

用于实现终端验证的方法、装置、系统、设备及存储介质

本申请要求于2020年07月13日提交的申请号为202010669766.4、发明名称为“实现仿冒终端检测的方法、装置和系统”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。

本申请要求于2020年10月31日提交的申请号为202011198953.5、发明名称为“用于实现终端验证的方法、装置、系统、设备及存储介质”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。

技术领域

本申请涉及通信技术领域，特别涉及一种用于实现终端验证的方法、装置、系统、设备及存储介质。

背景技术

在智慧园区、高教、制造、金融等行业，经常出现一些异常终端非法访问服务器的情况。而异常终端的种类有很多，以仿冒终端为例，越来越多的物联网(the internet of things, IOT)终端支持网络接入功能，相比于智能终端(例如电脑、平板、手机等)，IOT终端的自身安全防护功能薄弱，极易被仿冒，为了避免仿冒终端带来安全隐患，网络设备一般通过对其接入的IOT终端进行验证，以确定IOT终端是否为仿冒终端。

目前，终端验证的过程一般是：当接收到一个IOT终端输出的数据流后，网络设备从该数据流中的报文内提取该IOT终端的互联网协议(internet protocol, IP)地址，并查询IP地址库，若IP地址库中存储有该IOT终端的IP地址，则该网络设备确定该IOT终端不是仿冒终端，对该IOT终端验证通过，若IP地址库中未存储该IOT终端的IP地址，则网络设备确定该IOT终端是仿冒终端，对该IOT终端不通过验证。

由于IOT终端的IP地址极易被仿冒，若仿冒终端通过仿冒IP地址库中的IP地址，向网络设备输出数据流，那么，网络设备从该仿冒终端输出的数据流中提取到的IP地址为IP地址库中的IP地址，则网络设备就会对该仿冒终端验证通过，可见，网络设备通过上述终端验证的过程，并不能准确地验证出仿冒终端，也即是终端验证的准确度低。

发明内容

本申请提供了一种用于实现终端验证的方法、装置、系统、设备及存储介质，能够提高终端验证的准确度。该技术方案如下：

第一方面，提供了一种用于实现终端验证的方法，所述方法包括：

获取第一终端的第一传输特征；基于所述第一传输特征，对所述第一传输特征进行重构，得到第二传输特征；若所述第一传输特征与所述第二传输特征之间的差异度大于或等于目标差异度，确定所述第一终端未通过验证；其中，所述第一传输特征为所述第一终端传输的至少一个第一数据流的总体传输特征，所述第二传输特征为重构出的所述第一传输特征。

需要说明的是，重构是指重新构造，所述基于所述第一传输特征，对所述第一传输特征进行重构是指：在所述第一传输特征的基础上，通过预设算法再重新构造出一个第二传输特征，重新构造出的所述第二传输特征尽可能与所述第一传输特征一致。

该预设算法用于尽可能重构出正常传输特征，该预设算法包括降维编码和升维解码，其中，降维编码为降低传输特征维度的一种编码方式，升维编码为升高传输特征维度的一种编码方式。可选地，所述基于所述第一传输特征对所述第一传输特征包括：对所述第一传输特征进行降维编码，对降维编码后的所述第一传输特征进行升维解码。可选地，该预设算法由下文的目标模型来表达。

本方法通过重构终端的传输特征，来对终端进行验证，例如若重构出的传输特征与终端的传输特征之间的差异较大，则说明该终端的传输特征出现异常，该终端为异常终端，则确定该终端未通过验证，由于终端具有特定的正常传输特征，正常传输特征不易仿冒，因此，本方法能够准确地验证出各种异常终端，提高了终端验证的准确度，而仿冒终端为异常终端的一种，因此，该本方法也能够准确的验证出仿冒终端，而不是通过简单的对该终端的IP地址进行验证的方式，以防对仿冒终端验证通过。

需要说明的是，正常终端的传输特征也即是终端的正常传输特征，异常终端的传输特征也即是终端的异常传输特征。

在一种可能的实现方式中，所述第一传输特征包括上行传输特征，所述上行传输特征为所述至少一个第一数据流中至少一个上行数据流的总体传输特征。

在一种可能的实现方式中，所述上行传输特征包括上行报文特征、上行流特征中的至少一个，所述上行报文特征为所述至少一个上行数据流中上行报文的总体特征，所述上行流特征为所述至少一个上行数据流的统计特征。

在一种可能的实现方式中，所述上行报文特征包括上行报文平均传输间隔、上行负载平均值、上行总负载大小、上行报文个数、上行目标报文个数、上行目标报文占比、上行报文负载波动值中的至少一个，所述上行报文平均传输间隔为在一个时间窗口内所述上行报文的平均传输间隔，所述上行负载平均值为在所述时间窗口内所述至少一个上行数据流中目标报文的负载的平均大小，所述上行总负载大小为在所述时间窗口内所述至少一个上行数据流中目标报文的负载的总大小，所述上行报文个数为在所述时间窗口内所述至少一个上行数据流中上行报文的个数，所述上行目标报文个数在所述时间窗口内所述至少一个上行数据流中目标报文的个数，所述上行目标报文占比为在所述时间窗口内所述至少一个上行数据流中目标报文的占比，所述上行报文负载波动值用于指示在所述时间窗口内所述至少一个上行数据流中目标报文的大小波动情况；

所述上行流特征包括上行终端端口波动值、上行数据流总个数、上行目标数据流个数、至少一种数据流类型中每种数据流类型下的上行数据流个数、至少一种传输协议类型中每种传输协议类型下的上行数据流个数中的至少一个，所述上行终端端口波动值用于指示在所述时间窗口内所述第一终端中所述至少一个上行数据流的输出端口的波动情况，所述上行目标数据流为所对应的服务器输入端口属于目标端口范围的上行数据流。

在一种可能的实现方式中，所述上行报文特征还包括第一接收窗口波动值、第一接收窗口大小平均值中的至少一个，所述第一接收窗口波动值用于指示在所述时间窗口内所述上行报文携带的接收窗口大小的波动情况。

在一种可能的实现方式中,所述第一接收窗口波动值为在所述时间窗口内所述上行报文携带的接收窗口大小的标准差。

在一种可能的实现方式中,所述第一传输特征还包括所述至少一个第一数据流的总个数、下行传输特征中的至少一个,所述下行传输特征为所述至少一个第一数据流中至少一个下行数据流的总体传输特征。

在一种可能的实现方式中,所述下行传输特征包括下行报文特征、下行流特征中的至少一个,所述下行报文特征为所述至少一个下行数据流中下行报文的总体特征,所述下行流特征为所述至少一个下行数据流的统计特征。

在一种可能的实现方式中,所述下行报文特征包括下行报文平均传输间隔、下行负载平均值、下行总负载大小、下行报文个数、下行目标报文个数、下行目标报文占比、下行报文负载波动值中的至少一个,所述下行报文平均传输间隔为在一个时间窗口内所述下行报文的平均传输间隔,所述下行负载平均值为在所述时间窗口内所述至少一个下行数据流中目标报文的负载的平均大小,所述下行总负载大小为在所述时间窗口内所述至少一个下行数据流中目标报文的负载的总大小,所述下行报文个数为在所述时间窗口内所述至少一个下行数据流中下行报文的个数,所述下行目标报文个数在所述时间窗口内所述至少一个下行数据流中目标报文的个数,所述下行目标报文占比为在所述时间窗口内所述至少一个下行数据流中目标报文的占比,所述下行报文负载波动值用于指示在所述时间窗口内所述至少一个下行数据流中目标报文的大小波动情况;

所述下行流特征包括下行终端端口波动值、下行数据流总个数、下行目标数据流个数、至少一种数据流类型中每种数据流类型下的下行数据流个数、至少一种传输协议类型中每种传输协议类型下的下行数据流个数中的至少一个,所述下行终端端口波动值用于指示在所述时间窗口内所述第一终端中所述至少一个下行数据流的输入端口的波动情况,所述下行目标数据流为对应的服务器输出端口属于目标端口范围的下行数据流。

在一种可能的实现方式中,所述下行报文特征还包括第二接收窗口波动值、第二接收窗口大小平均值中的至少一个,所述第二接收窗口波动值用于指示所述下行报文携带的接收窗口大小的波动情况。

在一种可能的实现方式中,所述第二接收窗口波动值为在所述时间窗口内所述下行报文携带的接收窗口大小的标准差。

在一种可能的实现方式中,所述获取第一终端的第一传输特征包括:

获取所述至少一个第一数据流中每个第一数据流的流传输特征;基于所述至少一个第一数据流的流传输特征,获取所述第一传输特征。

在一种可能的实现方式中,一个第一数据流的流传输特征包括所述第一数据流的传输信息、数据流类型、目标端口类型、报文特征中的至少一个,所述传输信息用于指示数据流的传输属性,所述目标端口类型为服务器中传输所述第一数据流的端口的端口类型,所述报文特征为所述第一数据流中报文的特征。

在一种可能的实现方式中,所述传输信息包括所述第一数据流的五元组中的至少一元;

所述报文特征包括报文传输间隔总和、负载大小、负载平方和、目标报文个数、报文总个数、接收窗口波动值、窗口总大小、窗口平方和中的至少一个,所述报文传输间隔总和为在一个时间窗口内所述第一数据流中报文之间的传输间隔的总时长,所述负载大小为在所述

时间窗内所述第一数据流中目标报文的负载的总大小,所述负载平方和为所述目标报文的负载大小平方和,所述目标报文个数为在所述时间窗口内所述报文中目标报文的总个数,所述报文总个数为在所述时间窗口内所述报文的总个数,所述接收窗口波动值用于指示在所述时间窗口内所述报文携带的接收窗口大小的波动情况,所述窗口总大小为在所述时间窗口内所述报文携带的接收窗口大小的总和,所述窗口平方和为所述滑动窗口的大小的平方和。

在一种可能的实现方式中,所述传输信息还包括方向标识、所述时间窗口的标识中的至少一个,所述方向标识用于指示所述第一数据流的传输方向。

在一种可能的实现方式中,所述基于所述第一传输特征,对所述第一传输特征进行重构,得到第二传输特征包括:

将所述第一传输特征输入目标模型,由所述目标模型基于输入的所述第一传输特征,重构所述第一传输特征,输出所述第二传输特征。

在一种可能的实现方式中,所述将所述第一传输特征输入目标模型之前,所述方法还包括:

将目标终端类型下至少一个第二终端的多个第三传输特征作为初始模型的输入和输出,进行训练,得到所述目标模型,所述目标终端类型为所述第一终端的终端类型,一个第三传输特征为一个第二终端传输的至少一个数据流的总体传输特征。

在一种可能的实现方式中,所述将所述第一传输特征输入目标模型之前,所述方法还包括:

将目标终端类型下多个目标终端的多个第四传输特征输入所述目标模型,由所述目标模型基于输入的所述多个第四传输特征,重构每个第四传输特征,输出多个第五传输特征;基于所述多个第五传输特征与所述多个第四传输特征,获取所述目标差异度;

其中,所述目标终端类型为所述第一终端的终端类型,所述多个第四传输特征与所述多个第五传输特征一一对应,一个第四传输特征为一个目标终端传输的至少一个数据流的总体传输特征。

在一种可能的实现方式中,所述基于所述多个第五传输特征与所述多个第四传输特征,获取所述目标差异度包括:

基于所述多个第五传输特征中至少一个第五传输特征与对应的第四传输特征之间的差异度,获取所述目标差异度。

在一种可能的实现方式中,所述将所述第一传输特征输入目标模型之前,所述方法还包括:

将目标终端类型下多个目标终端的多个第六传输特征输入所述目标模型,由所述目标模型基于输入的所述多个第六传输特征,重构每个第六传输特征,输出多个第七传输特征;基于所述多个第七传输特征与对应的第六传输特征之间的差异度,确定所述目标模型通过验证;

其中,所述目标终端类型为所述第一终端的终端类型,所述多个第六传输特征与所述多个第七传输特征一一对应,一个第六传输特征为一个目标终端传输的至少一个数据流的总体传输特征。

在一种可能的实现方式中,所述将所述第一传输特征输入目标模型之前,所述方法还包括:

获取所述至少一个第二终端传输的至少一个第二数据流的传输信息;将所述传输信息与

所述第二终端的终端类型进行关联存储；基于所述终端类型关联的传输信息，获取所述至少一个第二终端的多个传输特征；

其中，所述传输信息用于指示数据流的传输属性，一个传输特征为终端传输的至少一个数据流的总体传输特征。

在一种可能的实现方式中，所述将所述第一传输特征输入目标模型之前，所述方法还包括：

从控制设备接收所述目标模型。

在一种可能的实现方式中，所述方法的执行主体为控制设备或网络设备。

第二方面，提供了一种用于实现终端验证的方法，所述方法包括：

获取目标终端类型的至少一个第二终端的多个第三传输特征；将所述多个第三传输特征作为初始模型的输入和输出，进行训练，得到目标模型；

其中，一个第三传输特征为一个第二终端传输的至少一个数据流的总体传输特征，所述目标模型用于重构所述目标终端类型的被验证终端的传输特征，以对所述被验证终端进行验证，所述传输特征为所述被验证终端传输的至少一个数据流的总体传输特征。

在一种可能的实现方式中，所述将所述多个第三传输特征作为初始模型的输入和输出，进行训练之后，所述方法还包括：

向网络设备发送所述目标模型。

在一种可能的实现方式中，所述将所述多个第三传输特征作为初始模型的输入和输出，进行训练之前，所述方法还包括：

将所述目标终端类型下多个目标终端的多个第四传输特征输入所述目标模型，由所述目标模型基于输入的所述多个第四传输特征，重构每个第四传输特征，输出多个第五传输特征；基于所述多个第五传输特征与所述多个第四传输特征，获取所述目标差异度；

其中，所述多个第四传输特征与所述多个第五传输特征一一对应，一个第四传输特征为一个目标终端传输的至少一个数据流的总体传输特征。

在一种可能的实现方式中，所述基于所述多个第五传输特征与所述多个第四传输特征，获取所述目标差异度包括：

基于所述多个第五传输特征中至少一个第五传输特征与对应的第四传输特征之间的差异度，获取所述目标差异度。

在一种可能的实现方式中，所述将所述多个第三传输特征作为初始模型的输入和输出，进行训练之前，所述方法还包括：

将所述目标终端类型下多个目标终端的多个第六传输特征输入所述目标模型，由所述目标模型基于输入的所述多个第六传输特征，重构每个第六传输特征，输出多个第七传输特征；基于所述多个第七传输特征与对应的第六传输特征之间的差异度，确定所述目标模型通过验证；

其中，所述多个第六传输特征与所述多个第七传输特征一一对应，一个第六传输特征为一个目标终端传输的至少一个数据流的总体传输特征。

在一种可能的实现方式中，所述获取目标终端类型的至少一个第二终端的多个第三传输特征之前，所述方法还包括：

获取所述至少一个第二终端传输的至少一个第二数据流的传输信息；将所述传输信息与

所述第二终端的终端类型进行关联存储；基于所述终端类型关联的传输信息，获取所述至少一个第二终端的多个传输特征；

其中，所述传输信息用于指示数据流的传输属性，一个传输特征为终端传输的至少一个数据流的总体传输特征。

第三方面，提供了一种用于实现终端验证的系统，所述系统包括控制设备和网络设备；

所述控制设备用于：

获取目标终端类型的至少一个第二终端的多个第三传输特征，一个第三传输特征为一个第二终端传输的至少一个数据流的总体传输特征；

将所述多个第三传输特征作为初始模型的输入和输出，进行训练，得到目标模型；

向所述网络设备发送所述目标模型；

所述网络设备用于：

获取所述目标终端类型的第一终端的第一传输特征，所述第一传输特征为所述第一终端传输的至少一个第一数据流的总体传输特征；

将所述第一传输特征输入所述目标模型，由所述目标模型基于输入的所述第一传输特征，重构所述第一传输特征，输出第二传输特征，所述第二传输特征为重构出的所述第一传输特征；

若所述第一传输特征与所述第二传输特征之间的差异度大于或等于目标差异度，确定所述第一终端未通过验证。

在一种可能的实现方式中，所述控制设备还用于：

将所述目标终端类型下多个目标终端的多个第四传输特征输入所述目标模型，由所述目标模型基于输入的所述多个第四传输特征，重构每个第四传输特征，输出多个第五传输特征；基于所述多个第五传输特征与所述多个第四传输特征，获取所述目标差异度；

其中，所述多个第四传输特征与所述多个第五传输特征一一对应，一个第四传输特征为一个目标终端传输的至少一个数据流的总体传输特征。

在一种可能的实现方式中，所述控制设备还用于：

基于所述多个第五传输特征中至少一个第五传输特征与对应的第四传输特征之间的差异度，获取所述目标差异度。

在一种可能的实现方式中，所述控制设备还用于：

将所述目标终端类型下多个目标终端的多个第六传输特征输入所述目标模型，由所述目标模型基于输入的所述多个第六传输特征，重构每个第六传输特征，输出多个第七传输特征；基于所述多个第七传输特征与对应的第六传输特征之间的差异度，确定所述目标模型通过验证；

其中，所述多个第六传输特征与所述多个第七传输特征一一对应，一个第六传输特征为一个目标终端传输的至少一个数据流的总体传输特征。

在一种可能的实现方式中，所述控制设备还用于：

获取所述至少一个第二终端传输的至少一个第二数据流的传输信息；将所述传输信息与所述第二终端的终端类型进行关联存储；基于所述终端类型关联的传输信息，获取所述至少一个第二终端的多个传输特征；

其中，所述传输信息用于指示数据流的传输属性，一个传输特征为终端传输的至少一个

数据流的总体传输特征。

在一种可能的实现方式中，所述第一传输特征包括上行传输特征，所述上行传输特征为所述至少一个第一数据流中至少一个上行数据流的总体传输特征。

在一种可能的实现方式中，所述上行传输特征包括上行报文特征、上行流特征中的至少一个，所述上行报文特征为所述至少一个上行数据流中上行报文的总体特征，所述上行流特征为所述至少一个上行数据流的统计特征。

在一种可能的实现方式中，所述上行报文特征包括上行报文平均传输间隔、上行负载平均值、上行总负载大小、上行报文个数、上行目标报文个数、上行目标报文占比、上行报文负载波动值中的至少一个，所述上行报文平均传输间隔为在一个时间窗口内所述上行报文的平均传输间隔，所述上行负载平均值为在所述时间窗口内所述至少一个上行数据流中目标报文的负载的平均大小，所述上行总负载大小为在所述时间窗口内所述至少一个上行数据流中目标报文的负载的总大小，所述上行报文个数为在所述时间窗口内所述至少一个上行数据流中上行报文的个数，所述上行目标报文个数在所述时间窗口内所述至少一个上行数据流中目标报文的个数，所述上行目标报文占比为在所述时间窗口内所述至少一个上行数据流中目标报文的占比，所述上行报文负载波动值用于指示在所述时间窗口内所述至少一个上行数据流中目标报文的大小波动情况；

所述上行流特征包括上行终端端口波动值、上行数据流总个数、上行目标数据流个数、至少一种数据流类型中每种数据流类型下的上行数据流个数、至少一种传输协议类型中每种传输协议类型下的上行数据流个数中的至少一个，所述上行终端端口波动值用于指示在所述时间窗口内所述第一终端中所述至少一个上行数据流的输出端口的波动情况，所述上行目标数据流为所对应的服务器输入端口属于目标端口范围的上行数据流。

在一种可能的实现方式中，所述上行报文特征还包括第一接收窗口波动值、第一接收窗口大小平均值中的至少一个，所述第一接收窗口波动值用于指示在所述时间窗口内所述上行报文携带的接收窗口大小的波动情况。

在一种可能的实现方式中，所述第一传输特征还包括所述至少一个第一数据流的总个数、下行传输特征中的至少一个，所述下行传输特征为所述至少一个第一数据流中至少一个下行数据流的总体传输特征。

在一种可能的实现方式中，所述下行传输特征包括下行报文特征、下行流特征中的至少一个，所述下行报文特征为所述至少一个下行数据流中下行报文的总体特征，所述下行流特征为所述至少一个下行数据流的统计特征。

在一种可能的实现方式中，所述下行报文特征包括下行报文平均传输间隔、下行负载平均值、下行总负载大小、下行报文个数、下行目标报文个数、下行目标报文占比、下行报文负载波动值中的至少一个，所述下行报文平均传输间隔为在一个时间窗口内所述下行报文的平均传输间隔，所述下行负载平均值为在所述时间窗口内所述至少一个下行数据流中目标报文的负载的平均大小，所述下行总负载大小为在所述时间窗口内所述至少一个下行数据流中目标报文的负载的总大小，所述下行报文个数为在所述时间窗口内所述至少一个下行数据流中下行报文的个数，所述下行目标报文个数在所述时间窗口内所述至少一个下行数据流中目标报文的个数，所述下行目标报文占比为在所述时间窗口内所述至少一个下行数据流中目标报文的占比，所述下行报文负载波动值用于指示在所述时间窗口内所述至少一个下行数据流

中目标报文的大小波动情况；

所述下行流特征包括下行终端端口波动值、下行数据流总个数、下行目标数据流个数、至少一种数据流类型中每种数据流类型下的下行数据流个数、至少一种传输协议类型中每种传输协议类型下的下行数据流个数中的至少一个，所述下行终端端口波动值用于指示在所述时间窗口内所述第一终端中所述至少一个下行数据流的输入端口的波动情况，所述下行目标数据流为对应的服务器输出端口属于目标端口范围的下行数据流。

在一种可能的实现方式中，所述下行报文特征还包括第二接收窗口波动值、第二接收窗口大小平均值中的至少一个，所述第二接收窗口波动值用于指示所述下行报文携带的接收窗口大小的波动情况。

在一种可能的实现方式中，所述网络设备还用于：

获取所述至少一个第一数据流中每个第一数据流的流传输特征；

基于所述至少一个第一数据流的流传输特征，获取所述第一传输特征。

在一种可能的实现方式中，一个第一数据流的流传输特征包括所述第一数据流的传输信息、数据流类型、目标端口类型、报文特征中的至少一个，所述传输信息用于指示数据流的传输属性，所述目标端口类型为服务器中传输所述第一数据流的端口的端口类型，所述报文特征为所述第一数据流中报文的特征。

在一种可能的实现方式中，所述传输信息包括所述第一数据流的五元组中的至少一元；

所述报文特征包括报文传输间隔总和、负载大小、负载平方和、目标报文个数、报文总个数、接收窗口波动值、窗口总大小、窗口平方和中的至少一个，所述报文传输间隔总和为在一个时间窗口内所述第一数据流中报文之间的传输间隔的总时长，所述负载大小为在所述时间窗口内所述第一数据流中目标报文的负载的总大小，所述负载平方和为所述目标报文的负载大小的平方和，所述目标报文个数为在所述时间窗口内所述报文中目标报文的总个数，所述报文总个数为在所述时间窗口内所述报文的总个数，所述接收窗口波动值用于指示在所述时间窗口内所述报文携带的接收窗口大小的波动情况，所述窗口总大小为在所述时间窗口内所述报文携带的接收窗口大小的总和，所述窗口平方和为所述滑动窗口的大小的平方和。

在一种可能的实现方式中，所述传输信息还包括方向标识、所述时间窗口的标识中的至少一个，所述方向标识用于指示所述第一数据流的传输方向。

第四方面，提供了一种用于实现终端验证的装置，用于执行上述用于实现终端验证的方法。具体地，该用于实现终端验证的装置包括用于执行上述第一方面或上述第一方面的任一种可选方式提供的用于实现终端验证的方法的功能模块。

第五方面，提供了一种用于实现终端验证的装置，用于执行上述用于实现终端验证的方法。具体地，该用于实现终端验证的装置包括用于执行上述第二方面或上述第二方面的任一种可选方式提供的用于实现终端验证的方法的功能模块。

第六方面，提供了一种电子设备，该电子设备包括处理器和存储器，该存储器中存储有至少一条程序代码，该程序代码由该处理器加载并执行以实现如上述第一方面或上述第一方面的任一种可选方式提供的用于实现终端验证的方法所执行的操作，或实现如上述第二方面或上述第二方面的任一种可选方式提供的用于实现终端验证的方法所执行的操作。

第七方面，提供了一种计算机可读存储介质，该存储介质中存储有至少一条程序代码，该程序代码由处理器加载并执行以实现如上述第一方面或上述第一方面的任一种可选方式提

供的用于实现终端验证的方法所执行的操作，或实现如上述第二方面或上述第二方面的任何一种可选方式提供的用于实现终端验证的方法所执行的操作。

第八方面，提供了一种计算机程序产品或计算机程序，该计算机程序产品或计算机程序包括程序代码，该程序代码存储在计算机可读存储介质中，电子设备的处理器从计算机可读存储介质读取该程序代码，处理器执行该程序代码，使得该电子设备执行上述第一方面或上述第一方面的任一种可选方式提供的用于实现终端验证的方法，或执行上述第二方面或上述第二方面的任一种可选方式提供的用于实现终端验证的方法。

附图说明

图 1 是本申请实施例提供的一种用于实现终端验证的系统的示意图；

图 2 是本申请实施例提供的一种电子设备的结构示意图；

图 3 是本申请实施例提供的一种终端类型识别的流程图；

图 4 是本申请实施例提供的一种存储终端类型的示意图；

图 5 是本申请实施例提供的一种模型获取方法的流程图；

图 6 是本申请实施例提供的一种开启训练的示意图；

图 7 是本申请实施例提供的一种传输特征获取的示意图；

图 8 是本申请实施例提供的一种用于实现终端验证的方法的流程图；

图 9 是本申请实施例提供的一种用于实现终端验证的方法的示意图；

图 10 是本申请实施例提供的一种用于实现终端验证的装置的结构示意图；

图 11 是本申请实施例提供的一种用于实现终端验证的装置的结构示意图。

具体实施方式

为使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请实施方式作进一步地详细描述。

图 1 是本申请实施例提供的一种用于实现终端验证的系统的示意图，参见图 1，该系统 100 包括多个终端 101、多个网络设备 102、多个服务器 103 以及控制设备 104。

一个终端 101，用于通过网络设备 102 向服务器 103 发送数据流。在一种可能的实现方式中，该终端 101 向网络设备 102 输出数据流，由网络设备 102 向服务器 103 转发该终端 101 输出的数据流，此时该终端 101 也即是输出数据流的设备，服务器 103 为输入数据流的设备。该终端 101 还用于通过网络设备 102 从服务器 103 接收数据流。在一种可能的实现方式中，服务器 103 向网络设备 102 输出数据流，由网络设备 102 向终端 101 转发服务器 103 输出的数据流，此时该终端 101 为输入数据流的设备，服务器 103 为输出数据流的设备。

为了便于描述，将输出数据流的设备记为“第一设备”，将输入数据流的设备记为“第二设备”。为了区分数据流的传输方向，将终端 101 输出的数据流记为“上行数据流”，此时终端 101 为第一设备，服务器 103 为第二设备；将终端 101 输入的数据流记为“下行数据流”，此时终端 101 为第二设备，服务器 103 为第一设备。其中，终端 101 的上行数据流和下行数据流均为终端 101 传输的数据流。在一种可能的实现方式中，终端 101 为 IOT 终端，例如摄像头、音响、打印机、IP 话机、自动取款机（automatic teller machine, ATM）或查询机等。

网络设备 102 除了用于转发数据流之外，还用于采集终端 101 的传输特征，并向控制设

备 104 上报采集到的终端 101 的传输特征, 由控制设备 104 基于终端 101 的传输特征, 对该终端 101 进行验证, 以确定该终端 101 为正常终端还是异常终端。

其中, 正常终端为行为正常的终端, 终端按照预设规则与服务器进行合法的交互, 则视为行为正常。例如, 若终端在预设规则所规定的时间段内通过访问服务器, 进行预设业务, 或者, 若终端在预设规则所规定的权限范围内与服务器进行合法交互, 则该终端的行为正常, 该终端为正常终端。异常终端为行为异常的终端, 终端未按照预设规则与服务器交互, 或者终端与服务器的交互不合法, 则视为行为异常。例如, 若终端仿冒具有预设规则所规定的权限的终端, 与服务器进行非法交互, 或者, 若终端在预设规则规定的权限外与服务器之间进行非法交互, 则该终端的行为异常, 该终端为异常终端。终端与服务器非法交互包括终端非法访问服务器中的特定内容, 或者终端在预设规则规定的时间段以外的时间访问服务器, 或者终端被黑客攻破作为跳板, 恶意攻击网络, 或者终端进行了非法业务等各种情况。

网络设备 102 采集的传输特征为终端 101 的实际传输特征, 且能够体现终端 101 的行为。可选地, 控制设备 104 具有对终端 101 的实际传输特征进行重构的能力, 控制设备 104 对终端 101 的实际传输特征进行重构, 得到重构传输特征, 其中, 重构传输特征也即是重构出的实际传输特征; 若该实际传输特征与该重构传输特征之间的差异度小于目标差异度, 说明该实际传输特征与该重构传输特征之间的差异较小, 该控制设备 104 确定该实际传输特征所体现的终端行为正常, 该实际传输特征为正常传输特征, 并确定该终端 101 是正常终端, 则该控制设备 104 对该终端 101 通过验证; 若该实际传输特征与该重构传输特征之间的差异度大于或等于目标差异度, 说明该实际传输特征与该重构传输特征之间的差异较大, 该控制设备 104 确定该实际传输特征所体现的终端行为异常, 该实际传输特征为异常传输特征, 并确定则该终端 101 是异常终端, 则该控制设备 104 对该终端 101 不通过验证。

在一种可能的实现方式中, 控制设备 104 基于目标模型重构实际传输特征。控制设备 104 基于目标模型重构实际传输特征之前, 先通过训练来获取该目标模型。可选地, 网络设备 102 采集同一种终端类型下至少一个正常终端 101 的多个传输特征, 并将该多个传输特征发送至控制设备 104, 由控制设备 104 将该多个传输特征作为初始模型的输入和输出, 进行训练, 得到该目标模型, 以便后续控制设备 104 基于该目标模型重构该终端类型下终端 101 的实际传输特征。可选地, 该控制设备 104 在进行训练的过程中, 还能够显示训练进度, 以使用户能够获悉训练进度。

需要说明的是, 上述介绍的网络设备 102 负责采集传输特征, 由控制设备 104 基于网络设备 102 采集到的传输特征, 训练出的目标模型, 并基于目标模型对终端 101 进行验证。而在一种可能的实现方式中, 网络设备 102 负责采集传输特征, 由该控制设备 104 基于网络设备 102 采集到的传输特征, 训练出至少一个目标模型, 每个目标模型对应一个终端类型, 并将该至少一个目标模型发送至网络设备 102, 由网络设备 102 在采集到任一终端 101 的传输特征后, 基于该任一终端 101 的终端类型, 确定该至少一个目标模型中该任一终端 101 的终端类型所对应的目标模型, 该网络设备 102 并基于确定出的目标模型重构该任一终端 101 的传输特征, 以对该任一终端 101 进行验证。

而在一种可能的实现方式中, 网络设备 102 将其转发的数据流转发至控制设备 104, 由控制设备 104 基于网络设备 102 转发的数据流, 采集终端 101 的传输特征, 并进行训练, 并基于训练出的目标模型对终端 101 进行验证。可选地, 网络设备 102 包括防火墙设备、路由

器和交换机中的一种。

上述介绍的网络设备 102 和控制设备 104 是分离的 2 个电子设备，而在另一种可能的实现方式中，网络设备 102 和控制设备 104 为同一个电子设备，该电子设备兼具网络设备 102 和控制设备 104 的功能。

图 2 是本申请实施例提供的一种电子设备的结构示意图，该电子设备 200 提供为上述的网络设备和/或控制设备，该电子设备 200 可因配置或性能不同而产生比较大的差异，包括一个或一个以上处理器 201 和一个或一个以上的存储器 202，其中，所述处理器 201 为中央处理器（central processing units, CPU）或其他类型的处理器，所述存储器 202 中存储有至少一条程序代码，所述至少一条程序代码由所述处理器 201 加载并执行以实现下述各个方法实施例提供的网络设备和/或控制设备所执行的步骤。当然，可选地，该电子设备 200 还具有有线或无线网络接口、键盘以及输入输出接口等部件，以便进行输入输出，该电子设备 200 还包括其他用于实现设备功能的部件，在此不做赘述。

在示例性实施例中，还提供了一种计算机可读存储介质，例如包括程序代码的存储器，上述程序代码可由终端中的处理器执行以完成下述实施例中的用于实现终端验证的方法。例如，该计算机可读存储介质是非临时计算机可读存储介质，如只读存储器（read-only memory, ROM）、随机存取存储器（random access memory, RAM）、只读光盘（compact disc read-only memory, CD-ROM）、磁带、软盘和光数据存储设备等。

在终端验证系统的初始化过程中，控制设备能够对该终端验证系统中的终端进行类型识别，以确定该终端验证系统中终端的终端类型，为了进一步说明控制设备对该终端验证系统中的终端进行类型识别的过程，参见如图 3 所示的本申请实施例提供的一种终端类型识别的流程图。

301、控制设备获取类型识别指令，该类型识别指令用于指示识别终端的终端类型。

该类型识别指令包括识别标识，该识别标识用于指示识别终端的终端类型。在一种可能的实现方式中，该类型识别指令由用户操作来触发。当该控制设备检测到用户在该控制设备上执行了用于触发该类型识别指令的操作时，触发该控制设备获取到该类型识别指令。

当终端验证系统的组网较为复杂时，终端验证系统中的控制设备还能够分为多级控制设备，分别为中心控制设备以及多个区域控制设备，其中，中心控制设备用于管理多个区域控制设备，每个区域控制设备用于管理至少一个网络区域中的网络设备。当中心控制设备基于用户操作获取到类型识别指令后，还能够向各个区域控制设备发送获取到的类型识别指令，以便各个区域控制设备均能从该中心控制设备接收到该类型识别指令，此时本步骤 301 中的该控制设备为区域控制设备。

在一种可能的实现方式中，当该控制设备每获取到一次该类型识别指令后，该控制设备执行一次终端类型识别的过程（也即是下述步骤 302-308）。在另一种可能的实现方式中，控制设备仅接收一次类型识别指令，当接收到该类型识别指令后，周期性地执行终端类型识别的过程。本申请实施例对终端类型识别的时机不作具体限定。

302、该控制设备向至少一个网络设备发送信息获取指令，该信息获取指令用于指示网络设备上传数据流的传输信息。

该至少一个网络设备为该控制设备负责管理的网络设备。数据流的传输信息用于指示该数据流的传输属性，例如传输地址、传输端口、传输协议、传输方向、传输时间分别是数据

流的一种传输属性。该信息获取指令包括至少一种传输属性的属性标识，以指示网络设备基于该至少一种传输属性的属性标识，上传数据流的至少一种传输属性。

303、对于该至少一个网络设备中的任一网络设备，该任一网络设备接收该信息获取指令。

304、该任一网络设备基于该信息获取指令，获取至少一个数据流的至少一个传输信息。

该至少一个数据流为该网络设备在一个时间窗口内传输的数据流，该时间窗口的时长为目标时长，该时间窗口为该任一网络设备检测至少一个数据流的检测时间。可选地，该至少一个数据流包括至少一个上行数据流，可选地，该至少一个数据流还包括至少一个下行数据流。一个数据流的传输信息包括该第一数据流的五元组中的至少一元，该第一数据流的五元组包括该数据流的源地址信息、源端口标识、目的地址信息、目的端口标识、传输协议类型。

该源地址信息用于指示输出该数据流的第一设备的网络地址，该第一设备为向该网络设备输出该数据流的设备，例如服务器或者终端，该源地址信息包括该第一设备的 IP 地址。源端口标识用于指示该第一设备中用于输出该数据流的输出端口。

该目的地址信息用于指示输入该数据流的第二设备的 IP 地址，该第二设备为输入该数据流的设备，也即是用于接收该网络设备转发的数据流的设备，例如服务器或终端，该目的地址信息包括该第二设备的网络地址。该目的端口标识用于指示该第二设备中用于输入该数据流的输入端口。

需要说明的是，该第一设备和该第二设备中的一个设备为终端，另一个设备为服务器，若该第一设备为终端，则该数据流也即是上行数据流，若该第二设备为终端，则该数据流的也即是下行数据流。可选地，一个设备的网络地址包括该设备的 IP 地址和媒体存取控制(media access control, MAC) 地址中的至少一个，该第一设备的网络地址也即是源网络地址，例如源 IP 地址、源 MAC 地址。该第二设备的网络地址也即是目的网络地址，例如目的 IP 地址、目的 MAC 地址。需要说明的是，在本申请实施例中以设备的网络地址为 IP 地址为例进行说明。

该传输协议类型用于指示该数据流所遵循的传输协议，例如传输控制协议(transmission control protocol, TCP)、用户数据报协议(user datagram protocol, UDP) 或互联网控制报文协议(internet control message protocol, ICMP)。

在一种可能的实现方式中，该传输信息还包括方向标识、该时间窗口的标识中的至少一个，该方向标识包括上行标识或下行标识，若该方向标识为上行标识，则指示该数据流为上行数据流；若该方向标识为下行标识，则指示该数据流为下行数据流。

该任一网络设备包括多个端口，分别为至少一个第一输入端口、至少一个第一输出端口、至少一个第二输入端口以及至少一个第二输出端口，其中，第一输入端口用于输入从终端输出的数据流，也即是用于输入上行数据流；第一输出端口用于向服务器输出该上行数据流；第二输入端口用于输入从服务器输出的数据流，也即是用于输入下行数据流；第二输出端口用于向终端输出该下行数据流。

该任一网络设备基于该任一网络设备内的输入端口或输出端口传输的数据流，获取该至少一个数据流的传输信息。在一种可能的实现方式中，该任一网络设备基于该任一网络设备内的输入端口以及该信息获取指令，获取该至少一个数据流的传输信息的过程由下述步骤 3041-3043 来实现。

步骤 3041、对于该至少一个第一输入端口或至少一个第二输入端口中的任一输入端口，该任一网络设备在一个时间窗口内获取该任一输入端口输入的多个报文的元数据。

该任一网络设备内设置有目标时长的时间窗口，该任一网络设备在该时间窗口内对该任一网络设备所传输的数据流进行检测，以获取该任一网络设备所传输的数据流在该时间窗口内的流传输特征，其中，数据流的传输信息属于数据流的流传输特征。该时间窗口为该任一网络设备接收到该信息获取指令后的目标时长所在的时间段，例如，该任一网络设备接收到该信息获取指令后的目标时长之内执行本步骤 3041，那么，该任一网络设备接收到该信息获取指令后的目标时长也即是该时间窗口。

该多个报文为在该时间窗口内该任一输入端口内输入的数据流中的报文。其中，一个报文的元数据包括该报文所属的数据流的流标识信息、源 MAC 地址以及目的 MAC 地址，可选地，数据流的流标识信息为一个五元组，包括该数据流的源 IP 地址、源端口标识、目的 IP 地址、目的端口标识以及传输协议类型。

对于该任一输入端口，该任一网络设备在该时间窗口内的多个时间点，从该任一输入端口输入的数据流中分别获取多个报文，并解析该多个报文，得到该多个报文的元数据 (metadata)。

步骤 3042、该任一网络设备对该多个报文的元数据进行去重，得到至少一个报文的元数据，该至少一个报文的元数据互不相同，且该至少一个报文中的每个报文分别属于不同的数据流。

在该时间窗口内该任一输入端口可能输入一个或多个数据流，则该多个报文中的部分报文可能属于同一个数据流，为了避免上传重复信息，该任一网络设备对该多个报文的元数据进行去重，得到至少一个报文的元数据。例如，该多个报文分别为报文 1-3，其中，报文 1 的元数据与报文 2 的元数据相同，与报文 3 的元数据不同，则报文 1 和报文 2 均属于数据流 1，而报文 3 属于数据流 2，则该任一网络设备通过对报文 1-3 的元数据进行去重，保留报文 1 的元数据和报文 3 的元数据。

步骤 3043、对于该至少一个报文中的任一报文，该任一网络设备基于信息获取指令，生成该任一报文所属的数据流的传输信息。

该任一网络设备基于信息获取指令包括的至少一种属性标识，生成该任一报文所属的数据流的传输信息。在一种可能的实现方式中，若该信息获取指令包括传输地址的属性标识，则该任一网络设备将该任一报文的元数据内的源 IP 地址、源 MAC 地址中的至少一个，确定为该数据流的源地址信息，该任一网络设备将该任一报文的元数据内的目的 IP 地址、目的 MAC 地址、中的至少一个，确定为该数据流的目标地址信息，并将该源地址信息以及该目的地址信息添加至该数据流的传输信息中；若该信息获取指令包括传输端口的属性标识，则该任一网络设备将任一报文的元数据内源端口标识以及目的端口标识添加至该数据流的传输信息中；若该信息获取指令包括传输协议的属性标识，则该任一网络设备将该任一报文的元数据内的传输协议类型添加至该数据流的传输信息中；若该信息获取指令包括传输方向的属性标识，则该任一网络设备基于该任一网络设备内用于传输该任一报文的端口或该数据流的源地址信息，确定该数据流的传输方向，并将用于指示该传输方向的方向标识添加至该数据流的传输信息中；若该信息获取指令携带传输时间的属性标识，则该任一网络设备将该时间窗口的标识添加至该数据流的传输信息中。

在一种可能的实现方式中，该任一网络设备基于该任一网络设备内用于传输该任一报文的端口或该数据流的源地址信息，确定该数据流的传输方向的过程为：若该任一网络设备内

用于输入该任一报文的端口为第一输入端口，或该任一网络设备内用于输出该任一报文的端口为第一输出端口，则该数据流为上行数据流，该任一网络设备确定该数据流的传输方向为上行；若该任一网络设备内用于输入该任一报文的端口为第二输入端口，或该任一网络设备内用于输出该任一报文的端口为第二输出端口，则该数据流为下行数据流，该任一网络设备确定该数据流的传输方向为下行；若该数据流的源地址信息所指示的第一设备为终端，则该数据流为上行数据流，该任一网络设备确定该数据流的传输方向为上行；若该数据流的源地址信息所指示的第二设备为服务器，则该数据流为下行数据流，该任一网络设备确定该数据流的传输方向为下行。

例如，在该时间窗口内，该任一网络设备共传输了 3 个数据流，分别为数据流 1-3，其中，数据流 1 和数据流 2 均为上行数据流，数据流 3 为下行数据流，通过本步骤 3043，该任一网络设备能够获取到表 1 所示的数据流 1-3 的传输信息。

表 1

数据流	源 IP 地址	源端口标识	源 MAC 地址	目的 IP 地址	目的端口标识	目的 MAC 地址	方向标识	传输类型
数据流 1	192.168.1.240	43360	AAA	10.137.5.6.31	30	DDD	上行标识	TCP
数据流 2	192.168.1.180	43361	BBB	10.137.5.6.32	40	EEE	上行标识	UDP
数据流 3	10.137.56.30	20	CCC	192.168.1.150	43362	FFF	下行标识	ICMP

若该任一网络设备传输的至少一个数据流包括第二终端传输的至少一个第二数据流，则本步骤 304 所示的过程也即是任一网络设备获取该第二终端传输的至少一个第二数据流的传输信息的过程。

305、该任一网络设备向该控制设备发送该至少一个传输信息。

306、该控制设备接收该至少一个传输信息。

若该至少一个数据流包括第二终端传输的至少一个第二数据流，则本步骤 306 所示的过程也即是控制设备获取该第二终端传输的至少一个第二数据流的传输信息的过程。

307、该控制设备存储该至少一个传输信息。

该控制设备提取每个传输信息中的至少一项信息，并该至少一项信息存储在配置表中，以实现资产识别。在一种可能的实现方式中，该控制设备将每个传输信息中的每一项信息均存储至配置表，则配置表如表 1 所示。

在一种可能的实现方式中，该控制设备将每个传输信息中的部分信息存储至配置表中，该部分信息包括方向标识以及终端的网络地址。可选地，该控制设备将包括同一个方向标识的至少一个传输信息中终端的网络地址与该方向标识进行关联存储。若终端的网络地址为 IP 地址，则该控制设备将方向标识与终端的 IP 地址进行关联存储，若一个传输信息中的方向标识为上行标识，则说明该传输信息所对应的数据流为上行数据流，该传输信息中的源 IP 地址为终端的 IP 地址，则该控制设备将该源 IP 地址添加在配置表中，并与上行标识对应，若一个传输信息中的方向标识为下行标识，则说明该传输信息所对应的数据流为下行数据流，该

传输信息中的目的 IP 地址为终端的 IP 地址,则该控制设备将该目的 IP 地址添加在配置表中,并与下行标识对应。

若该至少一个传输信息如表 1 所示,则该控制设备在表 1 中提取上行标识对应的源 IP 地址以及下行标识对应的目的 IP 地址,并将提取到的源 IP 地址与上行标识关联存储在表 2 所示配置表中,并将提取到的目的 IP 地址与下行标识关联存储在表 2 所示的配置表中。

表 2

上行标识	下行标识
源 IP 地址	目的 IP 地址
192.168.1.240	192.168.1.150
192.168.1.180	

308、对于该至少一个传输信息中的任一传输信息,该控制设备将该任一传输信息与第一目标终端的终端类型进行关联存储,其中,该第一目标终端用于传输该任一传输信息所对应的数据流。

终端类型包括摄像头、音响、打印机、IP 话机、ATM 或查询机。该控制设备将该任一传输信息中的至少一项信息与该目标终端的终端类型进行关联存储。可选地,该控制设备将该至少一项信息与该第一目标终端的终端类型关联存储在资产表中,该资产表用于存储多种终端类型,该资产表存储在控制设备的本地或云空间。

该控制设备从配置表中获取该任一传输信息中的至少一项信息,并基于该至少一项信息,查询资产表中是否存在该至少一项信息所对应的终端类型,若存在,说明该至少一项信息所对应的终端类型为第一目标终端的终端类型,该控制设备已经将该至少一项信息与第一目标终端的终端类型进行关联存储,则控制设备无须再次执行本步骤 308,若不存在,则该控制设备将该至少一项信息与第一目标终端的终端类型关联存储在资产表中。

在一种可能的实现方式中,若资产表中不存在该至少一项信息所对应的终端类型,则该控制设备在终端类型添加界面中显示终端类型添加信息,以提示用户在资产表中添加该至少一项信息所对应的终端类型,其中,该终端类型添加信息用于指示在资产表中添加该至少一项信息对应的终端类型,该终端类型添加信息包括该至少一项信息以及添加标识,该添加标识用于指示在资产表中添加该至少一项信息对应的终端类型。

用户基于该终端类型添加信息中的至少一项信息,确定该第一目标终端的终端类型,并在该终端类型添加界面中添加第一目标终端的终端类型,当控制设备检测到用户在该终端类型界面执行了添加操作后,触发控制设备将该至少一项信息与用户所添加的终端类型关联存储在资产表中。

若该至少一项信息包括终端的网络地址,且终端的网络地址若为 IP 地址,则对于配置表中的任一 IP 地址,该网络设备将该任一 IP 地址所指示的终端的终端类型与该任一 IP 地址关联存储在资产表中。仍以表 2 所示的配置表为例,若 IP 地址 192.168.1.240 所指示的终端为摄像头,IP 地址 192.168.1.180 所指示的终端为摄像头,IP 地址 192.168.1.150 所指示的终端为音响,则该控制设备将这 3 个 IP 地址与对应的终端类型关联存储资产表中,得到表 3。

表 3

终端类型	终端的 IP 地址
摄像头	192.168.1.240

	192.168.1.180
音响	192.168.1.150

若该至少一个数据流为第二终端传输的至少一个第二数据流，本步骤 308 所示的过程即是该控制设备将至少一个第二数据流的至少一个传输信息与该第二终端的终端类型进行关联存储的过程。

为了进一步说明步骤 301-308 所示的过程，参见图 4 所示的本申请实施例提供的一种存储终端类型的示意图。对于网络设备传输的数据流，该网络设备获取传输的该数据流的传输信息，并将获取到的传输信息发送至控制设备，控制设备存储接收到的传输信息，并查询资产表中是否存在该传输信息对应的终端类型，若不存在，则控制设备提示用户在资产表中添加该传输信息对应的终端类型，控制设备再基于用户的操作在资产表中添加该传输信息对应的终端类型。

本申请实施例所示的方法，通过网络设备向控制设备上传数据流的传输信息，以便控制设备将终端验证系统中终端传输的各个数据流的传输信息与终端类型进行关联存储，从而达到统计终端验证系统中终端的终端类型的目的。

需要说明的是，上述步骤 301-308 所示的过程由网络设备基于信息获取指令，向控制设备上传数据流的传输信息，由控制设备存储网络设备上传的传输信息。在另一种可能的实现方式中，控制设备不向网络设备发送该信息获取指令，而是向网络设备发送数据流获取指令，当网络设备接收到数据流获取指令后，该网络设备将在时间窗口内传输的至少一个数据流中的多个报文复制一份，上传至控制设备，由控制设备基于网络设备上传的至少一个数据流中的多个报文，获取该至少一个数据流的传输信息，并执行步骤 307-308。其中，控制设备基于网络设备上传的至少一个数据流中的多个报文，获取该至少一个数据流的至少一个传输信息的过程与步骤 3041-3043 所示的过程同理，在此，本申请实施例对控制设备基于网络设备上传的至少一个数据流中的多个报文，获取该至少一个数据流的至少一个传输信息的过程不做赘述。在一种可能的实现方式中，若终端验证系统中不存在控制设备，则由网络设备周期性的执行步骤 304、步骤 307 以及步骤 308。

对于资产表中记录的任一终端类型，该控制设备从至少一个网络设备获取该任一终端类型下终端的多个传输特征，并基于获取到的多个传输特征，进行训练，得到该任一终端类型对应的目标模型。为了进一步说明该过程，参见图 5 所示的本申请实施例提供的一种模型获取方法的流程图。

501、控制设备确定待获取的目标模型所对应的目标终端类型。

在一种可能的实现方式中，该控制设备基于用户操作，确定该目标终端类型。用户在该控制设备的训练界面内输入该目标终端类型，并进行确认操作，以实现开启训练的过程，当控制设备在该训练界面内检测到用户进行了确认操作后，该控制设备从该训练界面获取该目标终端类型。

502、该控制设备向至少一个网络设备发送传输特征获取指令，该传输特征获取指令用于指示获取该目标终端类型下终端的传输特征。

该传输特征获取指令包括该目标终端类型以及该目标终端类型对应的至少一个网络地址，每个网络地址对应一个终端，一个终端的传输特征为该终端传输的至少一个数据流的总体传输特征。

在一种可能的实现方式中，该控制设备在资产表中查询该目标终端类型所对应的至少一个网络地址，将查询到的至少一个网络地址组成一个终端地址列表，并将该终端地址列表添加在传输特征获取指令中。其中，终端地址列表用于记录目标终端类型、该目标终端类型对应的至少一个网络地址。以目标终端类型对应的至少一个网络地址为终端的 IP 地址为例，参见表 4 所示的终端地址列表。

表 4

目标终端类型	IP 地址
摄像头	192.168.1.2
	192.168.1.5
	192.168.1.6

为了进一步说明步骤 501-502 所示的过程，参见图 6 所示的本申请实施例提供的一种开启训练的示意图，用户配置目标终端类型为待获取的目标模型所对应的终端类型（也即是配置目标终端类型进行训练），控制设备基于用户配置的目标终端类型查询资产表，得到该目标终端类型对应的至少一个网络地址，并将该目标终端类型以及该至少一个网络地址下发至网络设备，以开启训练的过程。

503、对于该至少一个网络设备中的任一网络设备，该任一网络设备接收传输特征获取指令。

504、该任一网络设备基于该传输特征获取指令，获取目标终端类型下至少一个第二终端的多个传输特征。

该至少一个第二终端为该传输特征指令中的至少一个网络地址所指示的终端。该至少一个第二终端的终端类型为目标终端类型。一个终端的一个传输特征为该终端传输的至少一个数据流的总体传输特征，该传输特征可能包括多个维度的特征，并不单指一个维度的特征。可选地，该传输特征为该至少一个数据流在一个时间窗口内的总体传输特征。

在一种可能的实现方式中，该传输特征包括上行传输特征，该上行传输特征为该至少一个数据流中至少一个上行数据流的总体传输特征，该上行数据流为该终端输出的数据流，上行数据流由上行报文组成。可选地，该上行传输特征包括上行报文特征、上行流特征中的一个，该上行报文特征为该至少一个上行数据流中上行报文的总体特征，该上行流特征为该至少一个上行数据流的统计特征。

可选地，该上行报文特征包括上行报文平均传输间隔、上行负载平均值、上行总负载大小、上行报文个数、上行目标报文个数、上行目标报文占比、上行报文负载波动值中的至少一个，该上行报文平均传输间隔为在一个时间窗口内该至少一个上行数据流中上行报文的平均传输间隔，该上行负载平均值为在该时间窗口内该至少一个上行数据流中目标报文的负载的平均大小，该上行总负载大小为在该时间窗口内该至少一个上行数据流中目标报文的负载的总大小，该上行报文个数为在该时间窗口内该至少一个上行数据流中上行报文的个数，该上行目标报文个数在该时间窗口内该至少一个上行数据流中目标报文的个数，该上行目标报文占比为在该时间窗口内该至少一个上行数据流中目标报文的占比，该上行报文负载波动值用于指示在该时间窗口内该至少一个上行数据流中目标报文的大小波动情况。该目标报文为具有负载的报文，可选地，该负载中的数据为业务数据。可选地，该上行报文特征还包括第一接收窗口波动值、第一接收窗口大小平均值中的至少一个，该第一接收窗口波动值用于指示在该时间窗口内该至少一个上行数据流中上行报文携带的接收窗口大小的波动情况，该第

一接收窗口大小平均值为在该时间窗口内该至少一个上行数据流中上行报文携带的接收窗口的平均大小。可选地，该接收窗口为 TCP 滑动窗口。可选地，该第一接收窗口波动值为在该时间窗口内该至少一个上行数据流中上行报文携带的接收窗口大小的标准差。

可选地，该上行流特征包括上行终端端口波动值、上行数据流总个数、上行目标数据流个数、至少一种数据流类型中每种数据流类型下的上行数据流个数、至少一种传输协议类型中每种传输协议类型下的上行数据流个数中的至少一个。该上行终端端口波动值用于指示在该时间窗口内终端中至少一个上行数据流的输出端口的波动情况，也即是在该时间窗内在该终端中有上行数据流传输的输出端口的波动情况。该上行目标数据流为所对应的服务器输入端口属于目标端口范围的上行数据流。可选地，该上行终端端口波动值为该至少一个上行数据流的输出端口的端口标识的方差值。该上行数据流总个数为该至少一个上行数据流的总个数，该上行目标数据流个数为该至少一个上行数据流中上行目标数据流的总个数。该至少一种传输数据流类型包括数据流、广播数据流和单播数据流。该至少一种传输协议类型包括 TCP、UDP 和 ICMP。该目标端口范围能够根据实际需求进行设置，例如该目标端口范围为知名端口的范围，本申请实施例对该目标端口范围不作具体限定。

在一种可能的实现方式中，该传输特征还包括该至少一个数据流的总个数、下行传输特征中的至少一个，该下行传输特征为该至少一个数据流中至少一个下行数据流的总体传输特征，该下行数据流为该终端输入的数据流，由下行报文组成。可选地，该下行传输特征包括下行报文特征、下行流特征中的至少一个，该下行报文特征为该至少一个下行数据流中下行报文的总体特征，该下行流特征为该至少一个下行数据流的统计特征。

可选地，该下行报文特征包括下行报文平均传输间隔、下行负载平均值、下行总负载大小、下行报文个数、下行目标报文个数、下行目标报文占比、下行报文负载波动值中的至少一个，该下行报文平均传输间隔为在一个时间窗口内该至少一个下行数据流中下行报文的平均传输间隔，下行负载平均值为在该时间窗口内该至少一个下行数据流中目标报文的负载的平均大小，该下行总负载大小为在该时间窗口内该至少一个下行数据流中目标报文的负载的总大小，该下行报文个数为在该时间窗口内该至少一个下行数据流中下行报文的个数，该下行目标报文个数在该时间窗口内该至少一个下行数据流中目标报文的个数，该下行目标报文占比为在该时间窗口内该至少一个下行数据流中目标报文的占比，该下行报文负载波动值用于指示在该时间窗口内所述该一个下行数据流中目标报文的大小波动情况。可选地，该下行报文特征还包括第二接收窗口波动值、第二接收窗口大小平均值中的至少一个，该第二接收窗口波动值用于指示该至少一个下行数据流中下行报文携带的接收窗口大小的波动情况，第二接收窗口大小平均值为在该时间窗口内该至少一个下行数据流中下行报文携带的接收窗口的平均大小。可选地，该第二接收窗口波动值为在该时间窗口内该至少一个下行数据流中下行报文携带的接收窗口大小的标准差。

可选地，该下行流特征包括下行终端端口波动值、下行数据流总个数、下行目标数据流个数、至少一种数据流类型中每种数据流类型下的下行数据流个数、至少一种传输协议类型中每种传输协议类型下的下行数据流个数中的至少一个。该下行终端端口波动值用于指示在该时间窗口内终端中该至少一个下行数据流的输入端口的波动情况，也即是在该时间窗内在该终端中有下行数据流传输的输入端口的波动情况。该下行目标数据流为对应的服务器输出端口属于目标端口范围的下行数据流。可选地，该下行终端端口波动值为在该时间窗口内该

终端中至少一个下行数据流的输入端口的端口标识的方差值。下行数据流总个数为该至少一个下行数据流的总个数，该下行目标数据流个数为该至少一个下行数据流中下行目标数据流的总个数。

当获取到该传输特征获取指令后，该任一网络设备从该传输特征指令中获取该目标终端类型所对应的至少一个网络地址（例如至少一个第二终端的 IP 地址），在多个时间窗口中的任一时间窗口内，该任一网络设备基于该至少一个网络地址中的任一网络地址、该任一网络地址所指示的第二终端传输的数据流，确定该第二终端的一个传输特征，从而在该任一时间窗口内，该任一网络设备能够获取到该至少一个第二终端的一个传输特征，在该多个时间窗口内，该任一网络设备能够获取到该至少一个第二终端的多个传输特征。

其中，在该任一时间窗口内，该任一网络设备基于该至少一个网络地址中的任一网络地址以及该任一网络地址所指示的第二终端传输的数据流，确定该第二终端的一个传输特征的方式包括方式 1 或方式 2。

方式 1、在该任一时间窗口内，该任一网络设备基于该第二终端传输的每个数据流，确定该第二终端的一个传输特征。

该任一网络设备先获取每个数据流的流传输特征，再基于获取到的至少一个流传输特征，获取该第二终端的一个传输特征。在一种可能的实现方式中，方式 1 能够由下述步骤 A-C 来实现。

步骤 A、在该任一时间窗口内，该任一网络设备基于该任一网络地址，确定该网络地址指示的该第二终端所传输的至少一个第三数据流。

其中，该至少一个第三数据流中的报文均为广域网报文。在该任一时间窗口内，若该任一网络设备所输入的任一报文携带有该任一网络地址，则该网络设备确定该任一报文所属的数据流为该第二终端传输的数据流；该任一网络设备通过比较该任一报文的源 IP 地址以及源 IP 地址，确定该任一报文是否为广域网报文，若该任一报文为广域网报文，则该任一网络设备确定该任一报文所属的数据流为该第二终端传输的一个第三数据流。

步骤 B、该任一网络设备获取该至少一个第三数据流中每个第一第三数据流的流传输特征，一个第三数据流的流传输特征为该第三数据流的传输特征。

一个数据流的流传输特征包括该数据流的传输信息、数据流类型、目标端口类型、报文特征中的至少一个。其中，该传输信息用于指示数据流的传输属性，该传输信息包括该数据流的源地址信息（源 IP 地址和/或源 MAC 地址）、源端口标识、目的地址信息（目的 IP 地址和/或目的 MAC 地址）、目的端口标识以及传输协议类型中的至少一个。可选地，该传输信息还包括方向标识、该时间窗口的标识中的至少一个，该方向标识用于指示该数据流的传输方向。

该目标端口类型为服务器中传输该数据流的端口的端口类型，其中，端口的端口类型分为第一端口类型、第二端口类型以及第三端口类型，可选地，第一端口类型对应的端口区间为知名端口区间 $[0, 1024)$ ，第二端口类型对应的端口区间为注册端口区间 $[1024, 49152)$ ，第三端口类型对应的端口区间为私有端口区间 $[49152, +\infty)$ 。需要说明的是，第一端口类型、第二端口类型以及第三端口类型所对应的端口区间均可根据具体实施场景进行设置，例如，若用户根据业务需求，将业务所对应的端口配置在区间 $[10001, 20000)$ ，则第一端口类型对应的端口区间为 $[0, 10001)$ ，第二端口类型对应的端口区间为 $[10001, 20000)$ ，第三端口类型

对应的端口区间为 $[20000, +\infty)$ 。在此, 本申请实施例对第一端口类型、第二端口类型以及第三端口类型所对应的端口区间不作具体限定。

该报文特征为该数据流中报文的特征。可选地, 该报文特征包括报文传输间隔总和、负载大小、负载平方和、目标报文个数、报文总个数、接收窗口波动值、窗口总大小、窗口平方和中的至少一个, 该报文传输间隔总和为在一个时间窗口内该数据流中报文之间的传输间隔的总时长, 该负载大小为在该时间窗口内该数据流中目标报文的负载的总大小, 该负载平方和为该目标报文的负载的大小平方和, 该目标报文个数为在该时间窗口内该报文中目标报文的总个数, 该报文总个数为在该时间窗口内该数据流中报文的总个数, 该接收窗口波动值用于指示在该时间窗口内该数据流中报文携带的接收窗口大小的波动情况, 该窗口总大小为在该时间窗口内该数据流中报文携带的接收窗口大小的总和, 该窗口平方和为该滑动窗口的大小的平方和。

对于该至少一个第三数据流中任一第三数据流, 任一网络设备获取该任一第三数据流的传输信息、数据流类型、目标端口类型、报文特征中的至少一个, 并将获取到的这些信息确定为该任一第三数据流的流传输特征。

其中, 该任一网络设备获取该任一第三数据流的传输信息的过程与步骤 304 中任一网络设备获取至少一个数据流的传输信息的过程同理, 在此本申请实施例对该任一网络设备获取该任一第三数据流的传输信息的过程不做赘述。

该任一网络设备获取该任一第三数据流的数据流类型的过程为: 该任一网络设备根据任一第三数据流中任一报文所携带的源 IP 地址以及目的 IP 地址, 确定该任一第三数据流为广播数据流还是组播数据流, 若该任一第三数据流既不是广播数据流也不是组播数据流, 则该任一网络设备确定该任一第三数据流为单播数据流。

该任一网络设备获取该任一第三数据流的目标端口类型的过程: 该任一网络设备获取该任一报文中服务器的端口标识, 并将该服务器的端口标识所属的端口类型确定为该目标端口类型。其中, 该服务器的端口标识为该任一报文的源端口标识或目的端口标识。

该任一网络设备获取该任一第三数据流的报文特征的过程为: 在该任一时间窗口内, 该任一网络设备记录该任一第三数据流传输第一个报文的第一时间, 以及从传输最后一个报文的第二时间, 并将该第二时间与第一时间之间的时间差, 确定为报文传输间隔总和; 在该任一时间窗口内, 该任一网络设备统计该任一第三数据流中目标报文的负载的总大小, 并将该总大小确定为负载大小; 在该任一时间窗口内, 该任一第三数据流每传输一个目标报文, 该任一网络设备计算该目标报文的负载的大小平方, 从而在该任一时间窗口内该任一网络设备能够得到至少一个该目标报文的负载的大小平方, 该任一网络设备对该至少一个该目标报文中负载的大小平方进行求和, 得到负载平方和; 该任一网络设备统计在该任一时间窗口内该任一第三数据流中目标报文的总个数, 得到目标报文个数; 该任一网络设备统计在该任一时间窗口内该任一第三数据流中报文的总个数, 得到报文总个数; 在该任一时间窗口内, 该任一网络设备对该任一第三数据流中报文携带的接收窗口大小进行求和, 得到窗口总大小; 在该任一时间窗口内, 该任一网络设备对该任一第三数据流中各个报文携带的接收窗口大小进行平方, 并对各个报文携带的接收窗口大小的平方进行求和, 得到窗口平方和; 该任一网络设备基于该窗口总大小以及窗口平方和, 获取报文携带的接收窗口大小的标准差, 并将该标准差确定为该接收窗口波动值; 该任一网络设备将该报文传输间隔总和、负载大小、负载平方和、

目标报文个数、报文总个数、接收窗口波动值、窗口总大小、窗口平方和中的至少一个确定为该报文特征。

以该至少一个第三数据流包括数据流 a-e 为例，传输数据流 a-e 的终端的 IP 地址分别为 192.168.1.2、192.168.1.2、192.168.1.5、192.168.1.5、192.168.1.6，数据流 a-e 的流传输特征如下表 5 所示。

表 5

流标识	源 IP 地址	目的 IP 地址	源端口标识	目的端口标识	传输协议类型	方向标识	数据流类型、目标端口类型、报文特征中的至少一个
数据流 a	192.168.1.2	10.137.56.40	45564	80	TCP	上行标识	
数据流 b	192.168.1.2	10.137.56.42	45564	123	UDP	上行标识	
数据流 c	192.168.1.5	10.137.56.42	45564	80	TCP	上行标识	
数据流 d	192.168.1.5	10.137.56.42	45564	123	UPD	上行标识	
数据流 e	10.137.56.42	192.168.1.6	80	45567	TCP	下行标识	

步骤 C、该任一网络设备基于该至少一个第三数据流的流传输特征，获取该第二终端的一个传输特征。

本步骤 C 由下述步骤 C1-C3 所示的过程来实现。

步骤 C1、该任一网络设备基于该至少一个第三数据流中至少一个上行数据流的流传输特征，获取上行传输特征。

该任一网络设备基于该至少一个上行数据流的流传输特征(简称“至少一个流传输特征”)，获取该至少一个上行数据流的上行报文特征、上行流特征中的至少一个，将获取到的上行报文特征、上行流特征中的至少一个确定为该上行传输特征。

其中，该任一网络设备基于该至少一个流传输特征，获取该上行报文特征的过程为：该任一网络设备将该至少一个流传输特征中的报文传输间隔总和进行求和，得到第一和值，该第一和值为该至少一个上行数据流中上行报文的报文传输间隔总和；该任一网络设备将该至少一个流传输特征中的报文总个数进行求和，得到上行报文个数；该任一网络设备将该第一和值除以该上行报文个数，得到上行报文平均传输间隔；该任一网络设备对该至少一个流传输特征中的负载大小进行求和，得到上行总负载大小；该任一网络设备对该至少一个流传输特征中的目标报文个数进行求和，得到上行目标报文个数；该任一网络设备将该上行目标报文个数除以该上行报文个数，得到上行目标报文占比；该任一网络设备将该上行总负载大小除以上行目标报文个数，得到上行负载平均值；该任一网络设备基于该至少一个流传输特征中的负载大小，计算在该时间窗口内该至少一个上行数据流中目标报文的大小的标准差，并

将该标准差作为上行报文负载波动值；该任一网络设备将该至少一个流传输特征中的接收窗口波动值求平均值，得到第一接收窗口波动值；该任一网络设备对该至少一个流传输特征中的窗口总大小进行求和，得到第二和值，该第二和值为在该时间窗口内该至少一个上行数据流中上行报文携带的接收窗口大小的总和；该任一网络设备将该第二和值除以该至少一个上行数据流中上行报文携带的接收窗口的总个数，得到第一接收窗口大小平均值；该任一网络设备将上行报文平均传输间隔、上行负载平均值、上行总负载大小、上行报文个数、上行目标报文个数、上行目标报文占比、上行报文负载波动值、第一接收窗口波动值、第一接收窗口大小平均值中的至少一个确定为该上行报文特征。

该任一网络设备基于该至少一个流传输特征，获取上行流特征的过程为：该任一网络设备从该至少一个流传输特征的传输信息中获取至少一种源端口标识，该任一网络设备计算该至少一种源端口标识的方差，并将该方差确定为上行终端端口波动值；该任一网络设备将该至少一个流传输特征的总个数，确定为上行数据流总个数；该任一网络设备统计该至少一个上行数据流中上行目标数据流的总个数，得到该上行目标数据流个数；该任一网络设备获取该至少一个流传输特征中的数据流类型，并基于获取到数据流类型，统计至少一种数据流类型中每种数据流类型下的上行数据流个数；该任一网络设备获取该至少一个流传输特征中的传输协议类型，并基于获取到传输协议类型，统计至少一种传输协议类型中每种传输协议类型下的上行数据流个数；该任一网络设备确定出上行终端端口波动值、上行数据流总个数、上行目标数据流个数、至少一种数据流类型中每种数据流类型下的上行数据流个数、至少一种传输协议类型中每种传输协议类型下的上行数据流个数中的至少一个，确定为该上行流特征。

例如至少一个上行数据流包括数据流1和数据流2，数据流1为组播数据流，数据流2为广播数据流，而至少一个数据流类型包括组播数据流、广播数据流以及单播数据流，则该至少一个数据流类型下的上行数据流个数分别为1、1、0。例如至少一个上行数据流包括数据流1和数据流2，数据流1的传输协议类型为TCP，数据流2的传输协议类型为UDP，而至少一个传输协议类型包括TCP、UDP以及ICMP，则该至少一个传输协议类型下的上行数据流个数分别为1、1、0。

步骤C2、该任一网络设备基于该至少一个第三数据流中至少一个下行数据流的流传输特征，获取下行传输特征。

本步骤C2与步骤C1所示的过程的同理，在此本申请实施例对本步骤C2不做赘述。

步骤C3、该任一网络设备将该上行传输特征和下行传输特征确定为该第二终端的一个传输特征。

在一种可能的实现方式，该任一网络设备将该上行传输特征确定为该第二终端的一个传输特征。在另一种可能的实现方式中，该任一网络设备将该上行传输特征、下行传输特征以及该至少一个第三数据流的总个数，确定为该第二终端的一个传输特征。

以表5为例，由于表5中数据流a和b的源IP地址相同，则数据流a和b为同一个第二终端输出的数据流，该任一设备基于表5中数据流a和b的流传输特征，获取该第二终端的一个传输特征。数据流c和d的源IP地址相同，则数据流c和d为同一个第二终端输出的数据流，该任一设备基于表5中数据流c和d的流传输特征，获取该第二终端的一个传输特征。该任一设备基于表5中数据流e的流传输特征，数据流e的目的IP地址所指示的第二终端的一个传输特征，最终得到表6所示的3个第二终端的传输特征。

表 6

IP 地址	至少一个第三数据流的总个数	上行报文特征	上行流特征	下行报文特征	下行流特征
192.168.1.2	2	...	...	0	0
192.168.1.5	2	...	...	0	0
192.168.1.6	1	0	0	...	...

为了进一步说明上述方式 1 所示的过程，参见图 7 所示的本申请实施例提供的一种传输特征获取的示意图。图 7 中的一个时间窗口的目标时长均为 1 小时，从 2016-09-22 至 2016-10-12 中的每一天划分为 24 个时间窗口，任一网络设备在每个时间窗口，获取第二终端的一个传输特征，在每个时间窗口内，当该任一网络设备输入该第二终端传输的任一第三数据流时，该任一网络设备获取该任一第三数据流的流传输特征，然后该任一网络设备基于在每个时间窗口内传输的至少一个第三数据流的流传输特征，获取该第二终端的一个传输特征，还能获取第二终端的终端类型，例如任一网络设备在 2016-09-24 的 5:00-5:59 所在的时间窗口，共输入第二终端传输的 344 个第三数据流，则该任一网络设备基于该 344 个第三数据流的流传输特征，采集在该时间窗口内该第二终端的一个传输特征，并配置采集到的传输特征，例如上/下行报文特征，上/下行流特征等。需要说明的是，上述举例是以 1 小时为一个时间窗口，统计的传输特征，而在另外一些实施例中，是以 1 分钟为一个时间窗口，实时统计在每分钟内的传输特征，时间窗口的窗口时长（也即是目标时长）可根据具体实施场景进行设置，在此，本申请实施例对时间窗口的窗口时长不作具体限定。

方式 2、在该任一时间窗口内，该任一网络设备根据该至少一个网络地址，确定第二终端的一个传输特征。

在任一时间窗口内，该任一网络设备获取携带该至少一个网络地址的多个上行报文的上行报文特征、该多个上行报文所在的上行数据流的上行流特征中的至少一个，该任一网络设备并将获取到的上行报文特征、上行流特征中的至少一个确定为上行传输特征。

在任一时间窗口，该任一网络设备获取携带该至少一个网络地址的多个上行报文的上行报文特征的过程为：该任一网络设备统计在该任一时间窗口内携带该至少一个网络地址的多个上行报文的总个数，得到上行报文个数；该任一网络设备记录在该任一时间窗口内该多个上行报文中首报文的到达时间以及尾报文的达到时间，并将这 2 个达到时间之间的时间差除以目标差值，得到上行报文平均传输间隔，其中，首报文为在该任一时间窗口内，携带该至少一个网络地址中任一网络地址且第一个达到该任一网络设备的上行报文，尾报文为在该任一时间窗口内，携带该至少一个网络地址中的任一网络地址且最后一个达到该任一网络设备的上行报文，该目标差值为上行报文个数与 1 的差值；该任一网络设备统计在该任一时间窗口内携带该至少一个网络地址的目标报文的个数，得到上行目标报文个数；该任一网络设备将该上行目标报文个数除以该上行报文个数，得到上行目标报文占比；该任一网络设备统计在该任一时间窗口内携带该至少一个网络地址的目标报文的负载总大小，得到上行总负载大小，该任一网络设备将该上行总负载大小除以上行目标报文个数，得到上行负载平均值；该任一网络设备统计在该任一时间窗口内携带该至少一个网络地址的多个目标报文的负载大小，并计算该多个目标报文的负载大小的标准差，并将该标准差确定为上行报文负载波动值；该任一网络设备将携带该至少一个网络地址的上行报文所携带的接收窗口大小求标准差，得到

第一接收窗口波动值；该任一网络设备对在该时间窗口内该多个上行报文携带的接收窗口大小进行求和，得到第一接收窗口总大小；该任一网络设备将该第一接收窗口总大小除以该多个上行报文携带的接收窗口大小的总个数，得到第一接收窗口大小平均值；该任一网络设备将上行报文平均传输间隔、上行负载平均值、上行总负载大小、上行报文个数、上行目标报文个数、上行目标报文占比、上行报文负载波动值、第一接收窗口波动值、第一接收窗口大小平均值中的至少一个确定为该上行报文特征。

在任一时间窗口内，该任一网络设备获取携带该至少一个网络地址的多个上行报文所在的上行数据流的上行流特征的过程为：在该任一时间窗口内，该任一网络设备获取携带该至少一个网络地址的多个上行报文中的多种源端口标识，该任一网络设备计算该多种源端口标识的方差，并将该方差确定为上行终端端口波动值；在该任一时间窗口内，该任一网络设备统计携带该至少一个网络地址的上行数据流的总个数，得到上行数据流总个数；在该任一时间窗口内，该任一网络设备统计携带该至少一个网络地址的上行数据流中上行目标数据流的总个数，得到上行目标数据流个数；在该任一时间窗口内，该任一网络设备统计至少一种数据流类型中每种数据流类型下携带该至少一个网络地址的上行数据流的个数，得到至少一种数据流类型中每种数据流类型下的上行数据流个数；在该任一时间窗口内，该任一网络设备统计至少一种传输协议类型中每种传输协议类型下携带该至少一个网络地址的上行数据流的个数，得到至少一种传输协议类型中每种传输协议类型下的上行数据流个数；该任一网络设备确定出上行终端端口波动值、上行数据流总个数、上行目标数据流个数、至少一种数据流类型中每种数据流类型下的上行数据流个数、至少一种传输协议类型中每种传输协议类型下的上行数据流个数中的至少一个，确定为该上行流特征。

该任一网络设备还能够参考方式 2 中获取上行传输特征的过程，来获取下行传输特征。并参照步骤 C3 所示的过程，来获取该第二终端的一个传输特征。

在该多个时间窗口中的每个时间窗口内，该任一网络设备基于上述方式 1 或方式 2，确定每个网络地址所指示的第二终端的一个传输特征，从而在多个时间窗口内，该任一网络设备能够获取到该至少一个第二终端的多个传输特征。

505、该任一网络设备向该控制设备发送该至少一个第二终端的多个传输特征。

506、该控制设备接收该至少一个第二终端的多个传输特征。

由于该至少一个网络设备中的任一网络设备均向该控制设备发送该至少一个第二终端的多个传输特征，因此，该控制设备能够从该至少一个网络设备分别接收该至少一个第二终端的多个传输特征。

507、该控制设备将该至少一个第二终端的多个第三传输特征作为初始模型的输入和输出，进行训练，得到目标模型。

该多个第三传输特征为该至少一个第二终端的多个传输特征中的部分传输特征。每个第二终端的一个传输特征为一个样本数据，每个第二终端均正常终端，当该控制设备接收到的该至少一个第二终端的多个传输特征的个数大于或等于目标个数时，说明正常终端的样本数据足够；该控制设备将接收到的该至少一个第二终端的多个传输特征划分为三部分，并将这三部分分别放入训练集、验证集以及测试集，也即是训练集、验证集以及测试集均包括该至少一个第二终端的多个传输特征中的部分传输特征，其中，训练集中的各个传输特征为第三传输特征，验证集中各个传输特征为第四传输特征，测试集中的各个传输特征为第六传输特征。

征。

可选地,该目标模型用于重构出正常传输特征。可选地,该目标模型为无监督深度神经网络模型,例如深度自编码器模型。该目标模型包括编码器(encoder)和解码器(decoder),传输特征 $X=[x_1, x_2, \dots, x_n]$ 作为编码器的输入信号输入编码器,编码器学习输入的传输特征 X 到隐编码,其学习的过程为编码器对传输特征 X 进行降维编码,得到编码特征 Z ,编码特征 Z 作为解码器的输入信号,输入至解码器中;解码器尽量将输入的编码特征 Z 重构成传输特征 X ,可选地,解码器对编码特征 Z 进行升维解码,输出传输特征 $X'=[x'_1, x'_2, \dots, x'_n]$,传输特征 X' 为解码器所还原出的传输特征 X ,其中, x_n 为传输特征 X 所包括的第 n 个特征,例如上行数据流总个数, n 为传输特征 X 的总维度或者是传输特征中特征的总个数, $n>1$, x'_n 为重构出的 x_n 。

在对初始模型进行训练的过程中,预设 q 次训练次数、目标损失函数以及预设阈值,该目标损失函数用于计算模型输入的传输特征与输出的传输特征之间的平均差异情况,在第 i 次训练过程中,控制设备将多个第三传输特征输入第 i 模型,该第 i 模型重构输入的每个第三传输特征,输出每个第三传输特征的重构传输特征,该控制设备将多个第三传输特征与对应的重构传输特征输入该目标损失函数,计算目标损失函数值;若该目标损失函数值大于或等于该预设阈值,且 $i < q$,则该控制设备基于优化算法,继续迭代,更新第 i 模型的模型参数,得到第 $i+1$ 模型,控制设备进入第 $i+1$ 次训练过程;若该目标损失函数值小于该预设阈值,则控制设备结束训练,将第 i 模型确定为该目标模型;若该目标损失函数值大于或等于预设差值且 $i \geq q$,则该控制设备结束训练,以避免控制设备在训练不出目标模型的情况下持续进行迭代训练,或者若模型的模型参数在相邻两次迭代之间的变化小于预设的模型参数变化值,该控制设备结束训练。

其中, $q \geq i \geq 1$,当 $i=1$ 时,第 i 模型为初始模型,当 $i>1$ 时,第 i 模型为在第 $i-1$ 次训练过程中,更新参数后的第 $i-1$ 模型。该优化算法包括梯度下降算法,该目标损失函数如下述公式(1)所示,其中, m 为多个第三传输特征的总个数, x_i^j 为第 j 个第三传输特征中第 i 个维度的数值, x'_i 是目标模型重构出的 x_i^j , $n \geq i > 0$, $m \geq j > 0$ 。

$$F(X, X') = \frac{1}{nm} \sum_j^m \sum_i^n (x_i^j - x'_i) \quad (1)$$

可选地,在进行训练的过程中,每进行一次训练,该控制设备还能够显示训练进度信息,该训练进度信息包括当前的训练次数、目标损失函数值,以使用户能够通过该训练进度信息获取训练进度。

508、该控制设备将目标终端类型下多个目标终端的多个第四传输特征输入该目标模型,由该目标模型基于输入的该多个第四传输特征,重构每个第四传输特征,输出多个第五传输特征,该多个第四传输特征与该多个第五传输特征一一对应,一个第四传输特征为一个目标终端传输的至少一个数据流的总体传输特征。

该多个目标终端包括至少一个第二终端以及至少一个第三终端,其中,该至少一个第二终端均为正常终端,该至少一个第三终端均为异常终端。一个第五传输特征为重构出的一个第四传输特征。

验证集除了包括至少一个第二终端的多个传输特征以外,还包括至少一个第三终端的多个传输特征,在该验证集中第二终端的传输特征和第三终端的传输特征均视为第四传输特征。

该控制设备从验证集中获取多个第四传输特征，并将获取到的多个第四传输特征输入该目标模型，由目标模型基于输入的多个第四传输特征，输出重构出的多个第四传输特征，其中，该多个第四传输特征属于至少一个第二终端和至少一个第三终端，重构出的多个第四传输特征也即是该多个第五传输特征，每个第五传输特征对应一个第四传输特征。

509、该控制设备基于该多个第五传输特征与对应的第四传输特征，获取目标差异度。

该控制设备基于该多个第五传输特征中至少一个第五传输特征与对应的第四传输特征之间的差异度，获取该目标差异度，一个第五传输特征与对应的第四传输特征之间的差异度用于指示该一个第五传输特征与对应的第四传输特征之间的差异情况，其中，该至少一个第五传输特征所对应的第四传输特征均为第二终端的传输特征。可选地，本步骤 509 由下述本步骤 5091-5093 所示的过程来实现。

步骤 5091、对于至少一个第二终端中任一第二终端的任一第四传输特征，该控制设备获取该任一第四传输特征与对应的第五传输特征之间的差异度。

可选地，该任一第四传输特征与对应的第五传输特征之间的差异度为该任一第四传输特征与对应的第五传输特征中相应特征之间的均方误差 (mean square error, MSE)，如公式 (2) 所示，其中， $MSE(X, X')$ 为该任一第四传输特征与对应的第五传输特征中相应特征之间的均方误差。

$$MSE(X, X') = \frac{1}{n} \sum_{i=1}^n (x_i - x'_i)^2 \quad (2)$$

该控制设备对至少一个第二终端中每个第二终端的每个第四传输特征均执行本步骤 5091，从而能够得到至少一个第二终端的多个第四传输特征与对应的第五传输特征之间的差异度。在一种可能的实现方式中，该控制设备将该至少一个第二终端的每个第四传输特征所对应的第五传输特征，确定为该至少一个第五传输特征中的一个。而在另一种可能的实现方式，该控制设备对该至少一个第二终端的多个第四传输特征所对应的多个第五传输特征进行进一步筛选，以得到该至少一个第五传输特征，具体参见下述步骤 5092。

步骤 5092、该控制设备基于该至少一个第二终端的多个第四传输特征与对应的第五传输特征之间的差异度，从该第二终端的多个第四传输特征所对应的第五传输特征中，确定至少一个第五传输特征。

对于该第二终端的多个第四传输特征中的任一第四传输特征，若该任一第四传输特征与对应的第五传输特征之间的差异度属于目标差异区间，则该差异度为正常值，该差异度能够参与计算目标差异度，该控制设备将该任一第四传输特征所对应的第五传输特征确定为该至少一个第五传输特征中的一个。

其中，该目标差异区间包括多个差异度，该多个差异度均为正常的值，均能够参与计算目标差异度。该目标差异区间中的差异度能够根据具体情况来设置，例如控制设备采取箱线图或者设置分位数，来确定该目标差异区间，再例如确定的目标差异区间为 [0, 0.1]，在此，本申请实施例对该目标差异区间的范围不作具体限定。

步骤 5093、该控制设备基于该至少一个第五传输特征与对应的第四传输特征之间的差值度，确定该目标差异度。

该控制设备基于至少一个差异度的平均值或分数位，获取该目标差异度，其中，该至少一个差异度包括该至少一个第五传输特征与对应的第四传输特征之间的差值度，分数位包括该至少一个差异度的中值。

该控制设备基于该至少一个差异度的平均值, 获取该目标差异度 θ , 如公式(3)所示。其中, $MSE[\cdot]$ 为该至少一个差异度所组成的数组, $AVE(MSE[\cdot])$ 为该至少一个差异度的平均值, $STD(MSE[\cdot])$ 为该至少一个差异度的标准差, 用于指示该至少一个差异度的波动情况, K 为灵敏度系数。

$$\theta = AVE(MSE[\cdot]) + K \times STD(MSE[\cdot]) \quad (3)$$

该目标模型除了用于完全重构出正常传输特征以外, 还用于不能完全重构出异常传输特征, 需要说明的是, 完全重构出正常传输特征是允许有一定的误差范围的。例如, 当该目标模型在重构一个实际传输特征时, 若该目标模型所输出的重构传输特征与该实际传输特征之间的差异度小于该目标差异度, 则说明该目标模型完全重构出了该实际传输特征, 若该实际传输特征为正常传输特征, 则说明本次重构准确, 若该实际传输特征为异常传输特征, 则说明本次重构失败; 当目标模型在重构一个实际传输特征时, 若该目标模型所输出的重构传输特征与该实际传输特征之间的差异度大于或等于该目标差异度, 则说明该目标模型未完全重构出该实际传输特征, 若该实际传输特征为正常传输特征, 则说明本次重构失败, 若该实际传输特征为异常传输特征, 则说明本次重构准确。其中, 该至少一个第四传输特征均为实际传输特征, 该至少一个第五传输特征均为重构传输特征, 正常传输特征为正常终端的传输特征, 也即是至少一个第二终端的传输特征; 异常传输特征为异常终端的传输特征, 也即是至少一个第三终端的传输特征。

该控制设备还能够根据该目标模型重构多个目标终端的多个第四传输特征的准确情况, 动态调整 K 的取值, 并通过调整后的 K , 来确定该目标差异度。在一种可能的实现方式中, 该控制设备通过执行 r 次 K 值更新过程, 以确定该目标差异度。其中, 在第 j 次 K 值更新的过程中, 该控制设备将 K_j 作为 K , 并基于公式(3)计算出一个差异度 θ_j , 若在差异度 θ_j 下, 该目标模型符合第一条条件, 则该控制设备将该差异度 θ_j 确定为目标差异度, 结束 K 值更新; 否则, 该控制设备将 K_j 更新为 K_{j+1} , 并以 K_{j+1} 作为 K , 执行在第 $j+1$ 次 K 值更新的过程。其中, $r \geq j \geq 1$, K_j 为第 j 次 K 值更新的过程中所使用的 K , θ_j 为基于 K_j 以及公式(3)所计算出的差异度。

该第一条条件包括下述至少一项: 在该差异度 θ_j 下, 该目标模型的第一查准率大于或等于第一查准率阈值, 且该目标模型的第一查全率大于或等于第一查全率阈值; 在该差异度 θ_j 下, 该目标模型的第二查准率大于或等于第二查准率阈值, 且该目标模型的第二查全率大于或等于第二查全率阈值。其中, 该第一查准率为该目标模型完全重构出正常传输特征的准确率; 该第一查全率为该目标模型完全重构出正常传输特征的概率; 该第二查准率为该目标模型未完全重构出异常传输特征的准确率; 该第二查全率为该目标模型未完全重构出异常传输特征的概率。本申请实施例对第一查准率阈值、第一查全率阈值、第二查准率阈值和第二查全率阈值的不作具体限定。

在一种可能的实现方式中, 该控制设备通过该多个第四传输特征的第一标签以及对应的第五传输特征的第二标签, 获取正常传输特征个数、第一正常个数、第二正常个数、异常传输特征个数、第一异常个数以及第二异常个数; 该控制设备基于该正常传输特征个数、第一正常个数以及第二正常个数, 确定该第一查准率以及第一查全率; 该控制设备基于该异常传输特征个数、第一异常个数以及第二异常个数, 确定该第二查准率以及第二查全率。

一个实际传输特征具有一个第一标签, 该第一标签用于指示该实际传输特征是否为正常

传输特征,若第一标签是第一正常标识,则说明该实际传输特征为正常传输特征,若第一标签为第一异常标识,则说明该实际传输特征是异常传输特征。该多个第四传输特征均为实际传输特征,该多个第四传输特征中正常传输特征的第一标签均为第一正常标识,该多个第四传输特征中异常传输特征的第一标签均为第一异常标识。本申请实施例对第一正常标识和第一异常标识的表示方式不作具体限定。

一个重构传输特征具有一个第二标签,该第二标签用于指示该重构传输特征所对应的实际传输特征是否为正常传输特征,若第二标签是第二正常标识,则说明该重构传输特征所对应的实际传输特征是正常传输特征,也即是该实际传输特征所属终端为正常终端;若第二标签为第二异常标识,则说明该重构传输特征所对应的实际传输特征是异常传输特征,该实际传输特征所属终端为异常终端。该多个第五传输特征均为重构传输特征,对于一个第五传输特征,若该第五传输特征与对应的第四传输特征之间的差异度小于该差异度 θ_j ,则说明在该差异度 θ_j 下,该第五传输特征所对应的第四传输特征为正常传输特征,则该第五传输特征的第二标签为第二正常标识,否则,说明在该差异度 θ_j 下,该第五传输特征所对应的第四传输特征为异常传输特征,则该第五传输特征的第二标签为第二异常标识。本申请实施例对第二正常标识和第二异常标识的表示方式不作具体限定。

该正常传输特征个数为该多个第四传输特征中第二终端的传输特征的总个数,也即是该多个第四传输特征中正常传输特征的总个数。第一正常个数为在该差异度 θ_j 下该多个第四传输特征中目标正常传输特征的总个数,该目标正常传输特征为该多个第四传输特征中目标模型能够准确重构的正常传输特征。第二正常个数为在差异度 θ_j 下第二标签为第二正常标识的第五数据流的个数。

该异常传输特征个数为该多个第四传输特征中第三终端的传输特征的总个数,也即是该多个第四传输特征中异常传输特征的总个数。第一异常个数为在该差异度 θ_j 下该多个第四传输特征中目标异常传输特征的总个数,该目标异常传输特征为该多个第四传输特征中目标模型重构失败的异常传输特征;第二异常个数为在差异度 θ_j 下第二标签为第二异常标识的第五数据流的个数。

在一种可能的实现方式中,该控制设备通过该多个第四传输特征的第一标签以及对应的第五传输特征的第二标签,获取正常传输特征个数、第一正常个数、第二正常个数、异常传输特征个数、第一异常个数以及第二异常个数包括:若一个第四传输特征的第一标签为第一正常标识,该第四传输特征为正常传输特征,则该控制设备将该多个第四传输特征的第一标签为第一正常标识的标签个数,确定为正常传输特征个数;若一个第四传输特征的第一标签为第一正常标识,且该第四传输特征所对应的第五传输特征的第二标签为第二正常标识,说明该目标模型重构该第四传输特征(正常传输特征)是准确的,则该控制设备将该第四传输特征确定为目标正常传输特征,该控制设备将该多个第四传输特征中目标正常传输特征的总个数确定为第一正常个数;该控制设备统计第二标签为第二正常标识的第五数据流的个数,并将统计出的个数确定为第二正常个数;若一个第四传输特征的第一标签为第一异常标识,该第四传输特征为异常传输特征,则该控制设备将该多个第四传输特征的第一标签为第一异常标识的标签个数,确定为异常传输特征个数;若一个第四传输特征的第一标签为第一异常标识,且该第四传输特征所对应的第五传输特征的第二标签为第二异常标识,说明该目标模型重构该第四传输特征(异常传输特征)失败,则该控制设备将该第四传输特征确定为目标

异常传输特征，该控制设备将该多个第四传输特征中目标异常传输特征的总个数确定为第一异常个数；该控制设备统计第二标签为第二异常标识的第五数据流的个数，并将统计出的个数确定为第二异常个数。

在一种可能的实现方式中，该控制设备基于该正常传输特征个数、第一正常个数以及第二正常个数，确定该第一查准率以及第一查全率包括：该控制设备将该第一正常个数与该第二正常个数之间的比值确定为该第一查准率，该控制设备将该第一正常个数与该正常传输特征个数之间的比值确定为该第一查全率。

在一种可能的实现方式中，该控制设备基于该异常传输特征个数、第一异常个数以及第二异常个数，确定该第二查准率以及第二查全率包括：该控制设备将该第一异常个数与该第二异常个数之间的比值确定为该第二查准率，该控制设备将该第一异常个数与该异常传输特征个数之间的比值确定为该第二查全率。

以下述表 7 为例，验证集包括 100 个第四传输特征，其中，90 个第四传输特征为正常传输特征，10 个第四传输特征为异常传输特征，也即是正常数据流个数为 90，异常数据流个数为 10。控制设备将 100 个第四传输特征输入该目标模型，该目标模型输出 100 个第五传输特征。在执行 r 次 K 值更新过程中，对于 100 个第五传输特征中的任一第五传输特征，若该任一第五传输特征与对应的第四传输特征之间的差异度小于该差异度 θ_j ，则该控制设备将任一第五传输特征的第二标签标记为第二正常标识，以指示该第五传输特征所对应的第四传输特征为正常传输特征（也即是预测的第五传输特征对应的第四传输特征为正常传输特征），否则，该控制设备将该第五传输特征的第五标签标记为第二异常标识，以指示该第五传输特征所对应的第四传输特征为异常传输特征（也即是预测的第五传输特征对应的第四传输特征为异常传输特征）。以该 100 个第五传输特征中第二标签为第二正常标识的第五传输特征个数为 88、该 100 个第五传输特征中第二标签为第二异常标识的第五传输特征个数为 12 为例，也即是第二正常个数为 88，第二异常个数为 12。其中，这 88 个第五传输特征所对应的 88 个第四传输特征中，86 个第四传输特征的第一标签为第一正常标识，说明这 86 个第四传输特征为目标正常传输特征，则该第一正常个数为 86，而这 88 个第四传输特征中 2 个第四传输特征的第一标签为第一异常标识，说明这 2 个第四传输特征实际是异常传输特征，在差异度 θ_j ，目标模型重构这个 2 个第四传输特征的结果不准确；这 12 个第五传输特征所对应的 12 个第四传输特征中，8 个第四传输特征的第一标签为第一异常标识，说明这 8 个第四传输特征为目标异常传输特征，则该第一异常个数为 8，而这 12 个第四传输特征中 4 个第四传输特征的第一标签为第一正常标识，说明这 4 个第四传输特征实际是正常传输特征，在差异度 θ_j ，目标模型重构这 4 个第四传输特征的结果不准确，则该第一查准率=第一正常个数 86/第二正常个数 88，第一查全率=第一正常个数 86/正常数据流个数 90，该第二查准率=第一异常个数 8/第二异常个数 12，第一查全率=第一异常个数 8/异常数据流个数 10。需要说明的是，预测的第五传输特征也即是重构出的第五传输特征。

表 7

	第二标签为第二正常标识（也即是预测的第五传输特征对应的第四传输特征为正常传输特	第二标签为第二异常标识（也即是预测的第五传输特征对应的第四传输特征为异常传	合计
--	---	---------------------------------------	----

	征)	输特征)	
第一标签为第一正常标识 (也即是正常传输特征的第4数传输特征)	86 (第一正常个数)	4	90 (正常数据流个数)
第一标签为第一异常标识 (也即是异常传输特征的第4传输特征)	2	8 (第一异常个数)	10 (异常数据流个数)
合计	88 (第二正常个数)	12 (异常数据流个数)	100

需要说明的是, 若该目标模型的第一查准率大于或等于第一查准率阈值, 则说明在差异度 θ_j 下, 该目标模型在重构正常传输特征时的输出结果基本上是准确的, 若该目标模型的第一查全率大于或等于第一查全率阈值, 说明该目标模型在差异度 θ_j 下能够大概率地完全重构出正常传输特征, 因此, 若该目标模型的第一查准率大于或等于第一查准率阈值且该目标模型的第一查全率大于或等于第一查全率阈值, 说明在该差异度 θ_j 下, 该目标模型具有完全重构出正常传输特征的功能。若该目标模型的第二查准率大于或等于第二查准率阈值, 则说明在差异度 θ_j 下, 该目标模型在重构异常传输特征时的输出结果基本上是准确的, 若该目标模型的第二查全率大于或等于第二查全率阈值, 说明该目标模型在差异度 θ_j 下大概率地不能完全重构出异常传输特征, 因此, 若该目标模型的第二查准率大于或等于第二查准率阈值且该目标模型的第二查全率大于或等于第二查全率阈值, 说明在该差异度 θ_j 下, 该目标模型不具有完全重构出异常传输特征的功能, 所以, 若在差异度 θ_j 下该目标模型符合第一条件, 则认为该差异度 θ_j 为可靠的, 该控制设备将该差异度 θ_j 确定为目标差异度。

在一种可能的实现方式中, 由用户根据经验来设定该目标差异度, 无须通过上述公式(3)以及更新的方式, 确定该目标差异度。

510、该控制设备将目标终端类型下多个目标终端的多个第六传输特征输入该目标模型, 由该目标模型基于输入的该多个第六传输特征, 重构每个第六传输特征, 输出多个第七传输特征, 该多个第六传输特征与该多个第七传输特征一一对应, 一个第六传输特征为一个目标终端传输的至少一个数据流的总体传输特征。

该多个目标终端包括至少一个第二终端以及至少一个第三终端, 其中, 该至少一个第二终端均为正常终端, 该至少一个第三终端均为异常终端。一个第七传输特征为重构出的一个第六传输特征。

测试集除了包括至少一个第二终端的多个传输特征以外, 还包括至少一个第三终端的多个传输特征, 在该测试集中第二终端的传输特征和第三终端的传输特征均视为第六传输特征。该控制设备从测试集中获取多个第六传输特征, 并将获取到的多个第六传输特征输入该目标模型, 由目标模型基于输入的多个第六传输特征, 输出重构出的多个第六传输特征, 其中, 该多个第六传输特征属于至少一个第二终端和至少一个第三终端, 重构出的多个第六传输特征也即是该多个第七传输特征, 每个第七传输特征对应一个第六传输特征。

511、该控制设备基于该多个第七传输特征与对应的第六传输特征之间的差异度, 确定该目标模型通过验证。

该控制设备基于该多个第七传输特征与对应的第六传输特征之间的差异度，确定该目标模型是否符合第二条件，若该目标模型符合第二条件，则该控制设备确定该目标模型通过验证，否则，该控制设备确定该目标模型未通过验证，若该目标模型未通过验证，则该控制设备跳转执行步骤 507-511，直至最终获取的目标模型能够通过验证。

其中，第二条件包括下述至少一项：该目标差异度下，该目标模型的第一查准率大于或等于第三查准率阈值，且该目标模型的第一查全率大于或等于第三查全率阈值；在该目标差异度下，该目标模型的第二查准率大于或等于第四查准率阈值，且该目标模型的第二查全率大于或等于第四查全率阈值。本申请实施例对第三查准率阈值、第三查全率阈值、第四查准率阈值和第四查全率阈值的不作具体限定。

其中，第一查准率、第一查全率、第二查准率、第二查全率的计算方式在步骤 5093 中有相关介绍，在此不做赘述。

需要说明的是，当该目标模型通过验证时，该控制设备将该目标模型添加至模型库中，并为该目标模型分配模型标识，该模型库用于指示至少一个终端类型所对应的目标模型。每个终端类型对应一个目标模型。

该控制设备还能将该目标模型与该目标终端类型进行关联存储。在一种可能的实现方式中，当该目标模型通过验证时，该控制设备将该目标模型的模型标识与该目标终端类型进行关联存储至目标模型列表，以便查询，其中，该目标模型列表用于记录至少一个终端类型所对应的目标模型。例如，该目标终端类型为摄像头，该目标终端类型对应的目标模型为目标模型 3，则该控制设备将摄像头和目标模型 3 关联存储在表 8 所示的目标模型列表。

表 8

模型标识	终端类型
目标模型 1	音响
目标模型 2	ATM
目标模型 3	摄像头

需要说明的是，在本申请实施例中，是由控制设备进行训练，以获取目标模型，而在另外的一些实施例中，网络设备也能进行训练，以获取目标模型，网络设备进行训练的过程与控制设备进行训练的过程同理，在此，本申请实施例对网络设备进行训练的过程不做赘述。

本申请实施例提供的方法，通过该控制设备将该目标终端类型对应的网络地址下发到至少一个网络设备，由每个网络设备基于下发的每个网络地址，收集每个网络地址所指示的第二终端的传输特征，再由控制设备基于每个网络设备上传的至少一个第二终端的多个传输特征，训练得到该目标终端类型对应的目标模型，以便后续基于该目标模型，验证该目标终端类型下的终端是否为异常终端。

该控制设备将该目标模型发送至少一个网络设备，由各个网络设备基于该目标模型对该目标终端类型下的终端进行验证，为了进一步说明该过程，参见图 8 所示的本申请实施例提供的一种用于实现终端验证的方法的流程图。

801、该控制设备向至少一个网络设备发送模型存储指令，该模型存储指令用于指示存储该目标模型。

该模型存储指令包括该目标模型、目标终端类型以及该目标终端类型对应的至少一个网络地址、目标差异度以及存储标识，该目标终端类型也即是第二终端的终端类型，该至少一

个网络地址也即是配置表中该目标终端类型所对应的网络地址，也即是至少一个第二终端的网络地址，该存储标识用于指示存储该目标模型。

在一种可能的实现方式中，用户在该控制设备的模型更新界面内输入该目标终端类型，当该控制设备在该模型更新界面检测到用户执行了确认操作时，则该触发该控制设备执行以下操作：该控制设备基于该模型更新界面中输入的该目标终端类型，在资产表中查询该目标终端类型对应的目标模型的模型标识，在配置表中查询该目标终端类型对应的至少一个网络地址，并在模型库中获取该模型标识对应的目标模型，该控制设备并将该目标终端类型、至少一个网络地址、目标模型以及存储标识添加在该模型存储指令中，并向该至少一个网络设备发送该模型存储指令。

802、对于该至少一个网络设备中的任一网络设备，该任一网络设备接收该模型存储指令。

803、该任一网络设备存储该模型存储指令中的目标模型。

该任一网络设备将该模型存储指令中的该目标模型、目标终端类型、该至少一个网络地址以及目标差异度进行关联存储。

804、该任一网络设备获取第一终端的第一传输特征，该第一传输特征为该第一终端传输的至少一个第一数据流的总体传输特征。

该第一终端的终端类型为该目标终端类型，该第一终端也即是目标终端类型的被验证终端。该第一终端的网络地址为该至少一个网络地址中的任一个，也即是该至少一个第二终端中任一第二终端的网络地址与该第一终端的网络地址相同。该至少一个第一数据流均携带该第一终端的网络地址。该第一传输特征也即是该第一终端的一个传输特征，也即是该一个时间窗口内该第一终端传输的至少一个第一数据流的总体传输特征。

若该第一终端不是预设业务所使用的终端，则该第一终端传输的报文所携带的第一终端的网络地址为一个第二终端的网络地址，若该第一终端是预设业务所使用的终端，则该第一终端为该至少一个第二终端中的任一个。而为了验证该第一终端是否是异常终端，该任一网络设备还需基于该第一终端的第一传输特征，来验证该第一终端是否为异常终端，因此，该任一网络设备还需获取该第一终端的第一传输特征。

对于该至少一个网络地址中的任一网络地址，当该任一网络设备接收到携带该任一网络地址的至少一个数据流时，该任一网络设备将该至少一个数据流确定为至少一个第一数据流，该任一网络设备将输出该至少一个第一数据流的终端，确定为第一终端；该任一网络设备基于该至少一个第一数据流，确定该第一终端的第一传输特征。

其中，该任一网络设备基于该至少一个第一数据流，确定该第一终端的第一传输特征的过程与上述步骤 504 中任一网络设备确定第二终端的一个传输特征的过程同理，在此，本申请实施例对该任一网络设备基于该至少一个第一数据流，确定该第一终端的第一传输特征的过程不做赘述。

805、该任一网络设备将该第一传输特征输入目标模型，由该目标模型基于输入的该第一传输特征，重构该第一传输特征，输出第二传输特征。

其中，该目标模型与目标终端类型对应，第二传输特征也即是该目标模型重构出的第一传输特征。本步骤 805 所示的过程也即是该任一网络设备基于该第一传输特征，重构该第一传输特征，得到第二传输特征的过程。

806、若该第一传输特征与该第二传输特征之间的差异度大于或等于目标差异度，该任一

网络设备确定该第一终端未通过验证，该目标差异度用于指示该第一传输特征与该第二传输特征之间的差异情况。

该第一传输特征与该第二传输特征之间的差异度为该第二传输特征与对应该第一传输特征中相应特征之间的均方误差。

该任一网络设备基于上述公式(2)计算，该第二传输特征与对应该第一传输特征中相应特征之间的均方误差，并将该均方误差确定为该第一传输特征与该第二传输特征之间的差异度；该任一网络设备将该第一传输特征与该第二传输特征之间的差异度与该目标差异度进行比较，以确定该第一传输特征与该第二传输特征之间的差异度是否大于或等于目标差异度；若该第一传输特征与该第二传输特征之间的差异度大于或等于目标差异度，则说明该目标模型没有完全重构出该第一传输特征，该第一传输特征为异常传输特征，该第一终端的行为异常，该第一终端是异常终端，则该任一网络设备确定该第一终端未通过验证；若该第一传输特征与该第二传输特征之间的差异度小于目标差异度，则说明该目标终端完全重构出该第一传输特征，该第一传输特征为正常传输特征，该第一终端的行为正常，该第一终端是正常终端，则该任一网络设备确定该第一终端通过验证。

807、该任一网络设备向该控制设备发送对该第一终端的验证结果，该验证结果用于指示该第一终端是否通过验证。

该验证结果包括验证标识以及该第一终端的网络地址。该验证标识用于指示该第一终端是否通过验证，该验证标识包括第一验证标识或第二验证标识，其中，第一验证标识用于指示该第一终端通过验证，该第二验证标识用于指示该第一终端未通过验证。若该第一终端通过验证，则该验证标识为第一验证标识，若该第一终端未通过验证，则该验证标识为第二验证标识。

808、该控制设备接收该验证结果。

809、若该第一终端未通过验证，则该控制设备显示第一提示信息，并向该任一网络设备发送断开接入指令

该第一提示信息用于提示用户该第一终端未通过验证，该第一提示信息包括该第二验证标识、第一终端的网络地址以及警告标识，该警告标识用于提示用户该第一终端未通过验证，也即是用于提示用户该第一终端为异常终端。该断开接入指令用于指示任一网络设备断开与该第一终端之间的连接，该断开接入指令包括该第一终端的网络地址以及断开标识，该断开标识用于指示任一网络设备断开与该第一终端之间的连接。

在一种可能的实现方式中，若该验证结果中的验证标识为第二验证标识，则触发该控制设备显示第一提示信息，并向该任一网络设备发送该断开接入指令。

在另一种可能的实现方式中，若该验证结果中的验证标识为第二验证标识，则触发该控制设备显示第一提示信息，用户可在该控制设备查阅该第一提示信息，若用户在该控制设备上还执行了用户触发该断开接入指令的操作，则触发该控制设备向该任一网络设备发送该断开接入指令。

若该第一终端通过验证，则该控制设备显示第二提示信息，该第二提示信息用于提示用户该第一终端通过验证，也即是用于提示该第一终端是正常终端，该第二提示信息包括该第一终端的IP地址以及第一验证标识。

810、该任一网络设备接收该断开接入指令，并基于该断开接入指令断开与该第一终端的

之间连接。

当该任一网络设备接收到该断开接入指令后，该任一网络设备从该断开接入指令中获取网络地址，并断开与该网络地址所指示的第一终端之间的连接。

在一种可能的实现中，该任一网络设备也能够显示该第一提示信息提示用户该第一终端未通过验证。在一种可能的实现中，若用户在该任一网络设备上进行了用于触发断开与该第一终端的连接的操作，则触发该任一网络设备直接断开与第一总段之间连接，而无须等待控制设备下发断开接入指令。

本申请实施例提供的方法，通过重构终端的传输特征，来对终端进行验证，例如若重构出的传输特征与终端的传输特征之间的差异较大，则说明该终端的传输特征出现异常，该终端为异常终端，则确定该终端未通过验证，由于终端具有特定的正常传输特征，正常传输特征不易仿冒，因此，该方法能够准确地验证出各种异常终端，提高了终端验证的准确度，而仿冒终端为异常终端的一种，因此，该方法也能够准确的验证出仿冒终端，而不是通过简单的对该终端的IP地址进行验证的方式，以防对仿冒终端验证通过。

为了进一步说明图3、图5和图8所示的过程，参见图9所示的本申请实施例提供的一种用于实现终端验证的方法的示意图。网络设备在接收到终端传输的数据流时，根据该数据流中的报文，获取该数据流的传输信息，并将传输信息上传至控制设备，由该控制设备提取该传输信息中终端的网络地址（也即是资产识别），以实现配置终端配置，并由用户基于该终端的网络地址，在资产表中标注该终端的终端类型（例如将该终端的网络地址与该终端的终端类型关联存储）。该控制设备将该目标终端类型对应的终端的网络地址信息（也即是设备信息）下发至网络设备，由网络设备基于下发的网络地址匹配对应设备类型的终端传输的至少一个数据流，并获取该至少一个数据流的流传输特征，该网络设备基于该至少一个数据流的流传输特征，获取对应终端的传输特征，并将对应终端的传输特征发送至控制设备中的样本库，由控制设备基于样本库中该目标终端类型下至少一个终端的传输特征，训练得到该目标终端类型对应的目标模型，并将该目标模型下发至网络设备，由网络设备基于该目标模型对该终端类型下的终端进行验证，若终端未通过验证，则显示警告信息也即是第一提示信息，由用户向该网络设备下发隔离策略，例如断开与未通过验证的终端之间的连接，则该网络设备接收到该隔离策略后，断开与未通过验证的终端之间的连接。

图10是本申请实施例提供的一种用于实现终端验证的装置的结构示意图，该装置1000包括：

第一获取模块1001，用于获取第一终端的第一传输特征，所述第一传输特征为所述第一终端传输的至少一个第一数据流的总体传输特征；

第一重构模块1002，用于基于所述第一传输特征，对所述第一传输特征进行重构，得到第二传输特征，所述第二传输特征为重构出的所述第一传输特征；

确定模块1003，用于若所述第一传输特征与所述第二传输特征之间的差异度大于或等于目标差异度，确定所述第一终端未通过验证。

可选地，所述第一传输特征包括上行传输特征，所述上行传输特征为所述至少一个第一数据流中至少一个上行数据流的总体传输特征。

可选地，所述上行传输特征包括上行报文特征、上行流特征中的至少一个，所述上行报文特征为所述至少一个上行数据流中上行报文的总体特征，所述上行流特征为所述至少一个

上行数据流的统计特征。

可选地，所述上行报文特征包括上行报文平均传输间隔、上行负载平均值、上行总负载大小、上行报文个数、上行目标报文个数、上行目标报文占比、上行报文负载波动值中的至少一个，所述上行报文平均传输间隔为在一个时间窗口内所述上行报文的平均传输间隔，所述上行负载平均值为在所述时间窗口内所述至少一个上行数据流中目标报文的负载的平均大小，所述上行总负载大小为在所述时间窗口内所述至少一个上行数据流中目标报文的负载的总大小，所述上行报文个数为在所述时间窗口内所述至少一个上行数据流中上行报文的个数，所述上行目标报文个数在所述时间窗口内所述至少一个上行数据流中目标报文的个数，所述上行目标报文占比为在所述时间窗口内所述至少一个上行数据流中目标报文的占比，所述上行报文负载波动值用于指示在所述时间窗口内所述至少一个上行数据流中目标报文的大小波动情况；

所述上行流特征包括上行终端端口波动值、上行数据流总个数、上行目标数据流个数、至少一种数据流类型中每种数据流类型下的上行数据流个数、至少一种传输协议类型中每种传输协议类型下的上行数据流个数中的至少一个，所述上行终端端口波动值用于指示在所述时间窗口内所述第一终端中所述至少一个上行数据流的输出端口的波动情况，所述上行目标数据流为所对应的服务器输入端口属于目标端口范围的上行数据流。

可选地，所述上行报文特征还包括第一接收窗口波动值、第一接收窗口大小平均值中的至少一个，所述第一接收窗口波动值用于指示在所述时间窗口内所述上行报文携带的接收窗口大小的波动情况。

可选地，所述第一接收窗口波动值为在所述时间窗口内所述上行报文携带的接收窗口大小的标准差。

可选地，所述第一传输特征还包括所述至少一个第一数据流的总个数、下行传输特征中的至少一个，所述下行传输特征为所述至少一个第一数据流中至少一个下行数据流的总体传输特征。

可选地，所述下行传输特征包括下行报文特征、下行流特征中的至少一个，所述下行报文特征为所述至少一个下行数据流中下行报文的总体特征，所述下行流特征为所述至少一个下行数据流的统计特征。

可选地，所述下行报文特征包括下行报文平均传输间隔、下行负载平均值、下行总负载大小、下行报文个数、下行目标报文个数、下行目标报文占比、下行报文负载波动值中的至少一个，所述下行报文平均传输间隔为在一个时间窗口内所述下行报文的平均传输间隔，所述下行负载平均值为在所述时间窗口内所述至少一个下行数据流中目标报文的负载的平均大小，所述下行总负载大小为在所述时间窗口内所述至少一个下行数据流中目标报文的负载的总大小，所述下行报文个数为在所述时间窗口内所述至少一个下行数据流中下行报文的个数，所述下行目标报文个数在所述时间窗口内所述至少一个下行数据流中目标报文的个数，所述下行目标报文占比为在所述时间窗口内所述至少一个下行数据流中目标报文的占比，所述下行报文负载波动值用于指示在所述时间窗口内所述至少一个下行数据流中目标报文的大小波动情况；

所述下行流特征包括下行终端端口波动值、下行数据流总个数、下行目标数据流个数、至少一种数据流类型中每种数据流类型下的下行数据流个数、至少一种传输协议类型中每种

传输协议类型下的下行数据流个数中的至少一个,所述下行终端端口波动值用于指示在所述时间窗口内所述第一终端中所述至少一个下行数据流的输入端口的波动情况,所述下行目标数据流为对应的服务器输出端口属于目标端口范围的下行数据流。

可选地,所述下行报文特征还包括第二接收窗口波动值、第二接收窗口大小平均值中的至少一个,所述第二接收窗口波动值用于指示所述下行报文携带的接收窗口大小的波动情况。

可选地,所述第二接收窗口波动值为在所述时间窗口内所述下行报文携带的接收窗口大小的标准差。

所述第一获取模块 1001 用于:

获取所述至少一个第一数据流中每个第一数据流的流传输特征;

基于所述至少一个第一数据流的流传输特征,获取所述第一传输特征。

可选地,一个第一数据流的流传输特征包括所述第一数据流的传输信息、数据流类型、目标端口类型、报文特征中的至少一个,所述传输信息用于指示数据流的传输属性,所述目标端口类型为服务器中传输所述第一数据流的端口的端口类型,所述报文特征为所述第一数据流中报文的特征。

可选地,所述传输信息包括所述第一数据流的五元组中的至少一元;

所述报文特征包括报文传输间隔总和、负载大小、负载平方和、目标报文个数、报文总个数、接收窗口波动值、窗口总大小、窗口平方和中的至少一个,所述报文传输间隔总和为在一个时间窗口内所述第一数据流中报文之间的传输间隔的总时长,所述负载大小为在所述时间窗口内所述第一数据流中目标报文的负载的总大小,所述负载平方和为所述目标报文的负载的大小平方和,所述目标报文个数为在所述时间窗口内所述报文中目标报文的总个数,所述报文总个数为在所述时间窗口内所述报文的总个数,所述接收窗口波动值用于指示在所述时间窗口内所述报文携带的接收窗口大小的波动情况,所述窗口总大小为在所述时间窗口内所述报文携带的接收窗口大小的总和,所述窗口平方和为所述滑动窗口的大小的平方和。

可选地,所述传输信息还包括方向标识、所述时间窗口的标识中的至少一个,所述方向标识用于指示所述第一数据流的传输方向。

可选地,所述第一重构模块 1002 用于:

将所述第一传输特征输入目标模型,由所述目标模型基于输入的所述第一传输特征,重构所述第一传输特征,输出所述第二传输特征。

可选地,所述装置 1000 还包括:

训练模块,用于将目标终端类型下至少一个第二终端的多个第三传输特征作为初始模型的输入和输出,进行训练,得到所述目标模型,所述目标终端类型为所述第一终端的终端类型,一个第三传输特征为一个第二终端传输的至少一个数据流的总体传输特征。

可选地,所述装置 1000 还包括:

第二重构模块,用于将目标终端模型下的多个目标终端的多个第四传输特征输入所述目标模型,由所述目标模型基于输入的所述多个第四传输特征,重构每个第四传输特征,输出多个第五传输特征,所述目标终端类型为所述第一终端的终端类型,所述多个第四传输特征与所述多个第五传输特征一一对应,一个第四传输特征为一个目标终端传输的至少一个数据流的总体传输特征;

第二获取模块,用于基于所述多个第五传输特征与所述多个第四传输特征,获取所述目

标差异度。

可选地，所述第二获取模块用于：

基于所述多个第五传输特征中至少一个第五传输特征与对应的第四传输特征之间的差异度，获取所述目标差异度。

可选地，所述装置 1000 还包括：

第三重构模块，用于将目标终端类型下多个目标终端的多个第六传输特征输入所述目标模型，由所述目标模型基于输入的所述多个第六传输特征，重构每个第六传输特征，输出多个第七传输特征，所述目标终端类型为所述第一终端的终端类型，所述多个第六传输特征与所述多个第七传输特征一一对应，一个第六传输特征为一个目标终端传输的至少一个数据流的总体传输特征；

所述确定模块 1003，还用于基于所述多个第七传输特征与对应的第六传输特征之间的差异度，确定所述目标模型通过验证。

可选地，所述装置 1000 还包括：

第三获取模块，用于获取所述至少一个第二终端传输的至少一个第二数据流的传输信息，所述传输信息用于指示数据流的传输属性；

存储模块，用于将所述传输信息与所述第二终端的终端类型进行关联存储；

所述第三获取模块，还用于基于所述终端类型关联的传输信息，获取所述至少一个第二终端的多个传输特征，一个传输特征为终端传输的至少一个数据流的总体传输特征。

可选地，所述装置 1000 还包括：

接收模块，用于从控制设备接收所述目标模型。

可选地，所述装置 1000 为控制设备或网络设备。

所述装置 1000 通过重构终端的传输特征，来对终端进行验证，例如若重构出的传输特征与终端的传输特征之间的差异较大，则说明该终端的传输特征出现异常，该终端为异常终端，则确定该终端未通过验证，由于终端具有特定的正常传输特征，正常传输特征不易仿冒，因此，所述装置 1000 能够准确地验证出各种异常终端，提高了终端验证的准确度，而仿冒终端为异常终端的一种，因此，所述装置 1000 也能够准确的验证出仿冒终端，而不是通过简单的对该终端的 IP 地址进行验证的方式，以防对仿冒终端验证通过。

图 11 是本申请实施例提供的一种用于实现终端验证的装置，所述 1100 装置包括：

获取模块 1101，用于获取目标终端类型的至少一个第二终端的多个第三传输特征，一个第三传输特征为一个第二终端传输的至少一个数据流的总体传输特征；

训练模块 1102，用于将所述多个第三传输特征作为初始模型的输入和输出，进行训练，得到目标模型，所述目标模型用于重构所述目标终端类型的被验证终端的传输特征，以对所述被验证终端进行验证，所述传输特征为所述被验证终端传输的至少一个数据流的总体传输特征。

可选地，所述装置 1100 还包括：

发送模块 1103，用于向网络设备发送所述目标模型。

可选地，所述装置 1100 还包括：

第一重构模块，用于将所述目标终端类型下多个目标终端的多个第四传输特征输入所述目标模型，由所述目标模型基于输入的所述多个第四传输特征，重构每个第四传输特征，输

出多个第五传输特征，所述多个第四传输特征与所述多个第五传输特征一一对应，一个第四传输特征为一个目标终端传输的至少一个数据流的总体传输特征；

第一目标获取模块，还用于基于所述多个第五传输特征与所述多个第四传输特征，获取所述目标差异度。

可选地，所述第一目标获取模块用于：

基于所述多个第五传输特征中至少一个第五传输特征与对应的第四传输特征之间的差异度，获取所述目标差异度。

可选地，所述装置 1100 还包括：

第二重构模块，用于将所述目标终端类型下多个目标终端的多个第六传输特征输入所述目标模型，由所述目标模型基于输入的所述多个第六传输特征，重构每个第六传输特征，输出多个第七传输特征，所述多个第六传输特征与所述多个第七传输特征一一对应，一个第六传输特征为一个目标终端传输的至少一个数据流的总体传输特征；

确定模块，用于基于所述多个第七传输特征与对应的第六传输特征之间的差异度，确定所述目标模型通过验证。

可选地，所述装置 1100 还包括：

第二目标获取模块，用于获取所述至少一个第二终端传输的至少一个第二数据流的传输信息，所述传输信息用于指示数据流的传输属性；

存储模块，用于将所述传输信息与所述第二终端的终端类型进行关联存储；

所述第二目标获取模块，还用于基于所述终端类型关联的传输信息，获取所述至少一个第二终端的多个传输特征，一个传输特征为终端传输的至少一个数据流的总体传输特征。

上述所有可选技术方案，可以采用任意结合形成本公开的可选实施例，在此不再一一赘述。

需要说明的是：上述实施例提供的用于实现终端验证的装置在验证终端时，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。另外，上述实施例提供的用于实现终端验证的方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

本申请实施例还提供了一种计算机程序产品或计算机程序，该计算机程序产品或计算机程序包括计算机指令，该计算机指令存储在计算机可读存储介质中，电子设备的处理器从计算机可读存储介质读取该计算机指令，处理器执行该计算机指令，使得该电子设备执行上述用于实现终端验证的方法。

本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

以上所述仅为本申请的示例性实施例，并不用以限制本申请，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，均应包含在本申请的保护范围之内。

权利要求书

1. 一种用于实现终端验证的方法，其特征在于，所述方法包括：

获取第一终端的第一传输特征，所述第一传输特征为所述第一终端传输的至少一个第一数据流的总体传输特征；

基于所述第一传输特征，对所述第一传输特征进行重构，得到第二传输特征，所述第二传输特征为重构出的所述第一传输特征；

若所述第一传输特征与所述第二传输特征之间的差异度大于或等于目标差异度，确定所述第一终端未通过验证。

2. 根据权利要求1所述的方法，其特征在于，所述第一传输特征包括上行传输特征，所述上行传输特征为所述至少一个第一数据流中至少一个上行数据流的总体传输特征。

3. 根据权利要求2所述的方法，其特征在于，所述上行传输特征包括上行报文特征、上行流特征中的至少一个，所述上行报文特征为所述至少一个上行数据流中上行报文的总体特征，所述上行流特征为所述至少一个上行数据流的统计特征。

4. 根据权利要求3所述的方法，其特征在于，所述上行报文特征包括上行报文平均传输间隔、上行负载平均值、上行总负载大小、上行报文个数、上行目标报文个数、上行目标报文占比、上行报文负载波动值中的至少一个，所述上行报文平均传输间隔为在一个时间窗口内所述上行报文的平均传输间隔，所述上行负载平均值为在所述时间窗口内所述至少一个上行数据流中目标报文的负载的平均大小，所述上行总负载大小为在所述时间窗口内所述至少一个上行数据流中目标报文的负载的总大小，所述上行报文个数为在所述时间窗口内所述至少一个上行数据流中上行报文的个数，所述上行目标报文个数在所述时间窗口内所述至少一个上行数据流中目标报文的个数，所述上行目标报文占比为在所述时间窗口内所述至少一个上行数据流中目标报文的占比，所述上行报文负载波动值用于指示在所述时间窗口内所述至少一个上行数据流中目标报文的大小波动情况；

所述上行流特征包括上行终端端口波动值、上行数据流总个数、上行目标数据流个数、至少一种数据流类型中每种数据流类型下的上行数据流个数、至少一种传输协议类型中每种传输协议类型下的上行数据流个数中的至少一个，所述上行终端端口波动值用于指示在所述时间窗口内所述第一终端中所述至少一个上行数据流的输出端口的波动情况，所述上行目标数据流为所对应的服务器输入端口属于目标端口范围的上行数据流。

5. 根据权利要求4所述的方法，其特征在于，所述上行报文特征还包括第一接收窗口波动值、第一接收窗口大小平均值中的至少一个，所述第一接收窗口波动值用于指示在所述时间窗口内所述上行报文携带的接收窗口大小的波动情况。

6. 根据权利要求2-5任一项权利要求所述的方法，其特征在于，所述第一传输特征还包

括所述至少一个第一数据流的总个数、下行传输特征中的至少一个，所述下行传输特征为所述至少一个第一数据流中至少一个下行数据流的总体传输特征。

7. 根据权利要求6所述的方法，其特征在于，所述下行传输特征包括下行报文特征、下行流特征中的至少一个，所述下行报文特征为所述至少一个下行数据流中下行报文的总体特征，所述下行流特征为所述至少一个下行数据流的统计特征。

8. 根据权利要求7所述的方法，其特征在于，所述下行报文特征包括下行报文平均传输间隔、下行负载平均值、下行总负载大小、下行报文个数、下行目标报文个数、下行目标报文占比、下行报文负载波动值中的至少一个，所述下行报文平均传输间隔为在一个时间窗口内所述下行报文的平均传输间隔，所述下行负载平均值为在所述时间窗口内所述至少一个下行数据流中目标报文的负载的平均大小，所述下行总负载大小为在所述时间窗口内所述至少一个下行数据流中目标报文的负载的总大小，所述下行报文个数为在所述时间窗口内所述至少一个下行数据流中下行报文的个数，所述下行目标报文个数在所述时间窗口内所述至少一个下行数据流中目标报文的个数，所述下行目标报文占比为在所述时间窗口内所述至少一个下行数据流中目标报文的占比，所述下行报文负载波动值用于指示在所述时间窗口内所述至少一个下行数据流中目标报文的大小波动情况；

所述下行流特征包括下行终端端口波动值、下行数据流总个数、下行目标数据流个数、至少一种数据流类型中每种数据流类型下的下行数据流个数、至少一种传输协议类型中每种传输协议类型下的下行数据流个数中的至少一个，所述下行终端端口波动值用于指示在所述时间窗口内所述第一终端中所述至少一个下行数据流的输入端口的波动情况，所述下行目标数据流为对应的服务器输出端口属于目标端口范围的下行数据流。

9. 根据权利要求8所述的方法，其特征在于，所述下行报文特征还包括第二接收窗口波动值、第二接收窗口大小平均值中的至少一个，所述第二接收窗口波动值用于指示所述下行报文携带的接收窗口大小的波动情况。

10. 根据权利要求1-9任一项权利要求所述的方法，其特征在于，所述获取第一终端的第一传输特征包括：

获取所述至少一个第一数据流中每个第一数据流的流传输特征；

基于所述至少一个第一数据流的流传输特征，获取所述第一传输特征。

11. 根据权利要求10所述的方法，其特征在于，一个第一数据流的流传输特征包括所述第一数据流的传输信息、数据流类型、目标端口类型、报文特征中的至少一个，所述传输信息用于指示数据流的传输属性，所述目标端口类型为服务器中传输所述第一数据流的端口的端口类型，所述报文特征为所述第一数据流中报文的特征。

12. 根据权利要求11所述的方法，其特征在于，所述传输信息包括所述第一数据流的五元组中的至少一元；

所述报文特征包括报文传输间隔总和、负载大小、负载平方和、目标报文个数、报文总个数、接收窗口波动值、窗口总大小、窗口平方和中的至少一个，所述报文传输间隔总和为在一个时间窗口内所述第一数据流中报文之间的传输间隔的总时长，所述负载大小为在所述时间窗口内所述第一数据流中目标报文的负载的总大小，所述负载平方和为所述目标报文的负载大小的平方和，所述目标报文个数为在所述时间窗口内所述报文中目标报文的总个数，所述报文总个数为在所述时间窗口内所述报文的总个数，所述接收窗口波动值用于指示在所述时间窗口内所述报文携带的接收窗口大小的波动情况，所述窗口总大小为在所述时间窗口内所述报文携带的接收窗口大小的总和，所述窗口平方和为所述滑动窗口的大小的平方和。

13. 根据权利要求 12 所述的方法，其特征在于，所述传输信息还包括方向标识、所述时间窗口的标识中的至少一个，所述方向标识用于指示所述第一数据流的传输方向。

14. 根据权利要求 1-13 任一项权利要求所述的方法，其特征在于，所述基于所述第一传输特征，对所述第一传输特征进行重构，得到第二传输特征包括：

将所述第一传输特征输入目标模型，由所述目标模型基于输入的所述第一传输特征，重构所述第一传输特征，输出所述第二传输特征。

15. 根据权利要求 14 所述的方法，其特征在于，所述将所述第一传输特征输入目标模型之前，所述方法还包括：

将目标终端类型下至少一个第二终端的多个第三传输特征作为初始模型的输入和输出，进行训练，得到所述目标模型，所述目标终端类型为所述第一终端的终端类型，一个第三传输特征为一个第二终端传输的至少一个数据流的总体传输特征。

16. 根据权利要求 14 或 15 所述的方法，其特征在于，所述将所述第一传输特征输入目标模型之前，所述方法还包括：

将目标终端类型下多个目标终端的多个第四传输特征输入所述目标模型，由所述目标模型基于输入的所述多个第四传输特征，重构每个第四传输特征，输出多个第五传输特征，所述目标终端类型为所述第一终端的终端类型，所述多个第四传输特征与所述多个第五传输特征一一对应，一个第四传输特征为一个目标终端传输的至少一个数据流的总体传输特征；

基于所述多个第五传输特征与所述多个第四传输特征，获取所述目标差异度。

17. 根据权利要求 16 所述的方法，其特征在于，所述基于所述多个第五传输特征与所述多个第四传输特征，获取所述目标差异度包括：

基于所述多个第五传输特征中至少一个第五传输特征与对应的第四传输特征之间的差异度，获取所述目标差异度。

18. 根据权利要求 14-17 任一项权利要求所述的方法，其特征在于，所述将所述第一传输特征输入目标模型之前，所述方法还包括：

将目标终端类型下多个目标终端的多个第六传输特征输入所述目标模型，由所述目标模

型基于输入的所述多个第六传输特征，重构每个第六传输特征，输出多个第七传输特征，所述目标终端类型为所述第一终端的终端类型，所述多个第六传输特征与所述多个第七传输特征一一对应，一个第六传输特征为一个目标终端传输的至少一个数据流的总体传输特征；

基于所述多个第七传输特征与对应的第六传输特征之间的差异度，确定所述目标模型通过验证。

19. 根据权利要求 14-18 任一项权利要求所述的方法，其特征在于，所述将所述第一传输特征输入目标模型之前，所述方法还包括：

获取所述至少一个第二终端传输的至少一个第二数据流的传输信息，所述传输信息用于指示数据流的传输属性；

将所述传输信息与所述第二终端的终端类型进行关联存储；

基于所述终端类型关联的传输信息，获取所述至少一个第二终端的多个传输特征，一个传输特征为终端传输的至少一个数据流的总体传输特征。

20. 根据权利要求 14 所述的方法，其特征在于，所述将所述第一传输特征输入目标模型之前，所述方法还包括：

从控制设备接收所述目标模型。

21. 根据权利要求 1-19 任一项权利要求所述的方法，其特征在于，所述方法的执行主体为控制设备或网络设备。

22. 一种用于实现终端验证的方法，其特征在于，所述方法包括：

获取目标终端类型的至少一个第二终端的多个第三传输特征，一个第三传输特征为一个第二终端传输的至少一个数据流的总体传输特征；

将所述多个第三传输特征作为初始模型的输入和输出，进行训练，得到目标模型，所述目标模型用于重构所述目标终端类型的被验证终端的传输特征，以对所述被验证终端进行验证，所述传输特征为所述被验证终端传输的至少一个数据流的总体传输特征。

23. 一种用于实现终端验证的装置，其特征在于，所述装置包括：

第一获取模块，用于获取第一终端的第一传输特征，所述第一传输特征为所述第一终端传输的至少一个第一数据流的总体传输特征；

第一重构模块，用于基于所述第一传输特征，对所述第一传输特征进行重构，得到第二传输特征，所述第二传输特征为重构出的所述第一传输特征；

确定模块，用于若所述第一传输特征与所述第二传输特征之间的差异度大于或等于目标差异度，确定所述第一终端未通过验证。

24. 根据权利要求 23 所述的装置，其特征在于，所述第一传输特征包括上行传输特征，所述上行传输特征为所述至少一个第一数据流中至少一个上行数据流的总体传输特征。

25. 根据权利要求 24 所述的装置, 其特征在于, 所述上行传输特征包括上行报文特征、上行流特征中的至少一个, 所述上行报文特征为所述至少一个上行数据流中上行报文的总体特征, 所述上行流特征为所述至少一个上行数据流的统计特征。

26. 根据权利要求 24 或 25 所述的装置, 其特征在于, 所述第一传输特征还包括所述至少一个第一数据流的总个数、下行传输特征中的至少一个, 所述下行传输特征为所述至少一个第一数据流中至少一个下行数据流的总体传输特征。

27. 根据权利要求 26 所述的装置, 其特征在于, 所述下行传输特征包括下行报文特征、下行流特征中的至少一个, 所述下行报文特征为所述至少一个下行数据流中下行报文的总体特征, 所述下行流特征为所述至少一个下行数据流的统计特征。

28. 根据权利要求 23-27 任一项权利要求所述的装置, 其特征在于, 所述第一获取模块用于:

获取所述至少一个第一数据流中每个第一数据流的流传输特征;

基于所述至少一个第一数据流的流传输特征, 获取所述第一传输特征。

29. 根据权利要求 28 所述的装置, 其特征在于, 一个第一数据流的传输特征流传输特征包括所述第一数据流的传输信息、数据流类型、目标端口类型、报文特征中的至少一个, 所述传输信息用于指示数据流的传输属性, 所述目标端口类型为服务器中传输所述第一数据流的端口的端口类型, 所述报文特征用于指示特征为所述第一数据流中报文的特点特征。

30. 根据权利要求 23-29 任一项权利要求所述的装置, 其特征在于, 所述第一重构模块用于:

将所述第一传输特征输入目标模型, 由所述目标模型基于输入的所述第一传输特征, 重构所述第一传输特征, 输出所述第二传输特征。

31. 根据权利要求 30 所述的装置, 其特征在于, 所述装置还包括:

训练模块, 用于将目标终端类型下至少一个第二终端的多个第三传输特征作为初始模型的输入和输出, 进行训练, 得到所述目标模型, 所述目标终端类型为所述第一终端的终端类型, 一个第三传输特征为一个第二终端传输的至少一个数据流的总体传输特征。

32. 根据权利要求 30 或 31 所述的装置, 其特征在于, 所述装置还包括:

第二重构模块, 用于将目标终端类型下多个目标终端的多个第四传输特征输入所述目标模型, 由所述目标模型基于输入的所述多个第四传输特征, 重构每个第四传输特征, 输出多个第五传输特征, 所述目标终端类型为所述第一终端的终端类型, 所述多个第四传输特征与所述多个第五传输特征一一对应, 一个第四传输特征为一个目标终端传输的至少一个数据流的总体传输特征;

第二获取模块, 用于基于所述多个第五传输特征与所述多个第四传输特征, 获取所述目

标差异度。

33. 根据权利要求 30-32 任一项权利要求所述的装置，其特征在于，所述装置还包括：

第三重构模块，用于将目标终端类型下多个目标终端的多个第六传输特征输入所述目标模型，由所述目标模型基于输入的所述多个第六传输特征，重构每个第六传输特征，输出多个第七传输特征，所述目标终端类型为所述第一终端的终端类型，所述多个第六传输特征与所述多个第七传输特征一一对应，一个第六传输特征为一个目标终端传输的至少一个数据流的总体传输特征；

所述确定模块，还用于基于所述多个第七传输特征与对应的第六传输特征之间的差异度，确定所述目标模型通过验证。

34. 一种用于实现终端验证的装置，其特征在于，所述装置包括：

获取模块，用于获取目标终端类型的至少一个第二终端的多个第三传输特征，一个第三传输特征为一个第二终端传输的至少一个数据流的总体传输特征；

训练模块，用于将所述多个第三传输特征作为初始模型的输入和输出，进行训练，得到目标模型，所述目标模型用于重构所述目标终端类型的被验证终端的传输特征，以对所述被验证终端进行验证，所述传输特征为所述被验证终端传输的至少一个数据流的总体传输特征。

35. 一种用于实现终端验证的系统，其特征在于，所述系统包括控制设备和网络设备；

所述控制设备用于：

获取目标终端类型的至少一个第二终端的多个第三传输特征，一个第三传输特征为一个第二终端传输的至少一个数据流的总体传输特征；

将所述多个第三传输特征作为初始模型的输入和输出，进行训练，得到目标模型；

向所述网络设备发送所述目标模型；

所述网络设备用于：

获取所述目标终端类型的第一终端的第一传输特征，所述第一传输特征为所述第一终端传输的至少一个第一数据流的总体传输特征；

将所述第一传输特征输入所述目标模型，由所述目标模型基于输入的所述第一传输特征，重构所述第一传输特征，输出第二传输特征，所述第二传输特征为重构出的所述第一传输特征；

若所述第一传输特征与所述第二传输特征之间的差异度大于或等于目标差异度，确定所述第一终端未通过验证。

36. 一种电子设备，其特征在于，所述电子设备包括处理器和存储器，所述存储器中存储有至少一条程序代码，所述程序代码由所述处理器加载并执行以实现如权利要求 1 至权利要求 22 任一项所述的方法所执行的操作。

37. 一种计算机可读存储介质，其特征在于，所述存储介质中存储有至少一条程序代码，所述程序代码由处理器加载并执行以实现如权利要求 1 至权利要求 22 任一项所述的方法所

执行的操作。