(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106936799 A
(43)申请公布日 2017.07.07

(21)申请号 201511030202.1

(22)申请日 2015.12.31

(71)申请人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 何卫斌

(74)专利代理机构 北京博浩百睿知识产权代理有限责任公司 11134
代理人 宋子良

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

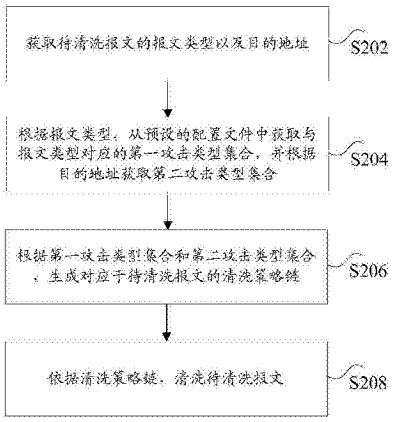
权利要求书3页 说明书11页 附图2页

(54)发明名称

报文清洗方法及装置

(57)摘要

本申请公开了一种报文清洗方法及装置。其中，该方法包括：获取待清洗报文的报文类型以及目的地址；根据所述报文类型，从预设的配置文件中获取与所述报文类型对应的第一攻击类型集合，并根据所述目的地址获取第二攻击类型集合，其中，所述第二攻击类型集合包含所述目的地址所指向的设备在预设时间段内受到的攻击类型；根据所述第一攻击类型集合和所述第二攻击类型集合，生成对应于所述待清洗报文的清洗策略链；依据所述清洗策略链，清洗所述待清洗报文。本申请解决了由于策略是事先配置好的造成的清洗设备的清洗效率较低的技术问题。



CN 106936799 A

1.一种报文清洗方法,其特征在于,包括:

获取待清洗报文的报文类型以及目的地址;

根据所述报文类型,从预设的配置文件中获取与所述报文类型对应的第一攻击类型集合,并根据所述目的地址获取第二攻击类型集合,其中,所述第二攻击类型集合包含所述目的地址所指向的设备在预设时间段内受到的攻击类型;

根据所述第一攻击类型集合和所述第二攻击类型集合,生成对应于所述待清洗报文的清洗策略链;

依据所述清洗策略链,清洗所述待清洗报文。

2.根据权利要求1所述的方法,其特征在于,所述根据所述第一攻击类型集合和所述第二攻击类型集合,生成对应于所述待清洗报文的清洗策略链包括:

计算所述第一攻击类型集合与所述第二攻击类型集合的交集,得到第三攻击类型集合,其中,所述第三攻击类型集合中包含所述第一攻击类型集合与所述第二攻击类型集合中相同的攻击类型;

根据所述第三攻击类型集合,生成所述清洗策略链。

3.根据权利要求2所述的方法,其特征在于,所述根据所述第三攻击类型结合,生成所述清洗策略链包括:

获取所述第三攻击类型集合中各个攻击类型的权重值;

按照所述权重值的大小,对各个攻击类型进行排序;

获取排序后的各个攻击类型对应的清洗策略,其中,各个清洗策略的排列顺序与排序后的各个攻击类型的排列顺序一致;

生成包含排序后的各个攻击类型对应的清洗策略的所述清洗策略链。

4.根据权利要求3所述的方法,其特征在于,所述依据所述清洗策略链,清洗所述待清洗报文包括:

按照所述清洗策略链中各个清洗策略的顺序,依次调用各个清洗策略对所述待清洗报文进行清洗,以确定是否丢弃所述待清洗报文。

5.根据权利要求4所述的方法,其特征在于,在确定不丢弃所述待清洗报文的情况下,所述方法还包括:

将所述待清洗报文发送至所述目的地址所指向的设备。

6.根据权利要求1所述的方法,其特征在于,所述获取待清洗报文的报文类型以及目的地址包括:

解析所述待清洗报文的报头;

基于所述报文类型对应的字段的偏移量,从所述待清洗报文中提取所述报文类型,以及基于所述目的地址对应的字段的偏移量,从所述待清洗报文中提取所述目的地址。

7.根据权利要求1所述的方法,其特征在于,所述根据所述报文类型,从预设的配置文件中获取与所述报文类型对应的第一攻击类型集合包括:

从所述预设的配置文件中,查找所述报文类型对应的攻击类型,其中,所述预设的配置文件中包含有所述报文类型与攻击类型之间的对应关系;

生成包含所述报文类型对应的攻击类型的所述第一攻击类型集合。

8.根据权利要求1至7中任一项所述的方法,其特征在于,所述报文类型包括以下一种

或几种：传输控制协议同步TCP SYN报文、传输控制协议确认TCP ACK报文以及传输控制协议复位TCP RST报文；所述攻击类型包括以下一种或几种：syn报文泛洪攻击SYN flood、ack报文泛洪攻击ACK flood、rst报文泛洪攻击RST flood以及udp报文泛洪攻击UDP flood。

9.一种报文清洗装置，其特征在于，包括：

第一获取单元，用于获取待清洗报文的报文类型以及目的地址；

第二获取单元，用于根据所述报文类型，从预设的配置文件中获取与所述报文类型对应的第一攻击类型集合，并根据所述目的地址获取第二攻击类型集合，其中，所述第二攻击类型集合包含所述目的地址所指向的设备在预设时间段内受到的攻击类型；

生成单元，用于根据所述第一攻击类型集合和所述第二攻击类型集合，生成对应于所述待清洗报文的清洗策略链；

清洗单元，用于依据所述清洗策略链，清洗所述待清洗报文。

10.根据权利要求9所述的装置，其特征在于，所述生成单元包括：

计算模块，用于计算所述第一攻击类型集合与所述第二攻击类型集合的交集，得到第三攻击类型集合，其中，所述第三攻击类型集合中包含所述第一攻击类型集合与所述第二攻击类型集合中相同的攻击类型；

生成模块，用于根据所述第三攻击类型集合，生成所述清洗策略链。

11.根据权利要求10所述的装置，其特征在于，所述生成模块用于执行以下步骤根据所述第三攻击类型集合，生成所述清洗策略链：

获取所述第三攻击类型集合中各个攻击类型的权重值；

按照所述权重值的大小，对各个攻击类型进行排序；

获取排序后的各个攻击类型对应的清洗策略，其中，各个清洗策略的排列顺序与排序后的各个攻击类型的排列顺序一致；

生成包含排序后的各个攻击类型对应的清洗策略的所述清洗策略链。

12.根据权利要求11所述的装置，其特征在于，所述清洗单元用于执行以下步骤依据所述清洗策略链，清洗所述待清洗报文：

按照所述清洗策略链中各个清洗策略的顺序，依次调用各个清洗策略对所述待清洗报文进行清洗，以确定是否丢弃所述待清洗报文。

13.根据权利要求12所述的装置，其特征在于，所述装置还包括：

发送单元，用于在确定不丢弃所述待清洗报文的情况下，将所述待清洗报文发送至所述目的地址所指向的设备。

14.根据权利要求9所述的装置，其特征在于，所述第一获取单元包括：

解析模块，用于解析所述待清洗报文的报头；

提取模块，用于基于所述报文类型对应的字段的偏移量，从所述待清洗报文中提取所述报文类型，以及基于所述目的地址对应的字段的偏移量，从所述待清洗报文中提取所述目的地址。

15.根据权利要求9所述的装置，其特征在于，所述第二获取单元用于执行以下步骤根据所述报文类型，从预设的配置文件中获取与所述报文类型对应的第一攻击类型集合：

从所述预设的配置文件中，查找所述报文类型对应的攻击类型，其中，所述预设的配置文件中包含有所述报文类型与攻击类型之间的对应关系；

生成包含所述报文类型对应的攻击类型的所述第一攻击类型集合。

16.根据权利要求9至15中任一项所述的装置，其特征在于，所述报文类型包括以下一种或几种：传输控制协议同步TCP SYN报文、传输控制协议确认TCP ACK报文以及传输控制协议复位TCP RST报文；所述攻击类型包括以下一种或几种：syn报文泛洪攻击SYN flood、ack报文泛洪攻击ACK flood、rst报文泛洪攻击RST flood以及udp报文泛洪攻击UDP flood。

报文清洗方法及装置

技术领域

[0001] 本申请涉及网络安全领域，具体而言，涉及一种报文清洗方法及装置。

背景技术

[0002] 在遭遇报文攻击时，一般会将流量牵引至专门的清洗设备，对攻击报文进行过滤。清洗设备的一般处理过程是这样的：报文从入方向进来，根据该报文目的IP，查询得到针对此目的IP的策略。根据策略，可以对报文做出“接受”、“通过”或者“丢弃”的决定。

[0003] 对目前的技术而言，对于某一种特定的攻击类型，会有一个或者多个对应的策略，清洗设备只需要机械地执行这些策略即可。在一般的工程实践中，策略是事先配置好的，即，针对某个被保护的IP，预测其可能遭受的攻击类型，然后把所有对应的策略都加入策略链。

[0004] 然而，这会带来这样的问题：报文会进入一些完全不需要进入的策略，造成误清洗，降低清洗设备的清洗效率。

[0005] 针对上述的问题，目前尚未提出有效的解决方案。

发明内容

[0006] 本申请实施例提供了一种报文清洗方法及装置，以至少解决由于策略是事先配置好的造成的清洗设备的清洗效率较低的技术问题。

[0007] 根据本申请实施例的一个方面，提供了一种报文清洗方法，包括：获取待清洗报文的报文类型以及目的地址；根据所述报文类型，从预设的配置文件中获取与所述报文类型对应的第一攻击类型集合，并根据所述目的地址获取第二攻击类型集合，其中，所述第二攻击类型集合包含所述目的地址所指向的设备在预设时间段内受到的攻击类型；根据所述第一攻击类型集合和所述第二攻击类型集合，生成对应于所述待清洗报文的清洗策略链；依据所述清洗策略链，清洗所述待清洗报文。

[0008] 根据本申请实施例的另一方面，还提供了一种报文清洗装置，包括：第一获取单元，用于获取待清洗报文的报文类型以及目的地址；第二获取单元，用于根据所述报文类型，从预设的配置文件中获取与所述报文类型对应的第一攻击类型集合，并根据所述目的地址获取第二攻击类型集合，其中，所述第二攻击类型集合包含所述目的地址所指向的设备在预设时间段内受到的攻击类型；生成单元，用于根据所述第一攻击类型集合和所述第二攻击类型集合，生成对应于所述待清洗报文的清洗策略链；清洗单元，用于依据所述清洗策略链，清洗所述待清洗报文。

[0009] 在本申请实施例中，采用获取待清洗报文的报文类型以及目的地址；根据报文类型，从预设的配置文件中获取与报文类型对应的第一攻击类型集合，并根据目的地址获取第二攻击类型集合，其中，第二攻击类型集合包含目的地址所指向的设备在预设时间段内受到的攻击类型；根据第一攻击类型集合和第二攻击类型集合，生成对应于待清洗报文的清洗策略链；依据清洗策略链，清洗待清洗报文的方式，通过基于待清洗报文的报文类型以

及目的地址得到一条对应于待清洗报文的动态的清洗策略链，达到了有针对性地进行报文清洗的目的，从而实现了提高报文清洗效率的技术效果，进而解决了由于策略是事先配置好的造成的清洗设备的清洗效率较低的技术问题。

附图说明

[0010] 此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

[0011] 图1是根据本申请实施例的一种运行报文清洗方法的计算机终端的硬件结构框图；

[0012] 图2是根据本申请实施例的一种可选的报文清洗方法的流程示意图；

[0013] 图3是根据本申请实施例的一种可选的报文清洗装置的结构示意图；

[0014] 图4是根据本申请实施例的一种可选的生成单元的结构示意图；

[0015] 图5是根据本申请实施例的另一种可选的报文清洗装置的结构示意图；

[0016] 图6是根据本申请实施例的一种可选的第一获取单元的结构示意图；

[0017] 图7是根据本申请实施例的一种计算机终端的结构框图。

具体实施方式

[0018] 为了使本技术领域的人员更好地理解本申请方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分的实施例，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他实施例，都应当属于本申请保护的范围。

[0019] 需要说明的是，本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本申请的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，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。

[0020] 实施例1

[0021] 根据本申请实施例，还提供了一种报文清洗方法的方法实施例，需要说明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0022] 本申请实施例一所提供的方法实施例可以在移动终端、计算机终端或者类似的运算装置中执行。以运行在计算机终端上为例，图1是本申请实施例的一种报文清洗方法的计算机终端的硬件结构框图。如图1所示，计算机终端10可以包括一个或多个(图中仅示出一个)处理器102(处理器102可以包括但不限于微处理器MCU或可编程逻辑器件FPGA等的处理装置)、用于存储数据的存储器104、以及用于通信功能的传输装置106。本领域普通技术人

员可以理解，图1所示的结构仅为示意，其并不对上述电子装置的结构造成限定。例如，计算机终端10还可包括比图1中所示更多或者更少的组件，或者具有与图1所示不同的配置。

[0023] 存储器104可用于存储应用软件的软件程序以及模块，如本申请实施例中的报文清洗方法对应的程序指令/模块，处理器102通过运行存储在存储器104内的软件程序以及模块，从而执行各种功能应用以及数据处理，即实现上述的报文清洗方法。存储器104可包括高速随机存储器，还可包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器104可进一步包括相对于处理器102远程设置的存储器，这些远程存储器可以通过网络连接至计算机终端10。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0024] 传输装置106用于经由一个网络接收或者发送数据。上述的网络具体实例可包括计算机终端10的通信供应商提供的无线网络。在一个实例中，传输装置106包括一个网络适配器(Network Interface Controller,NIC)，其可通过基站与其他网络设备相连从而可与互联网进行通讯。在一个实例中，传输装置106可以为射频(Radio Frequency,RF)模块，其用于通过无线方式与互联网进行通讯。

[0025] 在上述运行环境下，本申请提供了如图2所示的报文清洗方法。图2是根据本申请实施例一的报文清洗方法的流程图。

[0026] 步骤S202，获取待清洗报文的报文类型以及目的地址。

[0027] 本申请步骤S202中，报文类型包括以下一种或几种：TCP SYN(Transmission Control Protocol synchronous，传输控制协议同步)报文、传输控制协议确认TCP ACK(Transmission Control Protocol acknowledge，传输控制协议确认)报文以及传输控制协议复位TCP RST(Transmission Control Protocol reset，传输控制协议复位)报文。目的地址用于指示所述待清洗报文需发送到达的设备。

[0028] 可选地，步骤S202，获取待清洗报文的报文类型以及目的地址可以包括：

[0029] 步骤S10，解析待清洗报文的报头。

[0030] 本申请步骤S10中，为了获取待清洗报文的报文类型和目的地址，首先需要解析出该待清洗报文的报头。

[0031] 步骤S12，基于报文类型对应的字段的偏移量，从待清洗报文中提取报文类型，以及基于目的地址对应的字段的偏移量，从待清洗报文中提取目的地址。

[0032] 本申请步骤S12中，在解析出待清洗报文的报头之后，基于报文类型对应的字段的偏移量，从待清洗报文中提取报文类型，以及基于目的地址对应的字段的偏移量，从待清洗报文中提取目的地址，其中，报文类型对应的字段的偏移量与目的地址对应的字段的偏移量可以从协议中确定。

[0033] 步骤S204，根据报文类型，从预设的配置文件中获取与报文类型对应的第一攻击类型集合，并根据目的地址获取第二攻击类型集合。

[0034] 本申请步骤S204中，对于进入的每个待清洗报文，分析出待清洗报文的报文类型，进而获取到与报文类型对应的第一攻击类型集合(记为AttackSet_1)。需要说明的是，每种攻击类型使用何种报文是确定的，因此，把攻击类型和报文类型的映射关系整理成一份配置文件，即可以在报文清洗时根据待清洗报文的报文类型，反向推测出该待清洗报文可能造成哪些攻击。

[0035] 其中，第一攻击类型集合包含与报文类型对应的攻击类型，攻击类型包括以下一种或几种：syn报文泛洪攻击SYN flood、ack报文泛洪攻击ACK flood、rst报文泛洪攻击RST flood以及udp报文泛洪攻击UDP flood。

[0036] 例如，如表1所示，为上述预设的配置文件，配置文件中包含有报文类型、攻击类型以及报文类型与攻击类型的对应关系：

[0037] 表1

[0038]

序号	报文类型	攻击类型
1	TCP SYN报文	SYN flood
2	TCP ACK报文	ACK flood
3	TCP RST报文	RST flood

[0039] 可选地，根据报文类型，从预设的配置文件中获取与报文类型对应的第一攻击类型集合可以包括：

[0040] 步骤S20，从预设的配置文件中，查找报文类型对应的攻击类型。

[0041] 本申请步骤S20中，预设的配置文件中包含有报文类型与攻击类型之间的对应关系，以待清洗报文的报文类型为TCP ACK报文为例，在表1中查找出报文类型为TCP ACK报文对应的攻击类型ACK flood。

[0042] 步骤S22，生成包含报文类型对应的攻击类型的第一攻击类型集合。

[0043] 本申请步骤S22中，仍以待清洗报文的报文类型为TCP ACK报文为例，基于从表1查找出的攻击类型ACK flood，生成第一攻击类型集合，即AttackSet_1＝{ACK flood}。

[0044] 进一步地，第二攻击类型集合包含目的地址所指向的设备在预设时间段内受到的攻击类型。

[0045] 例如，对于目的地址所指向的设备，黑客正在实施DDOS攻击(Distributed Denial of Service，是指攻击者通过控制大量的僵尸主机，向被攻击目标发送大量精心构造的攻击报文，造成被攻击者所在网络的链路拥塞、系统资源耗尽，从而使被攻击者产生拒绝向正常用户的请求提供服务的效果)，而且黑客同时发动了多种类型的DDOS攻击，例如有SYN flood、RST flood以及UDP flood，那么，第二攻击类型集合(记为AttackSet_2)中就会有{SYN flood，RST flood，UDP flood}。

[0046] 需要补充的是，第一攻击类型集合的权重值可以是从报文清洗装置获取到的，第二攻击类型集合的权重值可以是预先设置的，也可以不预先设置，而使用默认值，其中，权重值可以用来指示后续生成的清洗策略链的排列组成，后续实施例中会进行详细描述，此处不作赘述。

[0047] 步骤S206，根据第一攻击类型集合和第二攻击类型集合，生成对应于待清洗报文的清洗策略链。

[0048] 本申请步骤S206中，在获取到第一攻击类型集合和第二攻击类型集合之后，可以根据第一攻击类型集合和第二攻击类型集合，生成对应于待清洗报文的清洗策略链。

[0049] 可选地，步骤S206，根据第一攻击类型集合和第二攻击类型集合，生成对应于待清洗报文的清洗策略链可以包括：

[0050] 步骤S30，计算第一攻击类型集合与第二攻击类型集合的交集，得到第三攻击类型

集合。

[0051] 本申请步骤S30中，第三攻击类型集合中包含第一攻击类型集合与第二攻击类型集合中相同的攻击类型。

[0052] 仍以待清洗报文的报文类型为TCP ACK报文为例，AttackSet_1＝{ACK flood}，AttackSet_2＝{SYN flood,RST flood,ACK flood}，计算AttackSet_1与AttackSet_2的交集，得到第三攻击类型集合(记为AttackSet_3)为{ACK flood}。

[0053] 步骤S32，根据第三攻击类型集合，生成清洗策略链。

[0054] 本申请步骤S32中，在得到第三攻击类型集合之后，可以基于第三攻击类型集合中每个攻击类型的权重值，生成针对于待清洗报文的清洗策略链。

[0055] 可选地，步骤S32，根据第三攻击类型集合，生成清洗策略链可以包括：

[0056] 步骤S40，获取第三攻击类型集合中各个攻击类型的权重值。

[0057] 本申请步骤S40中，权重值可以是用来衡量某个攻击类型在第一攻击类型集合和第二攻击类型集合中所占比例的一个指标。例如，假设造成SYN flood的TCP SYN报文PPS(Packets per Second，数据包每秒)是10000，造成RST flood的TCP RST报文PPS是5000，造成UDP flood的UDP报文TCP PPS是20000，那么，SYN flood的权重就是2，RST flood的权重就是1，UDP flood的权重是4。权重值也可以是预先设定的，例如设定第一攻击类型集合中的ACK flood的权重是3。

[0058] 步骤S42，按照权重值的大小，对各个攻击类型进行排序。

[0059] 步骤S44，获取排序后的各个攻击类型对应的清洗策略，其中，各个清洗策略的排列顺序与排序后的各个攻击类型的排列顺序一致。

[0060] 本申请步骤S44中，在对各个攻击类型进行排序的基础上，获取排序后的各个攻击类型对应的清洗策略，例如Rule_a,Rule_b,Rule_c,Rule_d。

[0061] 步骤S46，生成包含排序后的各个攻击类型对应的清洗策略的清洗策略链。

[0062] 本申请步骤S46中，最终得到清洗策略链(记为RuleList)，RuleList＝{Rule_a，Rule_b,Rule_c,Rule_d}。

[0063] 又例如，AttackSet_3包含的攻击类型是Attack_1和Attack_2。根据配置文件，Attack_1的清洗策略集合是RuleSet_1，RuleSet_1中包含的清洗策略是Rule_a、Rule_b，Attack_2的清洗策略集合是RuleSet_2，RuleSet_2中包含的清洗策略是Rule_b、Rule_c。

[0064] 1、如果Attack_1的权重高于Attack_2，那么最终策略链RuleList的生成逻辑可以用如下公式来表示：

[0065] RuleList＝{RuleSet_1、RuleSet_2}＝{Rule_a、Rule_b、Rule_b、Rule_c}＝{Rule_a、Rule_b、Rule_c}

[0066] 2、如果Attack_2的权重高于Attack_1，那么最终策略链RuleList的生成逻辑可以用如下公式来表示：

[0067] RuleList＝{RuleSet_2、RuleSet_1}＝{Rule_b、Rule_c、Rule_a、Rule_b}＝{Rule_b、Rule_c、Rule_a}

[0068] 此处需要说明的是，攻击类型的取集合动作是交集，清洗策略的取集合动作是并集。

[0069] 需要补充的是，如果清洗设备不支持权重值，则使用默认权重值，RuleList中的策

略Rule_a、Rule_b、Rule_c，就不需要有先后顺序，只需要简单取交集即可。

[0070] 步骤S208，依据清洗策略链，清洗待清洗报文。

[0071] 本申请步骤S208中，待清洗报文进入清洗策略链时，根据上一步骤生成的清洗策略链，顺序调用每个清洗策略。如果待清洗报文被“丢弃”，则结束清洗策略链，丢弃待清洗报文。如果待清洗报文被“通过”，则根据清洗策略的顺序，调用后续的清洗策略。如果待清洗报文被“接受”，或者通过所有清洗策略后，未被“丢弃”，则将待清洗报文送入出方向通道，转发至原始目的地(即目的地址所指向的设备)。

[0072] 需要补充说明的是，本实施例的报文清洗方法中，所有清洗策略的输入、输出需要保持一致。例如，所有的输入统一为报文的指针，所有的输出统一为针对报文的动作(比如：“接受”、“通过”、“拒绝”)。所有清洗策略统一注册。比如将所有清洗策略的函数指针统一注册到某个全部变量。对所有清洗策略统一编号，程序内部通过编号来引用某个清洗策略，清洗策略链，本质上就是一个元素为策略编号的向量。

[0073] 由上可知，本申请上述实施例一所提供的方案，通过基于待清洗报文的报文类型以及目的地址得到一条对应于待清洗报文的动态的清洗策略链，达到了有针对性地进行报文清洗的目的，从而实现了提高报文清洗效率的技术效果，进而解决了由于策略是事先配置好的造成的清洗设备的清洗效率较低的技术问题。

[0074] 可选地，所述依据所述清洗策略链，清洗所述待清洗报文包括：按照所述清洗策略链中各个清洗策略的顺序，依次调用各个清洗策略对所述待清洗报文进行清洗，以确定是否丢弃所述待清洗报文。

[0075] 进一步地，在确定不丢弃所述待清洗报文的情况下，本实施例的报文清洗方法还可以包括：将所述待清洗报文发送至所述目的地址所指向的设备。

[0076] 由上可知，现有技术存在的由于策略是事先配置好的，即，针对某个被保护的I P，预测其可能遭受的攻击类型，然后把所有对应的策略都查询出，使得报文会进入一些完全不需要进入的策略，造成误清洗，降低清洗设备的清洗效率的问题，本申请提出一种报文清洗方法，通过基于待清洗报文的报文类型以及目的地址得到一条对应于待清洗报文的动态的清洗策略链，达到了有针对性地进行报文清洗的目的，从而实现了提高报文清洗效率的技术效果。

[0077] 需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本申请并不受所描述的动作顺序的限制，因为依据本申请，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本申请所必须的。

[0078] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，或者网络设备等)执行本申请各个实施例所述的方法。

[0079] 实施例2

[0080] 根据本申请实施例，还提供了一种用于实施上述方法实施例的装置实施例，本申请上述实施例所提供的装置可以在计算机终端上运行。

[0081] 图3是根据本申请实施例的报文清洗装置的结构示意图。

[0082] 如图3所示，该报文清洗装置可以包括第一获取单元302、第二获取单元304、生成单元306以及清洗单元308。

[0083] 其中，第一获取单元302，用于获取待清洗报文的报文类型以及目的地址；第二获取单元304，用于根据所述报文类型，从预设的配置文件中获取与所述报文类型对应的第一攻击类型集合，并根据所述目的地址获取第二攻击类型集合，其中，所述第二攻击类型集合包含所述目的地址所指向的设备在预设时间段内受到的攻击类型；生成单元306，用于根据所述第一攻击类型集合和所述第二攻击类型集合，生成对应于所述待清洗报文的清洗策略链；清洗单元308，用于依据所述清洗策略链，清洗所述待清洗报文。

[0084] 由上可知，本申请上述实施例二所提供的方案，通过基于待清洗报文的报文类型以及目的地址得到一条对应于待清洗报文的动态的清洗策略链，达到了有针对性地进行报文清洗的目的，从而实现了提高报文清洗效率的技术效果，进而解决了由于策略是事先配置好的造成的清洗设备的清洗效率较低的技术问题。

[0085] 此处需要说明的是，上述第一获取单元302、第二获取单元304、生成单元306以及清洗单元308对应于实施例一中的步骤S202至步骤S208，四个模块与对应的步骤所实现的示例和应用场景相同，但不限于上述实施例一所公开的内容。需要说明的是，上述模块作为装置的一部分可以运行在实施例一提供的计算机终端10中，可以通过软件实现，也可以通过硬件实现。

[0086] 可选地，如图4所示，所述生成单元306包括：计算模块402和生成模块404。

[0087] 其中，计算模块402，用于计算所述第一攻击类型集合与所述第二攻击类型集合的交集，得到第三攻击类型集合，其中，所述第三攻击类型集合中包含所述第一攻击类型集合与所述第二攻击类型集合中相同的攻击类型；生成模块404，用于根据所述第三攻击类型集合，生成所述清洗策略链。

[0088] 此处需要说明的是，上述计算模块402和生成模块404对应于实施例一中的步骤S30至步骤S32，两个模块与对应的步骤所实现的示例和应用场景相同，但不限于上述实施例一所公开的内容。需要说明的是，上述模块作为装置的一部分可以运行在实施例一提供的计算机终端10中，可以通过软件实现，也可以通过硬件实现。

[0089] 可选地，生成模块404用于执行以下步骤根据所述第三攻击类型集合，生成所述清洗策略链：获取所述第三攻击类型集合中各个攻击类型的权重值；按照所述权重值的大小，对各个攻击类型进行排序；获取排序后的各个攻击类型对应的清洗策略，其中，各个清洗策略的排列顺序与排序后的各个攻击类型的排列顺序一致；生成包含排序后的各个攻击类型对应的清洗策略的所述清洗策略链。

[0090] 可选地，清洗单元308用于执行以下步骤依据所述清洗策略链，清洗所述待清洗报文：按照所述清洗策略链中各个清洗策略的顺序，依次调用各个清洗策略对所述待清洗报文进行清洗，以确定是否丢弃所述待清洗报文。

[0091] 可选地，如图5所示，报文清洗装置还包括：发送单元502，用于在确定不丢弃所述待清洗报文的情况下，将所述待清洗报文发送至所述目的地址所指向的设备。

[0092] 可选地，如图6所示，所述第一获取单元302包括：解析模块602和提取模块604。

[0093] 其中，解析模块602，用于解析所述待清洗报文的报头；提取模块604，用于基于所述报文类型对应的字段的偏移量，从所述待清洗报文中提取所述报文类型，以及基于所述目的地址对应的字段的偏移量，从所述待清洗报文中提取所述目的地址。

[0094] 此处需要说明的是，上述解析模块602和提取模块604对应于实施例一中的步骤S10至步骤S12，两个模块与对应的步骤所实现的示例和应用场景相同，但不限于上述实施例一所公开的内容。需要说明的是，上述模块作为装置的一部分可以运行在实施例一提供的计算机终端10中，可以通过软件实现，也可以通过硬件实现。

[0095] 可选地，所述第二获取单元304用于执行以下步骤根据所述报文类型，从预设的配置文件中获取与所述报文类型对应的第一攻击类型集合：从所述预设的配置文件中，查找所述报文类型对应的攻击类型，其中，所述预设的配置文件中包含有所述报文类型与攻击类型之间的对应关系；生成包含所述报文类型对应的攻击类型的所述第一攻击类型集合。

[0096] 可选地，所述报文类型包括以下一种或几种：传输控制协议同步TCP SYN报文、传输控制协议确认TCP ACK报文以及传输控制协议复位TCP RST报文；所述攻击类型包括以下一种或几种：syn报文泛洪攻击SYN flood、ack报文泛洪攻击ACK flood、rst报文泛洪攻击RST flood以及udp报文泛洪攻击UDP flood。

[0097] 实施例3

[0098] 本申请的实施例可以提供一种计算机终端，该计算机终端可以是计算机终端群中的任意一个计算机终端设备。可选地，在本实施例中，上述计算机终端也可以替换为移动终端等终端设备。

[0099] 可选地，在本实施例中，上述计算机终端可以位于计算机网络的多个网络设备中的至少一个网络设备。

[0100] 在本实施例中，上述计算机终端可以执行报文清洗方法中以下步骤的程序代码：获取待清洗报文的报文类型以及目的地址；根据所述报文类型，从预设的配置文件中获取与所述报文类型对应的第一攻击类型集合，并根据所述目的地址获取第二攻击类型集合，其中，所述第二攻击类型集合包含所述目的地址所指向的设备在预设时间段内受到的攻击类型；根据所述第一攻击类型集合和所述第二攻击类型集合，生成对应于所述待清洗报文的清洗策略链；依据所述清洗策略链，清洗所述待清洗报文。

[0101] 可选地，图7是根据本申请实施例的一种计算机终端的结构框图。如图7所示，该计算机终端A可以包括：一个或多个(图中仅示出一个)处理器702、存储器704、以及传输装置706。

[0102] 其中，存储器704可用于存储软件程序以及模程序块，如本申请实施例中的报文清洗方法及装置对应的程序指令/模程序块，处理器702通过运行存储在存储器704内的软件程序以及模程序块，从而执行各种功能应用以及数据处理，即实现上述的报文清洗方法。存储器704可包括高速随机存储器，还可以包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器704可进一步包括相对于处理器远程设置的存储器，这些远程存储器可以通过网络连接至终端A。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0103] 上述的传输装置706用于经由一个网络接收或者发送数据。上述的网络具体实例

可包括有线网络及无线网络。在一个实例中，传输装置706包括一个网络适配器(Network Interface Controller,NIC)，其可通过网线与其他网络设备与路由器相连从而可与互联网或局域网进行通讯。在一个实例中，传输装置706为射频(Radio Frequency,RF)模块，其用于通过无线方式与互联网进行通讯。

[0104] 其中，具体地，存储器704用于存储预设动作条件和预设权限用户的信息、以及应用程序。

[0105] 处理器702可以通过传输装置调用存储器存储的信息及应用程序，以执行下述步骤：获取待清洗报文的报文类型以及目的地址；根据所述报文类型，从预设的配置文件中获取与所述报文类型对应的第一攻击类型集合，并根据所述目的地址获取第二攻击类型集合，其中，所述第二攻击类型集合包含所述目的地址所指向的设备在预设时间段内受到的攻击类型；根据所述第一攻击类型集合和所述第二攻击类型集合，生成对应于所述待清洗报文的清洗策略链；依据所述清洗策略链，清洗所述待清洗报文。

[0106] 由上可知，本申请上述实施例三所提供的方案，通过基于待清洗报文的报文类型以及目的地址得到一条对应于待清洗报文的动态的清洗策略链，达到了有针对性地进行报文清洗的目的，从而实现了提高报文清洗效率的技术效果，进而解决了由于策略是事先配置好的造成的清洗设备的清洗效率较低的技术问题。

[0107] 可选的，上述处理器702还可以执行如下步骤的程序代码：计算所述第一攻击类型集合与所述第二攻击类型集合的交集，得到第三攻击类型集合，其中，所述第三攻击类型集合中包含所述第一攻击类型集合与所述第二攻击类型集合中相同的攻击类型；根据所述第三攻击类型集合，生成所述清洗策略链。

[0108] 可选的，上述处理器702还可以执行如下步骤的程序代码：获取所述第三攻击类型集合中各个攻击类型的权重值；按照所述权重值的大小，对各个攻击类型进行排序；获取排序后的各个攻击类型对应的清洗策略，其中，各个清洗策略的排列顺序与排序后的各个攻击类型的排列顺序一致；生成包含排序后的各个攻击类型对应的清洗策略的所述清洗策略链。

[0109] 可选的，上述处理器702还可以执行如下步骤的程序代码：按照所述清洗策略链中各个清洗策略的顺序，依次调用各个清洗策略对所述待清洗报文进行清洗，以确定是否丢弃所述待清洗报文。

[0110] 可选的，上述处理器702还可以执行如下步骤的程序代码：将所述待清洗报文发送至所述目的地址所指向的设备。

[0111] 可选的，上述处理器702还可以执行如下步骤的程序代码：解析所述待清洗报文的报头；基于所述报文类型对应的字段的偏移量，从所述待清洗报文中提取所述报文类型，以及基于所述目的地址对应的字段的偏移量，从所述待清洗报文中提取所述目的地址。

[0112] 可选的，上述处理器702还可以执行如下步骤的程序代码：从所述预设的配置文件中，查找所述报文类型对应的攻击类型，其中，所述预设的配置文件中包含有所述报文类型与攻击类型之间的对应关系；生成包含所述报文类型对应的攻击类型的所述第一攻击类型集合。

[0113] 本领域普通技术人员可以理解，图7所示的结构仅为示意，计算机终端也可以是智能手机(如Android手机、iOS手机等)、平板电脑、掌声电脑以及移动互联网设备(Mobile

Internet Devices,MID)、PAD等终端设备。图7其并不对上述电子装置的结构造成限定。例如,计算机终端10还可包括比图7中所示更多或者更少的组件(如网络接口、显示装置等),或者具有与图7所示不同的配置。

[0114] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令终端设备相关的硬件来完成,该程序可以存储于一计算机可读存储介质中,存储介质可以包括:闪存盘、只读存储器(Read-Only Memory,ROM)、随机存取器(Random Access Memory,RAM)、磁盘或光盘等。

[0115] 实施例4

[0116] 本申请的实施例还提供了一种存储介质。可选地,在本实施例中,上述存储介质可以用于保存上述实施例一所提供的报文清洗方法所执行的程序代码。

[0117] 可选地,在本实施例中,上述存储介质可以位于计算机网络中计算机终端群中的任意一个计算机终端中,或者位于移动终端群中的任意一个移动终端中。

[0118] 可选地,在本实施例中,存储介质被设置为存储用于执行以下步骤的程序代码:获取待清洗报文的报文类型以及目的地址;根据所述报文类型,从预设的配置文件中获取与所述报文类型对应的第一攻击类型集合,并根据所述目的地址获取第二攻击类型集合,其中,所述第二攻击类型集合包含所述目的地址所指向的设备在预设时间段内受到的攻击类型;根据所述第一攻击类型集合和所述第二攻击类型集合,生成对应于所述待清洗报文的清洗策略链;依据所述清洗策略链,清洗所述待清洗报文。

[0119] 可选地,存储介质还被设置为存储用于执行以下步骤的程序代码:计算所述第一攻击类型集合与所述第二攻击类型集合的交集,得到第三攻击类型集合,其中,所述第三攻击类型集合中包含所述第一攻击类型集合与所述第二攻击类型集合中相同的攻击类型;根据所述第三攻击类型集合,生成所述清洗策略链。

[0120] 可选地,存储介质还被设置为存储用于执行以下步骤的程序代码:获取所述第三攻击类型集合中各个攻击类型的权重值;按照所述权重值的大小,对各个攻击类型进行排序;获取排序后的各个攻击类型对应的清洗策略,其中,各个清洗策略的排列顺序与排序后的各个攻击类型的排列顺序一致;生成包含排序后的各个攻击类型对应的清洗策略的所述清洗策略链。

[0121] 可选地,存储介质还被设置为存储用于执行以下步骤的程序代码:按照所述清洗策略链中各个清洗策略的顺序,依次调用各个清洗策略对所述待清洗报文进行清洗,以确定是否丢弃所述待清洗报文。

[0122] 可选地,存储介质还被设置为存储用于执行以下步骤的程序代码:将所述待清洗报文发送至所述目的地址所指向的设备。

[0123] 可选地,存储介质还被设置为存储用于执行以下步骤的程序代码:解析所述待清洗报文的报头;基于所述报文类型对应的字段的偏移量,从所述待清洗报文中提取所述报文类型,以及基于所述目的地址对应的字段的偏移量,从所述待清洗报文中提取所述目的地址。

[0124] 可选地,存储介质还被设置为存储用于执行以下步骤的程序代码:从所述预设的配置文件中,查找所述报文类型对应的攻击类型,其中,所述预设的配置文件中包含有所述报文类型与攻击类型之间的对应关系;生成包含所述报文类型对应的攻击类型的所述第一

攻击类型集合。

[0125] 可选地，在本实施例中，上述存储介质可以包括但不限于：U盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

[0126] 可选地，本实施例中的具体示例可以参考上述实施例1中所描述的示例，本实施例在此不再赘述。

[0127] 上述本申请实施例序号仅仅为了描述，不代表实施例的优劣。

[0128] 在本申请的上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

[0129] 在本申请所提供的几个实施例中，应该理解到，所揭露的订单信息的处理装置，可通过其它的方式实现。其中，以上所描述的装置实施例仅仅是示意性的，例如所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，单元或模块的间接耦合或通信连接，可以是电性或其它的形式。

[0130] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0131] 另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0132] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可为个人计算机、服务器或者网络设备等)执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

[0133] 以上所述仅是本申请的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本申请原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本申请的保护范围。

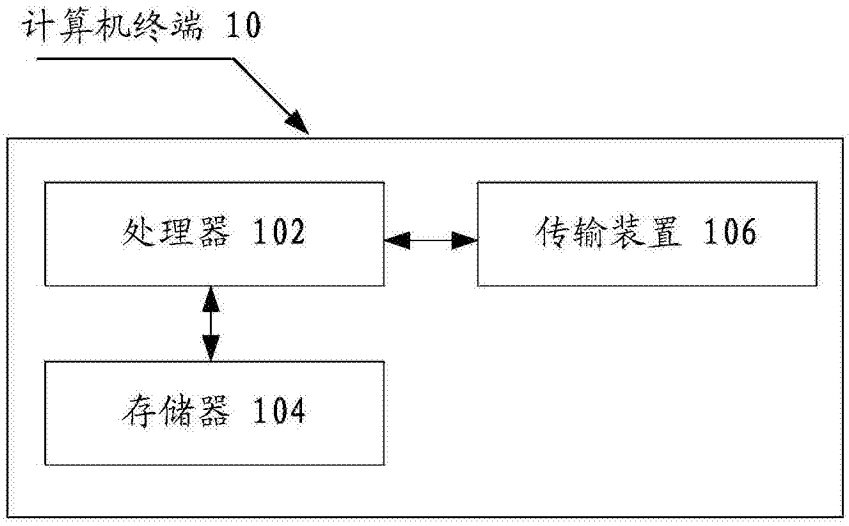

计算机终端 10
处理器 102
传输装置 106
存储器 104

图1

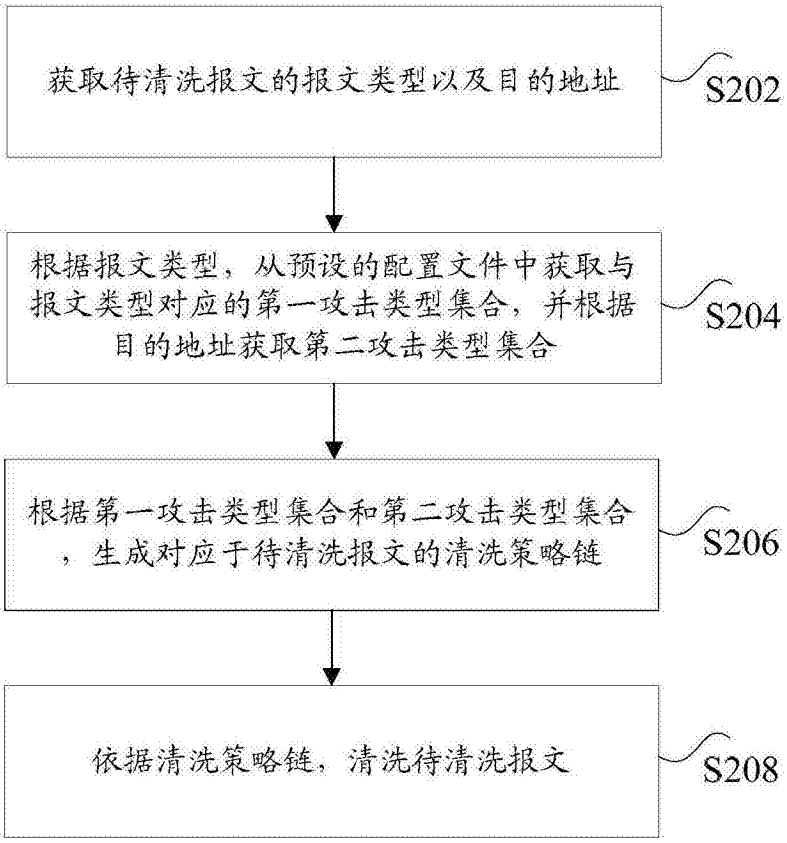

获取待清洗报文的报文类型以及目的地址
S202
根据报文类型，从预设的配置文件中获取与报文类型对应的第一攻击类型集合，并根据目的地址获取第二攻击类型集合
S204
根据第一攻击类型集合和第二攻击类型集合，生成对应于待清洗报文的清洗策略链
S206
依据清洗策略链，清洗待清洗报文
S208

图2

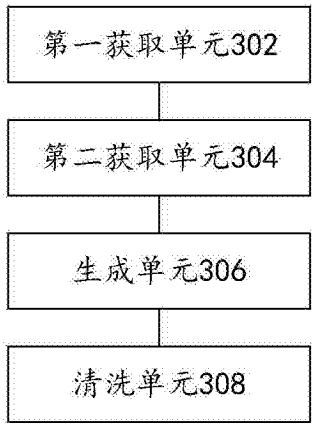

第一获取单元302
第二获取单元304
生成单元306
清洗单元308

图3

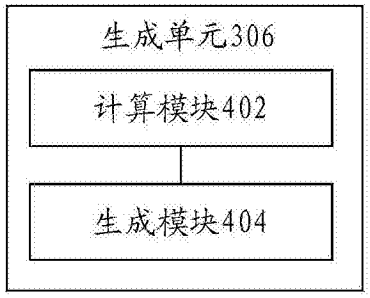
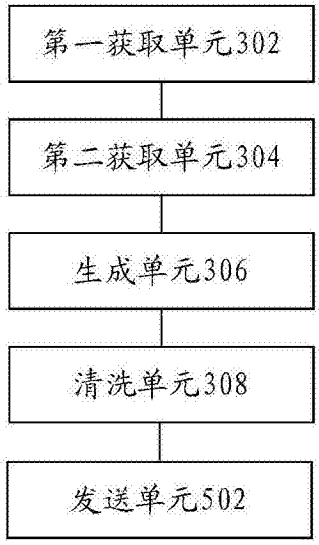

生成单元306
计算模块402
生成模块404

图4


第一获取单元302
第二获取单元304
生成单元306
清洗单元308
发送单元502

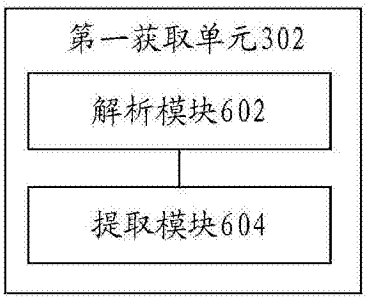

第一获取单元302
解析模块602
提取模块604

图6

图5

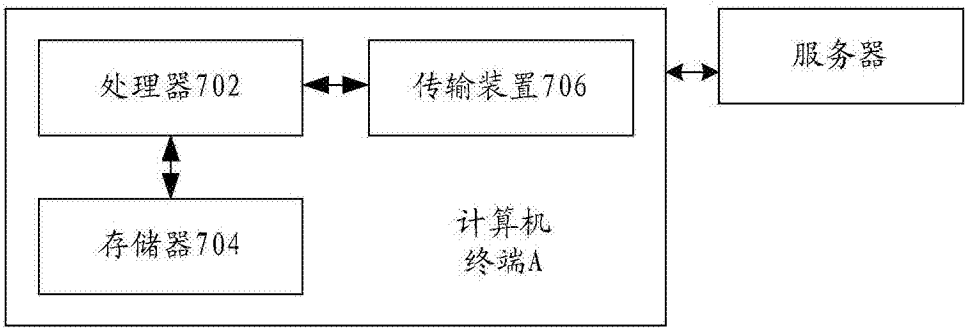

处理器702
传输装置706
服务器
存储器704
计算机
终端A

图7