(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 111740883 B
(45)授权公告日 2021.01.26

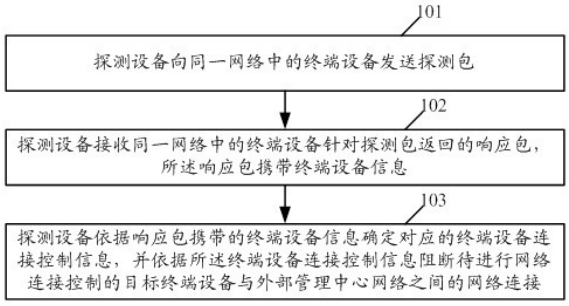
(21)申请号 202010849749.9
(22)申请日 2020.08.21
(65)同一申请的已公布的文献号
申请公布号 CN 111740883 A
(43)申请公布日 2020.10.02
(66)本国优先权数据
202010802647.1 2020.08.11 CN
(73)专利权人 杭州海康威视数字技术股份有限公司
地址 310051 浙江省杭州市滨江区阡陌路555号
(72)发明人 王滨 刘松 万里 何承润 倪俊伟 林克章 陈加栋 王星 王国云
(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 杨春香
(51)Int.Cl.
H04L 12/26(2006.01)
H04L 29/06(2006.01)
H04L 29/12(2006.01)
(56)对比文件
CN 107707560 A,2018.02.16
CN 107087008 A,2017.08.22
CN 105791047 A,2016.07.20
CN 106899444 A,2017.06.27
CN 109981344 A,2019.07.05
CN 110830516 A,2020.02.21
CN 110868429 A,2020.03.06
US 2016/0357424 A1,2016.12.08
审查员 程梦莉
权利要求书3页 说明书18页 附图6页

(54)发明名称

连接控制方法、系统、装置及电子设备

(57)摘要

本申请提供了连接控制方法、系统、装置及电子设备。本申请中，通过探测设备探测同一网络中的终端设备的连接控制信息，并依据探测到的终端设备的连接控制信息阻断待进行网络连接控制的目标终端设备与外部管理中心网络之间的网络连接，这实现了对终端设备与外部管理中心网络之间的网络连接进行连接控制，提高外部管理中心网络的安全。



CN 111740883 B

1.一种连接控制方法,其特征在于,该方法应用于无线局域网络中为实现所述连接控制方法新部署的探测设备,包括:

向同一无线局域网络中的终端设备发送所述探测设备生成的组播探测包或广播探测包;同一无线局域网络中的所有终端设备属于所述组播探测包所对应的组播组;所述终端设备为视频监控终端设备;

接收同一无线局域网络中的终端设备针对所述组播探测包或广播探测包返回的响应包;所述响应包携带终端设备的终端设备信息;

依据所述响应包携带的终端设备信息确定对应的终端设备连接控制信息,并依据所述终端设备连接控制信息阻断待进行网络连接控制的目标终端设备与外部管理中心网络之间的网络连接,所述外部管理中心网络为用于视频监控管理的管理中心网络;其中,当所述终端设备信息包括两个以上参数,其中一个参数为终端设备的IP地址时,若已存储该终端设备信息对应的参考终端设备信息,则当该终端设备信息与所述参考终端设备信息中有至少一个参数不同且该终端设备信息中的IP地址不在已配置的IP白名单时,或者当若未存储有所述参考终端设备信息且所述IP地址不在已配置的IP白名单时,确定所述终端设备信息对应的终端设备为所述目标终端设备。

2.根据权利要求1所述的方法,其特征在于,所述依据所述终端设备连接控制信息阻断待进行网络连接控制的目标终端设备与外部管理中心网络之间的网络连接包括:

向已部署的连接控制设备发送终端设备连接控制信息,以触发所述连接控制设备依据所述终端设备连接控制信息确定待进行网络连接控制的目标终端设备并阻断目标终端设备与外部管理中心网络之间的网络连接。

3.根据权利要求1所述的方法,其特征在于,所述依据所述响应包携带的终端设备信息确定终端设备对应的终端设备连接控制信息包括:

将已接收的所述响应包携带的终端设备信息确定为对应的终端设备连接控制信息;或者,

依据已接收的所述响应包携带的终端设备信息确定该终端设备信息对应的终端设备是否为待进行网络连接控制的目标终端设备,当终端设备信息对应的终端设备为待进行网络连接控制的目标终端设备时,将用于指示该终端设备为待进行网络连接控制的目标终端设备的指示信息确定为对应的终端设备连接控制信息。

4.根据权利要求3所述的方法,其特征在于,

当所述终端设备信息包括一个参数时,所述依据已接收的响应包携带的终端设备信息确定该终端设备信息对应的终端设备是否为待进行网络连接控制的目标终端设备包括:针对接收的每一响应包,当该响应包携带的终端设备信息不在已配置的终端设备信息白名单中,确定该响应包携带的终端设备信息所对应的终端设备为待进行网络连接控制的目标终端设备。

5.根据权利要求1所述的方法,其特征在于,所述探测设备串接在所述网络中、且处于所述网络中各终端设备与外部管理中心网络进行通信的通信路径上;

所述阻断所述目标终端设备与所述外部管理中心网络之间的网络连接包括:截获所述目标终端设备与所述外部管理中心网络进行通信时的数据包并丢弃。

6.一种连接控制方法,其特征在于,该方法应用于连接控制设备,包括:

从已部署的探测设备中获得与所述探测设备处于同一无线局域网络中的各终端设备对应的终端设备连接控制信息;所述探测设备为无线局域网络中为实现所述连接控制方法新部署的;所述终端设备为视频监控终端设备;所述终端设备连接控制信息依据响应包携带的终端设备信息确定的;所述响应包用于响应所述探测设备向同一无线局域网络中的终端设备发送所述探测设备生成的组播探测包或广播探测包;

依据已获得的终端设备连接控制信息确定待进行网络连接控制的目标终端设备;其中,当所述终端设备信息包括两个以上参数,其中一个参数为终端设备的IP地址时,若已存储该终端设备信息对应的参考终端设备信息,当该终端设备信息与所述参考终端设备信息中有至少一个参数不同且该终端设备信息中的IP地址不在已配置的IP白名单时,或者当未存储有所述参考终端设备信息且所述IP地址不在已配置的IP白名单时,确定所述终端设备信息对应的终端设备为所述目标终端设备;

阻断所述目标终端设备与外部管理中心网络之间的网络连接。

7.根据权利要求6所述的方法,其特征在于,

所述终端设备连接控制信息为用于指示终端设备为待进行网络连接控制的目标终端设备的指示信息;所述依据已获得的终端设备连接控制信息确定待进行网络连接控制的目标终端设备,包括:将所述指示信息指示的终端设备确定为所述目标终端设备;或者,

所述终端设备连接控制信息为终端设备信息,所述终端设备信息包括一个参数;所述依据已获得的终端设备连接控制信息确定待进行网络连接控制的目标终端设备,包括:当终端设备信息不在已配置的终端设备信息白名单中,确定终端设备信息对应的终端设备为所述目标终端设备。

8.根据权利要求6所述的方法,其特征在于,当所述连接控制设备串接在所述无线局域网络中各终端设备与外部管理中心网络进行通信的通信路径上时;所述阻断所述目标终端设备与所述外部管理中心网络之间的网络连接包括:截获所述目标终端设备与所述外部管理中心网络进行通信时的数据包并丢弃;

当所述连接控制设备旁挂在核心路由器上时,所述核心路由器为连接在所述无线局域网络与外部管理中心网络之间的路由器;所述阻断所述目标终端设备与所述外部管理中心网络之间的网络连接包括:从所述核心路由器获得所述目标终端设备与所述外部管理中心网络进行通信时的数据包,依据所述数据包生成用于指示所述数据包的目标端不可达的伪造包并向所述核心路由器发送,以通过所述核心路由器向所述数据包的源端发送所述伪造包,所述伪造包用于中断目标终端设备与所述外部管理中心网络之间的网络连接。

9.一种连接控制系统,其特征在于,所述连接控制系统包括探测设备和连接控制设备;

所述探测设备用于执行如权利要求1至5任一方法执行的步骤;

所述连接控制设备用于执行如权利要求6至8任一方法执行的步骤。

10.一种连接控制装置,其特征在于,该装置应用于无线局域网络中为实现连接控制方法新部署的探测设备,包括:

发送单元,用于向同一无线局域网络中的终端设备发送所述探测设备生成的组播探测包或广播探测包;同一无线局域网络中的所有终端设备属于所述组播探测包所对应的组播组;所述终端设备为视频监控终端设备;

接收单元,用于接收同一无线局域网络中的终端设备针对所述组播探测包或广播探测

包返回的响应包;所述响应包携带终端设备的终端设备信息;

连接控制单元,用于依据所述响应包携带的终端设备信息确定对应的终端设备连接控制信息,并依据所述终端设备连接控制信息阻断待进行网络连接控制的目标终端设备与外部管理中心网络之间的网络连接,所述外部管理中心网络为用于视频监控管理的管理中心网络;其中,当所述终端设备信息包括两个以上参数,其中一个参数为终端设备的IP地址时,若已存储该终端设备信息对应的参考终端设备信息,当该终端设备信息与所述参考终端设备信息中有至少一个参数不同且该终端设备信息中的IP地址不在已配置的IP白名单时,或者当未存储有所述参考终端设备信息且所述IP地址不在已配置的IP白名单时,确定所述终端设备信息对应的终端设备为所述目标终端设备。

11.一种连接控制装置,其特征在于,该装置应用于连接控制设备,包括:

获得单元,用于从已部署的探测设备中获得与所述探测设备处于同一无线局域网络中的各终端设备对应的终端设备连接控制信息;所述探测设备为无线局域网络中为实现连接控制方法新部署的;所述终端设备为视频监控终端设备;所述终端设备连接控制信息依据响应包携带的终端设备信息确定的;所述响应包用于响应所述探测设备向同一无线局域网络中的终端设备发送所述探测设备生成的组播探测包或广播探测包;

确定单元,用于依据已获得的终端设备连接控制信息确定待进行网络连接控制的目标终端设备;其中,当所述终端设备信息包括两个以上参数,其中一个参数为终端设备的IP地址时,若已存储该终端设备信息对应的参考终端设备信息,当该终端设备信息与所述参考终端设备信息中有至少一个参数不同且该终端设备信息中的IP地址不在已配置的IP白名单时,或者当未存储有所述参考终端设备信息且所述IP地址不在已配置的IP白名单时,确定所述终端设备信息对应的终端设备为所述目标终端设备;

阻断单元,用于阻断所述目标终端设备与外部管理中心网络之间的网络连接。

12.一种电子设备,其特征在于,该电子设备包括: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;

所述处理器用于执行机器可执行指令,以实现权利要求1-8任一项的方法步骤。

连接控制方法、系统、装置及电子设备

技术领域

[0001] 本申请涉及数据安全技术，特别涉及连接控制方法、系统、装置及电子设备。

背景技术

[0002] 目前，在一些应用场景下，终端设备网络中与管理中心网络连接的终端设备可能会被私接假冒。这里的终端设备可为诸如门禁主机、摄像头、视频监控终端设备等前端设备。以终端设备为视频监控终端设备为例，这里的管理中心网络可为用于视频监控管理的管理中心网络。

[0003] 而一旦私接假冒的终端设备连接管理中心网络，则会给管理中心网络带来很大风险，比如破坏管理中心网络中的管理设备等。

发明内容

[0004] 本申请提供了连接控制方法、系统、装置及电子设备，以对终端设备与外部管理中心网络之间的网络连接进行连接控制。

[0005] 本申请提供一种连接控制方法，该方法应用于探测设备，包括：

[0006] 向同一网络中的终端设备发送探测包；

[0007] 接收同一网络中的终端设备针对所述探测包返回的响应包；所述响应包携带终端设备信息；

[0008] 依据所述响应包携带的终端设备信息确定对应的终端设备连接控制信息，并依据所述终端设备连接控制信息阻断待进行网络连接控制的目标终端设备与外部管理中心网络之间的网络连接。

[0009] 可选地，采用以下任一方式向同一网络中的终端设备发送探测包包括：

[0010] 向同一网络中的终端设备发送组播探测包；同一网络中的所有终端设备属于所述组播探测包所对应的组播组；

[0011] 向同一网络中的各终端设备分别发送单播探测包；

[0012] 向同一网络中的各终端设备发送广播探测包。

[0013] 可选地，所述依据所述终端设备连接控制信息阻断待进行网络连接控制的目标终端设备与外部管理中心网络之间的网络连接包括：

[0014] 向已部署的连接控制设备发送终端设备连接控制信息，以触发所述连接控制设备依据所述终端设备连接控制信息确定待进行网络连接控制的目标终端设备并阻断目标终端设备与外部管理中心网络之间的网络连接。

[0015] 可选地，所述依据所述响应包携带的终端设备信息确定终端设备对应的终端设备连接控制信息包括：

[0016] 将已接收的所述响应包携带的终端设备信息确定为对应的终端设备连接控制信息；或者，

[0017] 依据已接收的所述响应包携带的终端设备信息确定该终端设备信息对应的终端

设备为是否为待进行网络连接控制的目标终端设备，当终端设备信息对应的终端设备为待进行网络连接控制的目标终端设备时，将用于指示该终端设备为待进行网络连接控制的目标终端设备的指示信息确定为对应的终端设备连接控制信息。

[0018] 可选地，所述终端设备信息包括一个参数；所述依据已接收的响应包携带的终端设备信息确定该终端设备信息对应的终端设备是否为待进行网络连接控制的目标终端设备包括：针对接收的每一响应包，当该响应包携带的终端设备信息不在已配置的终端设备信息白名单中，确定该响应包携带的终端设备信息所对应的终端设备为待进行网络连接控制的目标终端设备；或者，

[0019] 所述终端设备信息包括两个以上参数，其中一个参数为终端设备的IP地址；所述依据已接收的所述响应包携带的终端设备信息确定该终端设备信息对应的终端设备是否为待进行网络连接控制的目标终端设备包括：

[0020] 针对每一响应包携带的终端设备信息，

[0021] 当已存储该终端设备信息对应的参考终端设备信息时，若该终端设备信息与所述参考终端设备信息中有至少一个参数不同，或者，若该终端设备信息与所述参考终端设备信息中有至少一个参数不同且该终端设备信息中IP地址不在已配置的IP白名单，则确定该终端设备信息对应的终端设备为待进行网络连接控制的目标终端设备；所述参考终端设备信息包含所述IP地址；或者，

[0022] 当未存储有所述参考终端设备信息，或者，当未存储有所述参考终端设备信息且所述IP地址不在已配置的IP白名单时，确定所述终端设备信息对应的终端设备为待进行网络连接控制的目标终端设备。

[0023] 可选地，所述探测设备串接在所述网络中、且处于所述网络中各终端设备与外部管理中心网络进行通信的通信路径上；所述阻断所述目标终端设备与所述外部管理中心网络之间的网络连接包括：截获所述目标终端设备与所述外部管理中心网络进行通信时的数据包并丢弃。

[0024] 本申请实施例提供一种连接控制方法，该方法应用于连接控制设备，包括：

[0025] 从已部署的探测设备中获得与所述探测设备处于同一网络中的各终端设备对应的终端设备连接控制信息；

[0026] 依据已获得的终端设备连接控制信息确定待进行网络连接控制的目标终端设备；

[0027] 阻断所述目标终端设备与所述外部管理中心网络之间的网络连接。

[0028] 可选地，所述终端设备连接控制信息为用于指示终端设备为待进行网络连接控制的目标终端设备的指示信息；所述依据已获得的终端设备连接控制信息确定待进行网络连接控制的目标终端设备，包括：将所述指示信息指示的终端设备确定为所述目标终端设备；或者，

[0029] 所述终端设备连接控制信息为终端设备信息，所述终端设备信息包括一个参数；所述依据已获得的终端设备连接控制信息确定待进行网络连接控制的目标终端设备，包括：当终端设备信息不在已配置的终端设备信息白名单中，确定终端设备信息对应的终端设备为所述目标终端设备；或者，

[0030] 所述终端设备连接控制信息为终端设备信息，所述终端设备信息包括两个以上参数，其中一个参数为终端设备的IP地址；所述依据已获得的终端设备连接控制信息确定待

进行网络连接控制的目标终端设备，包括：

[0031] 针对每一终端设备信息，在未存储有该终端设备信息对应的参考终端设备信息，或者，在未存储有所述参考终端设备信息且该终端设备信息中的IP不在已配置的IP白名单时，确定该终端设备信息对应的终端设备为所述目标终端设备；该终端设备信息与所述参考终端设备信息中的IP地址相同；或者，

[0032] 针对每一终端设备信息，在存储有该终端设备信息对应的参考终端设备信息时，若该终端设备信息与所述参考终端设备信息中有至少一个参数不同，或者，若该终端设备信息与所述参考终端设备信息中有至少一个参数不同且该终端设备信息中的IP不在已配置的IP白名单，则确定该终端设备信息对应的终端设备为所述目标终端设备。

[0033] 可选地，所述连接控制设备旁挂在核心路由器上，所述核心路由器为连接在所述网络与外部管理中心网络之间的路由器；所述阻断所述目标终端设备与所述外部管理中心网络之间的网络连接包括：从所述核心路由器获得所述目标终端设备与所述外部管理中心网络进行通信时的数据包，依据所述数据包生成用于指示所述数据包的目标端不可达的伪造包并向所述核心路由器发送，以通过所述核心路由器向所述数据包的源端发送所述伪造包，所述伪造包用于中断目标终端设备与所述外部管理中心网络之间的网络连接；或者，

[0034] 所述连接控制设备串接在所述网络中各终端设备与外部管理中心网络进行通信的通信路径上；所述阻断所述目标终端设备与所述外部管理中心网络之间的网络连接包括：截获所述目标终端设备与所述外部管理中心网络进行通信时的数据包并丢弃。

[0035] 本申请实施例提供一种连接控制系统，所述连接控制系统包括探测设备和连接控制设备；

[0036] 所述探测设备用于执行如第一种方法执行的步骤；

[0037] 所述连接控制设备用于执行如第二种方法执行的步骤。

[0038] 本申请实施例提供一种连接控制装置，该装置应用于探测设备，包括：

[0039] 发送单元，用于向同一网络中的终端设备发送探测包；

[0040] 接收单元，用于接收同一网络中的终端设备针对所述探测包返回的响应包；所述响应包携带终端设备信息；

[0041] 连接控制单元，用于依据所述响应包携带的终端设备信息确定对应的终端设备连接控制信息，并依据所述终端设备连接控制信息阻断待进行网络连接控制的目标终端设备与外部管理中心网络之间的网络连接。

[0042] 作为一个实施例，所述发送单元采用以下任一方式向同一网络中的终端设备发送探测包包括：

[0043] 向同一网络中的终端设备发送组播探测包；同一网络中的所有终端设备属于所述组播探测包所对应的组播组；

[0044] 向同一网络中的各终端设备分别发送单播探测包；

[0045] 向同一网络中的各终端设备发送广播探测包。

[0046] 作为一个实施例，所述连接控制单元依据所述终端设备连接控制信息阻断待进行网络连接控制的目标终端设备与外部管理中心网络之间的网络连接包括：

[0047] 向已部署的连接控制设备发送终端设备连接控制信息，以触发所述连接控制设备依据所述终端设备连接控制信息确定待进行网络连接控制的目标终端设备并阻断目标终

端设备与外部管理中心网络之间的网络连接。

[0048] 作为一个实施例,所述连接控制单元依据所述响应包携带的终端设备信息确定终端设备对应的终端设备连接控制信息包括:

[0049] 将已接收的所述响应包携带的终端设备信息确定为对应的终端设备连接控制信息;或者,

[0050] 依据已接收的所述响应包携带的终端设备信息确定该终端设备信息对应的终端设备为是否为待进行网络连接控制的目标终端设备,当终端设备信息对应的终端设备为待进行网络连接控制的目标终端设备时,将用于指示该终端设备为待进行网络连接控制的目标终端设备的指示信息确定为对应的终端设备连接控制信息。

[0051] 可选地,所述终端设备信息包括一个参数;作为一个实施例,所述连接控制单元依据已接收的响应包携带的终端设备信息确定该终端设备信息对应的终端设备是否为待进行网络连接控制的目标终端设备包括:针对接收的每一响应包,当该响应包携带的终端设备信息不在已配置的终端设备信息白名单中,确定该响应包携带的终端设备信息所对应的终端设备为待进行网络连接控制的目标终端设备;或者,

[0052] 所述终端设备信息包括两个以上参数,其中一个参数为终端设备的IP地址;所述依据已接收的所述响应包携带的终端设备信息确定该终端设备信息对应的终端设备是否为待进行网络连接控制的目标终端设备包括:

[0053] 针对每一响应包携带的终端设备信息,

[0054] 当已存储该终端设备信息对应的参考终端设备信息时,若该终端设备信息与所述参考终端设备信息中有至少一个参数不同,或者,若该终端设备信息与所述参考终端设备信息中有至少一个参数不同且该终端设备信息中IP地址不在已配置的IP白名单,则确定该终端设备信息对应的终端设备为待进行网络连接控制的目标终端设备;所述参考终端设备信息包含所述IP地址;或者,

[0055] 当未存储有所述参考终端设备信息,或者,当未存储有所述参考终端设备信息且所述IP地址不在已配置的IP白名单时,确定所述终端设备信息对应的终端设备为待进行网络连接控制的目标终端设备。

[0056] 作为一个实施例,所述探测设备串接在所述网络中、且处于所述网络中各终端设备与外部管理中心网络进行通信的通信路径上;基于此,作为一个实施例,所述连接控制单元阻断所述目标终端设备与所述外部管理中心网络之间的网络连接包括:截获所述目标终端设备与所述外部管理中心网络进行通信时的数据包并丢弃。

[0057] 本申请实施例提供另一种连接控制装置,包括:

[0058] 获得单元,用于从已部署的探测设备中获得与所述探测设备处于同一网络中的各终端设备对应的终端设备连接控制信息;

[0059] 确定单元,用于依据已获得的终端设备连接控制信息确定待进行网络连接控制的目标终端设备;

[0060] 阻断单元,用于阻断所述目标终端设备与所述外部管理中心网络之间的网络连接。

[0061] 作为一个实施例,所述终端设备连接控制信息为用于指示终端设备为待进行网络连接控制的目标终端设备的指示信息;所述确定单元依据已获得的终端设备连接控制信息

确定待进行网络连接控制的目标终端设备，包括：将所述指示信息指示的终端设备确定为所述目标终端设备；或者，

[0062] 所述终端设备连接控制信息为终端设备信息，所述终端设备信息包括一个参数；所述确定单元依据已获得的终端设备连接控制信息确定待进行网络连接控制的目标终端设备，包括：当终端设备信息不在已配置的终端设备信息白名单中，确定终端设备信息对应的终端设备为所述目标终端设备；或者，

[0063] 所述终端设备连接控制信息为终端设备信息，所述终端设备信息包括两个以上参数，其中一个参数为终端设备的IP地址；所述确定单元依据已获得的终端设备连接控制信息确定待进行网络连接控制的目标终端设备，包括：

[0064] 针对每一终端设备信息，在未存储有该终端设备信息对应的参考终端设备信息，或者，在未存储有所述参考终端设备信息且该终端设备信息中的IP不在已配置的IP白名单时，确定该终端设备信息对应的终端设备为所述目标终端设备；该终端设备信息与所述参考终端设备信息中的IP地址相同；或者，

[0065] 针对每一终端设备信息，在存储有该终端设备信息对应的参考终端设备信息时，若该终端设备信息与所述参考终端设备信息中有至少一个参数不同，或者，若该终端设备信息与所述参考终端设备信息中有至少一个参数不同且该终端设备信息中的IP不在已配置的IP白名单，则确定该终端设备信息对应的终端设备为所述目标终端设备。

[0066] 作为一个实施例，所述连接控制设备旁挂在核心路由器上，所述核心路由器为连接在所述网络与外部管理中心网络之间的路由器；所述阻断单元阻断所述目标终端设备与所述外部管理中心网络之间的网络连接包括：从所述核心路由器获得所述目标终端设备与所述外部管理中心网络进行通信时的数据包，依据所述数据包生成用于指示所述数据包的目标端不可达的伪造包并向所述核心路由器发送，以通过所述核心路由器向所述数据包的源端发送所述伪造包，所述伪造包用于中断目标终端设备与所述外部管理中心网络之间的网络连接；或者，

[0067] 所述连接控制设备串接在所述网络中各终端设备与外部管理中心网络进行通信的通信路径上；所述阻断单元阻断所述目标终端设备与所述外部管理中心网络之间的网络连接包括：截获所述目标终端设备与所述外部管理中心网络进行通信时的数据包并丢弃。

[0068] 本申请实施例还提供了一种电子设备。该电子设备包括：处理器和机器可读存储介质；

[0069] 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；

[0070] 所述处理器用于执行机器可执行指令，以实现上述公开的方法的步骤。

[0071] 由以上技术方案可以看出，本申请中，探测设备通过探测同一网络中的终端设备的连接控制信息，并依据所述终端设备连接控制信息阻断待进行网络连接控制的目标终端设备与外部管理中心网络之间的网络连接，这实现了对终端设备与外部管理中心网络之间的网络连接进行连接控制，提高外部管理中心网络的安全。

[0072] 进一步地，本实施例中，由探测设备通过终端设备反馈的响应包即可确定待进行网络连接控制的目标终端设备比如私接假冒的终端设备等，相比现有通过流量分析目标终端设备(比如私接假冒的终端设备等)，方案实现简单，及时发现异常的终端设备(即上述目标终端设备，比如私接假冒的终端设备等)，且无需流量分析，不会影响流量传输。

附图说明

[0073] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本公开的实施例，并与说明书一起用于解释本公开的原理。

[0074] 图1为本申请实施例提供的方法流程图；

[0075] 图2为本申请实施例提供的应用实施例示意图；

[0076] 图3为本申请实施例提供的终端设备信息示意图；

[0077] 图4为本申请实施例提供的探测设备发送终端设备连接控制信息至连接控制设备的示意图；

[0078] 图5为本申请实施例提供的另一方法流程图；

[0079] 图6为本申请实施例提供的伪造包发送示意图；

[0080] 图7为本申请实施例提供的另一应用实施例示意图；

[0081] 图8为本申请实施例提供的系统结构图；

[0082] 图9为本申请实施例提供的装置结构图；

[0083] 图10为本申请实施例提供的另一装置结构图；

[0084] 图11为本申请实施例提供的电子设备结构图。

具体实施方式

[0085] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

[0086] 在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。

[0087] 为了使本领域技术人员更好地理解本申请实施例提供的技术方案，并使本申请实施例的上述目的、特征和优点能够更加明显易懂，下面结合附图对本申请实施例中技术方案作进一步详细的说明。

[0088] 参见图1，图1为本申请实施例提供的连接控制方法流程图。该流程应用于探测设备。这里，探测设备是为实现本实施例提供的连接控制方法而新部署的。可选地，本实施例中，探测设备的结构可有多种，比如探测设备可为探针等，本实施例并不具体限定。

[0089] 在一个例子中，每一网络可部署一个探测设备，部署的探测设备可执行下述图1所示流程。在另一个例子中，不同网络可共享同一个探测设备，在此前提下，探测设备针对该不同网络执行下述图1所示流程(这里可默认探测设备与共享该探测设备的任一网络均属于同一网络)。可选地，这里的网络是根据实际业务需求对终端设备网络进行划分得到的。这里的网络可相当于一个无线局域网(WLAN:Wireless Local Area Network)。比如，对一个公司而言，下属每一子公司或者每一分公司可认为是一个网络。图2举例示出了网络的示意图。图2举例示出网络1、网络2分别部署了探测设备。

[0090] 如图1所示，该流程可包括以下步骤：

[0091] 步骤101，探测设备向同一网络中的终端设备发送探测包。

[0092] 作为一个实施例，本步骤101中，探测设备可周期或者定时向同一网络中的终端设备发送探测包。这里，终端设备可为NVR、摄像头、门禁主机、报警主机等设备，本实施例并不具体限定。

[0093] 本实施例中，探测设备向同一网络中的终端设备发送探测包有很多实现形式。作为一个实施例，探测设备向同一网络中的终端设备发送探测包可包括：向同一网络中的终端设备发送组播探测包。这里，同一网络中的所有终端设备属于所述组播探测包所对应的组播组。在一个例子中，组播探测包的目的IP地址为上述组播组的IP地址(组播组的IP地址可为预先设定的一个IP地址，比如该IP地址可为预留组播IP地址段中的一个IP地址)，当组播探测包的目的IP地址为上述组播组的IP地址，则表示组播探测包对应上述组播组。

[0094] 作为另一个实施例，探测设备向同一网络中的终端设备发送探测包可包括：向同一网络中的各终端设备分别发送单播探测包。单播探测包的目的IP地址为终端设备的IP地址。

[0095] 作为又一个实施例，探测设备向同一网络中的终端设备发送探测包可包括：向同一网络中的各终端设备发送广播探测包。

[0096] 步骤102，探测设备接收同一网络中的终端设备针对探测包返回的响应包，所述响应包携带终端设备信息。

[0097] 如步骤101描述，当探测设备向同一网络中的终端设备发送组播探测包后，则同一网络中的任一终端设备在接收到组播探测包时，返回响应包。这里。终端设备可以单播方式返回响应包。类似地，当探测设备向同一网络中的各终端设备发送单播探测包后，则收到单播探测包的终端设备会单播返回一个响应包；或者，当探测设备向同一网络中的各终端设备发送广播探测包后，接收到广播探测包的任一终端设备也会单播返回一个响应包。即，如步骤102描述，探测设备最终会收到同一网络中的终端设备针对探测包返回的响应包。

[0098] 如步骤102描述，终端设备返回的响应包中携带终端设备信息。这里，终端设备信息用于表征终端设备，其可包含用于描述终端设备的参数，比如可包含：IP地址、MAC地址、设备类型、设备品牌、设备型号、设备版本号等中的至少一个。图3举例示出了终端设备信息的一种形式(包括IP地址、MAC地址、设备类型、设备品牌、设备型号、设备版本号)。

[0099] 步骤103，探测设备依据响应包携带的终端设备信息确定对应的终端设备连接控制信息，并依据所述终端设备连接控制信息阻断待进行网络连接控制的目标终端设备与外部管理中心网络之间的网络连接。

[0100] 本实施例中，步骤103中探测设备依据响应包携带的终端设备信息确定对应的终端设备连接控制信息，在具体实现时有很多实现形式，下文会举例描述，这里暂不赘述。

[0101] 本实施例中，探测设备依据终端设备连接控制信息阻断待进行网络连接控制的目标终端设备与外部管理中心网络之间的网络连接有很多方式。作为其中一种实现方式，探测设备依据终端设备连接控制信息阻断待进行网络连接控制的目标终端设备与外部管理中心网络之间的网络连接可包括：探测设备向已部署的连接控制设备发送终端设备连接控制信息，以触发连接控制设备依据所述终端设备连接控制信息确定待进行网络连接控制的目标终端设备并阻断目标终端设备与外部管理中心网络之间的网络连接。这里，连接控制设备是为实现本实施例提供的连接控制方法而新部署的，其可部署在探测设备所处的网络中，或者部署在网络与外部管理中心网络之间，下文会举例进行描述。探测设备与连接控制

设备是互通的。为保证探测设备发送的终端设备连接控制信息不被泄露，探测设备可在向已部署的连接控制设备发送终端设备连接控制信息之前，对终端设备连接控制信息进行加密，之后，再向已部署的连接控制设备发送终端设备连接控制信息。至于具体加密方法，其可采用目前比较成熟的加密算法，这里不再一一限定。当连接控制设备接收到加密的终端设备连接控制信息，则采用加密方法对应的解密方法对加密的终端设备连接控制信息进行解密得到终端设备连接控制信息。之后，依据终端设备连接控制信息确定待进行网络连接控制的目标终端设备并阻断目标终端设备与外部管理中心网络之间的网络连接，具体见下文图5所示流程，这里暂不赘述。

[0102] 作为另一个实现方式，探测设备依据终端设备连接控制信息阻断待进行网络连接控制的目标终端设备与外部管理中心网络之间的网络连接可包括：探测设备主动依据终端设备连接控制信息确定待进行网络连接控制的目标终端设备，并主动阻断待进行网络连接控制的目标终端设备与外部管理中心网络之间的网络连接。在另一个例子中，探测设备主动依据终端设备连接控制信息确定待进行网络连接控制的目标终端设备有很多实现方式，下文会举例描述，这里暂不赘述。一旦探测设备主动依据终端设备连接控制信息确定待进行网络连接控制的目标终端设备，则当探测设备主动阻断目标终端设备与外部管理中心网络之间的网络连接时，探测设备可截获所述目标终端设备与所述外部管理中心网络进行通信时的数据包并丢弃。本实施例中，为保证探测设备截获目标终端设备与外部管理中心网络进行通信时的数据包，可将探测设备串接在网络中、且处于网络中各终端设备与外部管理中心网络进行通信的通信路径上，这样，探测设备即可截获网络中任一目标终端设备与外部管理中心网络进行通信时的数据包并丢弃，达到阻断目标终端设备与外部管理中心网络之间的网络连接的目的。

[0103] 至此，完成图1所示流程。

[0104] 通过图1所示流程可以看出，本实施例中，探测设备通过探测同一网络中的终端设备的连接控制信息，并依据所述终端设备连接控制信息阻断待进行网络连接控制的目标终端设备与外部管理中心网络之间的网络连接，这实现了对终端设备与外部管理中心网络之间的网络连接进行连接控制，提高外部管理中心网络的安全。

[0105] 进一步地，本实施例中，由探测设备通过终端设备反馈的响应包即可确定待进行网络连接控制的目标终端设备比如私接假冒的终端设备等，相比现有通过流量分析目标终端设备(比如私接假冒的终端设备等)，方案实现简单，及时发现异常的终端设备(即上述目标终端设备，比如私接假冒的终端设备等)，且无需流量分析，不会影响流量传输。

[0106] 以探测设备向已部署的连接控制设备发送终端设备连接控制信息为例，通过图2对图1所示流程进行示例描述：

[0107] 参见图2，图2为本申请实施例提供的应用实施例示意图。如图2所示，终端设备网络被划分为两个网络，其中一个为网络1，另一个为网络2。网络1和网络2分别部署了探测设备。网络1中部署的探测设备记为21，网络2中部署的探测设备记为22。

[0108] 在一个例子中，网络1中部署的探测设备21和网络1中各终端设备均连接在网络1的交换机上。同样，网络2中部署的探测设备22和网络2中各终端设备均连接在网络2的交换机上。网络1或网络2中的终端设备可为NVR、摄像头、门禁主机、报警主机等。

[0109] 以网络1为例，网络2类似，则：

[0110] 探测设备21在探测周期到达时向网络1中各终端设备发送组播探测包。网络1中各终端设备属于同一组播组，该组播组的组播地址为该组播数据包的目的地址(也即，该组播组与该组播数据包对应)。基于此，当网络1中任一终端设备接收到组播探测包时，向探测设备21返回响应包。响应包携带发送该响应包的终端设备所对应的终端设备信息，比如图3所示的终端设备信息。

[0111] 探测设备21在本探测周期内接收到任一终端设备发送的响应包时，依据响应包携带的终端设备信息确定对应的终端设备连接控制信息，并在本探测周期结束时，将本探测周期确定的各终端设备连接控制信息发送至已部署的连接控制设备。以连接控制设备部署在网络1与外部管理中心网络之间为例，图4举例示出了探测设备21将终端设备连接控制信息发送至连接控制设备的示意图。

[0112] 最终，实现了网络1中探测设备21将探测到的同一网络中终端设备的连接控制信息发送至连接控制设备。网络2中探测设备22类似，也会将探测到的同一网络中终端设备的连接控制信息发送至连接控制设备。当连接控制设备接收到终端设备的连接控制信息时，其会依据接收的终端设备连接控制信息确定待进行网络连接控制的目标终端设备并阻断目标终端设备与外部管理中心网络之间的网络连接。具体可参见图5所示流程，这里暂不赘述。

[0113] 至此，完成图2所示的实施例描述。

[0114] 作为一个实施例，在上述步骤103或者在图2所示的描述中，上述探测设备依据响应包携带的终端设备信息确定对应的终端设备连接控制信息可包括步骤a：

[0115] 步骤a：探测设备将已接收的响应包携带的终端设备信息确定为对应的终端设备连接控制信息。

[0116] 在一个例子中，当探测设备按照步骤a确定出终端设备连接控制信息后，探测设备可向已部署的连接控制设备发送终端设备连接控制信息，以触发连接控制设备依据所述终端设备连接控制信息确定待进行网络连接控制的目标终端设备并阻断目标终端设备与外部管理中心网络之间的网络连接。至于连接控制设备依据所述终端设备连接控制信息确定待进行网络连接控制的目标终端设备并阻断目标终端设备与外部管理中心网络之间的网络连接具体可见图5所示流程，这里暂不赘述。

[0117] 在另一个例子中，当探测设备按照步骤a确定出终端设备连接控制信息后，探测设备可依据终端设备连接控制信息(也即响应包携带的终端设备信息)确定待进行网络连接控制的目标终端设备，并主动阻断目标终端设备与外部管理中心网络之间的网络连接。这里，依据终端设备连接控制信息(也即响应包携带的终端设备信息)确定待进行网络连接控制的目标终端设备具体可参见下述步骤b。至于探测设备主动阻断目标终端设备与外部管理中心网络之间的网络连接具体见上文描述，这里不再赘述。

[0118] 作为另一个实施例，在上述步骤103或者在图2所示的描述中，上述探测设备依据响应包携带的终端设备信息确定对应的终端设备连接控制信息可包括步骤b：

[0119] 步骤b：依据已接收的响应包携带的终端设备信息确定该终端设备信息对应的终端设备为是否为待进行网络连接控制的目标终端设备，当终端设备信息对应的终端设备为待进行网络连接控制的目标终端设备时，将用于指示该终端设备为待进行网络连接控制的目标终端设备的指示信息确定为对应的终端设备连接控制信息。

[0120] 作为一个实施例,在上述步骤b中,依据已接收的响应包携带的终端设备信息确定该终端设备信息对应的终端设备为是否为待进行网络连接控制的目标终端设备可根据已配置的连接控制策略确定。

[0121] 比如:该连接控制策略要求终端设备信息包括一个参数,该参数比如为IP地址、或MAC地址、或设备版本号等等。需要说明的是,假若该连接控制策略要求终端设备信息包括一个参数,则还需要预先针对各终端设备进行配置,以使各终端设备在返回上述响应包时至少携带连接控制策略要求的参数。在此前提下,基于连接控制策略可确定待进行网络连接控制的目标终端设备,具体为:当所述终端设备信息不在已配置的终端设备信息白名单中,确定所述终端设备信息对应的终端设备为待进行网络连接控制的目标终端设备。这里,连接控制策略,终端设备信息白名单都是预先根据实际需求配置,本实施例并不具体限定。

[0122] 再比如:该连接控制策略要求终端设备信息包括两个以上参数,其中一个参数为终端设备的IP地址。需要说明的是,假若该连接控制策略要求终端设备信息包括两个以上参数(其中一个还包括IP地址),则还需要预先针对各终端设备进行配置,以使各终端设备在返回上述响应包时至少携带连接控制策略要求的参数。在此前提下,基于连接控制策略确定待进行网络连接控制的目标终端设备有很多方式。

[0123] 作为其中一个实现方式,上述确定待进行网络连接控制的目标终端设备可包括:当响应包携带的终端设备信息与已存储的参考终端设备信息(之前已接收的包含上述IP地址的终端设备信息)中有至少一个参数不同(下文会举例描术),则确定终端设备信息对应的终端设备为待进行网络连接控制的目标终端设备。这里,参考终端设备信息为之前已接收的包含所述IP地址的终端设备信息,比如可为该终端设备在注册至探测设备时提交的该终端设备的设备信息(包含上述IP地址),或者也可为探测设备在上一探测周期发送的该终端设备的设备信息(包含上述IP地址)。

[0124] 作为另一个实现方式,上述确定待进行网络连接控制的目标终端设备可包括:当响应包携带的终端设备信息与已存储的参考终端设备信息中有至少一个参数不同且所述IP地址不在已配置的IP白名单时,确定终端设备信息对应的终端设备为待进行网络连接控制的目标终端设备。

[0125] 在上面描述中,响应包携带的终端设备信息与已存储的上述参考终端设备信息中有至少一个参数不同有很多方式。比如,连接控制策略要求终端设备信息包括两个参数,该两个参数分别为:IP地址、MAC地址,基于此,上述响应包携带的终端设备信息与已存储的参考终端设备信息中有至少一个参数不同可为:响应包携带的终端设备信息中的MAC地址与已存储的参考终端设备信息中的MAC地址不同。再比如,连接控制策略要求终端设备信息包括三个参数,该三个参数分别为:IP地址、MAC地址和设备品牌,基于此,上述响应包携带的终端设备信息与已存储的参考终端设备信息中有至少一个参数不同可为:响应包携带的终端设备信息中的MAC地址与已存储的参考终端设备信息中的MAC地址不同,和/或,响应包携带的终端设备信息中的设备品牌与已存储的参考终端设备信息中的设备品牌不同。再比如,连接控制策略要求终端设备信息包括四个参数,该四个参数分别为:IP地址、MAC地址、设备品牌和设备型号,基于此,上述响应包携带的终端设备信息与已存储的参考终端设备信息中有至少一个参数不同可为:响应包携带的终端设备信息中的MAC地址与已存储的参考终端设备信息中的MAC地址不同,和/或,响应包携带的终端设备信息中的设备品牌与已

存储的参考终端设备信息中的设备品牌不同，和/或，响应包携带的终端设备信息中的设备型号与已存储的参考终端设备信息中的设备型号不同。依次类推，这里不再一一举例。

[0126] 作为又一个实现方式，上述确定待进行网络连接控制的目标终端设备可包括：在当前未存储有上述参考终端设备信息，或者，在当前未存储有上述参考终端设备信息且所述IP地址不在已配置的IP白名单时，确定所述终端设备信息对应的终端设备为待进行网络连接控制的终端设备。需要说明的是，上面描述中IP白名单可根据实际需求预先设置。对于IP地址处于上述IP白名单中的终端设备，其与外部管理中心网络的网络连接不需要进行控制。

[0127] 在一个例子中，当探测设备按照步骤b确定出终端设备连接控制信息后，探测设备可向已部署的连接控制设备发送终端设备连接控制信息，以触发连接控制设备依据所述终端设备连接控制信息确定待进行网络连接控制的目标终端设备并阻断目标终端设备与外部管理中心网络之间的网络连接，具体可见图5所示流程，这里暂不赘述。

[0128] 在另一个例子中，当探测设备按照步骤b确定出终端设备连接控制信息后，探测设备可直接将终端设备连接控制信息对应的终端设备确定为待进行网络连接控制的目标终端设备，并主动阻断目标终端设备与外部管理中心网络之间的网络连接。这里探测设备主动阻断目标终端设备与外部管理中心网络之间的网络连接具体见上文描述，这里不再赘述。

[0129] 以上站在探测设备的角度对本实施例提供的连接控制方法进行了描述，下面站在连接控制设备的角度对本实施例提供的连接控制方法进行描述：

[0130] 参见图5，图5为本申请实施例提供的另一连接控制方法流程图。该方法应用于连接控制设备。在本实施例中，连接控制设备是为实现本实施例提供的连接控制方法而新部署于网络中的。在一个例子中，连接控制设备可部署在网络中。每一网络可部署一个连接控制设备。每一网络部署的连接控制设备可执行图5所示流程。在另一个例子中，连接控制设备可部署在网络与外部管理中心网络之间，可执行图5所示流程。

[0131] 如图5所示，该流程可包括以下步骤：

[0132] 步骤501，连接控制设备从已部署的探测设备中获得与所述探测设备处于同一网络中的各终端设备对应的终端设备连接控制信息。

[0133] 作为一个实施例，在上述图1或图2所示流程，探测设备在收到同一网络中的终端设备返回的响应包(用于响应探测设备发送的探测包)时，会依据响应包携带的终端设备信息确定对应的终端设备连接控制信息，并向已部署的连接控制设备发送终端设备连接控制信息。当连接控制设备接收到探测设备发送的终端设备连接控制信息，则意味着实现步骤501中连接控制设备从已部署的探测设备中获得与探测设备处于同一网络中的各终端设备的连接控制信息。

[0134] 作为另一个实施例，即使在上述图1或图2所示流程中，探测设备在确定对应的终端设备连接控制信息后并未向已部署的连接控制设备发送终端设备连接控制信息，此时，连接控制设备也可主动从探测设备获得与探测设备处于同一网络中的各终端设备对应的终端设备连接控制信息，比如连接控制设备向探测设备发送请求，以请求终端设备连接控制信息；探测设备接收到请求时将同一网络中各终端设备的连接控制信息反馈给连接控制设备向探测设备。即实现了步骤501中连接控制设备从已部署的探测设备中获得与探测设

备处于同一网络中的各终端设备的连接控制信息。

[0135] 步骤502,依据已获得的各终端设备的连接控制信息确定待进行网络连接控制的目标终端设备。

[0136] 如上面步骤b描述,终端设备的连接控制信息为用于指示该终端设备为待进行网络连接控制的终端设备的指示信息。基于此,本步骤502中依据已获得的各终端设备的连接控制信息确定待进行网络连接控制的目标终端设备,可包括:将所述指示信息指示的终端设备确定为所述目标终端设备。

[0137] 如上面步骤a描述,终端设备的连接控制信息为终端设备信息。当终端设备的连接控制信息为终端设备信息时,本步骤502中依据已获得的各终端设备的连接控制信息确定待进行网络连接控制的目标终端设备可根据已配置的连接控制策略确定。

[0138] 作为一个实施例,假若连接控制策略要求终端设备信息包括一个参数,该参数比如为IP地址、或MAC地址、或设备版本号等。需要说明的是,假若连接控制策略要求终端设备信息包括一个参数,则还需要预先针对各终端设备进行配置,以使各终端设备在返回上述响应包时至少携带连接控制策略要求的参数。在此前提下,本步骤502中依据已获得的各终端设备的连接控制信息确定待进行网络连接控制的目标终端设备,包括:当终端设备信息不在已配置的终端设备信息白名单中,确定终端设备信息对应的终端设备为所述目标终端设备。

[0139] 作为一个实施例,假若连接控制策略要求终端设备信息包括两个以上参数,其中一个参数为终端设备的IP地址。需要说明的是,假若该连接控制策略要求终端设备信息包括两个以上参数(其中一个还包括IP地址),则还需要预先针对各终端设备进行配置,以使各终端设备在返回上述响应包时至少携带连接控制策略要求的参数。在此前提下,本步骤502中依据已获得的各终端设备的连接控制信息确定待进行网络连接控制的目标终端设备有很多实现方式。

[0140] 作为其中一种实现方式,本步骤502中依据已获得的各终端设备的连接控制信息确定待进行网络连接控制的目标终端设备可包括:

[0141] 针对每一终端设备信息,在未存储有该终端设备信息对应的参考终端设备信息,或者,在未存储有所述参考终端设备信息且该终端设备信息中的IP不在已配置的IP白名单时,确定该终端设备信息对应的终端设备为所述目标终端设备;该终端设备信息与所述参考终端设备信息中的IP地址相同。这里,参考终端设备信息可为最近获得的包含上述终端设备信息中IP地址的其他终端设备信息;或者注册配置中的终端设备信息(包含上述终端设备信息中IP地址)等。

[0142] 作为另一种实现方式,本步骤502中依据已获得的各终端设备的连接控制信息确定待进行网络连接控制的目标终端设备可包括:

[0143] 针对每一终端设备信息,在存储有该终端设备信息对应的参考终端设备信息时,若该终端设备信息与所述参考终端设备信息中有至少一个参数不同,或者,若该终端设备信息与所述参考终端设备信息中有至少一个参数不同且该终端设备信息中的IP不在已配置的IP白名单,则确定该终端设备信息对应的终端设备为所述目标终端设备。

[0144] 在一个例子中,上述终端设备信息与所述参考终端设备信息中有至少一个参数不同有很多方式。比如,假若连接控制策略要求终端设备信息包括两个参数,该两个参数分别

为:IP地址、MAC地址,基于此,上述终端设备信息与已存储的参考终端设备信息中有至少一个参数不同可为:携带的终端设备信息中的MAC地址与已存储的参考终端设备信息中的MAC地址不同。再比如,假若连接控制策略要求终端设备信息包括三个参数,该三个参数分别为:IP地址、MAC地址和设备品牌,基于此,上述终端设备信息与已存储的参考终端设备信息中有至少一个参数不同可为:终端设备信息中的MAC地址与已存储的参考终端设备信息中的MAC地址不同,和/或,终端设备信息中的设备品牌与已存储的参考终端设备信息中的设备品牌不同。再比如,假若连接控制策略要求终端设备信息包括四个参数,该四个参数分别为:IP地址、MAC地址、设备品牌和设备型号,基于此,上述终端设备信息与已存储的参考终端设备信息中有至少一个参数不同可为:终端设备信息中的MAC地址与已存储的参考终端设备信息中的MAC地址不同,和/或,终端设备信息中的设备品牌与已存储的参考终端设备信息中的设备品牌不同,和/或,终端设备信息中的设备型号与已存储的参考终端设备信息中的设备型号不同。其他情况依次类推,这里不再一一举例。

[0145] 至此,完成上述步骤502中如何依据已获得的各终端设备的连接控制信息确定待进行网络连接控制的目标终端设备。需要说明的是,上述只是举例描述如何依据已获得的各终端设备的连接控制信息确定待进行网络连接控制的目标终端设备,并非用于限定。

[0146] 一旦上述步骤502确定出待进行网络连接控制的目标终端设备,则就表示该目标终端设备异常,比如目标终端设备为私接假冒设备等。针对此种情况,执行下述步骤503。

[0147] 步骤503,阻断目标终端设备与所述外部管理中心网络之间的网络连接。

[0148] 作为一个实施例,假若上述连接控制设备旁挂在核心路由器上。这里,核心路由器为连接在网络与外部管理中心网络之间的路由器,比如为处于网络与外部管理中心网络之间的骨干网上的路由器。在此前提下,本步骤503中阻断所述目标终端设备与所述外部管理中心网络之间的网络连接可包括:从所述核心路由器获得所述目标终端设备与所述外部管理中心网络进行通信时的数据包,依据所述数据包生成用于指示所述数据包的目标端不可达的伪造包并向所述核心路由器发送,以通过所述核心路由器向所述数据包的源端发送所述伪造包,所述伪造包用于中断目标终端设备与所述外部管理中心网络之间的网络连接。这里,目标终端设备与外部管理中心网络进行通信时的数据包可为:目标终端设备发向外部管理中心网络的数据包;和/或,外部管理中心网络发向目标终端设备的数据包。在一个例子中,这里的数据包可为协议数据报,比如TCP数据包或者UDP数据包等。以数据包为TCP数据包为例,图6举例示出伪造包为连接复位(RST:Connection reset)包。按照TCP协议,RST包的序列号(sequence number)为数据包携带的sequence number与1之和。

[0149] 需要说明的是,上述之所以依据获得的数据包生成用于指示所述数据包的目标端不可达的伪造包并向所述核心路由器发送,以通过所述核心路由器向所述数据包的源端发送所述伪造包,其原因是:连接控制设备旁挂在核心路由器,而在核心路由器与数据包的源端之间路径是互通的,如果不通过核心路由器向数据包的源端发送上述伪造包,而核心路由器有可能会直接将数据包转发至数据包的目的端,无法达到中断目标终端设备与外部管理中心网络之间的网络连接的目的,基于此,当连接控制设备旁挂在核心路由器时,核心路由器会将目标终端设备与外部管理中心网络进行通信时的数据包镜像至连接控制设备,以由连接控制设备依据获得的数据包生成用于指示数据包的目标端不可达的伪造包并向所述核心路由器发送,以通过所述核心路由器向所述数据包的源端发送所述伪造包。

[0150] 作为另一个实施例，连接控制设备串接在网络与外部管理中心网络之间，其处于网络中各终端设备与外部管理中心网络进行通信的通信路径上。基于此，上述步骤503中阻断所述目标终端设备与所述外部管理中心网络之间的网络连接包括：截获所述目标终端设备与所述外部管理中心网络进行通信时的数据包并丢弃。这里，目标终端设备与外部管理中心网络进行通信时的数据包可为：目标终端设备发向外部管理中心网络的数据包；和/或，外部管理中心网络发向目标终端设备的数据包。在一个例子中，这里的数据包可为协议数据报，比如TCP数据包或者UDP数据包等。因为连接控制设备处于网络中各终端设备与外部管理中心网络进行通信的通信路径上，当接收到目标终端设备与外部管理中心网络进行通信时的数据包，其直接丢弃，这就保证数据包始终无法到达目的地，实现了阻断目标终端设备与外部管理中心网络之间的网络连接的目的。

[0151] 至此，完成图5所示流程。

[0152] 下面以图7所示实施例对图5所示流程进行描述：

[0153] 参见图7，图7为本申请提供的实施例应用示意图。如图7所示，连接控制设备旁挂在核心路由器上。假若根据上述步骤501、步骤502确定图7所示网络1中的终端设备700_a1(IP地址:10.19.10.12)为目标终端设备。比如，终端设备700_a1的MAC地址发生了变化，与之前已存储的包含IP地址10.19.10.12的终端设备信息中的MAC不同，此时可将终端设备700_a1确定为上述目标终端设备。

[0154] 当设备700_a1确定为目标终端设备后，核心路由器会实时监控终端设备700_a1发出的数据包比如TCP数据包，以及实时监控外部管理中心网络发向终端设备700_a1的数据包比如TCP数据包。一旦核心路由器监控到终端设备700_a1发出的数据包比如TCP数据包，或者监控到外部管理中心网络发向终端设备700_a1的数据包比如TCP数据包，其会将监控到的数据包比如TCP数据包镜像至旁挂的连接控制设备。

[0155] 以核心路由器监控到终端设备700_a1发出的数据包比如TCP数据包为例，当连接控制设备接收到核心路由器镜像的数据包(外部管理中心网络发向终端设备700_a1的数据包比如TCP数据包)时，其会根据接收的数据包伪造RST包。RST包的序列号为接收的数据包的序列号与1之和，其表面上相当于用于指示数据包的目标端(外部管理中心网络)返回的数据包。之后，连接控制设备将RST包发送至核心路由器，核心路由器向终端设备700_a1的数据包的源端(终端设备700_a1)发送RST包。当终端设备700_a1接收到RST包，则认为外部管理中心网络不可达，此时终端设备700_a1与外部管理中心网络之间的网络连接就相当于中断。最终实现了阻断目标终端设备与外部管理中心网络之间的网络连接的目的。

[0156] 至此，完成图7所示实施例的描述。

[0157] 下面对本申请实施例提供的系统进行描述：

[0158] 参见图8，图8为本申请实施例提供的系统结构描述。如图8所示，该系统可包括：探测设备和连接控制设备。

[0159] 在一个例子中，探测设备用于执行如图1所示方法执行的步骤；

[0160] 连接控制设备用于执行如图5所示方法执行的步骤。

[0161] 可选地，如图9所示，本申请实施例提供了一种应用于上述探测设备的连接控制装置。如图9所示，该装置可包括：

[0162] 发送单元，用于向同一网络中的终端设备发送探测包；

[0163] 接收单元，用于接收同一网络中的终端设备针对所述探测包返回的响应包；所述响应包携带终端设备信息；

[0164] 连接控制单元，用于依据所述响应包携带的终端设备信息确定对应的终端设备连接控制信息，并依据所述终端设备连接控制信息阻断待进行网络连接控制的目标终端设备与外部管理中心网络之间的网络连接。

[0165] 作为一个实施例，所述发送单元采用以下任一方式向同一网络中的终端设备发送探测包包括：

[0166] 向同一网络中的终端设备发送组播探测包；同一网络中的所有终端设备属于所述组播探测包所对应的组播组；

[0167] 向同一网络中的各终端设备分别发送单播探测包；

[0168] 向同一网络中的各终端设备发送广播探测包。

[0169] 作为一个实施例，所述连接控制单元依据所述终端设备连接控制信息阻断待进行网络连接控制的目标终端设备与外部管理中心网络之间的网络连接包括：

[0170] 向已部署的连接控制设备发送终端设备连接控制信息，以触发所述连接控制设备依据所述终端设备连接控制信息确定待进行网络连接控制的目标终端设备并阻断目标终端设备与外部管理中心网络之间的网络连接。

[0171] 作为一个实施例，所述连接控制单元依据所述响应包携带的终端设备信息确定终端设备对应的终端设备连接控制信息包括：

[0172] 将已接收的所述响应包携带的终端设备信息确定为对应的终端设备连接控制信息；或者，

[0173] 依据已接收的所述响应包携带的终端设备信息确定该终端设备信息对应的终端设备为是否为待进行网络连接控制的目标终端设备，当终端设备信息对应的终端设备为待进行网络连接控制的目标终端设备时，将用于指示该终端设备为待进行网络连接控制的目标终端设备的指示信息确定为对应的终端设备连接控制信息。

[0174] 可选地，所述终端设备信息包括一个参数；作为一个实施例，所述连接控制单元依据已接收的响应包携带的终端设备信息确定该终端设备信息对应的终端设备是否为待进行网络连接控制的目标终端设备包括：针对接收的每一响应包，当该响应包携带的终端设备信息不在已配置的终端设备信息白名单中，确定该响应包携带的终端设备信息所对应的终端设备为待进行网络连接控制的目标终端设备；或者，

[0175] 所述终端设备信息包括两个以上参数，其中一个参数为终端设备的IP地址；所述依据已接收的所述响应包携带的终端设备信息确定该终端设备信息对应的终端设备是否为待进行网络连接控制的目标终端设备包括：

[0176] 针对每一响应包携带的终端设备信息，

[0177] 当已存储该终端设备信息对应的参考终端设备信息时，若该终端设备信息与所述参考终端设备信息中有至少一个参数不同，或者，若该终端设备信息与所述参考终端设备信息中有至少一个参数不同且该终端设备信息中IP地址不在已配置的IP白名单，则确定该终端设备信息对应的终端设备为待进行网络连接控制的目标终端设备；所述参考终端设备信息包含所述IP地址；或者，

[0178] 当未存储有所述参考终端设备信息，或者，当未存储有所述参考终端设备信息且

所述IP地址不在已配置的IP白名单时，确定所述终端设备信息对应的终端设备为待进行网络连接控制的目标终端设备。

[0179] 作为一个实施例，所述探测设备串接在所述网络中、且处于所述网络中各终端设备与外部管理中心网络进行通信的通信路径上；基于此，作为一个实施例，所述连接控制单元阻断所述目标终端设备与所述外部管理中心网络之间的网络连接包括：截获所述目标终端设备与所述外部管理中心网络进行通信时的数据包并丢弃。

[0180] 至此，完成图9所示装置的结构描述。

[0181] 参见图10，图10为本申请实施例提供的应用于连接控制设备的连接控制装置结构图。如图10所示，该装置可包括：

[0182] 获得单元，用于从已部署的探测设备中获得与所述探测设备处于同一网络中的各终端设备对应的终端设备连接控制信息；

[0183] 确定单元，用于依据已获得的终端设备连接控制信息确定待进行网络连接控制的目标终端设备；

[0184] 阻断单元，用于阻断所述目标终端设备与所述外部管理中心网络之间的网络连接。

[0185] 作为一个实施例，所述终端设备连接控制信息为用于指示终端设备为待进行网络连接控制的目标终端设备的指示信息；所述确定单元依据已获得的终端设备连接控制信息确定待进行网络连接控制的目标终端设备，包括：将所述指示信息指示的终端设备确定为所述目标终端设备；或者，

[0186] 所述终端设备连接控制信息为终端设备信息，所述终端设备信息包括一个参数；所述确定单元依据已获得的终端设备连接控制信息确定待进行网络连接控制的目标终端设备，包括：当终端设备信息不在已配置的终端设备信息白名单中，确定终端设备信息对应的终端设备为所述目标终端设备；或者，

[0187] 所述终端设备连接控制信息为终端设备信息，所述终端设备信息包括两个以上参数，其中一个参数为终端设备的IP地址；所述确定单元依据已获得的终端设备连接控制信息确定待进行网络连接控制的目标终端设备，包括：

[0188] 针对每一终端设备信息，在未存储有该终端设备信息对应的参考终端设备信息，或者，在未存储有所述参考终端设备信息且该终端设备信息中的IP不在已配置的IP白名单时，确定该终端设备信息对应的终端设备为所述目标终端设备；该终端设备信息与所述参考终端设备信息中的IP地址相同；或者，

[0189] 针对每一终端设备信息，在存储有该终端设备信息对应的参考终端设备信息时，若该终端设备信息与所述参考终端设备信息中有至少一个参数不同，或者，若该终端设备信息与所述参考终端设备信息中有至少一个参数不同且该终端设备信息中的IP不在已配置的IP白名单，则确定该终端设备信息对应的终端设备为所述目标终端设备。

[0190] 作为一个实施例，所述连接控制设备旁挂在核心路由器上，所述核心路由器为连接在所述网络与外部管理中心网络之间的路由器；所述阻断单元阻断所述目标终端设备与所述外部管理中心网络之间的网络连接包括：从所述核心路由器获得所述目标终端设备与所述外部管理中心网络进行通信时的数据包，依据所述数据包生成用于指示所述数据包的目标端不可达的伪造包并向所述核心路由器发送，以通过所述核心路由器向所述数据包的

源端发送所述伪造包，所述伪造包用于中断目标终端设备与所述外部管理中心网络之间的网络连接；或者，

[0191] 所述连接控制设备串接在所述网络中各终端设备与外部管理中心网络进行通信的通信路径上；所述阻断单元阻断所述目标终端设备与所述外部管理中心网络之间的网络连接包括：截获所述目标终端设备与所述外部管理中心网络进行通信时的数据包并丢弃。

[0192] 至此，完成图10所示的装置结构图。

[0193] 本申请实施例还提供了图9或图10所示装置的硬件结构。参见图11，图11为本申请实施例提供的电子设备结构图。如图11所示，该硬件结构可包括：处理器和机器可读存储介质，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；所述处理器用于执行机器可执行指令，以实现本申请上述示例公开的方法。

[0194] 基于与上述方法同样的申请构思，本申请实施例还提供一种机器可读存储介质，所述机器可读存储介质上存储有若干计算机指令，所述计算机指令被处理器执行时，能够实现本申请上述示例公开的方法。

[0195] 示例性的，上述机器可读存储介质可以是任何电子、磁性、光学或其它物理存储装置，可以包含或存储信息，如可执行指令、数据，等等。例如，机器可读存储介质可以是：RAM(Radom Access Memory，随机存取存储器)、易失存储器、非易失性存储器、闪存、存储驱动器(如硬盘驱动器)、固态硬盘、任何类型的存储盘(如光盘、dvd等)，或者类似的存储介质，或者它们的组合。

[0196] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机，计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[0197] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[0198] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请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，本申请实施例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。

[0199] 本申请是参照根据本申请实施例的方法、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。应理解可以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、嵌入式处理机或其它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它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。

[0200] 而且，这些计算机程序指令也可以存储在能引导计算机或其它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者多个流程和/或方框图一个方框或者多个方框中指定的功能。

[0201] 这些计算机程序指令也可装载到计算机或其它可编程数据处理设备上，使得在计算机或者其它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，从而在计算机或其它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。

[0202] 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理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权利要求范围之内。

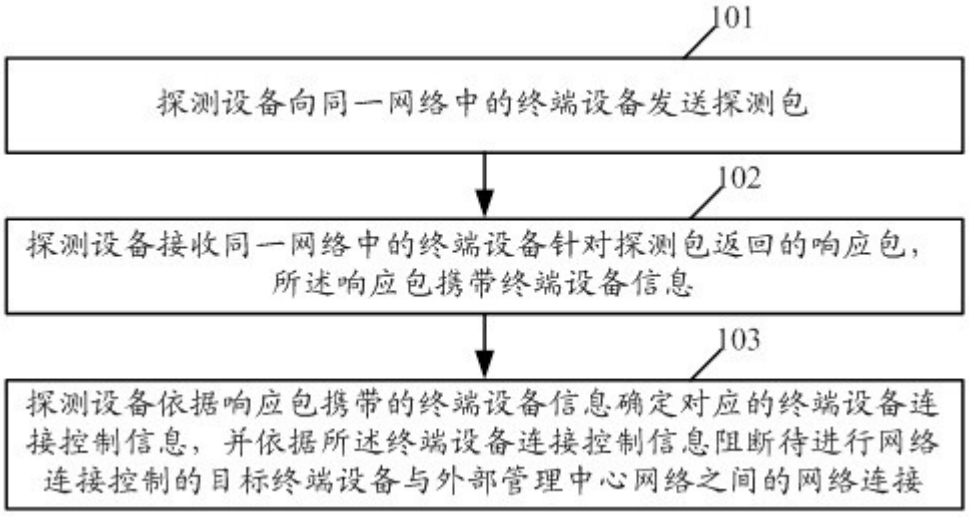

101
探测设备向同一网络中的终端设备发送探测包
102
探测设备接收同一网络中的终端设备针对探测包返回的响应包，所述响应包携带终端设备信息
103
探测设备依据响应包携带的终端设备信息确定对应的终端设备连接控制信息，并依据所述终端设备连接控制信息阻断待进行网络连接控制的目标终端设备与外部管理中心网络之间的网络连接

图1

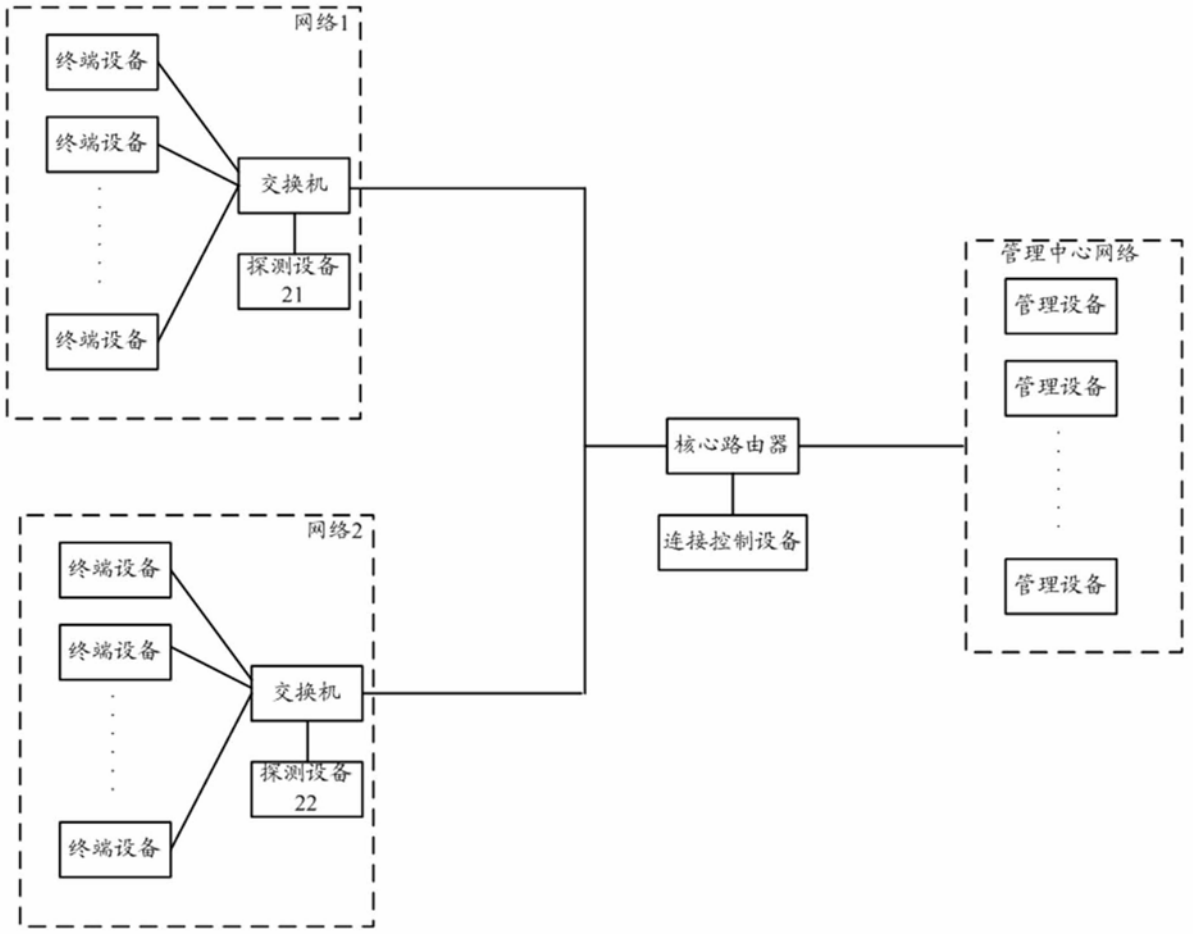

网络1
终端设备
终端设备
终端设备
交换机
探测设备21
网络2
终端设备
终端设备
终端设备
交换机
探测设备22
核心路由器
连接控制设备
管理中心网络
管理设备
管理设备
管理设备

图2

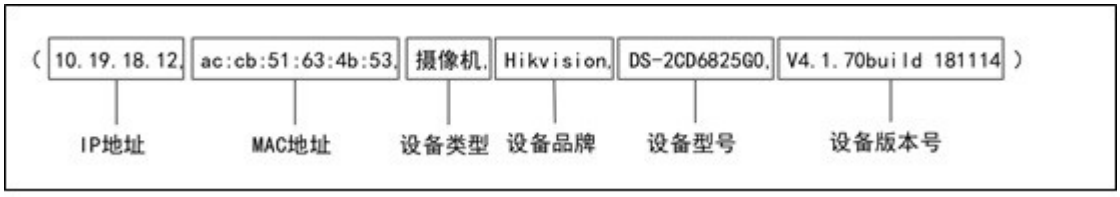

(
10.19.18.12,
ac:cb:51:63:4b:53,
摄像机,
Hikvision,
DS-2CD6825G0,
V4.1.70build 181114
)
IP地址
MAC地址
设备类型
设备品牌
设备型号
设备版本号

图3

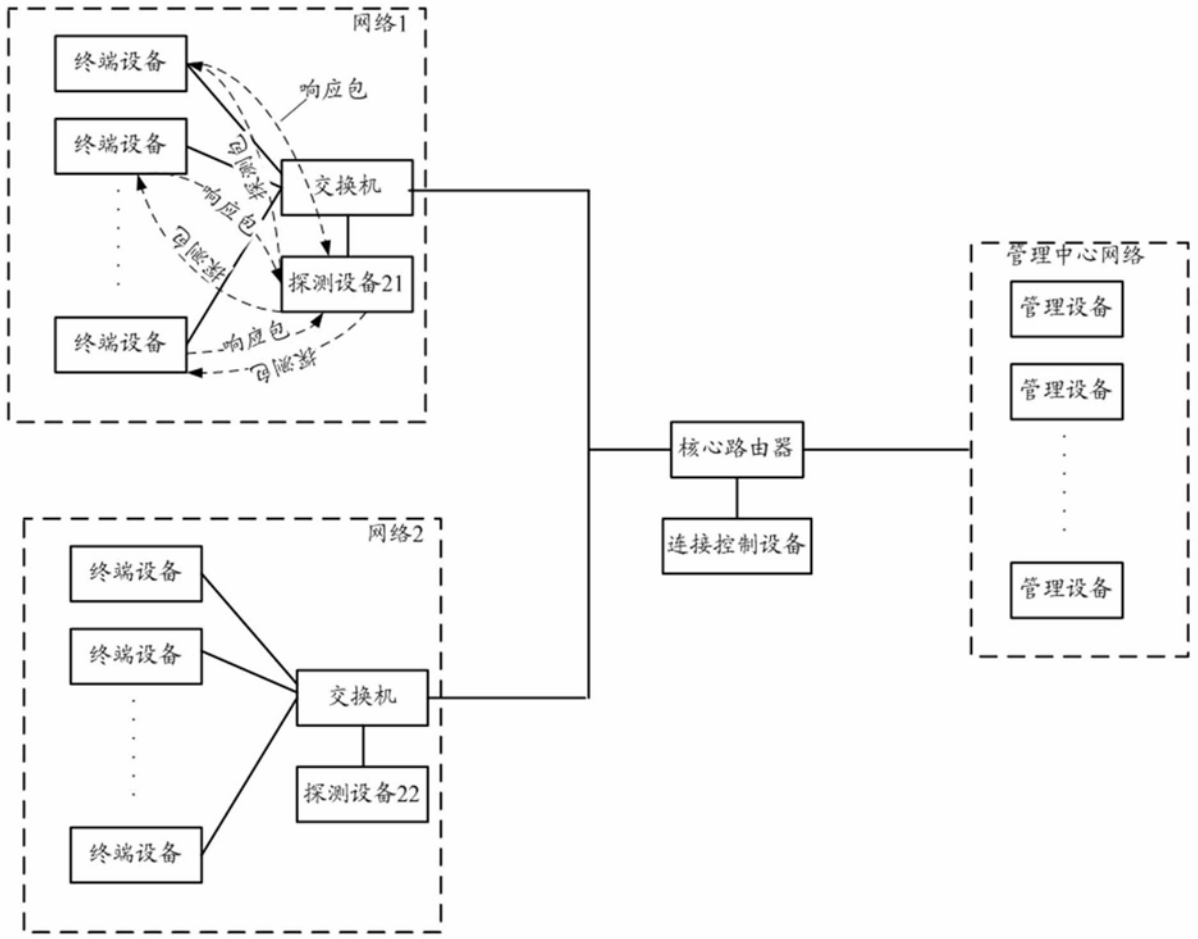

网络1
终端设备
终端设备
终端设备
响应包
探测包
响应包
探测包
交换机
探测设备21
响应包
探测包
网络2
终端设备
终端设备
终端设备
交换机
探测设备22
核心路由器
连接控制设备
管理中心网络
管理设备
管理设备
管理设备

图4

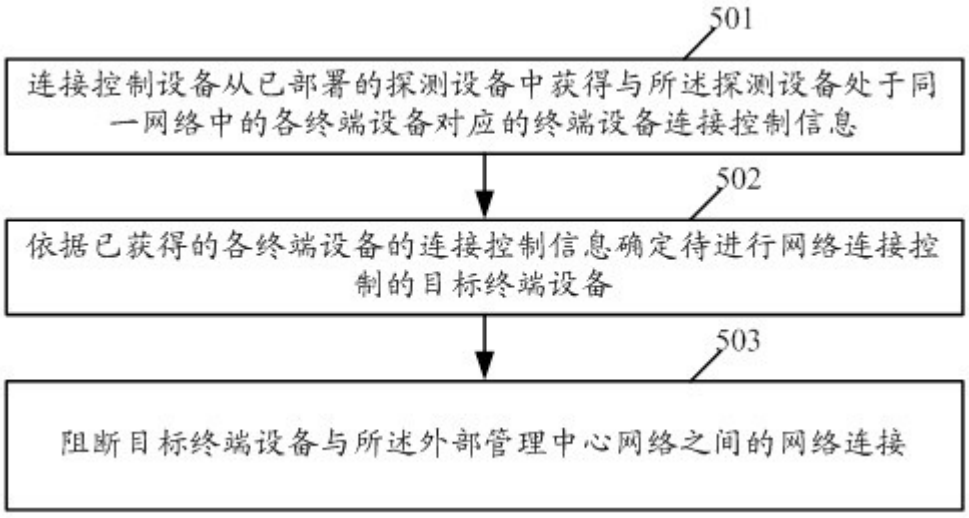

501
连接控制设备从已部署的探测设备中获得与所述探测设备处于同一网络中的各终端设备对应的终端设备连接控制信息
502
依据已获得的各终端设备的连接控制信息确定待进行网络连接控制的目标终端设备
503
阻断目标终端设备与所述外部管理中心网络之间的网络连接

图5

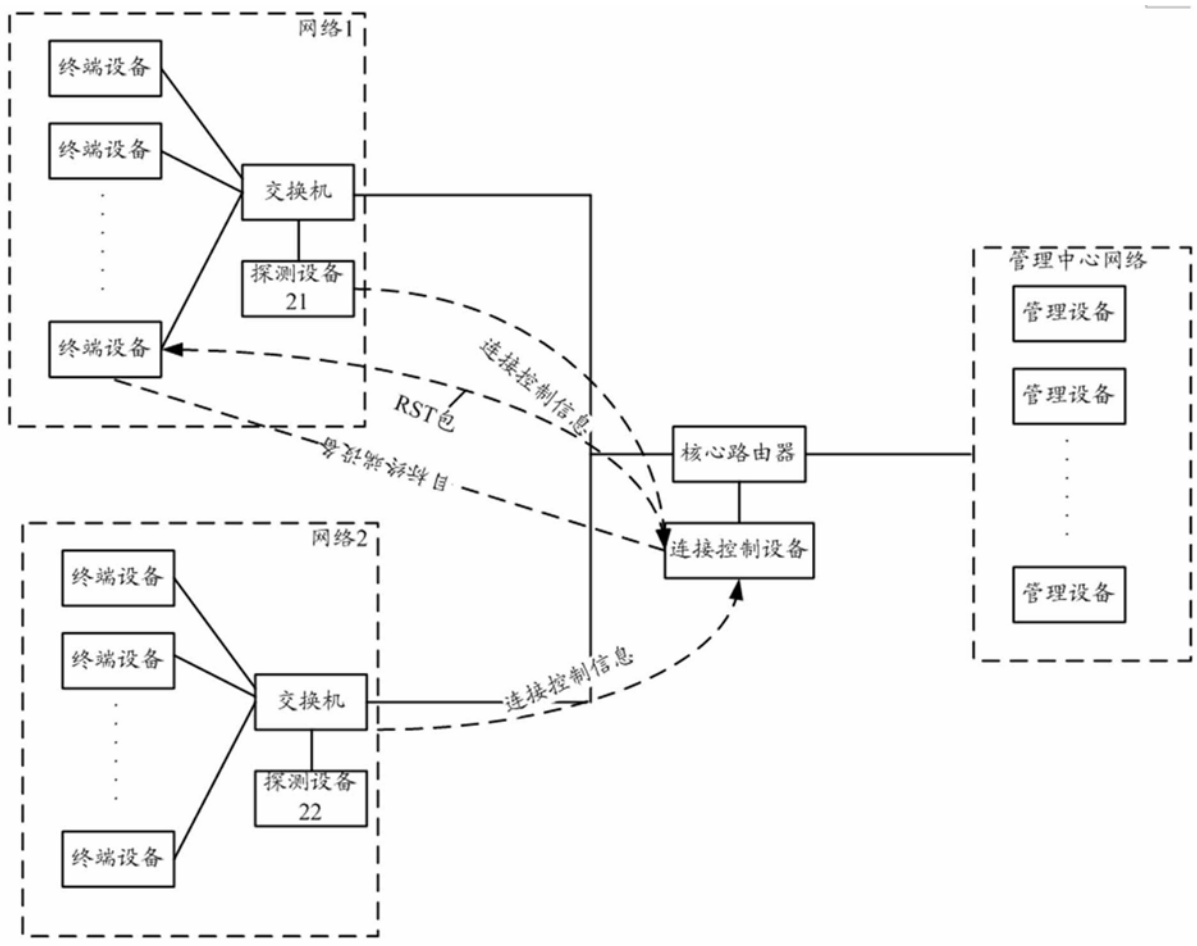

网络1
终端设备
终端设备
交换机
探测设备21
终端设备
RST包
连接控制信息
目标终端设备
核心路由器
管理中心网络
管理设备
管理设备
管理设备
连接控制设备
网络2
终端设备
终端设备
交换机
连接控制信息
探测设备22
终端设备

图6

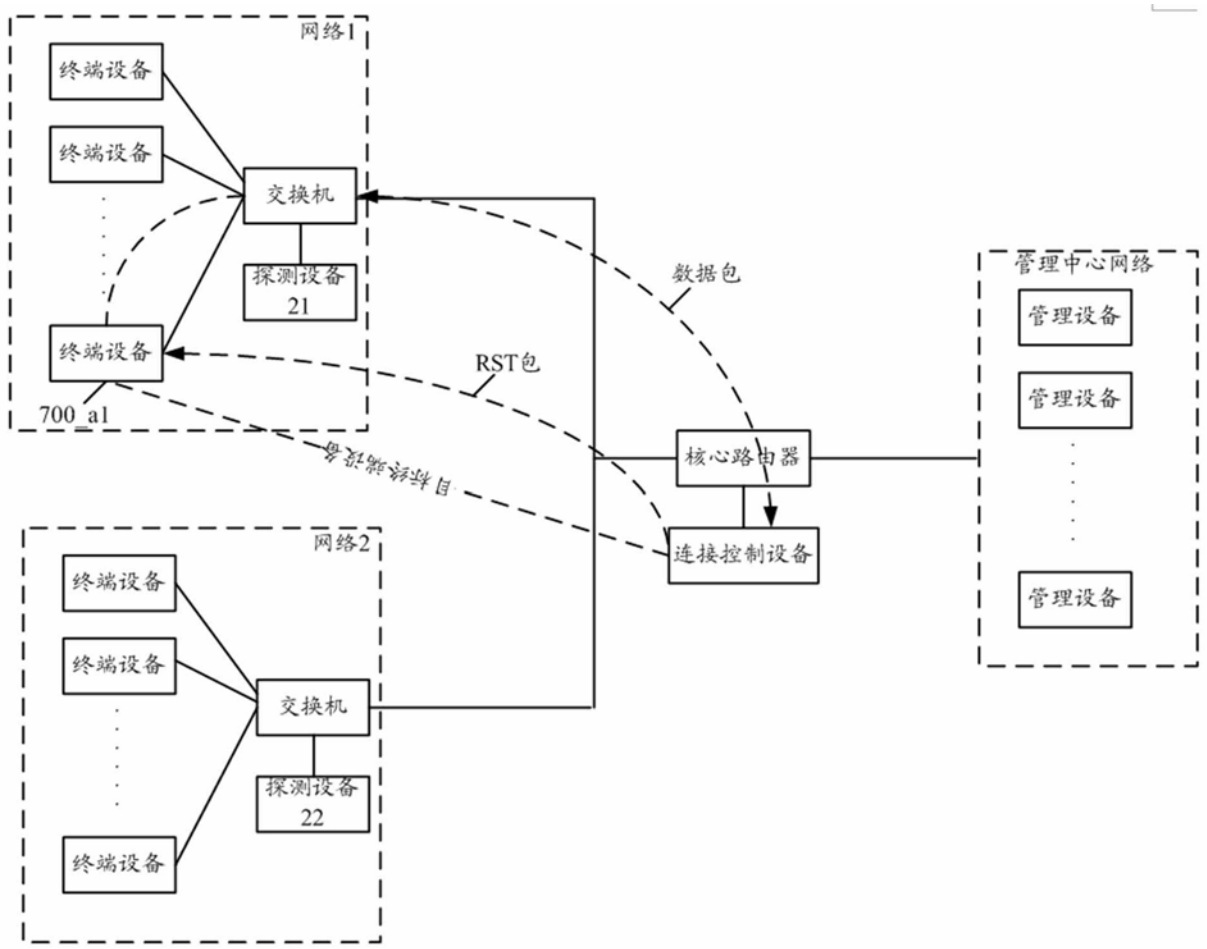

网络1
终端设备
终端设备
交换机
探测设备
21
终端设备
700_a1
数据包
RST包
目标终端设备
核心路由器
连接控制设备
管理中心网络
管理设备
管理设备
管理设备
网络2
终端设备
终端设备
交换机
探测设备
22
终端设备

图7

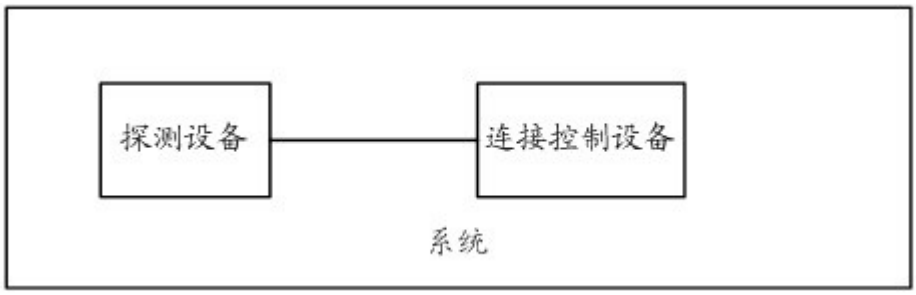

探测设备
连接控制设备
系统

图8

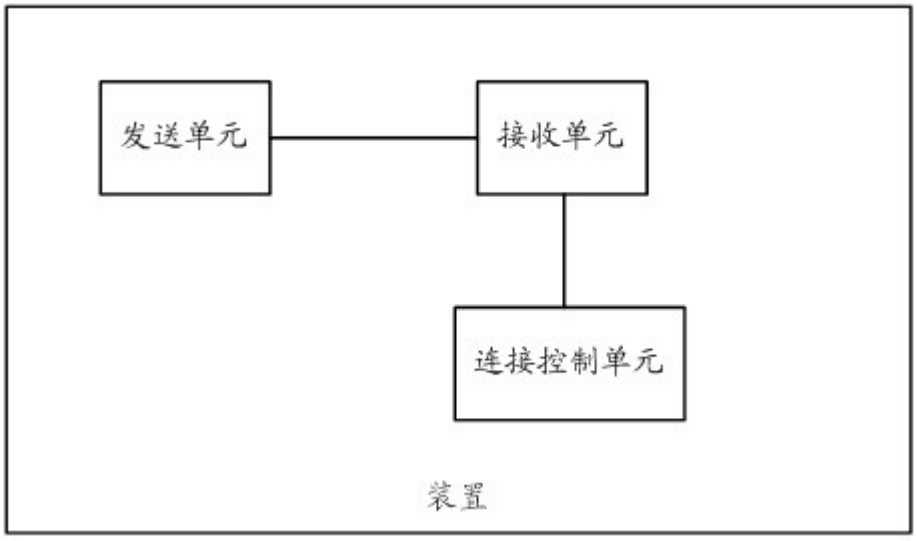


图9

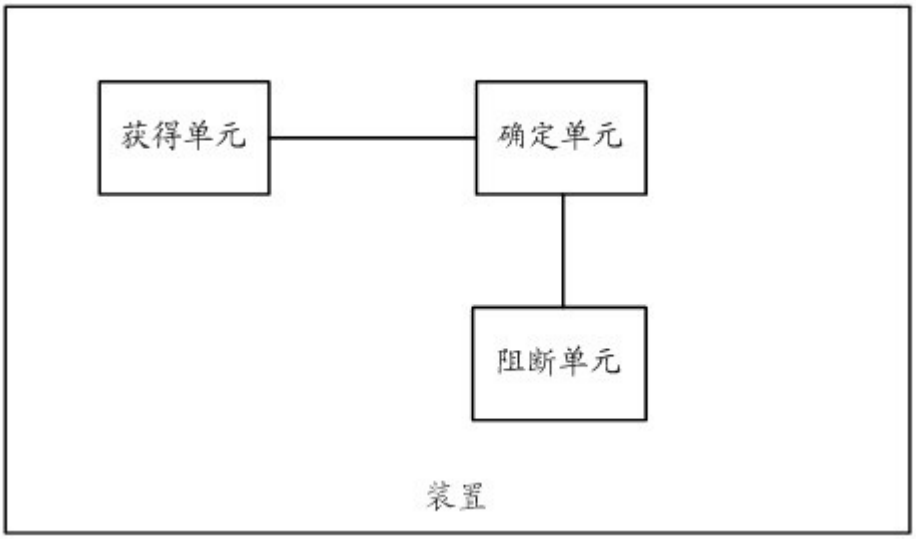


图10

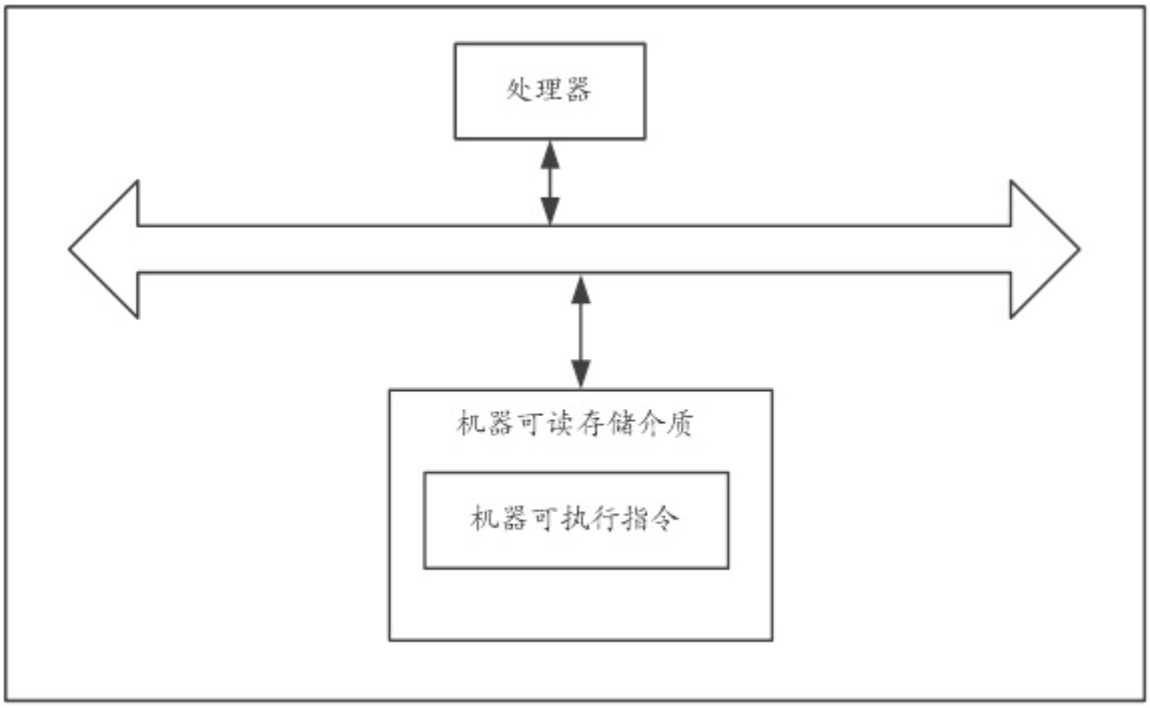


图11