(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 107426211 A
(43)申请公布日 2017.12.01

(21)申请号 201710613907.9

(22)申请日 2017.07.25

(71)申请人 北京长亭科技有限公司
地址 100083 北京市海淀区学院路甲5号1幢三层1#厂房西区2-007

(72)发明人 刘超 朱文雷 吴雷 李昌志 刘金钊 张酉夫 李扬

(74)专利代理机构 北京金思港知识产权代理有限公司 11349
代理人 邵毓琴 赵勇

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

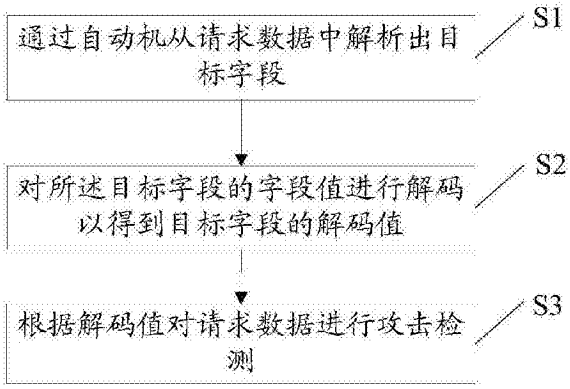
权利要求书2页 说明书11页 附图5页

(54)发明名称

网络攻击的检测方法及装置、终端设备和计算机存储介质

(57)摘要

本发明实施方式提供了网络攻击的检测方法及装置、终端设备和计算机存储介质，涉及网络安全技术领域。其中，所述网络攻击的检测方法包括：通过自动机从请求数据中解析出目标字段；对所述目标字段的字段值进行解码，以得到所述目标字段的解码值；根据所述解码值对所述请求数据进行攻击检测。在本发明提供的技术方案中，通过自动机对请求数据进行解析，因此，能够高效率地执行请求数据的解析过程。



CN 107426211 A

1.一种网络攻击的检测方法，其特征在于，所述方法包括：

通过自动机从请求数据中解析出目标字段；

对所述目标字段的字段值进行解码，以得到所述目标字段的解码值；

根据所述解码值对所述请求数据进行攻击检测。

2.如权利要求1所述的方法，其特征在于，通过自动机从请求数据中解析出目标字段包括：

通过第一自动机直接从所述请求数据中解析出所述目标字段。

3.如权利要求1所述的方法，其特征在于，通过自动机从请求数据中解析出目标字段包括：

通过第一自动机从请求数据中解析出载体字段；

通过第二自动机从所述载体字段的字段值中解析出所述目标字段。

4.如权利要求2或3所述的方法，其特征在于，所述方法还包括：

基于与所述请求数据对应的通信标准构建所述第一自动机。

5.如权利要求3所述的方法，其特征在于，所述方法还包括：

基于与所述载体字段对应的通信标准构建所述第二自动机。

6.如权利要求5所述的方法，其特征在于，基于与所述载体字段对应的通信标准构建所述第二自动机包括：

从内容类型的维度，确定一个或多个请求体通信标准；

对应于所述一个或多个请求体通信标准，构建一个或多个所述第二自动机。

7.如权利要求6所述的方法，其特征在于，通过第二自动机从所述载体字段的字段值中解析出目标字段包括：

确定所述请求体字段的疑似内容类型；

根据所述疑似内容类型选取第二自动机；

通过选取出的第二自动机从所述请求体字段的字段值中解析出目标字段。

8.如权利要求7所述的方法，其特征在于，确定所述请求体字段的疑似内容类型包括：

将所述请求体字段的字段值与设定的媒体格式特征进行匹配；

根据匹配成功的媒体格式特征，确定所述请求体字段的疑似内容类型。

9.一种网络攻击的检测装置，其特征在于，所述装置包括：

解析模块，用于通过自动机从请求数据中解析出目标字段；

解码模块，用于对所述目标字段的字段值进行解码，以得到所述目标字段的解码值；

检测模块，用于根据所述解码值对所述请求数据进行攻击检测。

10.如权利要求9所述的装置，其特征在于，

所述解析模块用于通过以下方式实现通过自动机从请求数据中解析出目标字段：通过第一自动机直接从所述请求数据中解析出所述目标字段。

11.如权利要求9所述的装置，其特征在于，所述解析模块包括：

载体字段解析单元，用于通过第一自动机从请求数据中解析出载体字段；

目标字段解析单元，用于通过第二自动机从所述载体字段的字段值中解析出所述目标字段。

12.如权利要求10或11所述的装置，其特征在于，所述装置还包括：

第一自动机构建模块，用于基于与所述请求数据对应的通信标准构建所述第一自动机。

13.如权利要求11所述的装置，其特征在于，所述装置还包括：

第二自动机构建模块，用于基于与所述载体字段对应的通信标准构建所述第二自动机。

14.如权利要求13所述的装置，其特征在于，所述第二自动机构建模块包括：

确定单元，用于从内容类型的维度，确定一个或多个请求体通信标准；

构建单元，用于对应于所述一个或多个请求体通信标准，构建一个或多个所述第二自动机。

15.如权利要求14所述的装置，其特征在于，所述目标字段解析单元包括：

确定组件，用于确定所述请求体字段的疑似内容类型；

选取组件，用于根据所述疑似内容类型选取第二自动机；

解析组件，用于通过选取出的第二自动机从所述请求体字段的字段值中解析出目标字段。

16.如权利要求15所述的装置，其特征在于，所述确定组件包括：

匹配子组件，用于将所述请求体字段的字段值与设定的媒体格式特征进行匹配；

确定子组件，用于根据匹配成功的媒体格式特征，确定所述请求体字段的疑似内容类型。

17.一种终端设备，包括存储器和处理器；其中，

所述存储器用于存储一条或多条计算机指令，其中，所述一条或多条计算机指令被所述处理器执行时能够实现如权利要求1至8中任一项所述的方法。

18.一种计算机存储介质，用于存储一条或多条计算机指令，其中，当所述一条或多条计算机指令被执行时能够实现如权利要求1至8中任一项所述的方法。

网络攻击的检测方法及装置、终端设备和计算机存储介质

技术领域

[0001] 本发明涉及网络安全技术领域，更为具体而言，涉及网络攻击的检测方法及装置、终端设备和计算机存储介质。

背景技术

[0002] Web(网络)应用防火墙(WAF)会对被保护的Web应用的网络请求进行检测，发现其中存在的威胁，并采取相应的告警或拦截行为。WAF本身不应该对其保护的Web应用造成功能上的影响，即必须要满足高效检测、低误报和低漏报等要求。现有的检测技术主要有基于规则的检测技术和基于语法分析的检测技术。对于基于规则的检测技术而言，为了能够检测出新的攻击或者减少误报，需要不断的增加和修改正则表达式，由此导致其维护成本会越来越高，从而降低检测的效率。同时，由于提取攻击模式作为检测规则的过程需要基于已有的攻击样本，所以基于规则的检测技术难以拥有对未知攻击的检测能力。而基于语法分析的检测技术可以在一定程度上解决基于规则的检测技术的部分问题，但其仍然存在一些缺陷，例如，现有的检测技术存在对HTTP(HyperText Transfer Protocol，超文本传输协议)请求的解析效率低的问题。

发明内容

[0003] 本发明实施方式提供了网络攻击的检测方法及装置、终端设备和计算机存储介质，用以解决现有技术中所存在的上述技术问题。

[0004] 第一方面，本发明实施方式提供了一种网络攻击的检测方法。

[0005] 具体地，所述方法包括：

[0006] 通过自动机从请求数据中解析出目标字段；

[0007] 对所述目标字段的字段值进行解码，以得到所述目标字段的解码值；

[0008] 根据所述解码值对所述请求数据进行攻击检测。

[0009] 由于在本发明中，通过自动机对请求数据进行解析，因此，本发明能够高效率地执行请求数据的解析过程。

[0010] 结合第一方面，在本发明的一些实现方式中，通过自动机从请求数据中解析出目标字段包括：

[0011] 通过第一自动机直接从所述请求数据中解析出所述目标字段。

[0012] 结合第一方面，在本发明的一些实现方式中，通过自动机从请求数据中解析出目标字段包括：

[0013] 通过第一自动机从请求数据中解析出载体字段；

[0014] 通过第二自动机从所述载体字段的字段值中解析出所述目标字段。

[0015] 结合第一方面，在本发明的一些实现方式中，所述方法还包括：

[0016] 基于与所述请求数据对应的通信标准构建所述第一自动机。

[0017] 结合第一方面，在本发明的一些实现方式中，所述方法还包括：

[0018] 基于与所述载体字段对应的通信标准构建所述第二自动机。

[0019] 结合第一方面，在本发明的一些实现方式中，基于与所述载体字段对应的通信标准构建所述第二自动机包括：

[0020] 从内容类型(content-type)的维度，确定一个或多个请求体通信标准；

[0021] 对应于所述一个或多个请求体通信标准，构建一个或多个所述第二自动机。

[0022] 结合第一方面，在本发明的一些实现方式中，通过第二自动机从所述载体字段的字段值中解析出目标字段包括：

[0023] 确定所述请求体字段的疑似内容类型；

[0024] 根据所述疑似内容类型选取第二自动机；

[0025] 通过选取出的第二自动机从所述请求体字段的字段值中解析出目标字段。

[0026] 由于本发明对请求体可能的内容类型进行分析，并执行与分析出的内容类型对应的解析处理，因此能够有效防止攻击者利用协议绕过攻击检测。

[0027] 结合第一方面，在本发明的一些实现方式中，确定所述请求体字段的疑似内容类型包括：

[0028] 将所述请求体字段的字段值与设定的媒体格式特征进行匹配；

[0029] 根据匹配成功的媒体格式特征，确定所述请求体字段的疑似内容类型。

[0030] 第二方面，本发明实施方式提供了一种网络攻击的检测装置。

[0031] 具体地，所述装置包括：

[0032] 解析模块，用于通过自动机从请求数据中解析出目标字段；

[0033] 解码模块，用于对所述目标字段的字段值进行解码，以得到所述目标字段的解码值；

[0034] 检测模块，用于根据所述解码值对所述请求数据进行攻击检测。

[0035] 由于在本发明中，通过自动机对请求数据进行解析，因此，本发明能够高效率地执行请求数据的解析过程。

[0036] 结合第二方面，在本发明的一些实现方式中，

[0037] 所述解析模块用于通过以下方式实现通过自动机从请求数据中解析出目标字段：通过第一自动机直接从所述请求数据中解析出所述目标字段。

[0038] 结合第二方面，在本发明的一些实现方式中，所述解析模块包括：

[0039] 载体字段解析单元，用于通过第一自动机从请求数据中解析出载体字段；

[0040] 目标字段解析单元，用于通过第二自动机从所述载体字段的字段值中解析出所述目标字段。

[0041] 结合第二方面，在本发明的一些实现方式中，所述装置还包括：

[0042] 第一自动机构建模块，用于基于与所述请求数据对应的通信标准构建所述第一自动机。

[0043] 结合第二方面，在本发明的一些实现方式中，所述装置还包括：

[0044] 第二自动机构建模块，用于基于与所述载体字段对应的通信标准构建所述第二自动机。

[0045] 结合第二方面，在本发明的一些实现方式中，所述第二自动机构建模块包括：

[0046] 确定单元，用于从内容类型的维度，确定一个或多个请求体通信标准；

[0047] 构建单元，用于对应于所述一个或多个请求体通信标准，构建一个或多个所述第二自动机。

[0048] 结合第二方面，在本发明的一些实现方式中，所述目标字段解析单元包括：

[0049] 确定组件，用于确定所述请求体字段的疑似内容类型；

[0050] 选取组件，用于根据所述疑似内容类型选取第二自动机；

[0051] 解析组件，用于通过选取出的第二自动机从所述请求体字段的字段值中解析出目标字段。

[0052] 由于本发明对请求体可能的内容类型进行分析，并执行与分析出的内容类型对应的解析处理，因此能够有效防止攻击者利用协议绕过攻击检测。

[0053] 结合第二方面，在本发明的一些实现方式中，所述确定组件包括：

[0054] 匹配子组件，用于将所述请求体字段的字段值与设定的媒体格式特征进行匹配；

[0055] 确定子组件，用于根据匹配成功的媒体格式特征，确定所述请求体字段的疑似内容类型。

[0056] 第三方面，本发明实施方式提供了一种终端设备。

[0057] 所述终端设备包括存储器和处理器；其中，

[0058] 所述存储器用于存储一条或多条计算机指令，其中，所述一条或多条计算机指令被所述处理器执行时能够实现上述任一项网络攻击的检测方法。

[0059] 由于在本发明中，通过自动机对请求数据进行解析，因此，本发明能够高效率地执行请求数据的解析过程。

[0060] 第四方面，本发明实施方式提供了一种计算机存储介质。

[0061] 所述计算机存储介质用于存储一条或多条计算机指令，其中，当所述一条或多条计算机指令被执行时能够实现上述任一项网络攻击的检测方法。

[0062] 由于在本发明中，通过自动机对请求数据进行解析，因此，本发明能够高效率地执行请求数据的解析过程。

[0063] 本发明的这些方面或其他方面在以下具体实施方式的描述中会更加简明易懂。

附图说明

[0064] 为了更清楚地说明本发明实施方式的技术方案，下面将对实施方式描述中所需要使用的附图作一简单的介绍，显而易见地，下面描述中的附图是本发明的一些实施方式，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0065] 图1是根据本发明方法实施方式1的网络攻击的检测方法的流程图；

[0066] 图2是根据本发明实施方式的有限状态自动机的结构示意图；

[0067] 图3示出了图1所示的处理S1的一种实施方式；

[0068] 图4示出了图3所示的处理S12的一种实施方式；

[0069] 图5示出了图4所示的处理S121的一种实施方式；

[0070] 图6是根据本发明产品实施方式1的网络攻击的检测装置的结构示意图；

[0071] 图7是根据本发明产品实施方式2的网络攻击的检测装置的结构示意图；

[0072] 图8示出了图7所示的解析模块12’的一种实施方式；

[0073] 图9是根据本发明产品实施方式3的网络攻击的检测装置的结构示意图；

[0074] 图10示出了图9所示的第二自动机构建模块16'的一种实施方式；

[0075] 图11示出了图7所示的目标字段解析单元122'的一种实施方式；

[0076] 图12示出了图11所示的确定组件1221'的一种实施方式。

具体实施方式

[0077] 以下结合附图和具体实施方式对本发明的各个方面进行详细阐述。其中，在本发明的各个具体实施方式中，众所周知的操作过程、程序模块、单元及其相互之间的连接、链接、通信或操作没有示出或未作详细说明。

[0078] 并且，所描述的特征、架构或功能可在一个或一个以上实施方式中以任何方式组合。

[0079] 此外，本领域技术人员应当理解，下述的各种实施方式只用于举例说明，而非用于限制本发明的保护范围。本领域的技术人员还可以容易理解，本文所述和附图所示的各实施方式中的程序模块、单元或步骤可以按多种不同配置进行组合和设计。

[0080] 对于未在本说明书中进行具体说明的技术术语，除非另有特定说明，都应以本领域最宽泛的意思进行解释。

[0081] 在本发明的说明书和权利要求书及上述附图中的描述的一些流程中，包含了按照特定顺序出现的多个操作，但是应该清楚了解，这些操作可以不按照其在本文中出现的顺序来执行或并行执行，操作的标号如101、102等，仅仅是用于区分开各个不同的操作，标号本身不代表任何的执行顺序。另外，这些流程可以包括更多或更少的操作，并且这些操作可以按顺序执行或并行执行。需要说明的是，本文中的“第一”、“第二”等描述，是用于区分不同的消息、设备、模块等，不代表先后顺序，也不限定“第一”和“第二”是不同的类型。

[0082] 下面将结合附图，对本发明实施方式中的技术方案进行清楚、完整地描述，显然，所描述的实施方式仅仅是本发明的一部分实施方式，而不是全部的实施方式。基于本发明中的实施方式，本领域技术人员在没有付出创造性劳动的前提下所获得的所有其他实施方式，都属于本发明保护的范围。

[0083] 【方法实施方式1】

[0084] 图1是根据本发明方法实施方式1的网络攻击的检测方法的流程图。参见图1，在本实施方式中，所述方法包括：

[0085] S1：通过自动机从请求数据中解析出目标字段。

[0086] S2：对所述目标字段的字段值进行解码，以得到所述目标字段的解码值。

[0087] S3：根据所述解码值对所述请求数据进行攻击检测。

[0088] 字段值是指请求数据中某一字段的取值。例如，“GET”为请求数据中方法字段的字段值。

[0089] 解码值是指对请求数据中某一字段值进行解码后所得到的解码结果。

[0090] 其中，所述自动机用于解析请求数据(例如HTTP请求)，在线性的时间内对整个请求数据完成扫描，并分析出请求数据的各组成部分以用于后续的检测过程。

[0091] 下面以有限状态自动机为例，对本发明中自动机的运行过程进行具体说明。

[0092] 有限状态自动机由状态结点和转移弧构成，每条转移弧都是从一个状态结点指向

另一个状态结点的有向边，转移弧上的标记表示自动机在前一个状态如果接收到该标记作为输入则会转移到后一个状态。如图2所示，自动机开始处于初态，即状态1，当接收到输入“G”时，便会转移到状态2，当从初态开始接收到输入串“GET”时，便会到达状态4，并在从状态3转移到状态4的过程中完成请求方法的记录，即“GET”。

[0093] 由于在本发明中，通过自动机对请求数据进行解析，因此，本发明能够高效率地执行请求数据的解析过程。

[0094] 【方法实施方式2】

[0095] 本实施方式所提供的方法包括方法实施方式1中的全部内容，在此不再赘述。其中，所述目标字段的直接载体可以是请求数据也可以是请求数据中的字段值。

[0096] 若目标字段的直接载体是请求数据，则通过以下方式实现处理S1：

[0097] 通过第一自动机直接从所述请求数据中解析出所述目标字段。

[0098] 相应地，在本实施方式所提供的方法中，基于与请求数据对应的通信标准构建所述第一自动机。

[0099] 如图3所示，若目标字段的直接载体是请求数据中的字段值，则通过以下方式实现处理S1：

[0100] S11：通过所述第一自动机从请求数据中解析出载体字段(含有目标字段的请求数据字段)。

[0101] S12：通过第二自动机从所述载体字段的字段值中解析出所述目标字段。

[0102] 相应地，在本实施方式所提供的方法中，基于与所述载体字段对应的通信标准构建所述第二自动机。

[0103] 所述载体字段例如包括请求体字段，相应地，基于与所述载体字段对应的通信标准构建所述第二自动机包括：

[0104] (1)从内容类型(content-type)的维度，确定一个或多个请求体通信标准；

[0105] (2)对应于所述一个或多个请求体通信标准，构建一个或多个所述第二自动机。

[0106] 【方法实施方式3】

[0107] 本实施方式所提供的方法包括方法实施方式2中的全部内容，在此不再赘述。如图4所示，在本实施方式中，S12包括以下处理：

[0108] S121：确定请求体字段的疑似内容类型(请求体字段可能的内容类型)。

[0109] S122：根据所述疑似内容类型选取第二自动机。

[0110] S123：通过选取出的第二自动机从所述请求体字段的字段值中解析出目标字段。

[0111] 由于本发明对请求体可能的内容类型进行分析，并执行与分析出的内容类型对应的解析处理，因此能够有效防止攻击者利用协议绕过攻击检测。

[0112] 【方法实施方式4】

[0113] 本实施方式所提供的方法包括了方法实施方式3中的全部内容，在此不再赘述。其中，如图5所示，在本实施方式中，通过以下方式实现处理S121：

[0114] S1211：将所述请求体字段的字段值与设定的媒体格式特征进行匹配。

[0115] S1212：根据匹配成功的媒体格式特征，确定所述请求体字段的疑似内容类型。

[0116] 媒体格式特征是指互联网媒体格式(例如JSON(JavaScript Object Notation，一种轻量级的数据交换格式)格式、XML(Extensible Markup Language，可扩展标记语言)格

式、表单格式等)的结构特征。

[0117] 【方法实施方式5】

[0118] 下面以对HTTP请求进行检测为例,对本实施方式提供的网络攻击的检测方法进行具体描述。在本实施方式中,所述方法包括:

[0119] 步骤1:通过自动机从HTTP请求中解析出目标字段。

[0120] 具体地,可以采用方法实施方式2至方法实施方式4中任一项所记载的方式实现步骤1,在此不再赘述。

[0121] 步骤2:对所述目标字段的字段值进行深度解码,以得到所述目标字段的结果解码值。

[0122] 所述结果解码值是指对请求数据中某一字段值进行深度解码后最终得到的解码结果。

[0123] 由于在本发明中,对请求数据中目标字段的字段值进行深度解码,因此,能够有效应对多层编码的情形,提高解码能力,进而提升了网络攻击检测的准确性。

[0124] 步骤3:根据所述结果解码值对该HTTP请求进行风险预估。若经所述风险预估确定该HTTP请求存在网络攻击的风险,则执行步骤4,若经所述风险预估确定该HTTP请求不存在网络攻击的风险,则结束当前流程。

[0125] 由于在本发明中,在进行攻击检测前先对请求数据进行风险预估,因此能够及时终止对正常的请求数据进行网络攻击检测,从而提高了网络攻击的检测效率。

[0126] 步骤4:对该HTTP请求进行攻击检测。

[0127] 针对上述步骤2而言,具体可以通过以下方式实现:

[0128] (1)对所述目标字段的字段值进行解码操作,以得到所述目标字段的中间解码值。

[0129] (2)判断所述中间解码值是否需要进行进一步解码操作,若是,则对所述中间解码值进行解码操作,以得到所述目标字段的另一中间解码值,并返回执行:判断所述中间解码值是否需要进行进一步解码操作;若否,则确定所述中间解码值为所述结果解码值。

[0130] 所述中间解码值是指在深度解码的过程中得到的解码结果。

[0131] 具体地,可以通过以下方式实现判断所述中间解码值是否需要进行进一步解码操作:

[0132] (1)根据与所述中间解码值对应的编码方式,更新所述目标字段的多层编码可能性参数。

[0133] 例如,先根据编码树确定所述编码方式的权重值,再根据所述权重值更新所述多层编码可能性参数。其中,所述编码树中各结点为相应父结点下可能的编码方式,结点记载了相应编码方式的权重值,该编码树可以基于网络流量数据和web(网络)应用的处理机制构建而成。

[0134] (2)根据更新后的多层编码可能性参数和设定阈值之间的比较结果,判断所述中间解码值是否需要进行进一步解码操作。

[0135] 由于在本发明中,在对中间解码值进行解码操作前,先对当前多层编码的可能性进行评估,因此能够及时终止可能性较低的深度解码,从而提高解码效率。

[0136] 另外,就解码操作而言,在本实施方式中,可以通过下述方式实现对所述目标字段的字段值进行解码操作:

[0137] (1)将所述字段值与设定的编码特征进行匹配。

[0138] 所述编码特征例如为某一编码方式中特有的编码符号，例如“%”。

[0139] (2)对所述字段值执行与匹配成功的编码特征对应的解码操作。

[0140] 若某一解码操作失败，则结束相应的解码路径，但仍继续尝试其他可能的解码方式。

[0141] 由于在本发明中，将字段值与设定的编码特征进行匹配，因此能够实现对编码方式进行智能化分析，从而保证良好的解码效果。

[0142] 当然，本领域的技术人员也可以基于类似的方式对中间解码值进行解码操作，具体而言，将中间解码值与设定的编码特征进行匹配；对中间解码值执行与匹配成功的编码特征对应的解码操作。

[0143] 针对步骤3而言，具体可以通过以下方式实现：利用自动机识别所述结果解码值是否存在网络攻击特征，若是，则确定该HTTP请求存在网络攻击的风险，若否，则确定该HTTP请求不存在网络攻击的风险。若该自动机识别出结果解码值存在网络攻击特征，则记录下与存在的网络攻击特征对应的网络攻击类型，以便于在步骤4中，针对自动机记录下的网络攻击类型有针对性的执行攻击检测。

[0144] 此外，该自动机例如为基于各种网络攻击特征而构造的确定性的有限状态自动机，由此可以实现仅需一次扫描即可分析出所有可能存在的网络攻击类型。

[0145] 并且，在本实施方式中，还可以根据自定义的流量限制规则执行流量整形处理。其中，该流量限制规则例如记载有：不允许出现的请求头、对请求头个数的限制规则、或者对请求头长度的限制规则。产品的用户可以根据自身web应用的需求，设置定制化的流量限制规则。

[0146] 【产品实施方式1】

[0147] 图6是根据本发明产品实施方式1的网络攻击的检测装置的结构示意图。参见图6，在本实施方式中，网络攻击的检测装置10包括：解析模块11、解码模块12和检测模块13，具体地：

[0148] 解析模块11用于通过自动机从请求数据中解析出目标字段。

[0149] 解码模块12用于对解析模块11解析出的目标字段的字段值进行解码，以得到所述目标字段的解码值。

[0150] 检测模块13用于根据解码模块12得到的解码值对所述请求数据进行攻击检测。

[0151] 由于在本发明中，通过自动机对请求数据进行解析，因此，本发明能够高效率地执行请求数据的解析过程。

[0152] 【产品实施方式2】

[0153] 图7是根据本发明产品实施方式2的网络攻击的检测装置的结构示意图。在本实施方式中，所述目标字段的直接载体可以是请求数据也可以是请求数据中的字段值。相应地，如图7所示，网络攻击的检测装置10’包括：解析模块11’、解析模块12’、解码模块13’和检测模块14’，具体地：

[0154] 解析模块11’用于在目标字段的直接载体为请求数据的情形下，通过第一自动机直接从所述请求数据中解析出所述目标字段。

[0155] 解析模块12’用于在目标字段的直接载体为请求数据中的字段值的情形下，通过

第一自动机和第二自动机从请求数据中解析出所述目标字段。具体而言，如图8所示，解析模块12’包括：载体字段解析单元121’和目标字段解析单元122’，具体地：

[0156] 载体字段解析单元121’用于通过所述第一自动机从请求数据中解析出载体字段。

[0157] 目标字段解析单元122’用于通过第二自动机从载体字段解析单元121’解析出的载体字段的字段值中解析出所述目标字段。

[0158] 解码模块13’和检测模块14’分别同产品实施方式1中的解码模块12和检测模块13，在此不再赘述。

[0159] 【产品实施方式3】

[0160] 本实施方式所提供的网络攻击的检测装置包括产品实施方式2中的全部内容，在此不再赘述。如图9所示，在本实施方式中，网络攻击的检测装置10’还包括：第一自动机构建模块15’和第二自动机构建模块16’，具体地：

[0161] 第一自动机构建模块15’用于基于与所述请求数据对应的通信标准构建所述第一自动机。

[0162] 第二自动机构建模块16’用于基于与所述载体字段对应的通信标准构建所述第二自动机。

[0163] 【产品实施方式4】

[0164] 本实施方式所提供的网络攻击的检测装置包括产品实施方式3中的全部内容，在此不再赘述。所述载体字段例如包括请求体字段，相应地，如图10所示，第二自动机构建模块16’包括：确定单元161’和构建单元162’，具体地：

[0165] 确定单元161’用于从内容类型(content-type)的维度，确定一个或多个请求体通信标准。

[0166] 构建单元162’用于对应于确定单元161’确定出的一个或多个请求体通信标准，构建一个或多个所述第二自动机。

[0167] 【产品实施方式5】

[0168] 本实施方式所提供的网络攻击的检测装置包括产品实施方式2至产品实施方式4中任一项的全部内容，在此不再赘述。如图11所示，在本实施方式中，目标字段解析单元122’包括：确定组件1221’、选取组件1222’和解析组件1223’，具体地：

[0169] 确定组件1221’用于确定所述请求体字段的疑似内容类型。

[0170] 选取组件1222’用于根据确定组件1221’确定出的疑似内容类型选取第二自动机。

[0171] 解析组件1223’用于通过选取组件1222’选取出的第二自动机从所述请求体字段的字段值中解析出目标字段。

[0172] 由于本发明对请求体可能的内容类型进行分析，并执行与分析出的内容类型对应的解析处理，因此能够有效防止攻击者利用协议绕过攻击检测。

[0173] 【产品实施方式6】

[0174] 本实施方式所提供的网络攻击的检测装置包括产品实施方式5中的全部内容，在此不再赘述。如图12所示，在本实施方式中，确定组件1221’包括：匹配子组件12211’和确定子组件12212’，具体地：

[0175] 匹配子组件12211’用于将所述请求体字段的字段值与设定的媒体格式特征进行匹配。

[0176] 确定子组件12212'用于根据匹配子组件12211'匹配成功的媒体格式特征，确定所述请求体字段的疑似内容类型。

[0177] 本发明的实施方式还提供了一种终端设备，包括存储器和处理器；其中，

[0178] 所述存储器用于存储一条或多条计算机指令，其中，所述一条或多条计算机指令被所述处理器执行时能够实现如方法实施方式1至方法实施方式5中任意一项所述的方法。

[0179] 此外，本发明的实施方式还提供一种计算机存储介质，所述计算机存储介质用于存储一条或多条计算机指令，其中，当所述一条或多条计算机指令被执行时能够实现如方法实施方式1至方法实施方式5中任意一项所述的方法。

[0180] 本领域的技术人员可以清楚地了解到本发明可全部通过软件实现，也可借助软件结合硬件平台的方式来实现。基于这样的理解，本发明的技术方案对背景技术做出贡献的全部或者部分可以以软件产品的形式体现出来，所述计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，智能手机或者网络设备等)执行本发明各个实施方式或者实施方式的某些部分所述的方法。

[0181] 本文中所使用的“软件”等词均指一般意义上的任意类型的计算机编码或者计算机可执行指令集，可以运行所述编码或者指令集来使计算机或其他处理器程序化以执行如上所述的本发明的技术方案的各个方面。此外，需要说明的是，根据实施方式的一个方面，在执行时实施本发明的技术方案的方法的一个或多个计算机程序不必须要在一台计算机或处理器上，而是可以分布于多个计算机或者处理器中的模块中，以执行本发明的技术方案的各个方面。

[0182] 计算机可执行指令可以有许多形式，如程序模块，可以由一台或多台计算机或是其他设备执行。一般地，程序模块包括例程、程序、对象、组件以及数据结构等等，执行特定的任务或是实施特定的抽象数据类型。特别地，在各种实施方式中，程序模块进行的操作可以根据各个不同实施方式的需要进行结合或者拆分。

[0183] 并且，本发明的技术方案可以体现为一种方法，并且已经提供了所述方法的至少一个示例。可以通过任何一种合适的顺序执行动作，所述动作表现为所述方法中的一部分。因此，实施方式可以构造成可以按照与所示出的执行顺序不同的顺序执行动作，其中，可以包括同时地执行一些动作(尽管在示出的实施方式中，这些动作是连续的)。

[0184] 本文所给出的和使用的定义，应当对照字典、通过引用而并入的文档中的定义、和/或其通常意思进行理解。

[0185] 在权利要求书中以及上述的说明书中，所有的过度短语，例如“包括”、“具有”、“包含”、“承载”、“具有”、“涉及”、“主要由…组成”以及类似词语是应理解为是开放式的，即，包含但不限于。

[0186] 本发明说明书中使用的术语和措辞仅仅为了举例说明，并不意味构成限定。本领域技术人员应当理解，在不脱离所公开的实施方式的基本原理的前提下，对上述实施方式中的各细节可进行各种变化。因此，本发明的范围只由权利要求确定，在权利要求中，除非另有说明，所有的术语应按最宽泛合理的意思进行理解。

[0187] 以上具体描述了本发明的各种不同的实施方式，下面以另一种形式描述本发明各实施方式的技术方案的各个方面或特征，并且其不限于下述一系列段落，为了清楚起见，可

给这些段落中的一些或所有段落指定字母数字。这些段落中的每一段可以以任何合适的方式与一个或多个其他段落的内容组合。在不限定合适的组合中的一些的实例的条件下，下文中的一些段落特别引用其他段落并且进一步限定其他段落。

[0188] A1、一种网络攻击的检测方法，所述方法包括：

[0189] 通过自动机从请求数据中解析出目标字段；

[0190] 对所述目标字段的字段值进行解码，以得到所述目标字段的解码值；

[0191] 根据所述解码值对所述请求数据进行攻击检测。

[0192] A2、如A1所述的方法中，通过自动机从请求数据中解析出目标字段包括：

[0193] 通过第一自动机直接从所述请求数据中解析出所述目标字段。

[0194] A3、如A1所述的方法中，通过自动机从请求数据中解析出目标字段包括：

[0195] 通过第一自动机从请求数据中解析出载体字段；

[0196] 通过第二自动机从所述载体字段的字段值中解析出所述目标字段。

[0197] A4、如A2或A3所述的方法中，所述方法还包括：

[0198] 基于与所述请求数据对应的通信标准构建所述第一自动机。

[0199] A5、如A3所述的方法中，所述方法还包括：

[0200] 基于与所述载体字段对应的通信标准构建所述第二自动机。

[0201] A6、如A5所述的方法中，基于与所述载体字段对应的通信标准构建所述第二自动机包括：

[0202] 从内容类型的维度，确定一个或多个请求体通信标准；

[0203] 对应于所述一个或多个请求体通信标准，构建一个或多个所述第二自动机。

[0204] A7、如A6所述的方法中，通过第二自动机从所述载体字段的字段值中解析出目标字段包括：

[0205] 确定所述请求体字段的疑似内容类型；

[0206] 根据所述疑似内容类型选取第二自动机；

[0207] 通过选取出的第二自动机从所述请求体字段的字段值中解析出目标字段。

[0208] A8、如A7所述的方法中，确定所述请求体字段的疑似内容类型包括：

[0209] 将所述请求体字段的字段值与设定的媒体格式特征进行匹配；

[0210] 根据匹配成功的媒体格式特征，确定所述请求体字段的疑似内容类型。

[0211] B9、一种网络攻击的检测装置，所述装置包括：

[0212] 解析模块，用于通过自动机从请求数据中解析出目标字段；

[0213] 解码模块，用于对所述目标字段的字段值进行解码，以得到所述目标字段的解码值；

[0214] 检测模块，用于根据所述解码值对所述请求数据进行攻击检测。

[0215] B10、如B9所述的装置中，所述解析模块用于通过以下方式实现通过自动机从请求数据中解析出目标字段：通过第一自动机直接从所述请求数据中解析出所述目标字段。

[0216] B11、如B9所述的装置中，所述解析模块包括：

[0217] 载体字段解析单元，用于通过第一自动机从请求数据中解析出载体字段；

[0218] 目标字段解析单元，用于通过第二自动机从所述载体字段的字段值中解析出所述目标字段。

[0219] B12、如B10或B11所述的装置中，所述装置还包括：

[0220] 第一自动机构建模块，用于基于与所述请求数据对应的通信标准构建所述第一自动机。

[0221] B13、如B11所述的装置中，所述装置还包括：

[0222] 第二自动机构建模块，用于基于与所述载体字段对应的通信标准构建所述第二自动机。

[0223] B14、如B13所述的装置中，所述第二自动机构建模块包括：

[0224] 确定单元，用于从内容类型的维度，确定一个或多个请求体通信标准；

[0225] 构建单元，用于对应于所述一个或多个请求体通信标准，构建一个或多个所述第二自动机。

[0226] B15、如B14所述的装置中，所述目标字段解析单元包括：

[0227] 确定组件，用于确定所述请求体字段的疑似内容类型；

[0228] 选取组件，用于根据所述疑似内容类型选取第二自动机；

[0229] 解析组件，用于通过选取出的第二自动机从所述请求体字段的字段值中解析出目标字段。

[0230] B16、如B15所述的装置中，所述确定组件包括：

[0231] 匹配子组件，用于将所述请求体字段的字段值与设定的媒体格式特征进行匹配；

[0232] 确定子组件，用于根据匹配成功的媒体格式特征，确定所述请求体字段的疑似内容类型。

[0233] C17、一种终端设备，包括存储器和处理器；其中，

[0234] 所述存储器用于存储一条或多条计算机指令，其中，所述一条或多条计算机指令被所述处理器执行时能够实现如A1至A8中任一项所述的方法。

[0235] D18、一种计算机存储介质，用于存储一条或多条计算机指令，其中，当所述一条或多条计算机指令被执行时能够实现如A1至A8中任一项所述的方法。

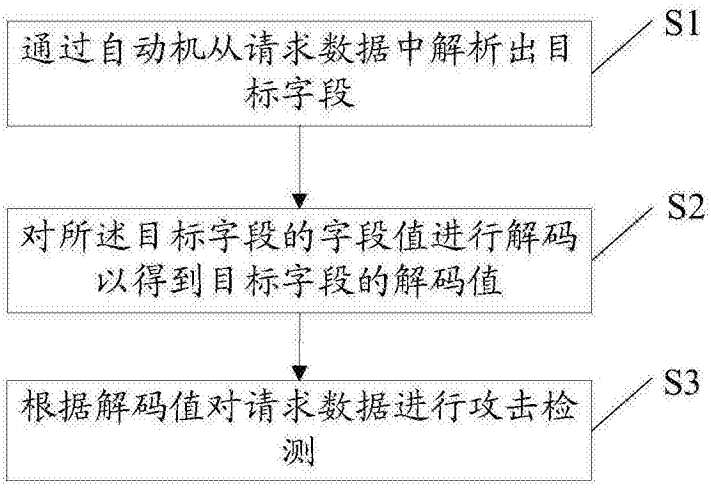

通过自动机从请求数据中解析出目标字段
S1
对所述目标字段的字段值进行解码以得到目标字段的解码值
S2
根据解码值对请求数据进行攻击检测
S3

图1

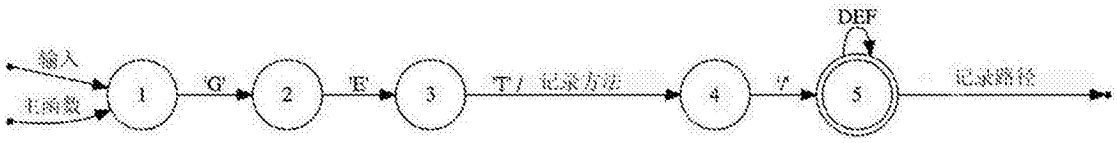

输入
1
G
2
E
3
T/ 记录方法
4
/
DEF
5
记录路径

图2

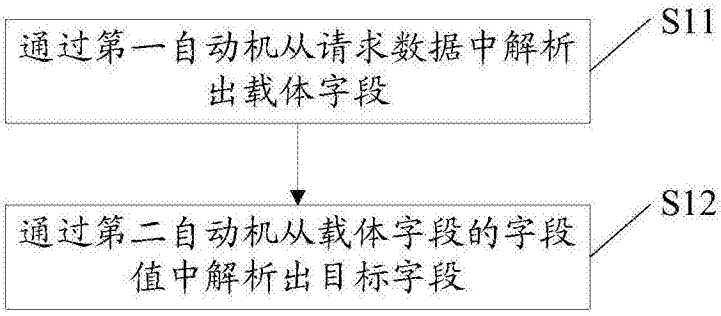

通过第一自动机从请求数据中解析出载体字段
S11
通过第二自动机从载体字段的字段值中解析出目标字段
S12

图3

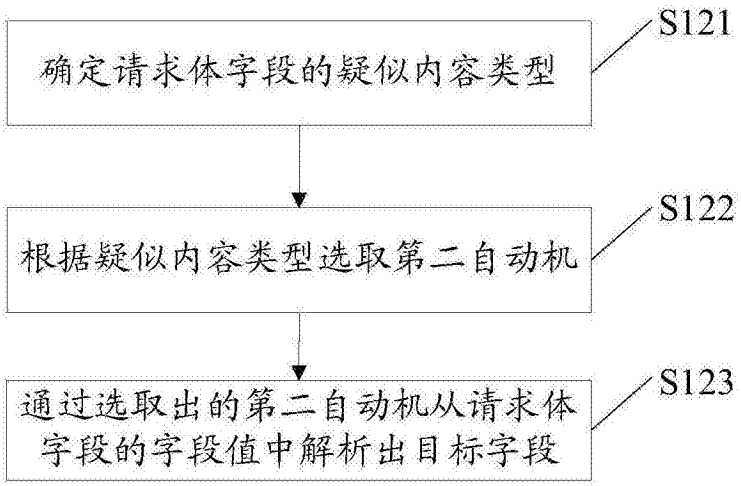

确定请求体字段的疑似内容类型
S121
根据疑似内容类型选取第二自动机
S122
通过选取出的第二自动机从请求体字段的字段值中解析出目标字段
S123

图4

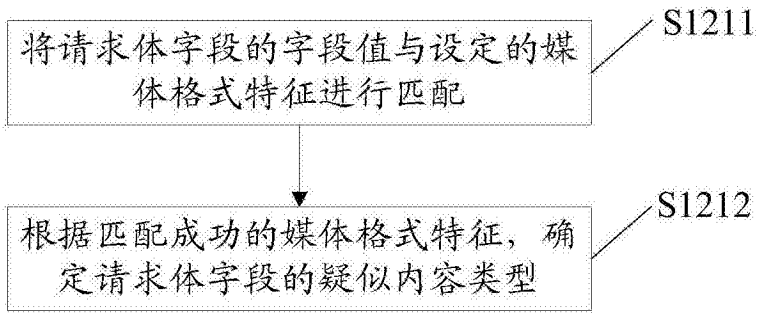

将请求体字段的字段值与设定的媒体格式特征进行匹配
S1211
根据匹配成功的媒体格式特征，确定请求体字段的疑似内容类型
S1212

图5

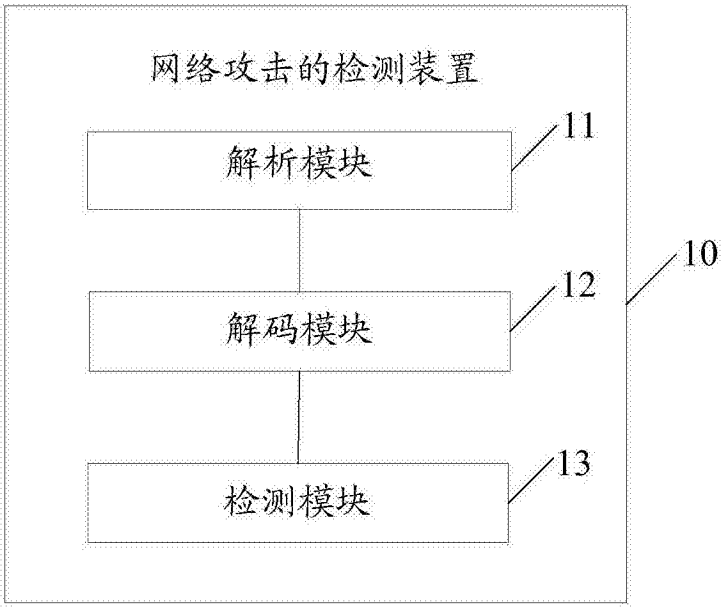

网络攻击的检测装置
解析模块
11
解码模块
12
检测模块
13
10

图6

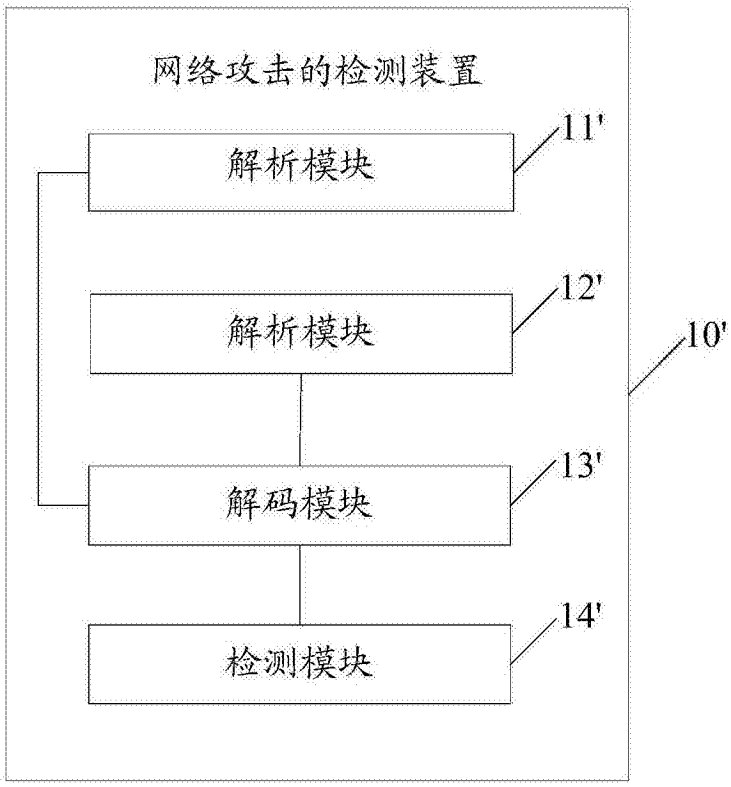

网络攻击的检测装置
解析模块
11'
解析模块
12'
10'
解码模块
13'
检测模块
14'

图7

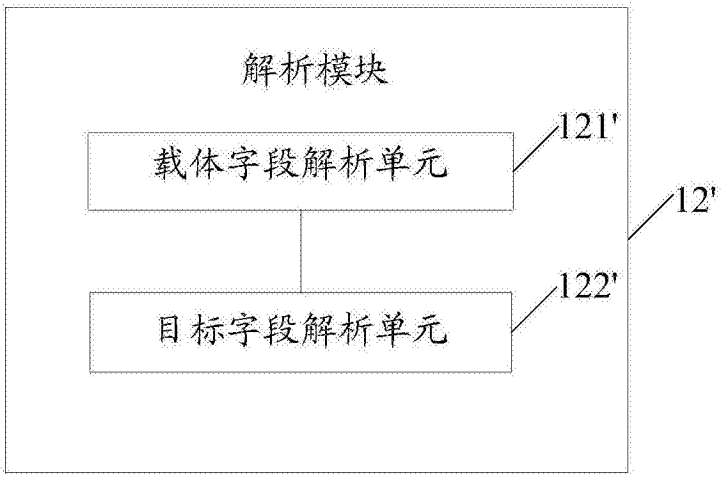

解析模块
载体字段解析单元
121'
12'
目标字段解析单元
122'

图8

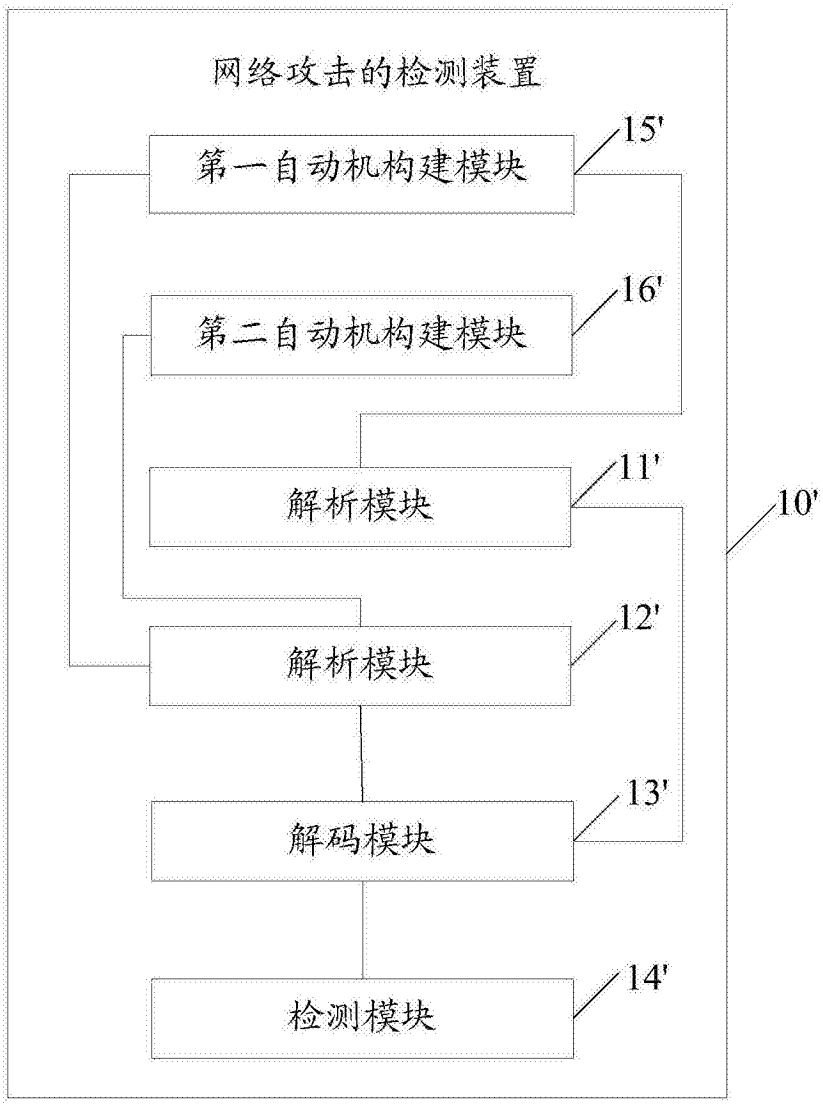

网络攻击的检测装置
第一自动机构建模块
15'
第二自动机构建模块
16'
解析模块
11'
10'
解析模块
12'
解码模块
13'
检测模块
14'

图9

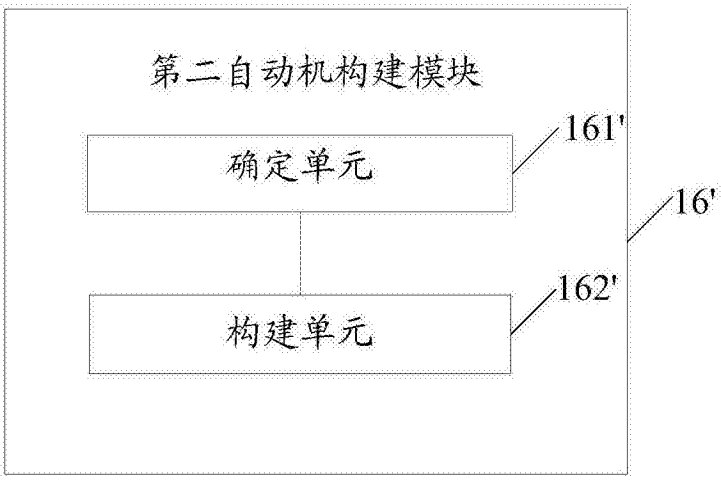

第二自动机构建模块
确定单元
161'
16'
构建单元
162'

图10

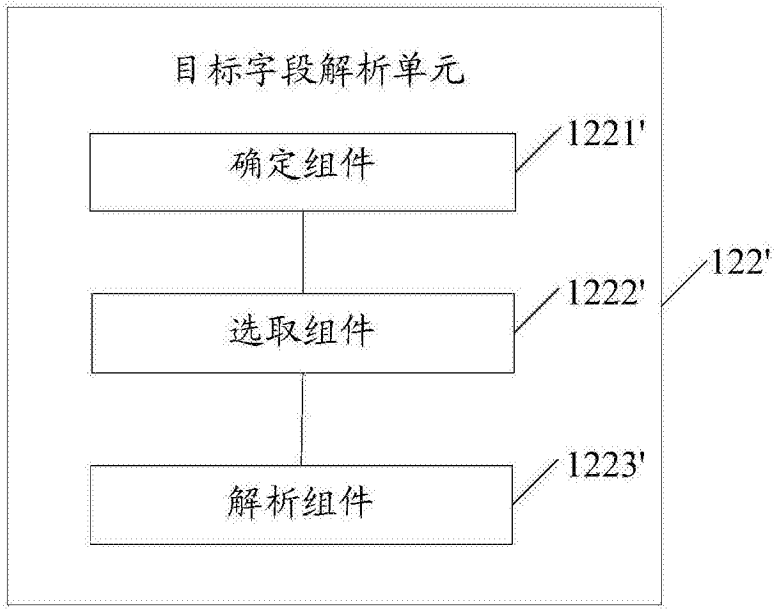

目标字段解析单元
确定组件
1221'
选取组件
1222'
122'
解析组件
1223'

图11

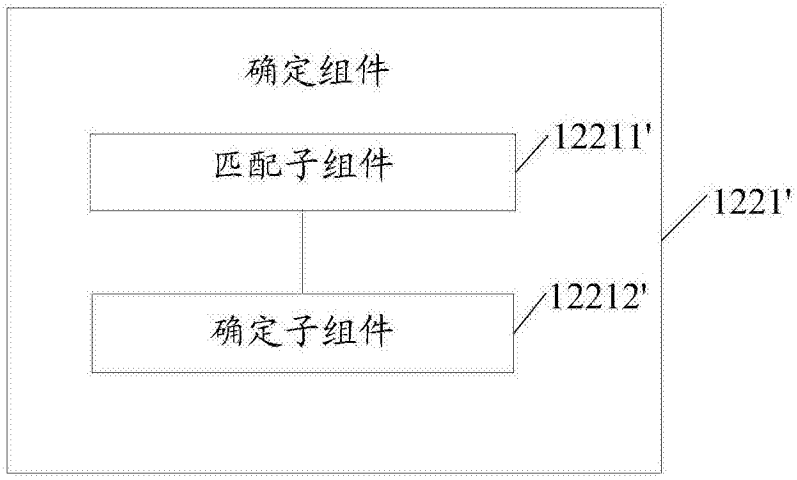

确定组件
匹配子组件
12211'
1221'
确定子组件
12212'

图12