (SYMBOL TECHNOLOGIES, INC.) 25 November 2010 (2010-11-25) entire document	1-13

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/102852

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	109067764	A	21 December 2018	None			
CN	101068179	A	07 November 2007	None			
CN	107548065	A	05 January 2018	None			
CN	106376003	A	01 February 2017	None			
CN	102802236	A	28 November 2012	None			
CN	104378369	A	25 February 2015	None			
WO	2010135085	A1	25 November 2010	US	2010296496	A1	25 November 2010
				EP	2433439	A1	28 March 2012

国际检索报告

国际申请号

PCT/CN2019/102852

A. 主题的分类

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; H04Q

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, EPDOC: 接入点, AP, 入侵防护, WIPS, 报文, 表项, 表, 临时, 关联, 信任, 安全, 可信, 终端, STA, 合法, 恶意, 类型, 阈值, access point, wireless intrusion prevention system, message, list, temporary, associate, trust, safe, terminal, legal, spite, type, threshold

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
PX	CN 109067764 A (新华三技术有限公司) 2018年 12月 21日 (2018 - 12 - 21) 权利要求1-14	1-13
A	CN 101068179 A (杭州华三通信技术有限公司) 2007年 11月 7日 (2007 - 11 - 07) 说明书第7页第1段至第12页第5段	1-13
A	CN 107548065 A (新华三技术有限公司) 2018年 1月 5日 (2018 - 01 - 05) 全文	1-13
A	CN 106376003 A (中移杭州信息技术有限公司等) 2017年 2月 1日 (2017 - 02 - 01) 全文	1-13
A	CN 102802236 A (杭州华三通信技术有限公司) 2012年 11月 28日 (2012 - 11 - 28) 全文	1-13
A	CN 104378369 A (上海斐讯数据通信技术有限公司) 2015年 2月 25日 (2015 - 02 - 25) 全文	1-13
A	WO 2010135085 A1 (SYMBOL TECHNOLOGIES, INC.) 2010年 11月 25日 (2010 - 11 - 25) 全文	1-13

☐ 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

2019年 11月 1日

国际检索报告邮寄日期

2019年 11月 27日

ISA/CN的名称和邮寄地址

中国国家知识产权局 (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

靳晶

电话号码 86-(10)-53961790

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/102852

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	109067764	A	2018年 12月 21日	无			
CN	101068179	A	2007年 11月 7日	无			
CN	107548065	A	2018年 1月 5日	无			
CN	106376003	A	2017年 2月 1日	无			
CN	102802236	A	2012年 11月 28日	无			
CN	104378369	A	2015年 2月 25日	无			
WO	2010135085	A1	2010年 11月 25日	US	2010296496	A1	2010年 11月 25日
				EP	2433439	A1	2012年 3月 28日

表 PCT/ISA/210 (同族专利附件) (2015年1月)