(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106789934 A
(43)申请公布日 2017.05.31

(21)申请号 201611073519.8

(22)申请日 2016.11.29

(71)申请人 北京神州绿盟信息安全科技股份有限公司
地址 100089 北京市海淀区北洼路4号益泰大厦三层
申请人 北京神州绿盟科技有限公司

(72)发明人 周年华

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 黄志华

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

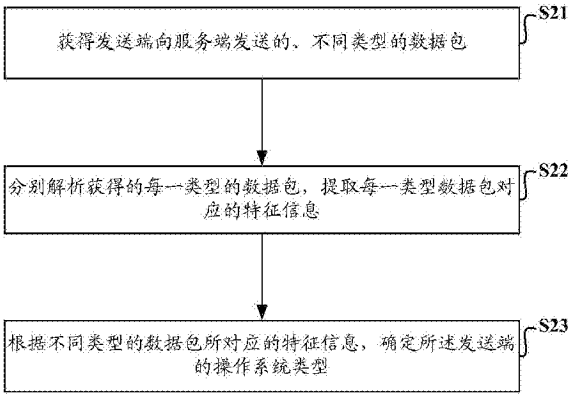
权利要求书2页 说明书7页 附图2页

(54)发明名称

一种网络设备识别方法及系统

(57)摘要

本发明公开了一种网络设备识别方法及系统，用以提高企业网络设备识别的准确度。所述网络设备识别方法，包括：获得发送端向服务端发送的、不同类型的数据包；分别解析获得的每一类型的数据包，提取每一类型数据包对应的特征信息；根据不同类型的数据包所对应的特征信息，确定所述发送端的操作系统类型。



CN 106789934 A

1.一种网络设备识别方法,其特征在于,包括:

获得发送端向服务端发送的、不同类型的数据包;

分别解析获得的每一类型的数据包,提取每一类型数据包对应的特征信息;

根据不同类型的数据包所对应的特征信息,确定所述发送端的操作系统类型。

2.如权利要求1所述的方法,其特征在于,所述不同类型的数据包包括以下任一类型数据包:传输控制协议/互联网协议TCP/IP连接建立时的第一个数据包SYN数据包、HTTP协议中使用GET操作方式得到的数据包GET数据包或者HTTP协议中使用POST操作方式得到的数据包POST数据包。

3.如权利要求2所述的方法,其特征在于,如果为SYN数据包,则

分别解析获得的每一类型的数据包,提取每一类型数据包对应的特征信息,具体包括:

分别解析获得的SYN数据包的每一字段,从所述SYN数据包中每一字段所对应的特征信息中提取以下至少一项作为所述SYN数据包对应的特征信息:生存时间TTL值信息、网络协议IP头选项长度信息、最大报文段长度MSS信息、传输控制协议TCP窗口大小信息、TCP窗口扩大因子信息以及TCP选项顺序信息。

4.如权利要求2所述的方法,其特征在于,如果为GET数据包或者POST数据包,则

分别解析获得的每一类型的数据包,提取每一类型数据包对应的特征信息,具体包括:

解析所述GET数据包或者POST数据包,从所述GET数据包或者POST数据包中提取用户代理UA特征信息作为所述GET数据包或者POST数据包对应的特征信息。

5.如权利要求1所述的方法,其特征在于,根据不同类型的数据包所对应的特征信息,确定所述发送端的操作系统类型,具体包括:

针对每一类型的数据包,利用该类型数据包所对应的特征信息,从预设的、该类型数据包对应的特征规则列表中匹配该类型数据包对应的不同操作系统类型及其可信度;

针对每一操作系统类型,确定该操作系统类型对应的可信度之和;

确定可信度之和大于等于预设值或者可信度之和最大的操作系统类型为所述发送端的操作系统类型。

6.一种网络设备识别系统,其特征在于,包括:

获得模块,用于获得发送端向服务端发送的、不同类型的数据包;

解析模块,用于分别解析获得模块获得的每一类型的数据包,提取每一类型数据包对应的特征信息;

确定模块,用于根据不同类型的数据包所对应的特征信息,确定所述发送端的操作系统类型。

7.如权利要求6所述的系统,其特征在于,所述不同类型的数据包包括以下任一类型数据包:传输控制协议/互联网协议TCP/IP连接建立时的第一个数据包SYN数据包、HTTP协议中使用GET操作方式得到的数据包GET数据包或者HTTP协议中使用POST操作方式得到的数据包POST数据包。

8.如权利要求7所述的系统,其特征在于,

所述解析模块,具体用于如果为SYN数据包,则分别解析获得的SYN数据包的每一字段,从所述SYN数据包中每一字段所对应的特征信息中提取以下至少一项作为所述SYN数据包对应的特征信息:生存时间TTL值信息、网络协议IP头选项长度信息、最大报文段长度MSS信

息、传输控制协议TCP窗口大小信息、TCP窗口扩大因子信息以及TCP选项顺序信息。

9.如权利要求7所述的系统，其特征在于，

所述解析模块，还用于如果为GET数据包或者POST数据包，则解析所述GET数据包或者POST数据包，从所述GET数据包或者POST数据包中提取用户代理UA特征信息作为所述GET数据包或者POST数据包对应的特征信息。

10.如权利要求6所述的系统，其特征在于，所述确定模块，具体包括：

匹配子模块，用于针对每一类型的数据包，利用该类型数据包所对应的特征信息，从预设的、该类型数据包对应的特征规则列表中匹配该类型数据包对应的不同操作系统类型及其可信度；

第一确定子模块，用于针对每一操作系统类型，确定该操作系统类型对应的可信度之和；

第二确定子模块，用于确定可信度之和大于等于预设值或者可信度之和最大的操作系统类型为所述发送端的操作系统类型。

一种网络设备识别方法及系统

技术领域

[0001] 本发明涉及信息安全技术领域，尤其涉及一种网络设备识别方法及系统。

背景技术

[0002] 现有技术中，对于以防火墙作为企业网关的出口设备，可以通过主动发送网络探测数据包扫描企业中的网络设备，以此获得企业中的网络设备对这些探测数据包的回应数据包，并通过分析该回应数据包获取这些企业网络设备的网络数据特征以识别出企业网络设备。通过这种主动发送网络探测数据包扫描的方式，当处理这些探测数据包时，会占用额外的网络资源，从而对企业设备的网络环境产生影响。并且，防火墙在对企业的网络设备进行监控时，一般只以IP地址作为某个网络设备的代表信息，即一个IP地址对应一个网络设备，然而，当IP地址发生变动时就不能准确地对应网络设备，使得识别网络设备的准确度大大降低。

发明内容

[0003] 本发明提供了一种网络设备识别方法及系统，用以提高企业网络设备识别的准确度。

[0004] 本发明实施例提供了一种网络设备识别方法，包括：

[0005] 获得发送端向服务端发送的、不同类型的数据包；

[0006] 分别解析获得的每一类型的数据包，提取每一类型数据包对应的特征信息；

[0007] 根据不同类型的数据包所对应的特征信息，确定所述发送端的操作系统类型。

[0008] 本发明实施例提供了一种网络设备识别系统，包括：

[0009] 获得模块，用于获得发送端向服务端发送的、不同类型的数据包；

[0010] 解析模块，用于分别解析获得模块获得的每一类型的数据包，提取每一类型数据包对应的特征信息；

[0011] 确定模块，用于根据不同类型的数据包所对应的特征信息，确定所述发送端的操作系统类型。

[0012] 本发明的有益效果包括：

[0013] 本发明提供的网络设备识别方法及系统，通过防火墙获得发送端网络设备向服务端发送的不同类型的数据包，分别解析获得的每一类型的数据包，提取每一类型数据包对应的特征信息，并根据不同类型的数据包所对应的特征信息，确定发送端网络设备的操作系统类型，上述过程中，无需发送探测数据包扫描网络设备和服务端之间交互的数据包，从而不会对两者之间的网络环境造成影响，也无需占用额外的网络处理资源，而且，针对网络设备还可以进一步识别出其操作系统类型，提高了企业网络设备识别的准确度。

[0014] 本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

附图说明

[0015] 此处所说明的附图用来提供对本发明的进一步理解，构成本发明的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0016] 图1为本发明实施例中，网络设备识别方法的应用场景示意图；

[0017] 图2为本发明实施例中，网络设备识别方法实施流程示意图；

[0018] 图3为本发明实施例中，确定发送端操作系统类型的流程示意图；

[0019] 图4为本发明实施例中，网络设备识别系统结构示意图。

具体实施方式

[0020] 本发明提供了一种网络设备识别方法和系统，用以提高企业网络设备识别的准确度。

[0021] 本发明实施例提供的网络设备识别方法实施原理是：本发明实施例提供的网络设备识别方法可以应用于防火墙中，通过防火墙获得发送端网络设备向服务端发送的不同类型的数据包，分别解析获得的每一类型的数据包，提取每一类型数据包对应的特征信息，并根据不同类型的数据包所对应的特征信息，确定发送端网络设备的操作系统类型，上述过程中，无需发送探测数据包扫描网络设备和服务端之间交互的数据包，从而不会对两者之间的网络环境造成影响，也无需占用额外的网络处理资源，而且，针对网络设备还可以进一步识别出其操作系统类型，提高了企业网络设备识别的准确度。

[0022] 以下结合说明书附图对本发明的优选实施例进行说明，应当理解，此处所描述的优选实施例仅用于说明和解释本发明，并不用于限定本发明，并且在不冲突的情况下，本发明中的实施例及实施例中的特征可以相互组合。

[0023] 首先参考图1，其为本发明实施例提供的网络设备识别方法的应用场景示意图，以用户通过客户端11访问服务端13的流程为例来进行说明，可以包括以下步骤：

[0024] 步骤一、防火墙获得客户端向服务端发送的TCP协议的SYN数据包，提取SYN数据包所对应的特征信息。

[0025] 具体地，服务器13以百度服务器为例，当用户在客户端11浏览器中输入www.baidu.com并提交后，DNS服务器会将www.baidu.com转换为百度服务器13的IP地址，获取此IP地址。SYN是TCP/IP建立连接时使用的握手信号，客户端11通过获取的IP地址发送TCP协议的SYN数据包给百度服务器13，在该SYN数据包到达防火墙12时，防火墙12对其进行扫描并解码，提取SYN数据包所对应的特征信息，然后，防火墙12将SYN数据包发送给百度服务器13，至此，完成如图1中所示过程(1)的第一次握手，其中，SYN数据包所对应的特征信息主要包括以下几项：TTL值(Time to live，生存时间)信息、IP头选项长度信息、MSS(Maximum segments size，最大报文段长度)信息、TCP窗口大小(Windows size value)信息、TCP窗口扩大因子(Window scale)信息、TCP选项顺序信息。百度服务器13接收到客户端11发送的SYN数据包，通过防火墙12向客户端11返回SYN ACK应答消息，即为图1中所示过程(1)中的第二次握手。客户端11接收到百度服务器13返回的SYN ACK应答消息，再通过防火墙12向百度服务器13发送一个ACK响应，至此，三次握手完成，客户端11和百度服务器13成功建立TCP/IP连接。

[0026] 步骤二、防火墙获得客户端向服务端发送的HTTP协议的GET数据包或者POST数据包，提取GET数据包或者POST数据包所对应的特征信息。

[0027] 本步骤中，当客户端11和百度服务器13建立TCP/IP连接以后，客户端11发送一个HTTP协议的GET数据包或者POST数据包给百度服务器13，防火墙12接收到该GET数据包或者POST数据包，对其进行扫描并解码，提取该GET数据包或者POST数据包所对应的特征信息，具体地，将提取到的用户代理UA特征信息作为GET数据包或者POST数据包所对应的特征信息，如图1所示过程(2)。

[0028] 步骤三、根据不同类型的数据包所对应的特征信息，确定客户端的操作系统类型。

[0029] 具体地，针对SYN数据包，利用防火墙解码提取的SYN数据包所对应的特征信息，从预设的SYN数据包对应的特征规则列表中匹配该SYN数据包对应的操作系统类型及可信度。同理，针对GET数据包或者POST数据包，利用防火墙解码提取的GET数据包或者POST数据包所对应的特征信息，从预设的GET数据包或者POST数据包对应的特征规则列表中匹配该GET数据包或者POST数据包对应的操作类型及可信度。确定针对根据SYN数据包对应的特征信息以及根据GET数据包或者POST数据包对应的特征信息匹配得到的同一操作系统类型的可信度之和，可信度之和大于等于预设值或者可信度之和最大的操作系统类型即确定为客户端的操作系统类型。

[0030] 下面结合图1的应用场景，参考图2-图3来描述根据本发明示例性实施方式的网络设备识别方法。需要注意的是，上述应用场景仅是为了便于理解本发明的精神和原理而示出，本发明的实施方式在此方面不受任何限制。相反，本发明的实施方式可以应用于适用的任何场景。

[0031] 本发明实施例提供的网络设备识别方法可以应用于图1所示的防火墙中。如图2所示，其为本发明实施例提供的网络设备识别方法实施流程示意图，可以包括：

[0032] S21、获得发送端向服务端发送的、不同类型的数据包。

[0033] 具体实施时，当发送端向服务端发送不同类型的数据包，通过防火墙时，防火墙获得这些不同类型的数据包，其中，不同类型的数据包即上述应用场景步骤一中的SYN数据包及步骤二中的GET数据包或者POST数据包。

[0034] S22、分别解析获得的每一类型的数据包，提取每一类型数据包对应的特征信息。

[0035] 具体实施时，防火墙分别解析获得的SYN数据包及GET数据包或者POST数据包，提取SYN数据包及GET数据包或者POST数据包分别对应的特征信息。

[0036] 如果防火墙获得的数据包为SYN数据包，则分别解析该SYN数据包的每一字段，从SYN数据包中每一字段所对应的特征信息中提取以下至少一项作为SYN数据包对应的特征信息：TTL值信息、网络协议IP头选项长度信息、最大报文段长度MSS信息、TCP窗口大小消息、TCP窗口扩大因子信息以及TCP选项顺序信息。

[0037] 比如防火墙解析SYN数据包得到以下对应的特征信息：

[0038] Time to live:128；

[0039] Windows size value:8192；

[0040] Options:(20bytes),maximum segment size,No-operation(Nop),window scale,sack permitted,Timestamps；

[0041] Maximum segments size:1460bytes；

[0042] Window scale:2(multiply by 4)。

[0043] 如果防火墙获得的数据包为GET或者POST数据包，则解析该GET数据包或者POST数据包，从GET数据包或者POST数据包中提取UA特征信息作为GET或者POST数据包对应的特征信息。以GET数据包为例，当发送端访问http://www.baidu.com/，就相当于提交了一个GET数据包，具体如下：

[0044] GET/HTTP/1.1

[0045] Host:www.baidu.com

[0046] 防火墙解析该GET数据包得到以下对应的UA特征信息：

[0047] User-Agent:Mozilla/5.0(Windows NT 6.1;rv:22.0)Gecko/20100101

[0048] Firefox/22.0。

[0049] S23、根据不同类型的数据包所对应的特征信息，确定所述发送端的操作系统类型。

[0050] 具体实施时，可以按照如图3所示的流程确定发送端的操作系统类型：

[0051] S31、针对每一类型的数据包，利用该类型数据包所对应的特征信息，从预设的、该类型数据包对应的特征规则列表中匹配该类型数据包对应的不同操作系统类型及其可信度。

[0052] 本步骤中，针对SYN数据包，利用SYN数据包对应的特征信息从预设的SYN数据包对应的特征规则列表中匹配SYN数据包对应的不同操作系统类型及其可信度。具体地，预设的SYN数据包对应的特征规则列表反应了SYN数据包对应的特征信息与对应的操作系统及其可信度的关系。例如预设的SYN数据包对应的特征规则列表如表1所示：

[0053] 表1

[0054]

		IP头选		TCP窗	TCP窗	TCP选项	操作系	可信

[0055]

ID	TTL	项长度	MSS	口大小	口扩大因子	顺序	统类型	度(%)
1	64	0	16376	mss*4	7	nop，mss，ws	Linux 3.2	10
2	64	0	16376	mss*10	4	ws,nop,mss	Linux 2.6	50
3	128	0	*	8192	2	mss，nop ws	Windows 7	95
4	128	0	1460	8192	2	mss，nop ws	Linux	30

[0056] 表1中特征规则列表由四条特征规则组成，其中：

[0057] 特征规则1表示：当TTL(Time to live)值为64、IP头选项长度为0、最大报文段长

度MSS(Maximum segments size)为16376、TCP窗口大小(windows size value)为MSS*4、TCP窗口扩大因子(Window scale)为7以及TCP选项顺序为“Nop、MSS、WS”时，操作系统类型为Linux 3.2的可信度为10％。

[0058] 特征规则2表示：当TTL值为64、IP头选项长度为0、最大报文段长度MSS为16373、TCP窗口大小为MSS*10、TCP窗口扩大因子为4以及TCP选项顺序为“WS、Nop、MSS”时，操作系统类型为Linux 2.6的可信度为50％。

[0059] 特征规则3表示：当TTL值为128、IP头选项长度为0、最大报文段长度MSS不限、TCP窗口大小为8192、TCP窗口扩大因子为2以及TCP选项顺序为“MSS、Nop、WS”时，操作系统类型为Windows 7的可信度为95％。

[0060] 特征规则4表示：当TTL值为128、IP头选项长度为0、最大报文段长度MSS为1460、TCP窗口大小为8192、TCP窗口扩大因子为2以及TCP选项顺序为“MSS、Nop、WS”时，操作系统类型为Linux的可信度为30％。

[0061] 将步骤S22中防火墙解析SYN数据包得到的对应的特征信息与上述特征规则列表进行匹配，可以看出步骤S22中防火墙解析SYN数据包得到的对应的特征信息可以与特征规则3、特征规则4相匹配，从而可以判定发送端的操作系统类型为Windows 7的可信度为95％、操作系统类型为Linux的可信度为30％。

[0062] 针对GET数据包或者POST数据包，利用GET数据包或者POST数据包对应的特征信息从预设的GET数据包或者POST数据包对应的特征规则列表中匹配GET数据包或者POST数据包对应的不同操作系统类型及其可信度。

[0063] 具体地，预设的GET数据包或者POST数据包对应的特征规则列表反应了GET数据包或者POST数据包对应的特征信息与对应的操作系统及其可信度的关系。例如预设的GET数据包或者POST数据包对应的特征规则列表如表2所示：

[0064] 表2

[0065]

ID	UA特征值	操作系统类型	可信度(％)
1	Windows NT 6.1	Windows 7	90
2	Windows NT 6.2	Windows 8	50
3	Linux	Linux	20
4	Windows NT 6.1	Linux	5

[0066] 特征规则1表示：当UA特征值为Windows NT 6.1时，操作系统类型为Windows 7的可信度为90％。

[0067] 特征规则2表示：当UA特征值为Windows NT 6.2时，操作系统类型为Windows 8的可信度为50％。

[0068] 特征规则3表示：当UA特征值为Linux时，操作系统类型为Linux的可信度为20％。

[0069] 特征规则4表示：当UA特征值为Windows NT 6.1时，操作系统类型为Linux的可信度为5％。

[0070] 将步骤S22中防火墙解析数据包得到的GET数据包对应的特征信息与上述特征规则列表进行匹配，可以看出步骤S22中防火墙解析GET数据包得到的对应的特征信息Windows NT6.1可以与特征规则1、特征规则4相匹配，从而可以判定发送端的操作系统类型

为Windows 7的可信度为90%，操作系统类型为Linux的可信度为5%。

[0071] 需要说明的是，特征规则列表中的特征规则条数可以根据需要设定，这里不进行限定。

[0072] S32、针对每一操作系统类型，确定该操作系统类型对应的可信度之和。

[0073] 具体地，步骤S31中操作系统类型为Windows 7对应的可信度分别为95%和90%，操作系统类型为Windows 7的可信度之和为:95%+90%＝185%，操作系统类型为Linux的可信度之和为:30%+5%＝35%。

[0074] S33、确定可信度之和大于等于预设值或者可信度之和最大的操作系统类型为发送端的操作系统类型。

[0075] 本步骤中，操作系统类型为Windows 7的可信度之和185%最大，从而可以确定发送端的操作类型为Windows 7。

[0076] 需要说明的是，当SYN数据包以及GET数据包匹配的相同操作系统类型的可信度均为100%时，则可以直接确定发送端的操作类型为该类型，从而达到网络设备识别的目的。

[0077] 本发明实施例提供的网络设备识别方法，通过防火墙获得发送端网络设备向服务端发送的不同类型的数据包，分别解析获得的每一类型的数据包，提取每一类型数据包对应的特征信息，并根据不同类型的数据包所对应的特征信息，确定发送端网络设备的操作系统类型，上述过程中，无需发送探测数据包扫描网络设备和服务端之间交互的数据包，从而不会对两者之间的网络环境造成影响，也无需占用额外的网络处理资源，而且，针对网络设备还可以进一步识别出其操作系统类型，提高了企业网络设备识别的准确度。

[0078] 基于同一发明构思，本发明实施例中还提供了网络设备识别系统，由于上述方法解决问题的原理与网络设备识别方法相似，因此上述方法的实施可以参见方法的实施，重复之处不再赘述。

[0079] 本发明实施例提供的网络设备识别系统可以应用于防火墙中。如图4所示，其为本发明实施例提供的网络设备识别系统在防火墙中的应用结构示意图，可以包括：

[0080] 获得模块41，用于获得发送端向服务端发送的、不同类型的数据包；

[0081] 解析模块42，用于分别解析获得模块41获得的每一类型的数据包，提取每一类型数据包对应的特征信息；

[0082] 确定模块43，用于根据不同类型的数据包所对应的特征信息，确定所述发送端的操作系统类型。

[0083] 较佳地，所述不同类型的数据包包括以下任一类型数据包：传输控制协议/互联网协议TCP/IP连接建立时的第一个数据包SYN数据包、HTTP协议中使用GET操作方式得到的数据包GET数据包或者HTTP协议中使用POST操作方式得到的数据包POST数据包。

[0084] 较佳地，所述解析模块，具体用于如果为SYN数据包，则分别解析获得的SYN数据包的每一字段，从所述SYN数据包中每一字段所对应的特征信息中提取以下至少一项作为所述SYN数据包对应的特征信息：生存时间TTL值信息、网络协议IP头选项长度信息、最大报文段长度MSS信息、传输控制协议TCP窗口大小信息、TCP窗口扩大因子信息以及TCP选项顺序信息。

[0085] 较佳地，所述解析模块，还可以用于如果为GET数据包或者POST数据包，则解析所述GET数据包或者POST数据包，从所述GET数据包或者POST数据包中提取用户代理UA特征信

息作为所述GET数据包或者POST数据包对应的特征信息。

[0086] 较佳地，所述确定模块，具体可以包括：

[0087] 匹配子模块，用于针对每一类型的数据包，利用该类型数据包所对应的特征信息，从预设的、该类型数据包对应的特征规则列表中匹配该类型数据包对应的不同操作系统类型及其可信度；

[0088] 第一确定子模块，用于针对每一操作系统类型，确定该操作系统类型对应的可信度之和；

[0089] 第二确定子模块，用于确定可信度之和大于等于预设值或者可信度之和最大的操作系统类型为所述发送端的操作系统类型。

[0090] 为了描述的方便，以上各部分按照功能划分为各模块(或单元)分别描述。当然，在实施本发明时可以把各模块(或单元)的功能在同一个或多个软件或硬件中实现。

[0091] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明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，本发明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。

[0092] 本发明是参照根据本发明实施例的方法、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。

[0093] 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。

[0094] 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。

[0095] 尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做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发明范围的所有变更和修改。

[0096] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

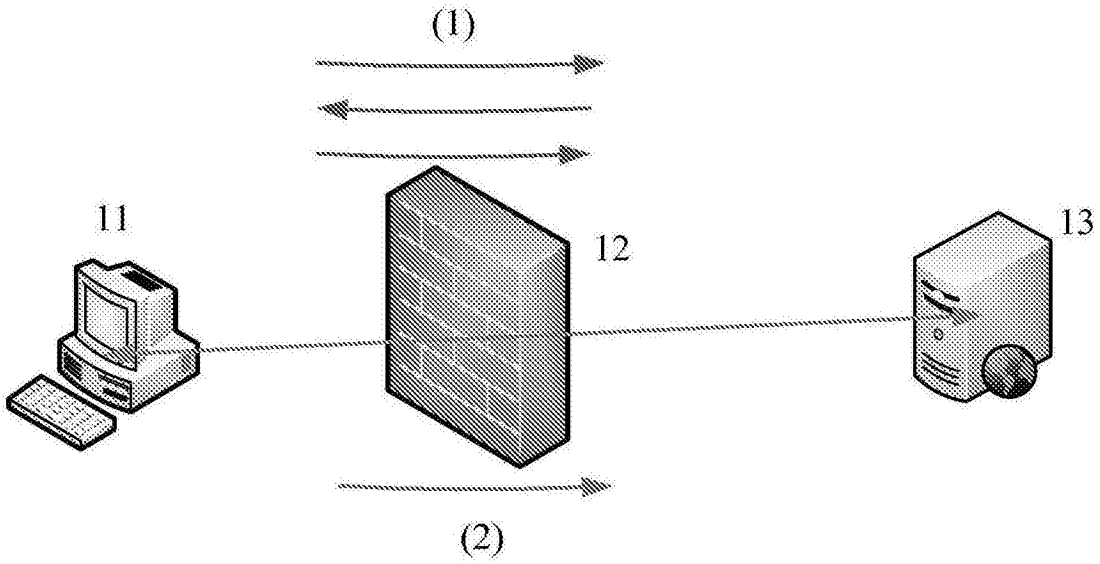

(1)
11
12
13
(2)

图1

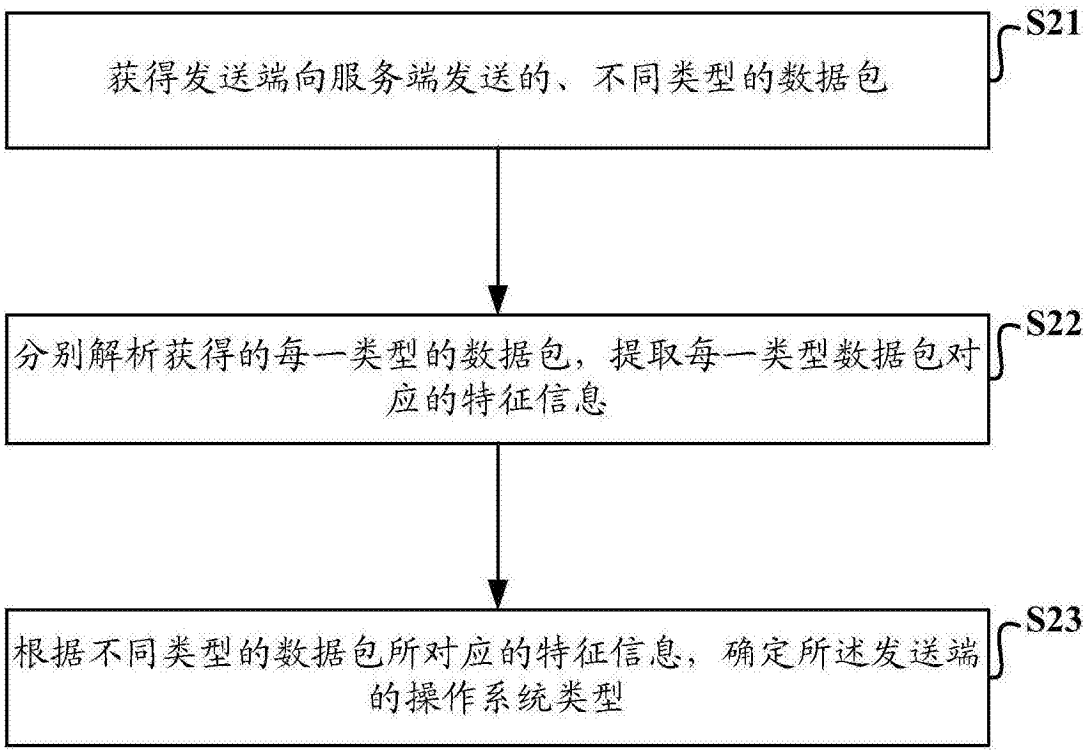

获得发送端向服务端发送的、不同类型的数据包
S21
分别解析获得的每一类型的数据包，提取每一类型数据包对应的特征信息
S22
根据不同类型的数据包所对应的特征信息，确定所述发送端的操作系统类型
S23

图2

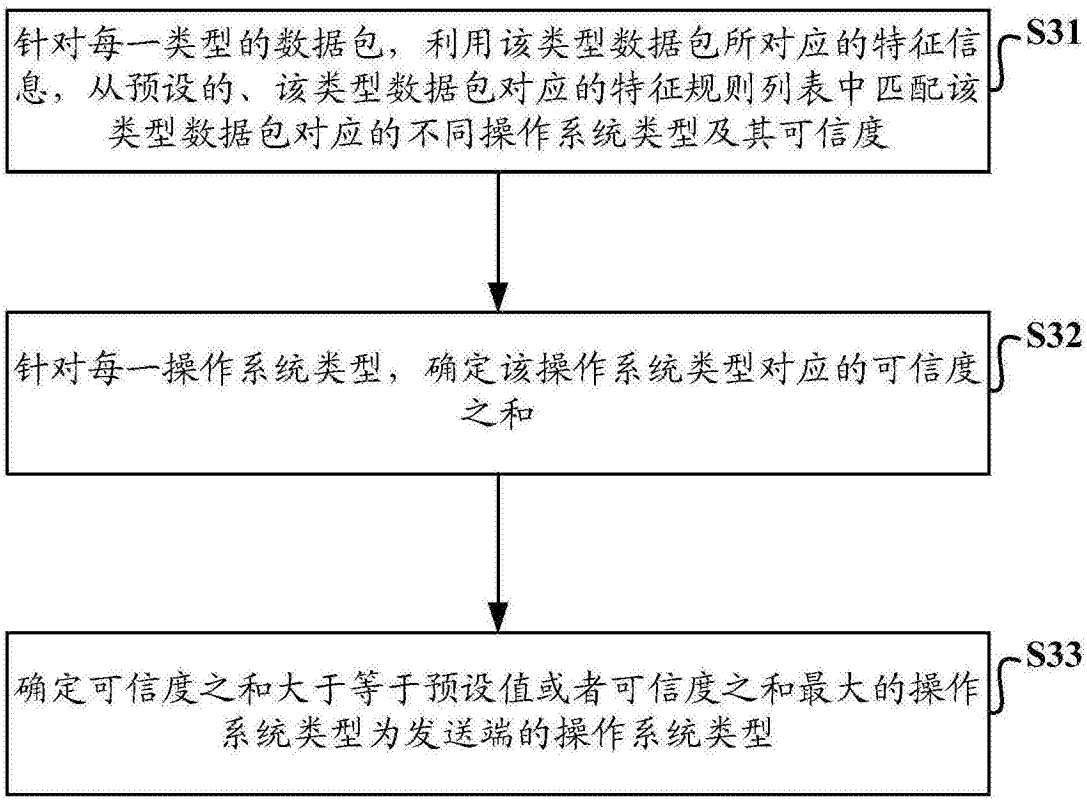

针对每一类型的数据包，利用该类型数据包所对应的特征信息，从预设的、该类型数据包对应的特征规则列表中匹配该类型数据包对应的不同操作系统类型及其可信度
S31
针对每一操作系统类型，确定该操作系统类型对应的可信度之和
S32
确定可信度之和大于等于预设值或者可信度之和最大的操作系统类型为发送端的操作系统类型
S33

图3


41
获得模块
42
解析模块
43
确定模块

图4