(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115296878 B
(45)授权公告日 2023.11.03

(21)申请号 202210891395.3
(22)申请日 2022.07.27
(65)同一申请的已公布的文献号
申请公布号 CN 115296878 A
(43)申请公布日 2022.11.04
(73)专利权人 天翼云科技有限公司
地址 100007 北京市东城区青龙胡同甲1号、3号2幢2层205-32室
(72)发明人 吴静勇 向祖庭 唐荣生 韩旺 兰培挺 王晓华
(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
专利代理师 朱琳爱义
(51)Int.Cl.
H04L 9/40(2022.01)
(56)对比文件
CN 103475653 A,2013.12.25
CN 104954346 A,2015.09.30
CN 110971601 A,2020.04.07
CN 111355696 A,2020.06.30
CN 111526134 A,2020.08.11
CN 112351002 A,2021.02.09
CN 112989337 A,2021.06.18
CN 112994931 A,2021.06.18
CN 113194058 A,2021.07.30
CN 113381993 A,2021.09.10
CN 114050926 A,2022.02.15
CN 114285624 A,2022.04.05
CN 114553546 A,2022.05.27
CN 1980240 A,2007.06.13
US 8291495 B1,2012.10.16
WO 2022088779 A1,2022.05.05
陈训逊,方滨兴,李蕾.高速网络环境下入侵检测系统结构研究.计算机研究与发展.2004,(第09期),全文.
耿风瑞;高仲合;李红伟.防火墙流过滤技术的分析与研究.计算机安全.2009,(第02期),全文.
(续)
审查员 王务鹏

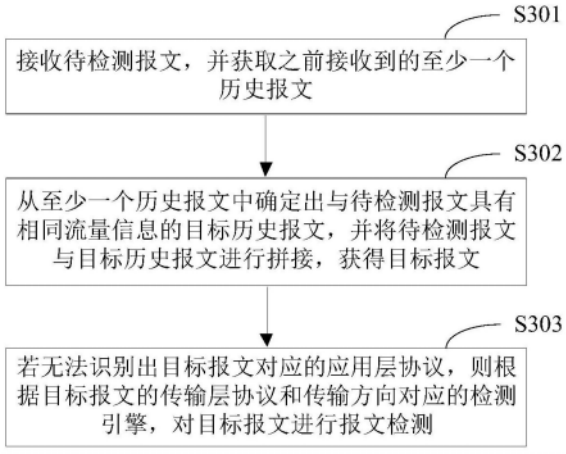
权利要求书2页 说明书14页 附图6页

(54)发明名称

一种报文检测方法、装置、电子设备及存储介质

(57)摘要

本申请提供一种报文检测方法、装置、电子设备及存储介质,涉及网络安全技术领域。在接收待检测报文,并获取之前接收到的至少一个历史报文之后,可以从至少一个历史报文中确定出与待检测报文具有相同流量信息的目标历史报文,并将待检测报文与目标历史报文进行拼接,获得目标报文,若无法识别出目标报文对应的应用层协议,则根据目标报文的传输层协议和传输方向对应的检测引擎,对目标报文进行报文检测。由于在对报文进行检测前,可以将报文与之前接收到的具有相同流量信息的报文进行拼接后再进行检测,从而可以解决恶意流量特征被拆分到多个报文中而绕过防火墙的问题,提高对报文进行检测的准确率。



CN 115296878 B

[转续页]

[接上页]

(56)对比文件

田立勤,林闯.报文分类技术的研究及其应用.计算机研究与发展.2003,(第06期),全文.

陈训逊,方滨兴,李蕾.高速网络环境下入侵检测系统结构研究.计算机研究与发展.2004,(第09期),全文.

耿风瑞;高仲合;李红伟.防火墙流过滤技术的分析与研究.计算机安全.2009,(第02期),全文.

田立勤,林闯.报文分类技术的研究及其应用.计算机研究与发展.2003,(第06期),全文.

1.一种报文检测方法,其特征在于,包括:

接收待检测报文,并获取之前接收到的至少一个历史报文;

从所述至少一个历史报文中确定出与所述待检测报文具有相同流量信息的目标历史报文,并将所述待检测报文与所述目标历史报文进行拼接,获得目标报文;

若无法识别出所述目标报文对应的应用层协议,则根据所述目标报文的传输层协议和传输方向对应的检测引擎,对所述目标报文进行报文检测;

所述根据所述目标报文的传输层协议和传输方向对应的检测引擎,对所述目标报文进行报文检测,包括:

获取所述目标报文的传输层协议和传输方向对应的检测引擎下的至少一个恶意传输规则,其中每个恶意传输规则包括多个恶意传输特征;

对于每个恶意传输规则,从所述多个恶意传输特征中确定一个恶意传输特征作为第一恶意传输特征;

根据每个恶意传输规则的第一恶意传输特征对所述目标报文进行检测,确定所述目标报文相对于每个恶意传输规则的初始检测结果;

若基于所述初始检测结果确定所述目标报文初步符合至少一个目标恶意传输规则,则对于每个目标恶意传输规则,将所述目标恶意传输规则中除所述第一恶意传输特征之外的其他恶意传输特征,分别与所述目标报文进行匹配;

若所述其他恶意传输特征与所述目标报文均匹配成功,则确定所述目标报文对应的目标检测结果为恶意报文;

若每个目标恶意传输规则对应的所述其他恶意传输特征中都有与所述目标报文匹配失败的其他恶意传输特征,则确定所述目标报文对应的目标检测结果为正常报文。

2.如权利要求1所述的方法,其特征在于,所述根据每个恶意传输规则的第一恶意传输特征对所述目标报文进行检测,确定所述目标报文相对于每个恶意传输规则的初始检测结果,包括:

基于AC状态机对所述目标报文进行匹配检测,确定每个第一恶意传输特征与所述目标报文的匹配结果;所述AC状态机是通过多模式匹配AC算法,根据每个恶意传输规则的第一恶意传输特征生成的;

若每个第一恶意传输特征与所述目标报文均匹配失败,则确定所述目标报文相对于每个恶意传输规则的初始检测结果为正常报文;

若至少一个所述第一恶意传输特征与所述目标报文匹配成功,则确定与所述目标报文匹配的所述第一恶意传输特征对应的目标恶意传输规则,并确定所述目标报文相对于每个目标恶意传输规则的初始检测结果为初步符合所述目标恶意传输规则。

3.如权利要求2所述的方法,其特征在于,所述基于AC状态机对所述目标报文进行匹配检测,确定每个第一恶意传输特征与所述目标报文的匹配结果,包括:

获取通过AC状态机对所述目标历史报文进行检测获得的结束状态和已检测字节数;

基于所述AC状态机,根据所述已检测字节数确定所述目标报文对应的待检测字符串中的未检测起始位置,并根据所述结束状态从所述未检测起始位置处对所述待检测字符串进行查找,从所述第一恶意传输特征对应的字符串中,确定出与所述待检测字符串相匹配的目标字符串;

根据所述目标字符串对应的目标恶意传输特征，确定每个第一恶意传输特征与所述目标报文的匹配结果。

4.如权利要求1~3中任一项所述的方法，其特征在于，所述获得目标报文之后，所述方法还包括：

若识别出所述目标报文对应的应用层协议，则获取所述应用层协议对应的检测引擎下的至少一个恶意应用规则；

根据所述至少一个恶意应用规则中包括的多个恶意应用特征，对所述目标报文进行检测，确定所述目标报文是否为恶意报文。

5.一种报文检测装置，其特征在于，包括：

报文接收单元，用于接收待检测报文，并获取之前接收到的至少一个历史报文；

报文拼接单元，用于从所述至少一个历史报文中确定出与所述待检测报文具有相同流量信息的目标历史报文，并将所述待检测报文与所述目标历史报文进行拼接，获得目标报文；

报文检测单元，用于若无法识别出所述目标报文对应的应用层协议，则根据所述目标报文的传输层协议和传输方向对应的检测引擎，对所述目标报文进行报文检测；

所述报文检测单元，具体用于：

获取所述目标报文的传输层协议和传输方向对应的检测引擎下的至少一个恶意传输规则，其中每个恶意传输规则包括多个恶意传输特征；

对于每个恶意传输规则，从所述多个恶意传输特征中确定一个恶意传输特征作为第一恶意传输特征；

根据每个恶意传输规则的第一恶意传输特征对所述目标报文进行检测，确定所述目标报文相对于每个恶意传输规则的初始检测结果；

若基于所述初始检测结果确定所述目标报文初步符合至少一个目标恶意传输规则，则对于每个目标恶意传输规则，将所述目标恶意传输规则中除所述第一恶意传输特征之外的其他恶意传输特征，分别与所述目标报文进行匹配；

若所述其他恶意传输特征与所述目标报文均匹配成功，则确定所述目标报文对应的目标检测结果为恶意报文；

若每个目标恶意传输规则对应的所述其他恶意传输特征中都有与所述目标报文匹配失败的其他恶意传输特征，则确定所述目标报文对应的目标检测结果为正常报文。

6.一种电子设备，其特征在于，其包括处理器和存储器，其中，所述存储器存储有程序代码，当所述程序代码被所述处理器执行时，使得所述处理器执行权利要求1~4中任一所述方法的步骤。

7.一种计算机可读存储介质，其特征在于，其包括程序代码，当所述程序代码在电子设备上运行时，所述程序代码用于使所述电子设备执行权利要求1~4中任一所述方法的步骤。

一种报文检测方法、装置、电子设备及存储介质

技术领域

[0001] 本申请实施例涉及网络安全技术领域，尤其涉及一种报文检测方法、装置、电子设备及存储介质。

背景技术

[0002] 互联网中的恶意流量泛滥，攻击手段层出不穷，时刻威胁着网络中的用户。常见的防火墙报文检测的基本原理是先将已有的特征库按照应用层协议分类，然后分别构建检测引擎，当收到待检测报文时，识别待检测报文的应用层协议，并进入相应的检测引擎对待检测报文进行特征匹配，如果匹配，则确定待检测报文是恶意报文，否则，确定待检测不是恶意报文。

[0003] 为了躲避防火墙的检测，恶意流量的制造者会使用多种手段进行隐藏，比如自定义一些私有应用层协议，同时对带有特征的报文进行拆包，拆分成若干个长度随机的小包，使得单个报文中不再具有完整的特征。当这些恶意报文到达防火墙后，防火墙无法识别出应用层协议，只能根据传输层协议做报文检测，而报文经过拆分后，单个报文已经不具备恶意流量的特征，因此会被防火墙认为是正常报文而放过。

发明内容

[0004] 为解决现有存在的技术问题，本申请实施例提供了一种报文检测方法、装置、电子设备及存储介质，可以解决恶意流量特征被拆分到多个报文中而绕过防火墙的问题，提高对恶意报文的检测准确率。

[0005] 为达到上述目的，本申请实施例的技术方案是这样实现的：

[0006] 第一方面，本申请实施例提供一种报文检测方法，包括：

[0007] 接收待检测报文，并获取之前接收到的至少一个历史报文；

[0008] 从所述至少一个历史报文中确定出与所述待检测报文具有相同流量信息的目标历史报文，并将所述待检测报文与所述目标历史报文进行拼接，获得目标报文；

[0009] 若无法识别出所述目标报文对应的应用层协议，则根据所述目标报文的传输层协议和传输方向对应的检测引擎，对所述目标报文进行报文检测。

[0010] 本申请实施例提供的报文检测方法，在接收待检测报文，并获取之前接收到的至少一个历史报文之后，可以从至少一个历史报文中确定出与待检测报文具有相同流量信息的目标历史报文，并将待检测报文与目标历史报文进行拼接，获得目标报文，若无法识别出目标报文对应的应用层协议，则根据目标报文的传输层协议和传输方向对应的检测引擎，对目标报文进行报文检测。由于在接收到待检测报文后，先将待检测报文与之前接收到的具有相同流量信息的报文进行拼接，再对拼接后的报文进行报文检测，从而可以解决恶意流量特征被拆分到多个报文中而绕过防火墙的问题，提高对报文进行检测的准确率，同时，在无法识别出报文对应的应用层协议时，可以根据报文的传输层协议和传输方向对应的检测引擎对报文进行检测，提高对报文进行检测的检测速度，并进一步提高检测准确率。

[0011] 在一种可选的实施例中，所述根据所述目标报文的传输层协议和传输方向对应的检测引擎，对所述目标报文进行报文检测，包括：

[0012] 获取所述目标报文的传输层协议和传输方向对应的检测引擎下的至少一个恶意传输规则，其中每个恶意传输规则包括多个恶意传输特征；

[0013] 对于每个恶意传输规则，从所述多个恶意传输特征中确定一个恶意传输特征作为第一恶意传输特征；

[0014] 根据每个恶意传输规则的第一恶意传输特征对所述目标报文进行检测，确定所述目标报文相对于每个恶意传输规则的初始检测结果；

[0015] 若基于所述初始检测结果确定所述目标报文初步符合至少一个目标恶意传输规则，则根据每个目标恶意传输规则中除所述第一恶意传输特征之外的其他恶意传输特征，对所述目标报文进行检测，确定所述目标报文相对于每个目标恶意传输规则的目标检测结果。

[0016] 在该实施例中，可以获取目标报文的传输层协议和传输方向对应的检测引擎下的至少一个恶意传输规则，对于每个恶意传输规则，从多个恶意传输特征中确定一个恶意传输特征作为第一恶意传输特征，并根据每个恶意传输规则的第一恶意传输特征对目标报文进行检测，确定目标报文相对于每个恶意传输规则的初始检测结果，若基于初始检测结果确定目标报文初步符合至少一个目标恶意传输规则，则根据每个目标恶意传输规则中除第一恶意传输特征之外的其他恶意传输特征，对目标报文进行检测，确定目标报文相对于每个目标恶意传输规则的目标检测结果。由于在通过传输层协议和传输方向对应的检测引擎，对目标报文进行报文检测时，是先通过该检测引擎下包括的每个恶意传输规则中的一个恶意传输特征对目标报文进行检测，确定目标报文是否初步符合一个或多个恶意传输规则，且在确定目标报文初步符合恶意传输规则后，再通过该恶意传输规则中的其他恶意传输特征对目标报文进行进一步检测，从而可以提高对报文进行检测的检测速度和检测准确率。

[0017] 在一种可选的实施例中，所述根据每个恶意传输规则的第一恶意传输特征对所述目标报文进行检测，确定所述目标报文相对于每个恶意传输规则的初始检测结果，包括：

[0018] 基于AC状态机对所述目标报文进行匹配检测，确定每个第一恶意传输特征与所述目标报文的匹配结果；所述AC状态机是通过多模式匹配AC算法，根据每个恶意传输规则的第一恶意传输特征生成的；

[0019] 若每个第一恶意传输特征与所述目标报文均匹配失败，则确定所述目标报文相对于每个恶意传输规则的初始检测结果为正常报文；

[0020] 若至少一个所述第一恶意传输特征与所述目标报文匹配成功，则确定与所述目标报文匹配的所述第一恶意传输特征对应的目标恶意传输规则，并确定所述目标报文相对于每个目标恶意传输规则的初始检测结果为初步符合所述目标恶意传输规则。

[0021] 在该实施例中，可以先获取通过多模式匹配AC算法，根据每个恶意传输规则的第一恶意传输特征生成的AC状态机，然后基于生成的AC状态机对目标报文进行匹配检测，确定每个第一恶意传输特征与目标报文的匹配结果，若每个第一恶意传输特征与目标报文均匹配失败，则确定目标报文相对于每个恶意传输规则的初始检测结果为正常报文，若至少一个第一恶意传输特征与目标报文匹配成功，则确定与目标报文匹配的第一恶意传输特征

对应的目标恶意传输规则，并确定目标报文相对于每个目标恶意传输规则的初始检测结果为初步符合目标恶意传输规则。由于在通过恶意传输规则中的一个恶意传输特征对目标报文进行检测时，可以通过根据每个恶意传输规则中的一个恶意传输特征构建生成的AC状态机对目标报文进行检测，从而可以提高对报文进行检测的检测速度，以及根据准确检测出的目标报文所匹配的恶意传输特征，进而确定目标报文为正常报文或初步符合恶意传输规则。

[0022] 在一种可选的实施例中，所述基于AC状态机对所述目标报文进行匹配检测，确定每个第一恶意传输特征与所述目标报文的匹配结果，包括：

[0023] 获取通过AC状态机对所述目标历史报文进行检测获得的结束状态和已检测字节数；

[0024] 基于所述AC状态机，根据所述已检测字节数确定所述目标报文对应的待检测字符串中的未检测起始位置，并根据所述结束状态从所述未检测起始位置处对所述待检测字符串进行查找，从所述第一恶意传输特征对应的字符串中，确定出与所述待检测字符串相匹配的目标字符串；

[0025] 根据所述目标字符串对应的目标恶意传输特征，确定每个第一恶意传输特征与所述目标报文的匹配结果。

[0026] 在该实施例中，可以获取通过AC状态机对目标历史报文进行检测获得的结束状态和已检测字节数，基于AC状态机，根据已检测字节数确定目标报文对应的待检测字符串中的未检测起始位置，并根据结束状态从未检测起始位置处对待检测字符串进行查找，从第一恶意传输特征对应的字符串中，确定出与待检测字符串相匹配的目标字符串，根据目标字符串对应的目标恶意传输特征，确定每个第一恶意传输特征与目标报文的匹配结果。由于在通过AC状态机对目标报文进行检测时，可以同时将上次对历史报文进行检测获得的结束状态和已检测字节数一起输入到AC状态机中，从而可以避免对目标报文进行重复检测，提高对报文进行检测的检测速度和检测性能。

[0027] 在一种可选的实施例中，所述根据每个目标恶意传输规则中除所述第一恶意传输特征之外的其他恶意传输特征，对所述目标报文进行检测，确定所述目标报文相对于每个目标恶意传输规则的目标检测结果，包括：

[0028] 对于每个目标恶意传输规则，将所述目标恶意传输规则中除所述第一恶意传输特征之外的其他恶意传输特征，分别与所述目标报文进行匹配；

[0029] 若所述其他恶意传输特征与所述目标报文均匹配成功，则确定所述目标报文对应的目标检测结果为恶意报文；

[0030] 若每个目标恶意传输规则对应的所述其他恶意传输特征中都有与所述目标报文匹配失败的其他恶意传输特征，则确定所述目标报文对应的目标检测结果为正常报文。

[0031] 在该实施例中，对于每个目标恶意传输规则，将目标恶意传输规则中除第一恶意传输特征之外的其他恶意传输特征，分别与目标报文进行匹配，若其他恶意传输特征与目标报文均匹配成功，则确定目标报文对应的目标检测结果为恶意报文，若每个目标恶意传输规则对应的其他恶意传输特征中都有与目标报文匹配失败的其他恶意传输特征，则确定目标报文对应的目标检测结果为正常报文。由于在确定目标报文初步符合目标恶意传输规则后，还需要根据目标恶意传输规则中的其他恶意传输特征对目标报文进行检测，以确定

目标报文是否为恶意报文，从而可以提高对报文进行检测的准确率。

[0032] 在一种可选的实施例中，所述获得目标报文之后，所述方法还包括：

[0033] 若识别出所述目标报文对应的应用层协议，则获取所述应用层协议对应的检测引擎下的至少一个恶意应用规则；

[0034] 根据所述至少一个恶意应用规则中包括的多个恶意应用特征，对所述目标报文进行检测，确定所述目标报文是否为恶意报文。

[0035] 在该实施例中，若识别出目标报文对应的应用层协议，则获取应用层协议对应的检测引擎下的至少一个恶意应用规则，并根据至少一个恶意应用规则中包括的多个恶意应用特征，对目标报文进行检测，确定目标报文是否为恶意报文。由于在识别出目标报文对应的应用层协议时，可以根据该应用层协议下的恶意应用规则对目标报文进行报文检测，从而可以提高对报文进行检测的检测准确率。

[0036] 第二方面，本申请实施例还提供了一种报文检测装置，包括：

[0037] 报文接收单元，用于接收待检测报文，并获取之前接收到的至少一个历史报文；

[0038] 报文拼接单元，用于从所述至少一个历史报文中确定出与所述待检测报文具有相同流量信息的目标历史报文，并将所述待检测报文与所述目标历史报文进行拼接，获得目标报文；

[0039] 报文检测单元，用于若无法识别出所述目标报文对应的应用层协议，则根据所述目标报文的传输层协议和传输方向对应的检测引擎，对所述目标报文进行报文检测。

[0040] 在一种可选的实施例中，所述报文检测单元，具体用于：

[0041] 获取所述目标报文的传输层协议和传输方向对应的检测引擎下的至少一个恶意传输规则，其中每个恶意传输规则包括多个恶意传输特征；

[0042] 对于每个恶意传输规则，从所述多个恶意传输特征中确定一个恶意传输特征作为第一恶意传输特征；

[0043] 根据每个恶意传输规则的第一恶意传输特征对所述目标报文进行检测，确定所述目标报文相对于每个恶意传输规则的初始检测结果；

[0044] 若基于所述初始检测结果确定所述目标报文初步符合至少一个目标恶意传输规则，则根据每个目标恶意传输规则中除所述第一恶意传输特征之外的其他恶意传输特征，对所述目标报文进行检测，确定所述目标报文相对于每个目标恶意传输规则的目标检测结果。

[0045] 在一种可选的实施例中，所述报文检测单元，还用于：

[0046] 基于AC状态机对所述目标报文进行匹配检测，确定每个第一恶意传输特征与所述目标报文的匹配结果；所述AC状态机是通过多模式匹配AC算法，根据每个恶意传输规则的第一恶意传输特征生成的；

[0047] 若每个第一恶意传输特征与所述目标报文均匹配失败，则确定所述目标报文相对于每个恶意传输规则的初始检测结果为正常报文；

[0048] 若至少一个所述第一恶意传输特征与所述目标报文匹配成功，则确定与所述目标报文匹配的所述第一恶意传输特征对应的目标恶意传输规则，并确定所述目标报文相对于每个目标恶意传输规则的初始检测结果为初步符合所述目标恶意传输规则。

[0049] 在一种可选的实施例中，所述报文检测单元，还用于：

[0050] 获取通过AC状态机对所述目标历史报文进行检测获得的结束状态和已检测字节数；

[0051] 基于所述AC状态机，根据所述已检测字节数确定所述目标报文对应的待检测字符串中的未检测起始位置，并根据所述结束状态从所述未检测起始位置处对所述待检测字符串进行查找，从所述第一恶意传输特征对应的字符串中，确定出与所述待检测字符串相匹配的目标字符串；

[0052] 根据所述目标字符串对应的目标恶意传输特征，确定每个第一恶意传输特征与所述目标报文的匹配结果。

[0053] 在一种可选的实施例中，所述报文检测单元，还用于：

[0054] 对于每个目标恶意传输规则，将所述目标恶意传输规则中除所述第一恶意传输特征之外的其他恶意传输特征，分别与所述目标报文进行匹配；

[0055] 若所述其他恶意传输特征与所述目标报文均匹配成功，则确定所述目标报文对应的目标检测结果为恶意报文；

[0056] 若每个目标恶意传输规则对应的所述其他恶意传输特征中都有与所述目标报文匹配失败的其他恶意传输特征，则确定所述目标报文对应的目标检测结果为正常报文。

[0057] 在一种可选的实施例中，所述报文检测单元，还用于：

[0058] 若识别出所述目标报文对应的应用层协议，则获取所述应用层协议对应的检测引擎下的至少一个恶意应用规则；

[0059] 根据所述至少一个恶意应用规则中包括的多个恶意应用特征，对所述目标报文进行检测，确定所述目标报文是否为恶意报文。

[0060] 第三方面，本申请实施例还提供了一种计算机可读存储介质，所述计算机可读存储介质内存储有计算机程序，所述计算机程序被处理器执行时，实现第一方面的报文检测方法。

[0061] 第四方面，本申请实施例还提供了一种电子设备，包括存储器和处理器，所述存储器上存储有可在所述处理器上运行的计算机程序，当所述计算机程序被所述处理器执行时，使得所述处理器实现第一方面的报文检测方法。

[0062] 第二方面至第四方面中任意一种实现方式所带来的技术效果可参见第一方面中对应的实现方式所带来的技术效果，此处不再赘述。

附图说明

[0063] 为了更清楚地说明本申请实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简要介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0064] 图1为本申请实施例提供的一种特征库增加传输方向字段的示意图；

[0065] 图2为本申请实施例提供的一种特征库分组构建检测引擎的示意图；

[0066] 图3为本申请实施例提供的一种报文检测方法的流程图；

[0067] 图4为本申请实施例提供的一种传输层报文检测引擎进行报文检测的流程图；

[0068] 图5为本申请实施例提供的一种确定初始检测结果的流程图；

[0069] 图6为本申请实施例提供的一种AC状态机对目标报文进行匹配检测的流程图；

[0070] 图7为本申请实施例提供的一种确定目标检测结果的流程图；

[0071] 图8为本申请实施例提供的另一种报文检测方法的流程图；

[0072] 图9为本申请实施例提供的一种报文检测装置的结构示意图；

[0073] 图10为本申请实施例提供的一种电子设备的结构示意图。

具体实施方式

[0074] 为了使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请作进一步地详细描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本申请保护的范围。

[0075] 需要说明的是，本申请的文件中涉及的术语“包括”和“具有”以及它们的变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0076] 下面将结合附图，对本申请实施例提供的技术方案进行详细说明。

[0077] 下文中所用的词语“示例性”的意思为“用作例子、实施例或说明性”。作为“示例性”所说明的任何实施例不必解释为优于或好于其它实施例。在本申请实施例的描述中，除非另有说明，“多个”的含义是两个或两个以上。

[0078] 在进行报文检测之前，首先根据传输层协议和传输方向，对已有的特征库进行分组，得到特征库分组。其中，已有的特征库中包含有所有可能识别出报文为恶意报文的特征。在对特征库进行分组后，再根据每个特征库分组构建检测引擎，以使在对报文进行检测时，可以将报文送入相应的构建好的检测引擎中进行检测，确定报文是否为恶意报文。

[0079] 其中，传输层协议可以包括TCP协议和UDP协议等，传输方向可以包括客户端到服务端和服务端到客户端。

[0080] 具体地，先对特征库进行特征设计，增加传输方向字段。示例性地，可以按照如图1所示的方式，对特征库增加传输方向字段。其中，图1中的tcp为传输层协议中的TCP协议，图1中的to_client对应的传输方向为服务端到客户端，图1中的to_server对应的传输方向为客户端到服务端。

[0081] 在特征库增加传输方向字段后，解析特征库，根据每条特征的传输层协议和传输方向字段对特征库分组，并对分好组的特征库分别构建各自的检测引擎。

[0082] 示例性地，可以按照如图2所示的方式，对特征库分组并构建检测引擎。如图2所示，传输层协议包括TCP协议、UDP协议和其他协议，传输方向包括客户端到服务端(toserver)和服务端到客户端(toclient)。根据传输层协议和传输方向，可以将特征库分为TCP协议_服务端到客户端(tcp_toclient)分组、TCP协议_客户端到服务端(toserver)分组、UDP协议_服务端到客户端(udp_toclient)分组、UDP协议_客户端到服务端(udp_toserver)分组、其他协议_服务端到客户端(其他协议_toclient)分组和其他协议_客户端到服务端(其他协议_toserver)分组。

[0083] 在每个分组内，根据特征是否包含应用层协议，可以将进一步地将特征分为应用

层特征和无应用层特征。并在每个分组内，根据应用层特征构建相应的应用层检测引擎，根据无应用层特征构建相应的传输层检测引擎。

[0084] 在对特征库分组构建检测引擎后，可以通过构建的检测引擎对报文进行检测。具体地，本申请实施例提供了一种报文检测方法，如图3所示，包括如下步骤：

[0085] 步骤S301，接收待检测报文，并获取之前接收到的至少一个历史报文。

[0086] 在接收到待检测报文的同时获取到在接收待检测报文之前所接收到的至少一个历史报文。

[0087] 步骤S302，从至少一个历史报文中确定出与待检测报文具有相同流量信息的目标历史报文，并将待检测报文与目标历史报文进行拼接，获得目标报文。

[0088] 在接收到待检测报文后，可以根据待检测报文的五元组查找待检测报文对应的流量信息。其中，待检测报文的五元组包括协议类型、源IP地址、源端口、目的IP地址和目的端口。

[0089] 根据每个历史报文分别对应的流量信息，可以从至少一个历史报文中确定出与待检测报文具有相同流量信息的目标历史报文，并将确定出的目标历史报文与待检测报文进行拼接，获得目标报文。

[0090] 具体地，可以对同一条流的多个报文进行缓存和重组，每次在对接收到的待检测报文进行检测前，均将其与之前接收到的同一条流的报文进行拼接，再对拼接后的报文进行检测。

[0091] 可选的，在接收到待检测报文后，若根据待检测报文对应的流量信息，从之前接收到的至少一个历史报文中无法确定出与待检测报文具有相同流量信息的目标历史报文，则可以将待检测报文作为目标报文。

[0092] 步骤S303，若无法识别出目标报文对应的应用层协议，则根据目标报文的传输层协议和传输方向对应的检测引擎，对目标报文进行报文检测。

[0093] 在获得目标报文后，首先对目标报文进行传输层协议识别和传输方向识别，在识别出目标报文的传输层协议和传输方向后，再对目标报文进行应用层协议识别，若无法识别出目标报文对应的应用层协议，则可以根据目标报文的传输层协议和传输方向对应的检测引擎，对目标报文进行报文检测。

[0094] 例如，传输层协议可以为TCP协议和UDP协议，传输方向可以为客户端到服务端和服务端到客户端。其中，TCP协议和客户端到服务端对应的检测引擎为第一检测引擎，TCP协议和服务端到客户端对应的检测引擎为第二检测引擎，UDP协议和客户端到服务端对应的检测引擎为第三检测引擎，UDP协议和服务端到客户端对应的检测引擎为第四检测引擎。假设识别出目标报文的传输层协议为UDP协议，目标报文的传输方向为客户端到服务端，且无法识别出目标报文对应的应用层协议，则可以采用第三检测引擎对目标报文进行报文检测。

[0095] 具体地，可以按照图4中示出的过程，根据目标报文的传输层协议和传输方向对应的检测引擎，对目标报文进行报文检测。如图4所示，包括如下步骤：

[0096] 步骤S401，获取目标报文的传输层协议和传输方向对应的检测引擎下的至少一个恶意传输规则。

[0097] 其中，每个恶意传输规则包括多个恶意传输特征。

[0098] 步骤S402,对于每个恶意传输规则,从多个恶意传输特征中确定一个恶意传输特征作为第一恶意传输特征。

[0099] 对于每个恶意传输规则,可以按照设定的选取规则,从该恶意传输规则包括的多个恶意传输特征中选取出一个恶意传输特征,并将该恶意传输特征作为第一恶意传输特征。

[0100] 步骤S403,根据每个恶意传输规则的第一恶意传输特征对目标报文进行检测,确定目标报文相对于每个恶意传输规则的初始检测结果。

[0101] 其中,目标报文相对于每个恶意传输规则的初始检测结果可以通过图5中示出的过程进行确定。如图5所示,包括如下步骤:

[0102] 步骤S4031,基于AC状态机对目标报文进行匹配检测,确定每个第一恶意传输特征与目标报文的匹配结果。

[0103] 其中,AC状态机是通过多模式匹配AC算法,根据每个恶意传输规则的第一恶意传输特征生成的。

[0104] 多模式匹配(Aho-Corasick,AC)算法是一种多模匹配字符串查找算法,其核心思想是先根据多个模式字符串生成一个AC状态机,待检测字符串作为该AC状态机的输入,扫描一次待检测字符串,便能得到所有匹配的模式字符串。

[0105] 无状态的AC算法每次查找待检测字符串时,都是从AC状态机的初始状态开始运转,每次对当前待检测字符串的检测都是一次独立的检测,与上次待检测字符串的匹配结果无关,如果某个模式字符串的前半部分在前一个待检测字符串,后半部分在后一个待检测字符串,那么这两个待检测字符串都无法匹配该模式字符串,从而导致检测引擎漏报。如果检测当前待检测字符串时,把上次待检测字符串一并作为输入进行检测,那么就会对上次待检测字符串执行两次查找,重复检测,从而导致检测引擎的性能下降。

[0106] 因此,本申请实施例提出一种带状态的AC算法,该带状态的AC算法相比于无状态的AC算法,改进点在于:

[0107] AC状态机的输入参数除了待检测字符串之外,增加两个输入参数:一个是上一次检测的结束状态,一个是已检测的字节数;AC状态机对待检测字符串进行查找时,先根据已检测的字节数进行偏移,得到待检测字符串的起始位置,然后从上一次检测的结束状态开始运转;查找结束后,记录本次检测的结束状态,作为下次检测的输入参数,记录本次已检测的字节数与输入的已检测字节数之和,作为下次检测的输入参数。如此,对多个待检测字符串的查找就如同对拼接好的一个待检测字符串查找一样,同时也避免了重复检测。

[0108] 具体地,每个第一恶意传输特征与目标报文的匹配结果可以根据图6中示出的过程来进行确定。如图6所示,包括如下步骤:

[0109] 步骤S40311,获取通过AC状态机对目标历史报文进行检测获得的结束状态和已检测字节数。

[0110] 步骤S40312,基于AC状态机,根据已检测字节数确定目标报文对应的待检测字符串中的未检测起始位置,并根据结束状态从未检测起始位置处对待检测字符串进行查找,从第一恶意传输特征对应的字符串中,确定出与待检测字符串相匹配的目标字符串。

[0111] 例如,生成AC状态机的模式字符串为“yes”、“her”和“use”,待检测字符串为“yesherusewe”,AC状态机对目标历史报文进行检测获得的结束状态为30,获得的已检测字

节数为7,则可以确定待检测字符串“yesherusewe”中的未检测起始位置为位于待检测字符串中的第8个字符“s”,即待检测字符串“yesherusewe”中的未检测字符串为“sewe”,并将状态30作为起始状态,从未检测字符串“sewe”中的“s”位置处开始进行查找,确定模式字符串“yes”、“her”和“use”中,与待检测字符串“yesherusewe”相匹配的目标字符串。

[0112] 步骤S40313,根据目标字符串对应的目标恶意传输特征,确定每个第一恶意传输特征与目标报文的匹配结果。

[0113] 步骤S4032,若每个第一恶意传输特征与目标报文均匹配失败,则确定目标报文相对于每个恶意传输规则的初始检测结果为正常报文。

[0114] 例如,目标报文的传输层协议和传输方向对应的检测引擎下包含有1、2、3、4、5、6共6个恶意传输规则,每个恶意传输规则中都包括有3个恶意传输特征。假设从恶意传输规则1中确定的第一恶意传输特征为特征A,从恶意传输规则2中确定的第一恶意传输特征为特征B,从恶意传输规则3中确定的第一恶意传输特征为特征C,从恶意传输规则4中确定的第一恶意传输特征为特征D,从恶意传输规则5中确定的第一恶意传输特征为特征E,从恶意传输规则6中确定的第一恶意传输特征为特征F。通过AC状态机确定特征A、特征B、特征C、特征D、特征E和特征F与目标报文均匹配失败,则可以确定目标报文为正常报文。

[0115] 步骤S4033,若至少一个第一恶意传输特征与目标报文匹配成功,则确定与目标报文匹配的第一恶意传输特征对应的目标恶意传输规则,并确定目标报文相对于每个目标恶意传输规则的初始检测结果为初步符合目标恶意传输规则。

[0116] 例如,目标报文的传输层协议和传输方向对应的检测引擎下包含有1、2、3、4、5、6共6个恶意传输规则,每个恶意传输规则中都包括有3个恶意传输特征。在从恶意传输规则1、2、3、4、5、6中确定出特征A、特征B、特征C、特征D、特征E、特征F后,通过AC状态机确定特征A、特征B和特征C与目标报文匹配成功,特征D、特征E和特征F与目标报文匹配失败,则可以确定目标报文分别初步符合恶意传输规则1、恶意传输规则2和恶意传输规则3。

[0117] 步骤S404,若基于初始检测结果确定目标报文初步符合至少一个目标恶意传输规则,则根据每个目标恶意传输规则中除第一恶意传输特征之外的其他恶意传输特征,对目标报文进行检测,确定目标报文相对于每个目标恶意传输规则的目标检测结果。

[0118] 其中,目标报文相对于每个恶意传输规则的目标检测结果可以通过图7中示出的过程进行确定。如图7所示,包括如下步骤:

[0119] 步骤S4041,对于每个目标恶意传输规则,将目标恶意传输规则中除第一恶意传输特征之外的其他恶意传输特征,分别与目标报文进行匹配。

[0120] 步骤S4042,若其他恶意传输特征与目标报文均匹配成功,则确定目标报文对应的目标检测结果为恶意报文。

[0121] 例如,目标恶意传输规则为1、2、3,目标恶意传输规则1中除第一恶意传输特征A之外,还包括恶意传输特征B和恶意传输特征C;目标恶意传输规则2中除第一恶意传输特征D之外,还包括恶意传输特征E和恶意传输特征F;目标恶意传输规则3中除第一恶意传输特征G之外,还包括恶意传输特征H和恶意传输特征I。将恶意传输特征B、C、E、F、H、I分别与目标报文进行匹配,当确定恶意传输特征B和恶意传输特征C与目标报文均匹配成功时,可以确定目标报文为恶意报文;或者,当确定恶意传输特征E和恶意传输特征F与目标报文均匹配成功时,可以确定目标报文为恶意报文;或者,当确定恶意传输特征H和恶意传输特征I与目

标报文均匹配成功时，可以确定目标报文为恶意报文。

[0122] 步骤S4043，若每个目标恶意传输规则对应的其他恶意传输特征中都有与目标报文匹配失败的其他恶意传输特征，则确定目标报文对应的目标检测结果为正常报文。

[0123] 例如，目标恶意传输规则为1、2、3，目标恶意传输规则1中除第一恶意传输特征A之外，还包括恶意传输特征B和恶意传输特征C；目标恶意传输规则2中除第一恶意传输特征D之外，还包括恶意传输特征E和恶意传输特征F；目标恶意传输规则3中除第一恶意传输特征G之外，还包括恶意传输特征H和恶意传输特征I。将恶意传输特征B、C、E、F、H、I分别与目标报文进行匹配，当确定恶意传输特征B和恶意传输特征C中至少存在一个恶意传输特征与目标报文匹配失败，且恶意传输特征E和恶意传输特征F中至少存在一个恶意传输特征与目标报文匹配失败，且恶意传输特征H和恶意传输特征I中至少存在一个恶意传输特征与目标报文匹配失败时，可以确定目标报文为正常报文。

[0124] 可选的，在从之前接收到的至少一个历史报文中确定出与待检测报文具有相同流量信息的目标历史报文，并将待检测报文与目标历史报文进行拼接，获得目标报文后，若识别出目标报文对应的应用层协议，则获取应用层协议对应的检测引擎下的至少一个恶意应用规则，并根据所述至少一个恶意应用规则中包括的多个恶意应用特征，对目标报文进行检测，确定目标报文是否为恶意报文。

[0125] 具体地，在识别出目标报文对应的应用层协议，并获取到该应用层协议对应的检测引擎下的至少一个恶意应用规则后，对于每个恶意应用规则，可以先从该恶意应用规则中包括的多个恶意应用特征中确定一个恶意应用特征作为目标恶意应用特征。

[0126] 将每个恶意应用规则中的目标恶意应用特征分别与目标报文进行匹配，若每个恶意应用规则中的目标恶意应用特征与目标报文均匹配失败，则确定目标报文为正常报文，若至少一个恶意应用规则中的至少一个目标恶意应用规则的目标恶意应用特征与目标报文匹配成功，则对于每个目标恶意应用规则，将该目标恶意应用规则中除目标恶意应用特征之外的其他恶意应用特征，分别与目标报文进行匹配，若该目标恶意应用规则中的其他恶意应用特征与目标报文均匹配成功，则可以确定目标报文为恶意报文，若每个目标恶意应用规则对应的其他恶意应用特征中都有与目标报文匹配失败的其他恶意应用特征，则可以确定目标报文为正常报文。

[0127] 在一些实施例中，本申请实施例中提供的报文检测方法，还可以按照如图8所示的过程进行实现，如图8所示，包括如下步骤：

[0128] 步骤S801，接收待检测报文，并根据待检测报文的五元组查找待检测报文对应的流量信息。

[0129] 步骤S802，将待检测报文和之前接收到的与待检测报文具有相同流量信息的目标历史报文进行拼接，获得目标报文。

[0130] 步骤S803，是否识别出目标报文对应的应用层协议；如果否，执行步骤S804；如果是，执行步骤S812。

[0131] 步骤S804，获取目标报文的传输层协议和传输方向对应的检测引擎下的至少一个恶意传输规则，并从每个恶意传输规则包括的多个恶意传输特征中确定一个恶意传输特征作为第一恶意传输特征。

[0132] 步骤S805，基于AC状态机对目标报文进行匹配检测。

[0133] 其中，AC状态机是通过多模式匹配AC算法，根据每个恶意传输规则的第一恶意传输特征生成的。且基于AC状态机对目标报文进行匹配检测，确定每个恶意传输规则的第一恶意传输特征与目标报文的匹配结果的具体过程可以参见图6，本实施例在此不作赘述。

[0134] 步骤S806，确定每个恶意传输规则的第一恶意传输特征与目标报文是否均匹配失败；如果是，执行步骤S807；如果否，执行步骤S808。

[0135] 步骤S807，确定目标报文为正常报文。

[0136] 步骤S808，从至少一个恶意传输规则中，确定出第一恶意传输特征与目标报文匹配成功的至少一个目标恶意传输规则。

[0137] 步骤S809，将每个目标恶意传输规则中除第一恶意传输特征之外的其他恶意传输特征，分别与目标报文进行匹配。

[0138] 步骤S810，确定每个目标恶意传输规则对应的其他恶意传输特征中是否都有与目标报文匹配失败的其他恶意传输特征；如果是，执行步骤S807；如果否，执行步骤S811。

[0139] 步骤S811，确定目标报文为恶意报文。

[0140] 步骤S812，获取应用层协议对应的检测引擎下的至少一个恶意应用规则，并从每个恶意应用规则包括的多个恶意应用特征中确定一个恶意应用特征作为目标恶意应用特征。

[0141] 步骤S813，将每个恶意应用规则中的目标恶意应用特征，分别与目标报文进行匹配。

[0142] 步骤S814，确定每个恶意应用规则的目标恶意应用特征与目标报文是否均匹配失败；如果是，执行步骤S807；如果否，执行步骤S815。

[0143] 步骤S815，从至少一个恶意应用规则中，确定出目标恶意应用特征与目标报文匹配成功的至少一个目标恶意应用规则。

[0144] 步骤S816，将每个目标恶意应用规则中除第一恶意应用特征之外的其他恶意应用特征，分别与目标报文进行匹配。

[0145] 步骤S817，确定每个目标恶意应用规则对应的其他恶意应用特征中是否都有与目标报文匹配失败的其他恶意应用特征；如果是，执行步骤S807；如果否，执行步骤S811。

[0146] 本申请提供的一种报文检测方法，可以解决无法识别接收报文的应用层协议，以及恶意流量特征被拆分到多个报文中而绕过防火墙的问题，通过在对接收到的报文进行检测前，先将报文与之前接收到的同一条流的报文进行拼接，再对拼接后的报文进行检测，并且在采用检测引擎对报文进行检测时，采用带状态的AC算法，即在将报文输入AC状态机的同时，将上次检测的结束状态和已检测字节数也输入AC状态机，来对报文进行匹配检测，从而可以避免对报文的重复检测，提高对报文进行检测的检测速度和检测准确率，同时也可以避免检测引擎的性能下降。

[0147] 此外，本申请实施例中提供的报文检测方法，可以根据传输层协议和传输方向对已有的特征库进行分组，构建出多个规模较小的子引擎，并且，通过分好组的特征库分别构建生成各自的传输层报文检测子引擎，每个传输层报文检测子引擎包含各自带状态的AC状态机，从而可以提高检测引擎的检测速度。

[0148] 与图3所示的报文检测方法基于同一发明构思，本申请实施例中还提供了一种报文检测装置。由于该装置是本申请报文检测方法对应的装置，并且该装置解决问题的原理

与该方法相似，因此该装置的实施可以参见上述方法的实施，重复之处不再赘述。

[0149] 图9示出了本申请实施例提供的一种报文检测装置的结构示意图，如图9所示，该报文检测装置包括报文接收单元901、报文拼接单元902和报文检测单元903。

[0150] 其中，报文接收单元901，用于接收待检测报文，并获取之前接收到的至少一个历史报文；

[0151] 报文拼接单元902，用于从至少一个历史报文中确定出与待检测报文具有相同流量信息的目标历史报文，并将待检测报文与目标历史报文进行拼接，获得目标报文；

[0152] 报文检测单元903，用于若无法识别出目标报文对应的应用层协议，则根据目标报文的传输层协议和传输方向对应的检测引擎，对目标报文进行报文检测。

[0153] 在一种可选的实施例中，报文检测单元903，具体用于：

[0154] 获取目标报文的传输层协议和传输方向对应的检测引擎下的至少一个恶意传输规则，其中每个恶意传输规则包括多个恶意传输特征；

[0155] 对于每个恶意传输规则，从多个恶意传输特征中确定一个恶意传输特征作为第一恶意传输特征；

[0156] 根据每个恶意传输规则的第一恶意传输特征对目标报文进行检测，确定目标报文相对于每个恶意传输规则的初始检测结果；

[0157] 若基于初始检测结果确定目标报文初步符合至少一个目标恶意传输规则，则根据每个目标恶意传输规则中除第一恶意传输特征之外的其他恶意传输特征，对目标报文进行检测，确定目标报文相对于每个目标恶意传输规则的目标检测结果。

[0158] 在一种可选的实施例中，报文检测单元903，还用于：

[0159] 基于AC状态机对目标报文进行匹配检测，确定每个第一恶意传输特征与目标报文的匹配结果；AC状态机是通过多模式匹配AC算法，根据每个恶意传输规则的第一恶意传输特征生成的；

[0160] 若每个第一恶意传输特征与目标报文均匹配失败，则确定目标报文相对于每个恶意传输规则的初始检测结果为正常报文；

[0161] 若至少一个第一恶意传输特征与目标报文匹配成功，则确定与目标报文匹配的第一恶意传输特征对应的目标恶意传输规则，并确定目标报文相对于每个目标恶意传输规则的初始检测结果为初步符合目标恶意传输规则。

[0162] 在一种可选的实施例中，报文检测单元903，还用于：

[0163] 获取通过AC状态机对目标历史报文进行检测获得的结束状态和已检测字节数；

[0164] 基于AC状态机，根据已检测字节数确定目标报文对应的待检测字符串中的未检测起始位置，并根据结束状态从未检测起始位置处对待检测字符串进行查找，从第一恶意传输特征对应的字符串中，确定出与待检测字符串相匹配的目标字符串；

[0165] 根据目标字符串对应的目标恶意传输特征，确定每个第一恶意传输特征与目标报文的匹配结果。

[0166] 在一种可选的实施例中，报文检测单元903，还用于：

[0167] 对于每个目标恶意传输规则，将目标恶意传输规则中除第一恶意传输特征之外的其他恶意传输特征，分别与目标报文进行匹配；

[0168] 若其他恶意传输特征与目标报文均匹配成功，则确定目标报文对应的目标检测结

果为恶意报文；

[0169] 若每个目标恶意传输规则对应的其他恶意传输特征中都有与目标报文匹配失败的其他恶意传输特征，则确定目标报文对应的目标检测结果为正常报文。

[0170] 在一种可选的实施例中，报文检测单元903，还用于：

[0171] 若识别出目标报文对应的应用层协议，则获取应用层协议对应的检测引擎下的至少一个恶意应用规则；

[0172] 根据至少一个恶意应用规则中包括的多个恶意应用特征，对目标报文进行检测，确定目标报文是否为恶意报文。

[0173] 与上述方法实施例基于同一发明构思，本申请实施例中还提供了一种电子设备。该电子设备可以用于进行报文检测。在该实施例中，电子设备的结构可以如图10所示，包括存储器1001以及一个或多个处理器1002。

[0174] 存储器1001，用于存储处理器1002执行的计算机程序。存储器1001可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统，以及运行即时通讯功能所需的程序等；存储数据区可存储各种即时通讯信息和操作指令集等。

[0175] 存储器1001可以是易失性存储器(volatile memory)，例如随机存取存储器(random-access memory，RAM)；存储器1001也可以是非易失性存储器(non-volatile memory)，例如只读存储器，快闪存储器(flash memory)，硬盘(hard disk drive，HDD)或固态硬盘(solid-state drive，SSD)、或者存储器1001是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。存储器1001可以是上述存储器的组合。

[0176] 处理器1002，可以包括一个或多个中央处理单元(central processing unit，CPU)或者为数字处理单元等等。处理器1002，用于调用存储器1001中存储的计算机程序时实现上述报文检测方法。

[0177] 本申请实施例中不限定上述存储器1001和处理器1002之间的具体连接介质。本公开实施例在图10中以存储器1001和处理器1002之间通过总线1003连接，总线1003在图10中以粗线表示，其它部件之间的连接方式，仅是进行示意性说明，并不引以为限。总线1003可以分为地址总线、数据总线、控制总线等。为便于表示，图10中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

[0178] 根据本申请的一个方面，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计算机指令，该计算机指令存储在计算机可读存储介质中。计算机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，使得该计算机设备执行上述实施例中的报文检测方法。

[0179] 程序产品可以采用一个或多个可读介质的任意组合。可读介质可以是可读信号介质或者可读存储介质。可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。可读存储介质的更具体的例子(非穷举的列表)包括：具有一个或多个导线的电连接、便携式盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。

[0180] 以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何

熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。

```
rule_id：1 {
    14：tcp
    dir：to_client
    ac：{
        pattern：“akdjkfKJKF”
    }
    others：{
        pattern：“D84899F”
    }
}
rule_id：2 {
    14：tcp
    dir：to_server
    ac：{
        pattern：“kklfiih”
    }
    others：{
        pattern：“4355284E”
    }
}
```

图1

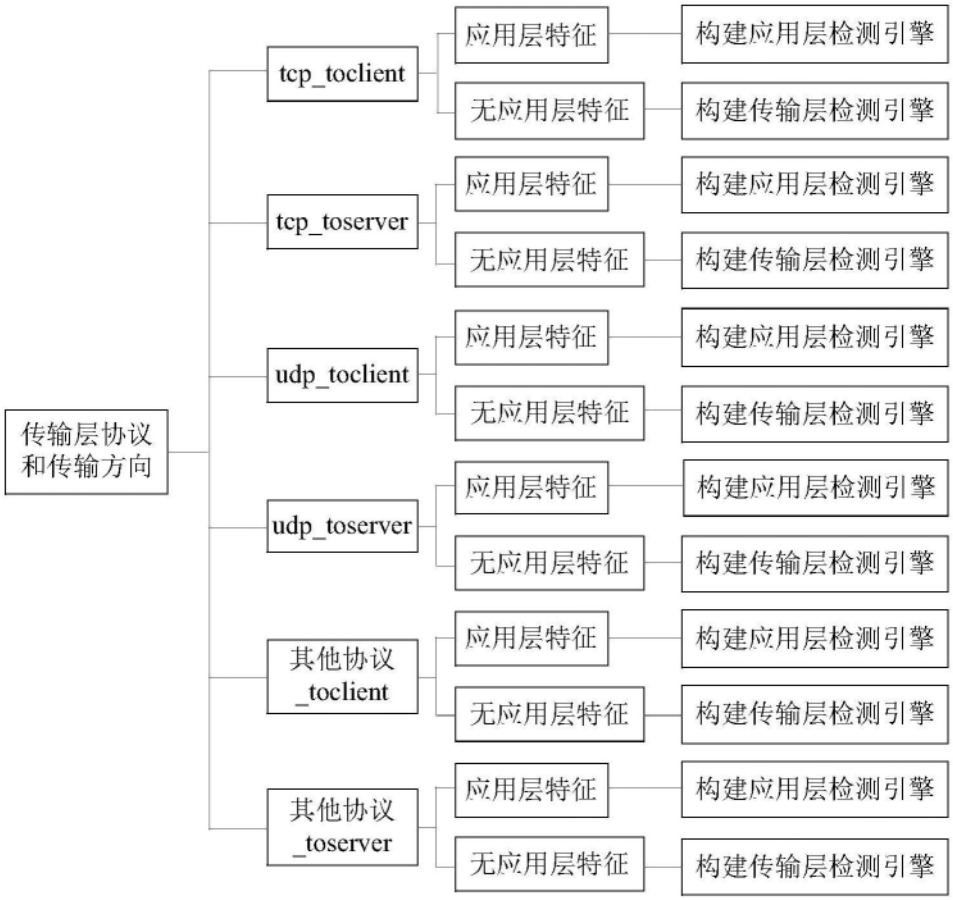

传输层协议和传输方向
tcp_toclient
tcp_toserver
udp_toclient
udp_toserver
其他协议_toclient
其他协议_toserver
应用层特征
无应用层特征
构建应用层检测引擎
构建传输层检测引擎

图2

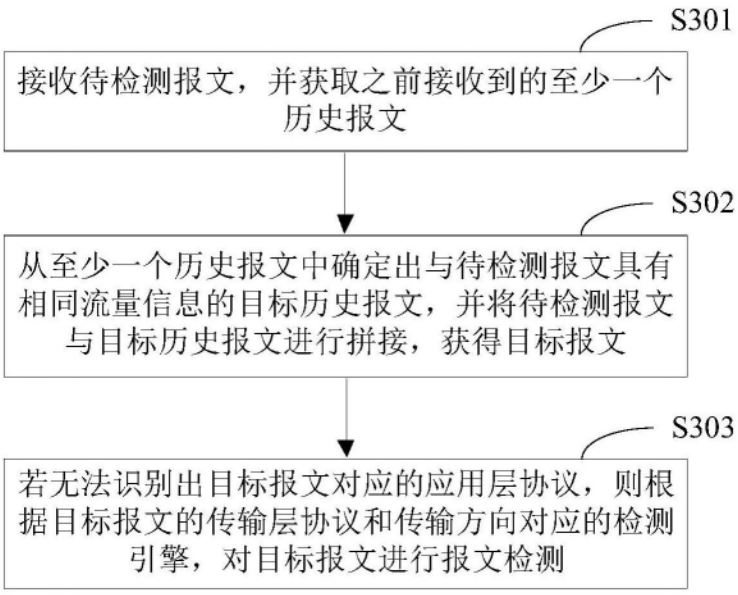

S301
接收待检测报文，并获取之前接收到的至少一个历史报文
S302
从至少一个历史报文中确定出与待检测报文具有相同流量信息的目标历史报文，并将待检测报文与目标历史报文进行拼接，获得目标报文
S303
若无法识别出目标报文对应的应用层协议，则根据目标报文的传输层协议和传输方向对应的检测引擎，对目标报文进行报文检测

图3

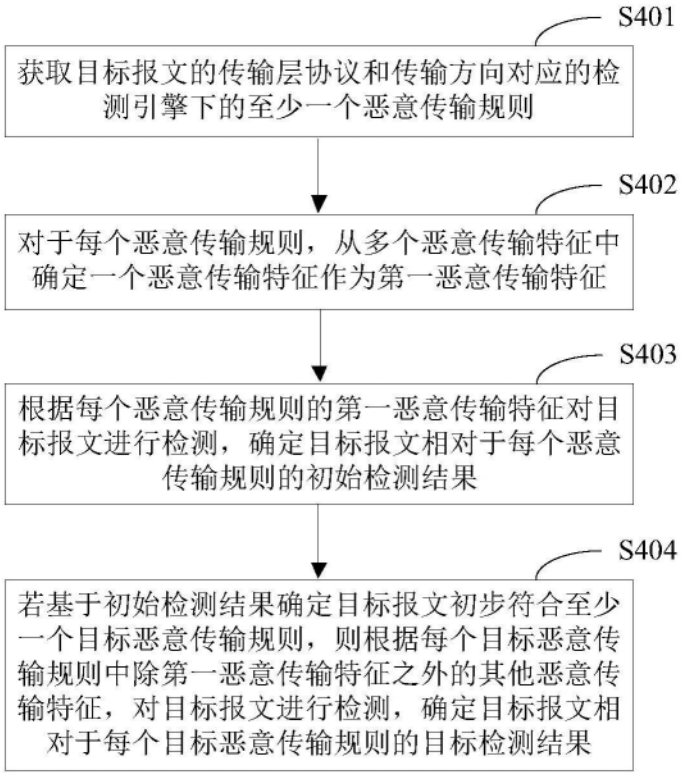

S401
获取目标报文的传输层协议和传输方向对应的检测引擎下的至少一个恶意传输规则
S402
对于每个恶意传输规则，从多个恶意传输特征中确定一个恶意传输特征作为第一恶意传输特征
S403
根据每个恶意传输规则的第一恶意传输特征对目标报文进行检测，确定目标报文相对于每个恶意传输规则的初始检测结果
S404
若基于初始检测结果确定目标报文初步符合至少一个目标恶意传输规则，则根据每个目标恶意传输规则中除第一恶意传输特征之外的其他恶意传输特征，对目标报文进行检测，确定目标报文相对于每个目标恶意传输规则的目标检测结果

图4

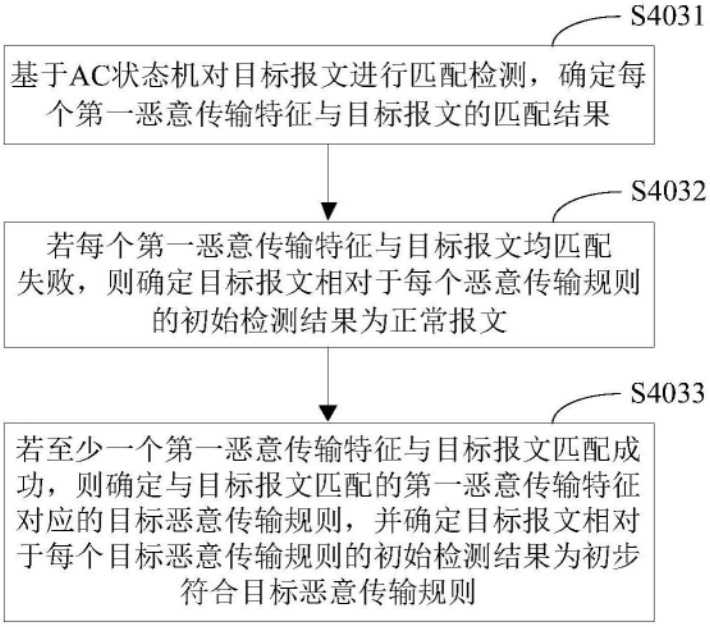

S4031
基于AC状态机对目标报文进行匹配检测，确定每个第一恶意传输特征与目标报文的匹配结果
S4032
若每个第一恶意传输特征与目标报文均匹配失败，则确定目标报文相对于每个恶意传输规则的初始检测结果为正常报文
S4033
若至少一个第一恶意传输特征与目标报文匹配成功，则确定与目标报文匹配的第一恶意传输特征对应的目标恶意传输规则，并确定目标报文相对于每个目标恶意传输规则的初始检测结果为初步符合目标恶意传输规则

图5

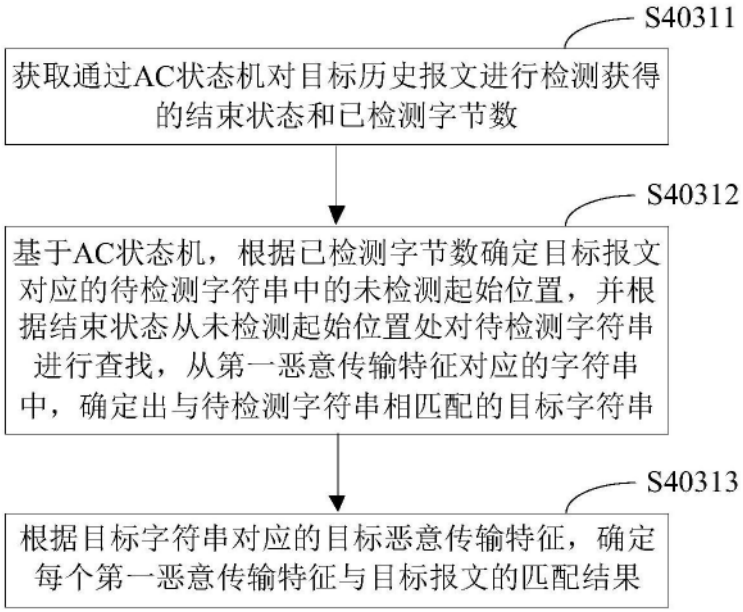

S40311
获取通过AC状态机对目标历史报文进行检测获得的结束状态和已检测字节数
S40312
基于AC状态机，根据已检测字节数确定目标报文对应的待检测字符串中的未检测起始位置，并根据结束状态从未检测起始位置处对待检测字符串进行查找，从第一恶意传输特征对应的字符串中，确定出与待检测字符串相匹配的目标字符串
S40313
根据目标字符串对应的目标恶意传输特征，确定每个第一恶意传输特征与目标报文的匹配结果

图6

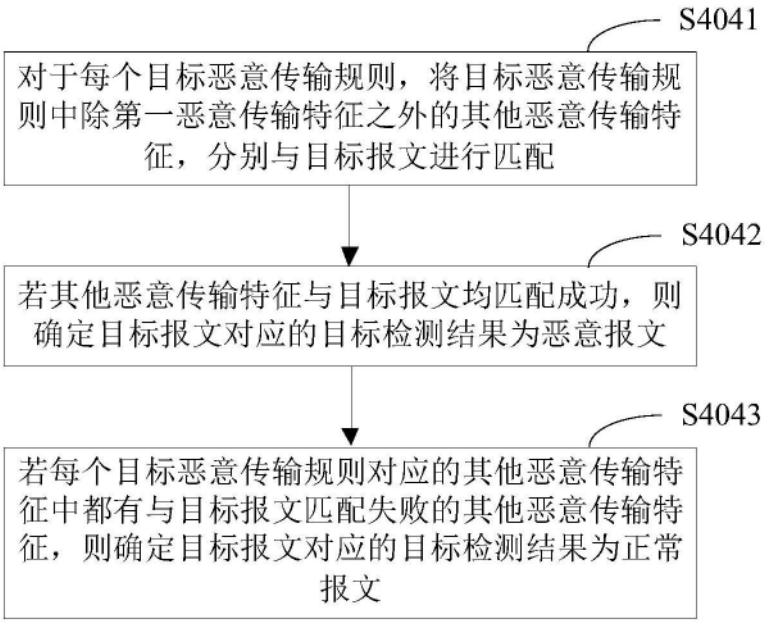

S4041
对于每个目标恶意传输规则，将目标恶意传输规则中除第一恶意传输特征之外的其他恶意传输特征，分别与目标报文进行匹配
S4042
若其他恶意传输特征与目标报文均匹配成功，则确定目标报文对应的目标检测结果为恶意报文
S4043
若每个目标恶意传输规则对应的其他恶意传输特征中都有与目标报文匹配失败的其他恶意传输特征，则确定目标报文对应的目标检测结果为正常报文

图7

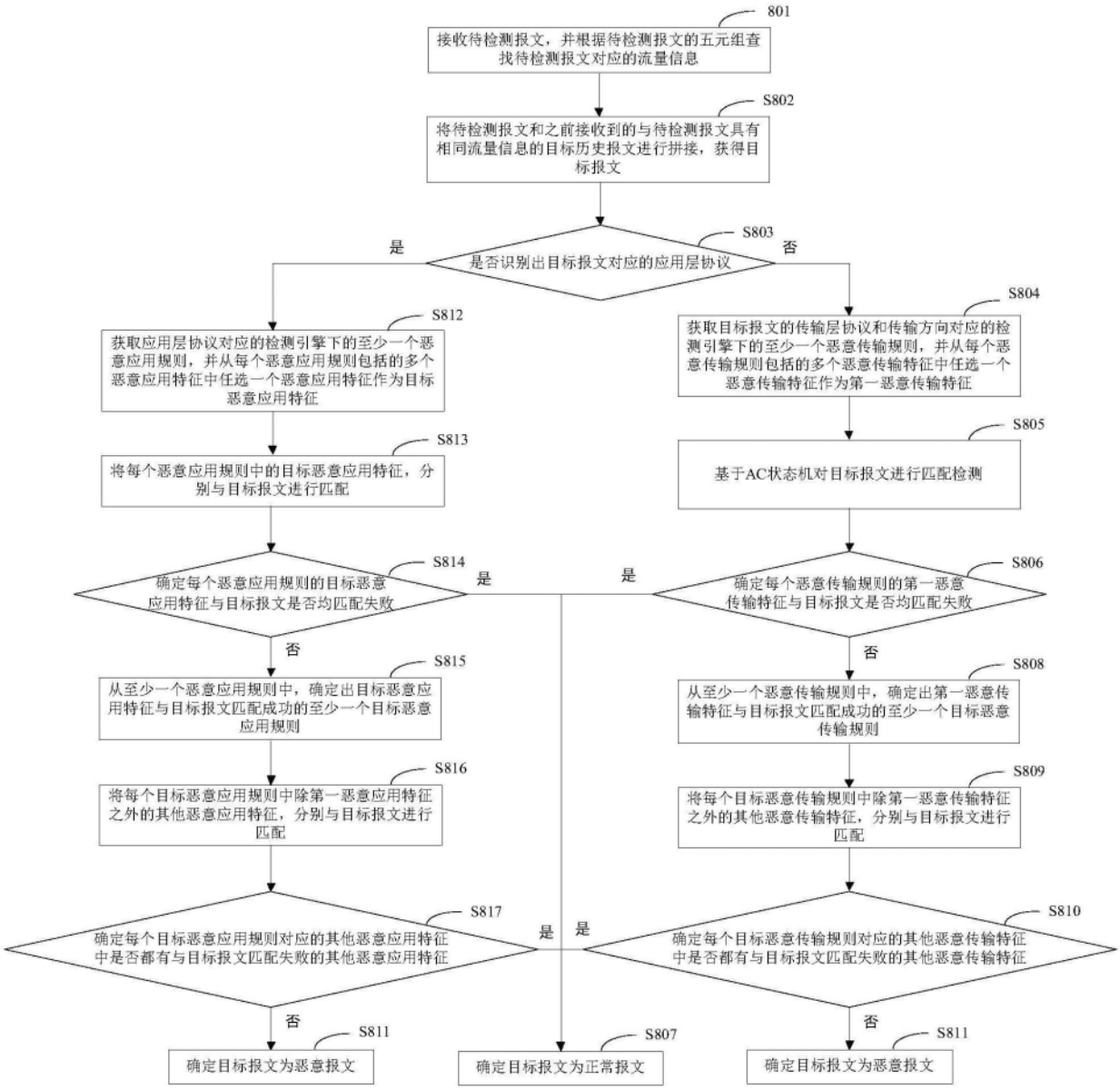

801
接收待检测报文，并根据待检测报文的五元组查找待检测报文对应的流量信息
S802
将待检测报文和之前接收到的与待检测报文具有相同流量信息的目标历史报文进行拼接，获得目标报文
S803
是否识别出目标报文对应的应用层协议
是
否
S812
获取应用层协议对应的检测引擎下的至少一个恶意应用规则，并从每个恶意应用规则包括的多个恶意应用特征中任选一个恶意应用特征作为目标恶意应用特征
S813
将每个恶意应用规则中的目标恶意应用特征，分别与目标报文进行匹配
S814
确定每个恶意应用规则的目标恶意应用特征与目标报文是否均匹配失败
是
否
S815
从至少一个恶意应用规则中，确定出目标恶意应用特征与目标报文匹配成功的至少一个目标恶意应用规则
S816
将每个目标恶意应用规则中除第一恶意应用特征之外的其他恶意应用特征，分别与目标报文进行匹配
S817
确定每个目标恶意应用规则对应的其他恶意应用特征中是否都有与目标报文匹配失败的其他恶意应用特征
是
否
S811
确定目标报文为恶意报文
S807
确定目标报文为正常报文
S804
获取目标报文的传输层协议和传输方向对应的检测引擎下的至少一个恶意传输规则，并从每个恶意传输规则包括的多个恶意传输特征中任选一个恶意传输特征作为第一恶意传输特征
S805
基于AC状态机对目标报文进行匹配检测
S806
确定每个恶意传输规则的第一恶意传输特征与目标报文是否均匹配失败
是
否
S808
从至少一个恶意传输规则中，确定出第一恶意传输特征与目标报文匹配成功的至少一个目标恶意传输规则
S809
将每个目标恶意传输规则中除第一恶意传输特征之外的其他恶意传输特征，分别与目标报文进行匹配
S810
确定每个目标恶意传输规则对应的其他恶意传输特征中是否都有与目标报文匹配失败的其他恶意传输特征
是
否
S811
确定目标报文为恶意报文

图8

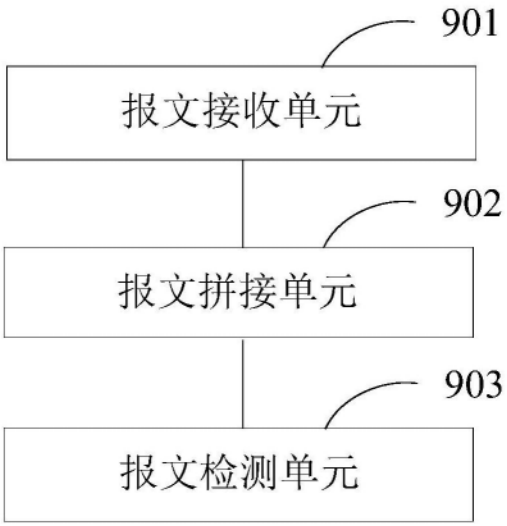


图9

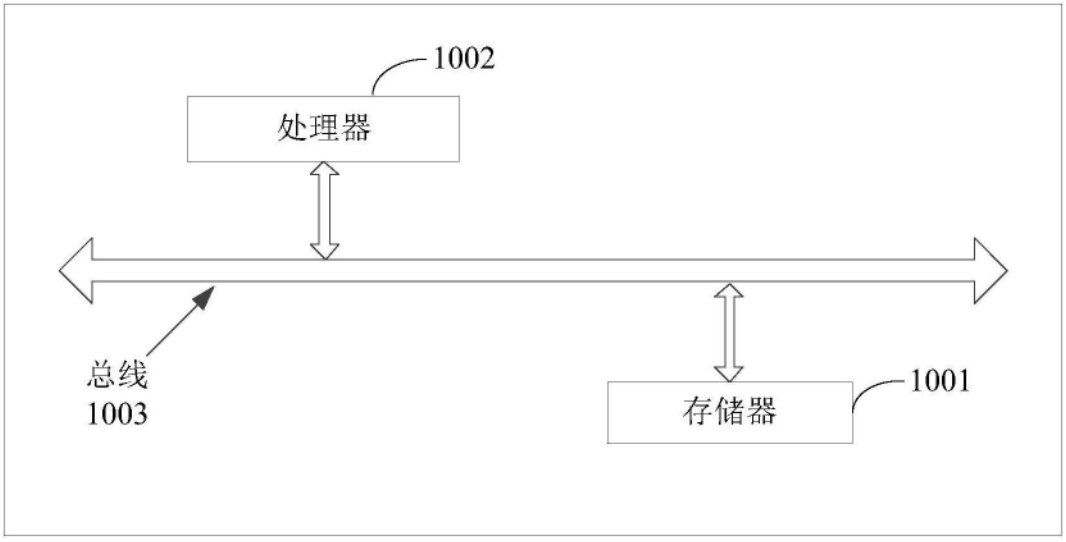


图10