(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116389274 A
(43)申请公布日 2023.07.04

(21)申请号 202211549481.2

(22)申请日 2022.12.05

(71)申请人 中国电信股份有限公司
地址 100033 北京市西城区金融大街31号

(72)发明人 槐正 徐冬冬 崔明 姬照中 付迎鑫 徐锐 王健 魏丫丫 徐蕾

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319
专利代理师 任亚娟

(51)Int.Cl.
H04L 41/12(2022.01)
H04L 41/0663(2022.01)
H04L 41/14(2022.01)

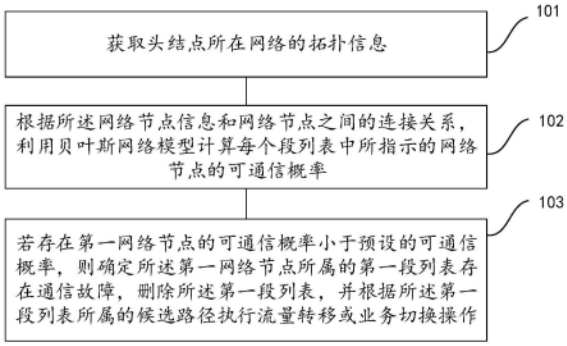
权利要求书3页 说明书11页 附图3页

(54)发明名称

故障处理方法、装置、电子设备及可读存储介质

(57)摘要

本发明实施例提供了一种故障处理方法、装置、电子设备和可读存储介质，所述方法包括：获取头结点所在网络的拓扑信息；根据所述网络节点信息和网络节点之间的连接关系，利用贝叶斯网络模型计算每个段列表中所指示的网络节点的可通信概率；若存在第一网络节点的可通信概率小于预设的可通信概率，则确定所述第一网络节点所属的第一段列表存在通信故障，删除所述第一段列表，并根据所述第一段列表所属的候选路径执行流量转移或业务切换操作。通过上述方法，分别实现了对于头结点的故障的智能感知以及在感知到头节点故障之后的及时处理和报文的有序调度，总体实现了对于头结点故障的系统化处理，提高了报文转发的安全性和效率。



CN 116389274 A

1.一种故障处理方法,其特征在于,所述方法包括:

获取头结点所在网络的拓扑信息,所述拓扑信息包括网络节点信息和网络节点之间的连接关系,所述头结点中配置有至少一个段列表,所述段列表用于指示网络报文在所述网络中的转发路径,所述段列表中包括段标识,所述段标识用于指示所述转发路径中的网络节点;

根据所述网络节点信息和网络节点之间的连接关系,利用贝叶斯网络模型计算每个段列表中所指示的网络节点的可通信概率;

若存在第一网络节点的可通信概率小于预设的可通信概率,则确定所述第一网络节点所属的第一段列表存在通信故障,删除所述第一段列表,并根据所述第一段列表所属的候选路径执行流量转移或业务切换操作,所述流量转移用于将所述第一段列表的流量分配给其他段列表或候选路径。

2.根据权利要求1所述的方法,其特征在于,所述根据所述网络节点信息和网络节点之间的连接关系,利用贝叶斯网络模型计算每个段列表中所指示的网络节点的可通信概率,包括:

根据所述网络节点信息,计算所述网络中网络节点与周边节点的条件通信概率;

根据所述条件通信概率和所述连接关系,构建所述头结点所在网络的贝叶斯网络模型;

利用所述贝叶斯网络模型,计算由所述头结点至每个段列表中所指示的网络节点的可通信概率。

3.根据权利要求1所述的方法,其特征在于,所述头结点用于标识第一业务策略,所述第一业务策略与候选路径相关联,所述候选路径包括优选路径和备选路径;当段列表没有发生通信故障时,所述段列表按照优选路径进行报文的转发处理;

所述根据所述第一段列表所属的候选路径执行流量转移或业务切换操作,包括:

在所述第一段列表所属的优选路径中的其他段列表没有发生通信故障的情况下,则执行第一流量转移操作,以将所述第一段列表的流量转移到所述其他段列表中。

4.根据权利要求3所述的方法,其特征在于,所述根据所述第一段列表所属的候选路径执行流量转移或业务切换操作,包括:

在所述第一段列表所属的优选路径中的其他段列表均发生通信故障的情况下,则执行第二流量转移操作的情况下,以将所述优选路径中的流量转移到所述备选路径中。

5.根据权利要求3所述的方法,其特征在于,所述根据所述第一段列表所属的候选路径执行流量转移或业务切换操作,包括:

在所述第一段列表所属的优选路径和对应的备选路径中的所有段列表均发生通信故障的情况下,则执行业务切换操作,以将所述第一业务策略切换为其他业务策略。

6.根据权利要求3所述的方法,其特征在于,所述根据所述第一段列表所属的候选路径执行流量转移或业务切换操作,包括:

在所述第一段列表所属的优选路径和备选路径中的所有段列表均发生通信故障且所述头结点的报文中段列表不存在所述候选路径的绑定标识的情况下,根据所述拓扑信息配置第二段列表,并执行第三流量转移操作,以使所述优选路径和备选路径中的流量转移到所述第二段列表所对应的候选路径中。

7.根据权利要求1所述的方法，其特征在于，在所述根据所述第一段列表所属的候选路径执行流量转移或业务切换操作之后，所述方法还包括：

获取所述第一网络节点对应的设备信息；

根据所述设备信息在预设的网络安全库中查询与所述设备信息相关的攻击溯源策略；

根据所述溯源策略进行溯源，找到导致所述第一网络节点发生故障的攻击源。

8.根据权利要求7所述的方法，其特征在于，所述根据所述设备信息在预设的网络安全库中查询与所述设备信息相关的攻击溯源策略，包括：

根据所述设备信息在预设的网络安全库中查询与所述设备信息相关的第一溯源策略；

若所述第一溯源策略为关联溯源策略，则以所述第一溯源策略为输入，利用所述网络安全库查询所述第一溯源策略的子溯源策略；

所述根据所述溯源策略进行溯源，找到导致所述第一网络节点发生故障的攻击源，包括：

执行所述子溯源策略，得到子溯源结果；

按照预设的所述第一溯源策略的关联规则，对所述子溯源结果进行逻辑运算，得到最终溯源结果；

根据所述最终溯源结果定位导致所述第一网络节点发生故障的攻击源。

9.根据权利要求1所述的方法，其特征在于，在所述根据所述第一段列表所属的候选路径执行流量转移或业务切换操作之后，所述方法还包括：

获取所述第一网络节点的故障信息，所述故障信息包括攻击源地址、攻击源端口、故障地址、故障端口和协议信息；

根据所述攻击源地址、攻击源端口、故障地址、故障端口和协议信息构建五元组；

根据所述五元组确定攻击所述第一网络节点的攻击类型；

利用多维数据关联和威胁分析模型库确定并执行所述攻击类型对应的攻击溯源策略，定位被攻击的所述第一网络节点。

10.一种故障处理装置，其特征在于，所述装置包括：

拓扑信息获取模块，用于获取头结点所在网络的拓扑信息，所述拓扑信息包括网络节点信息和网络节点之间的连接关系，所述头结点中配置有至少一个段列表，所述段列表用于指示网络报文在所述网络中的转发路径，所述段列表中包括段标识，所述段标识用于指示所述转发路径中的网络节点；

贝叶斯网络模型模块，用于根据所述网络节点信息和网络节点之间的连接关系，利用贝叶斯网络模型计算每个段列表中所指示的网络节点的可通信概率；

调度模块，用于若存在第一网络节点的可通信概率小于预设的可通信概率，则确定所述第一网络节点所属的第一段列表存在通信故障，删除所述第一段列表，并根据所述第一段列表所属的候选路径执行流量转移或业务切换操作，所述流量转移用于将所述第一段列表的流量分配给其他段列表或候选路径。

11.一种电子设备，其特征在于，包括：

处理器、存储器以及存储在所述存储器上并可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现如权利要求1-9中任一所述的故障处理方法。

12.一种可读存储介质，其特征在于，当所述存储介质中的指令由电子设备的处理器执

行时,使得电子设备能够执行权利要求1-9中一个或多个所述的故障处理方法。

故障处理方法、装置、电子设备及可读存储介质

技术领域

[0001] 本发明属于计算机技术领域，特别是涉及一种故障处理方法、装置、电子设备及可读存储介质。

背景技术

[0002] 随着5G、云业务和物联网等新业务的发展，更多网络设备的接入对于地址扩展的需求和网络可编程的需求都在增加。基于SRv6可以更好地满足这些业务的需求，推动网络业务的发展，促使网络进入一个基于IPv6迎来万物互联的智简网络时代。

[0003] 然而在现有的SRv6组网中进行数据转发过程中，由于业务数据的关系过于复杂，转发过程中依赖层次过多，调度过于复杂，导致报文转发过程中网络节点及路由容易发生故障，报文转发的效率和安全性较低。

发明内容

[0004] 本发明提供一种故障处理方法、装置、电子设备及可读存储介质，以便解决报文转发过程中因为容易出现故障导致的报文转发效率和安全性较低的问题。

[0005] 为了解决上述技术问题，本发明是这样实现的：

[0006] 第一方面，本发明提供一种故障处理方法，所述方法包括：

[0007] 获取头结点所在网络的拓扑信息，所述拓扑信息包括网络节点信息和网络节点之间的连接关系，所述头结点中配置有至少一个段列表，所述段列表用于指示网络报文在所述网络中的转发路径，所述段列表中包括段标识，所述段标识用于指示所述转发路径中的网络节点；

[0008] 根据所述网络节点信息和网络节点之间的连接关系，利用贝叶斯网络模型计算每个段列表中所指示的网络节点的可通信概率；

[0009] 若存在第一网络节点的可通信概率小于预设的可通信概率，则确定所述第一网络节点所属的第一段列表存在通信故障，删除所述第一段列表，并根据所述第一段列表所属的候选路径执行流量转移或业务切换操作，所述流量转移用于将所述第一段列表的流量分配给其他段列表或候选路径。

[0010] 第二方面，本发明提供一种装置，所述装置包括：

[0011] 拓扑信息获取模块，用于获取头结点所在网络的拓扑信息，所述拓扑信息包括网络节点信息和网络节点之间的连接关系，所述头结点中配置有至少一个段列表，所述段列表用于指示网络报文在所述网络中的转发路径，所述段列表中包括段标识，所述段标识用于指示所述转发路径中的网络节点；

[0012] 贝叶斯网络模型模块，用于根据所述网络节点信息和网络节点之间的连接关系，利用贝叶斯网络模型计算每个段列表中所指示的网络节点的可通信概率；

[0013] 调度模块，用于若存在第一网络节点的可通信概率小于预设的可通信概率，则确定所述第一网络节点所属的第一段列表存在通信故障，删除所述第一段列表，并根据所述

第一段列表所属的候选路径执行流量转移或业务切换操作，所述流量转移用于将所述第一段列表的流量分配给其他段列表或候选路径。

[0014] 第三方面，本发明提供一种电子设备，包括：处理器、存储器以及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述处理器执行所述程序时实现上述故障处理方法。

[0015] 第四方面，本发明提供一种可读存储介质，当所述存储介质中的指令由电子设备的处理器执行时，使得电子设备能够执行上述故障处理方法。

[0016] 在本发明实施例中，在获取到头结点所在网络的拓扑信息后，根据所述网络节点信息和网络节点之间的连接关系，利用贝叶斯网络模型计算每个段列表中所指示的网络节点的可通信概率，并通过所述可通信概率与预设的通信概率的对比确定存在故障的第一段列表，最后根据第一段列表所属的候选路径来执行相应的流量转移或业务切换操作。利用贝叶斯网络模型计算可通信概率并进行对比，实现了对于头结点的故障的智能感知，执行流量转移或业务切换操作实现了在感知到头节点故障之后的及时处理和报文的有序调度，提高了报文转发的安全性和效率。

附图说明

[0017] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，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。

[0018] 图1是本发明实施例提供的一种故障处理方法的步骤流程图；

[0019] 图2是本发明实施例的一种网络节点的贝叶斯网络模型的示意图；

[0020] 图3是本发明实施例的一种网络攻击架构图；

[0021] 图4是本发明实施例的一种对头结点的故障溯源的步骤流程图

[0022] 图5是本发明实施例提供的一种故障处理装置的结构图；

[0023] 图6是本发明实施例提供的一种电子设备的结构图。

具体实施方式

[0024] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0025] 图1是本发明实施例提供的一种故障处理方法的步骤流程图，如图1所示，该方法可以包括：

[0026] 步骤101、获取头结点所在网络的拓扑信息。

[0027] 所述拓扑信息包括网络节点信息和网络节点之间的连接关系，所述头结点中配置有至少一个段列表，所述段列表用于指示网络报文在所述网络中的转发路径，所述段列表中包括段标识，所述段标识用于指示所述转发路径中的网络节点。

[0028] 其中，所述头结点是用于标识分布式网络策略(SRv6 Policy)的节点，可以将报文

转发时所需的流量导入当前的SRv6 Policy,具体地,一个SRv6Policy可以指代一个网络业务的执行策略。一个SRv6 Policy对应一个头结点,一个SRv6 Policy可以关联多个候选路径,而一个候选路径可以对应多个段列表。在执行报文转发时,需要在头结点将待转发的网络报文头内封装段列表,所述段列表用于指示网络报文在所述网络中的转发路径,因此可以认为所述头结点中配置有至少一个段列表(segment list),所述段列表中包括段标识(segment id,sid),所述段标识用于指示所述转发路径中的网络节点。具体地,在进行报文转发时,通常需要将指示报文转发路径的段列表封装在报文头中,使得报文沿段列表所记录的路径进行转发。

[0029] 网络拓扑(Network Topology)信息是指用传输介质互连各种设备的物理布局,具体可以指构成网络的成员间特定的物理的即真实的,或者逻辑的即虚拟的排列方式。

[0030] 在SRv网络中,可以根据内部网关协议(Interior Gateway Protocol,IGP)获取头结点所在网络的拓扑信息。进一步地,BGP-LS(Border Gateway Protocol Link State)是基于边界网关协议(Border Gateway Protocol,BGP)来传递IGP链路状态的一种BGP多协议拓展,并且BGP-LS会汇总IGP协议收集的拓扑信息上送给上层控制器,因此头结点所在网络的控制器可以通过BGP-LS收集网络的拓扑信息,更有利于报文转发路径的计算。

[0031] 步骤102、根据所述网络节点信息和网络节点之间的连接关系,利用预先构建的贝叶斯网络模型计算每个段列表中所指示的网络节点的可通信概率。

[0032] 所述网络节点的可通信概率指由头结点到段列表中段标识所指示的网络节点的可通信概率,所述可通信概率用于表示由头结点到段标识所指示的目标网络节点之间的路由是否可达,以及可达的概率。

[0033] 贝叶斯网络模型是一种基于贝叶斯原理的概率图型模型,在本发明实施例中,以网络节点为变量,以网络节点之间的连接关系来表示不同网络节点之间的依赖或关联关系,从而构建起基于头结点所在网络的贝叶斯网络模型,用来预测由头结点到目标节点的可通信概率。具体地,可以按照如下公式计算不同网络节点的联合通信概率即不同网络节点构成的转发路径的可

[0034] 通信概率:$P(x_1,x_2,\cdots,x_k)=P(x_k|x_1,\cdots,x_{k-1})\times P(x_{k-1}|x_1,\cdots,x_{k-2})\times\cdots\times P(x_1)$, (1)

[0035] 其中,x_k表示第k个网络节点,$P(x_1)$表示节点x_1的可通信概率,公式(1)表示不同网络节点构成的转发路径的可通信概率是在x_1-x_k所表示的转发路径上各个节点的局部条件可通信概率的基础上计算得到的。

[0036] 参照图2所示的本发明实施例的一种网络节点的贝叶斯网络模型的示意图,作为公式(1)的示例,其中x_1-x_7分别表示七个网络节点变量,图中的连接线用于表示网络节点之间的连接关系,若要计算报文转发路径为x_1-x_5-x_7之间的可通信概率,则可以根据图示的贝叶斯网络按照下述公式进行计算:

[0037] $P(x_1,x_5,x_7)=P(x_7|x_5,x_1)\times P(x_5|x_1)\times P(x_1)$ (2),

[0038] 其中,公式(1)左边表示报文转发路径为x_1-x_5-x_7的通信概率,$P(x_7|x_5,x_1)$表示在经由节点x_5和x_1的基础上可以到达节点x_7的通信概率,后续以此类推,$P(x_1)$则表示网络节点x_1的可通信概率,单个网络节点的可通信概率在实际网络路由的计算中可以根据网络流量负载等多个因素进行调整,例如在节点x_1正常的情况下,节点x_1的可通信概率为1。

[0039] 按照图2所述示例，在本发明实施例中，所述网络节点信息包括但不限于网络节点的位置信息、网络节点的流量负载信息以及网络节点所连接的链路的负载信息，因此在计算相邻节点之间的可通信概率时，可以将网络节点信息作为网络节点变量加入到贝叶斯网络中去，以计算相邻接点之间的可通信概率。因为贝叶斯网络中所包含的头结点所在网络的信息越多，意味着变量即通信的影响因素越多，那么可通信概率的计算就越精确，可以作为通信概率的影响因素不止网络节点信息，因此对于加入到贝叶斯网络中的变量，本发明不作限定。

[0040] 因此，两个相邻网络节点之间的可通信概率是计算贝叶斯网络任意两个或两个以上节点的可通信概率的基础。进一步地，要计算头结点和目标节点之间的可通信概率，可以通过对头结点和目标节点之间的报文转发路径的可通信概率进行叠加计算得到。

[0041] 基于头结点所在网络的贝叶斯网络模型可以准确地描述不同网络节点之间的相互关系，其中网络节点信息等头结点所在网络的相关变量信息更可以精确描述头结点所在网络中各个变量之间的因果关系，那么对于计算得到的段列表中不同网络节点的可通信概率具有很高的参考价值。进一步地，利用贝叶斯网络计算段标识所指示的网络节点的可通信概率，因为贝叶斯网络反映的是头结点所在网络的整体通信概率分布，因此即使在网络环境波动或获取到的网络节点信息不全面等信息缺失的情况下，依然可以家里建立的通信概率分布模型，精确的预测段列表中不同网络节点的可通信概率。

[0042] 步骤103、若存在第一网络节点的可通信概率小于预设的可通信概率，则确定所述第一网络节点所属的第一段列表存在通信故障，删除所述第一段列表，并根据所述第一段列表所属的候选路径执行流量转移或业务切换操作，所述流量转移用于将所述第一段列表的流量分配给其他段列表或候选路径。

[0043] 在本发明实施例中，在通过步骤102计算得到段列表中所标识的转发路径上的不同网络节点的可通信概率后，可以通过对比预设的可通信概率来判断网络节点是否可路由，若网络节点的可通信概率过低，则确定该网络节点存在通信故障，属于第一网络节点。

[0044] 所述第一段列表是第一网络节点所对应的段标识所属的段列表。所述流量转移是指将段列表或候选路径所分配到的路由流量转移给其他段列表或候选路径，所述业务切换是指在所述头结点所标识的SRv6 Policy关联的路径均发生故障无法进行报文转发时，及时地切换SRv6 Policy，执行其他业务，避免路由故障所带来的网络堵塞等问题。

[0045] 在第一网络节点存在通信故障的情况下，按照第一网络节点对应的报文转发路径不可能实现业务的报文转发，那么所述第一网络节点对应的段标识所属的段列表相应的便属于无效段列表，不能用于指示报文的转发路径，因此需要删除第一段列表，并将所述第一段列表所分配到的流量转移到其他段列表或候选路径中，以避免网络报文在根据无效的段列表进行报文转发时引起连锁的网络故障，及时地删除了报文转发过程中故障项，提高了网络报文转发的效率和安全性。

[0046] 作为示例地，在一个SRv6 Policy中，只要Segment List中有一个SID在拓扑中不存在或者路由不可达即SID所指示的网络节点不可通信，设备就将Segment List的状态置为Down，并删除Segment List表项，同时将删除的Segment List表项的流量转移给其他Segment List表项或候选路径。

[0047] 可选地，步骤102所述根据所述网络节点信息和网络节点之间的连接关系，利用贝

叶斯网络模型计算每个段列表中所指示的网络节点的可通信概率，包括：

[0048] 步骤S100、根据所述网络节点信息，计算所述网络中网络节点与周边节点的条件通信概率；

[0049] 步骤S101、根据所述条件通信概率和所述连接关系，构建所述头结点所在网络的贝叶斯网络模型；

[0050] 步骤S102、利用所述贝叶斯网络模型，计算由所述头结点至每个段列表中所指示的网络节点的可通信概率。

[0051] 其中，所述条件通信概率表示相邻的网络节点之间的可通信概率。根据述条件通信概率和所述连接关系，构建头结点所在网络的贝叶斯网络模型，从而得到头结点所在网络的通信概率分布。获取到头结点所在网络的贝叶斯网络清晰的展现了当前网络的通信概率分布，更直观地表示了头结点所在网络的网络路由情况，更有助于技术人员了解网络的路由情况。

[0052] 在头结点所在网络的贝叶斯网络模型的基础上，可以根据前文所述的公式(1)计算段列表所指示的报文转发路径的可通信概率，但考虑到网络节点之间连接关系的复杂度过高，单一的报文转发路径的可通信概率所反映的信息过于单一，而相比之下以网络节点为衡量单位，通过利用构建好的贝叶斯网络模型计算头结点至每个段列表中所指示的网络节点的可通信概率，具备的可参考价值更高。

[0053] 可选地，所述头结点用于标识第一业务策略，所述第一业务策略与候选路径相关联，所述候选路径包括优选路径和备选路径；当段列表没有发生通信故障时，所述段列表按照优选路径进行报文的转发处理；

[0054] 步骤103所述根据所述第一段列表对应的候选路径执行流量转移或业务切换操作，还包括：

[0055] 步骤S200、在所述第一段列表所属的优选路径中的其他段列表没有发生通信故障的情况下，则执行第一流量转移操作，以将所述第一段列表的流量转移到所述其他段列表中。

[0056] 所述第一业务策略用于指代所述头结点标识的SRv6 Policy，所述优选路径表示在进行报文转发时优先级最高的候选路径，备选路径的优先级低于优选路径。在执行报文转发时，若第一业务策略所对应的段列表没有发生通信故障，所述段列表通常会按照优选路径进行报文的转发。

[0057] 但是，若所述第一段列表所述的优选路径中的其他断裂表没有发生通信故障或优选路径中仅有少数段列表发生通信故障，那么在删除掉发生通信故障的段列表后，可以将分配给被删除的段列表的流量转移给优选路径中的其他段列表即第一流量转移操作，以保证路由资源的充分利用。具体地，可以通过在所述头结点所在的网络中预置一个程序A，当检测到所述第一段列表所属的优选路径中的其他段列表没有发生通信故障时，程序A执行第一流量转移操作。

[0058] 可选地，步骤103所述根据所述第一段列表对应的候选路径执行流量转移或业务切换操作，可以包括：

[0059] 步骤S300、在所述第一段列表所属的优选路径中的其他段列表均发生通信故障的情况下，则执行第二流量转移操作的情况下，以将所述优选路径中的流量转移到所述备选

路径中。

[0060] 若所述第一段列表所属的优选路径所有段列表均发生通信故障，则将分配给优选路径的流量转移到备选路径中即执行第二流量转移操作。具体地，可以通过在所述头结点所在的网络中预置一个程序B，当检测到第一段列表所属的优选路径中的所有段列表均发生通信故障时，程序B通过执行第二流量转移操作。

[0061] 可选地，步骤103所述根据所述第一段列表对应的候选路径执行流量转移或业务切换操作，可以包括：

[0062] 步骤S400、在所述第一段列表所属的优选路径和对应的备选路径中的所有段列表均发生通信故障的情况下，则执行业务切换操作，以将所述第一业务策略切换为其他业务策略。

[0063] 优选路径和对应的备选路径中的所有段列表均发生通信故障，表示第一业务策略在这种情况下无法进行报文转发进而无法进行相应的业务处理，因此需要切换业务策略，避免了路由资源的浪费，将第一业务策略切换为其他业务策略，保证进行网络路由时流量的充分利用。具体地，可以通过在所述头结点所在的网络中预置一个程序C，当优选路径和对应的备选路径中的所有段列表均发生通信故障，执行业务切换操作，保证进行网络路由时网络资源的充分利用。

[0064] 可选地，步骤103所述根据所述第一段列表所属的候选路径执行流量转移或业务切换操作，可以包括：

[0065] 步骤S500、在所述第一段列表所属的优选路径和备选路径中的所有段列表均发生通信故障且所述头结点的报文中不存在所述候选路径的绑定标识的情况下，根据所述拓扑信息配置第二段列表，并执行第三流量转移操作，以使所述优选路径和备选路径中的流量转移到所述第二段列表所对应的候选路径中。

[0066] 所述绑定标识(Binding SID)用于标识整个候选路径，报文中如果携带候选路径对应的Binding SID，则在报文转发时会按照绑定标识所对应的候选路径进行报文转发。

[0067] 当第一业务策略的候选路径中的所有段标识均发生通信故障且头结点的报文中不存在绑定标识时，可以根据步骤101获取的网络拓扑信息或步骤S101所构建的贝叶斯网络模型，以当前网络上不同链路的时延为变量，重新确定新的报文转发路径，并在头结点中为报文配置对应的第二段列表继续进行报文转发，具体地，在本发明实施例中，可以在头结点所在的网络中预置一个程序D执行上述步骤S500所述的操作。

[0068] 可选地，在本发明实施例中，通过在头结点所在的网络中预置程序A、B、C、D，执行步骤S200-S500所述的方法，那么当第一业务策略段列表或优选路径或候选路径发生通信故障时，通过执行对应的预置程序，及时排除发生通信故障的部分，避免局部通信故障所带来的连锁反应，保证网络中的正常路由和网络资源的充分利用。

[0069] 可选地，在步骤103所述根据所述第一段列表所属的候选路径执行流量转移或业务切换操作之后，所述方法可以包括：

[0070] 步骤S600、获取所述第一网络节点对应的设备信息；

[0071] 步骤S601、根据所述设备信息在预设的网络安全库中查询与所述设备信息相关的攻击溯源策略；

[0072] 步骤S602、根据所述溯源策略进行溯源，找到导致所述第一网络节点发生故障的

攻击源。

[0073] 对于头节点故障的处理方法还可以包括对于故障的溯源方法，其中，所述设备信息包括但不限于所述第一网络节点对应的主机资产信息以及对应的漏洞信息。

[0074] 具体地，可以根据第一网络节点的ip确定对应的主机，并查询所述主机被攻击的部分，通过被攻击的部分利用多维数据关联和威胁分析(Multi-dimensional Data Association and Threat Analysis，MDATA)网络安全知识库查询该部分所具有的漏洞，并以所述漏洞为查询条件在MDATA网络安全知识库寻找与该漏洞相关联的攻击威胁并获取有关攻击的溯源策略，最后执行所述溯源策略，就可以溯源到攻击源，并针对攻击源进行相应的安全部署，从而实现对头节点中故障的感知、治愈和溯源的综合处理，极大地提高了网络的安全性和报文转发效率。

[0075] 作为一种示例地，参照图3所示的本发明实施例的一种网络攻击架构图，攻击者利用一个被攻击者远程控制的地址为192.168.134.128计算机作为攻击主机，发现了地址为10.2.1.35的且安装了应用程序E的服务器具有结构化查询语言(Structured Query Language，SQL)注入漏洞，并利用该漏洞向服务器注入一个反弹端口，实现了让服务器通过反弹端口主动与地址为192.168.134.130的控制主机相互通信从而盗取信息的攻击。在攻击事件之后，需要找出攻击者所处网络节点和控制主机的定位信息，可以通过MDATA网络安全知识库查询与应用程序E相关的溯源策略，通过溯源策略定位攻击者所处网络节点和控制主机。

[0076] 可选地，参照图4所示的本发明实施例的一种对头结点的故障溯源的步骤流程图，步骤S601所述根据所述设备信息在预设的网络安全库中查询与所述设备信息相关的攻击溯源策略，可以包括：

[0077] 步骤S700、根据所述设备信息在预设的网络安全库中查询与所述设备信息相关的第一溯源策略

[0078] 步骤S701、若所述第一溯源策略为关联溯源策略，则以所述第一源策略为输入，利用所述网络安全库查询所述第一溯源策略的子溯源策略；

[0079] 相应地，步骤S602所述根据所述溯源策略进行溯源，找到导致所述第一网络节点发生故障的攻击源，包括：

[0080] 步骤S800、执行所述子溯源策略，得到子溯源结果；

[0081] 步骤S801、按照预设的所述第一溯源策略的关联规则，对所述子溯源结果进行逻辑运算，得到最终溯源结果；

[0082] 步骤S802、根据所述最终溯源结果定位导致所述第一网络节点发生故障的攻击源。

[0083] 其中，所述关联溯源策略是指存在多个下位的相互关联的子策略的溯源策略，例如执行策略A可以根据对象不同划分为三个部分B、C、D来分别执行，若针对不同对象执行策略，B、C、D可以作为子策略单独执行，那么策略A可以成为关联策略。而通过多个子策略来解决关联溯源策略的问题时，需要根据关联溯源策略的关联规则将子策略的溯源结果进行逻辑运算，具体地，所述关联规则可以是不同子策略之间的权重比例，当然本发明实施例对此不作限定。

[0084] 在获取到第一网络节点对应的设备信息后，根据设备信息在预设的网络安全库中

查询与第一网络节点发生的故障相关的第一溯源策略，为了进行更加准确的故障溯源，需要确定网络安全库中记载的第一溯源策略是否为关联策略，若是则继续以第一溯源策略为查询条件查询其子溯源策略直到所述自溯源策略不是关联溯源策略，然后递归地执行所述子溯源策略，获取子溯源的结果，并根据关联溯源策略的关联规则综合所述子溯源策略得到最终的溯源结果，并根据溯源结果定位导致所述第一网络节点发生故障的攻击源。

[0085] 通过网络安全库查询溯源策略，并进一步利用关联溯源策略，提高了故障溯源的准确率，与前文所述的头节点故障的处理方法构成了系统的头节点故障处理体系，提高了网络报文转发的安全性和效率。

[0086] 可选地，在步骤103所述根据所述第一段列表所属的候选路径执行流量转移或业务切换操作之后，所述方法可以包括：

[0087] 步骤S900、获取所述第一网络节点的故障信息，所述故障信息包括攻击源地址、攻击源端口、故障地址、故障端口和协议信息；

[0088] 步骤S901、根据所述攻击源地址、攻击源端口、故障地址、故障端口和协议信息构建五元组；

[0089] 步骤S902、根据所述五元组确定攻击所述第一网络节点的攻击类型；

[0090] 步骤S903、利用多维数据关联和威胁分析模型库确定并执行所述攻击类型对应的攻击溯源策略，定位被攻击的所述第一网络节点。

[0091] 图4描述了根据设备信息确定攻击源的溯源方法，相应的，在本发明实施例中，也可以根据网络节点的故障信息来溯源定位网络节点。

[0092] 具体地，可以某种攻击威胁为基础，获取该攻击威胁相关的地址和协议信息，构建基于攻击源地址、攻击源端口、故障地址、故障端口和协议信息的五元组，来确定所述攻击威胁的类型，然后通过在MDATA网络安全知识库查询与所述攻击威胁对应的溯源策略并执行，找出所述攻击威胁所留下的痕迹和位置，最后定位到被攻击的设备。

[0093] 综上所述，本发明提供了一种故障处理方法。在获取到头结点所在网络的拓扑信息后，根据所述网络节点信息和网络节点之间的连接关系，利用贝叶斯网络模型计算每个段列表中所指示的网络节点的可通信概率，并通过所述可通信概率与预设的通信概率的对比确定存在故障的第一段列表，最后根据第一段列表所属的候选路径来执行相应的流量转移或业务切换操作。利用贝叶斯网络模型计算可通信概率并进行对比，实现了对于头结点的故障的智能感知，执行流量转移或业务切换操作实现了在感知到头节点故障之后的及时处理和报文的有序调度，进一步地，实现了对于头结点故障的系统化处理，提高了报文转发的安全性和效率。

[0094] 图5是本发明实施例提供的一种故障处理装置的结构图，该装置500可以包括：

[0095] 拓扑信息获取模块501，用于获取头结点所在网络的拓扑信息，所述拓扑信息包括网络节点信息和网络节点之间的连接关系，所述头结点中配置有至少一个段列表，所述段列表用于指示网络报文在所述网络中的转发路径，所述段列表中包括段标识，所述段标识用于指示所述转发路径中的网络节点；

[0096] 贝叶斯网络模型模块502，用于根据所述网络节点信息和网络节点之间的连接关系，利用贝叶斯网络模型计算每个段列表中所指示的网络节点的可通信概率；

[0097] 调度模块503，用于若存在第一网络节点的可通信概率小于预设的可通信概率，则

确定所述第一网络节点所属的第一段列表存在通信故障，删除所述第一段列表，并根据所述第一段列表所属的候选路径执行流量转移或业务切换操作，所述流量转移用于将所述第一段列表的流量分配给其他段列表或候选路径。

[0098] 可选地，所述贝叶斯网络模型模块，可以包括：

[0099] 条件通信概率计算子模块，用于根据所述网络节点信息，计算所述网络中网络节点与周边节点的条件通信概率；

[0100] 贝叶斯网络模型构建子模块，用于根据所述条件通信概率和所述连接关系，构建所述头结点所在网络的贝叶斯网络模型；

[0101] 可通信概率计算子模块，用于利用所述贝叶斯网络模型，计算由所述头结点至每个段列表中所指示的网络节点的可通信概率。

[0102] 可选地，所述头结点用于标识第一业务策略，所述第一业务策略与候选路径相关联，所述候选路径包括优选路径和备选路径；当段列表没有发生通信故障时，所述段列表按照优选路径进行报文的转发处理；

[0103] 可选地，所述调度模块可以包括：

[0104] 第一流量转移操作子模块，用于在所述第一段列表所属的优选路径中的其他段列表没有发生通信故障的情况下，则执行第一流量转移操作，以将所述第一段列表的流量转移到所述其他段列表中。

[0105] 可选地，所述调度模块可以包括：

[0106] 第二流量转移操作子模块，用于在所述第一段列表所属的优选路径中的其他段列表均发生通信故障的情况下，则执行第二流量转移操作的情况下，以将所述优选路径中的流量转移到所述备选路径中。

[0107] 可选地，所述调度模块可以包括：

[0108] 业务切换操作子模块，用于在所述第一段列表所属的优选路径和对应的备选路径中的所有段列表均发生通信故障的情况下，则执行业务切换操作，以将所述第一业务策略切换为其他业务策略。

[0109] 可选地，所述调度模块可以包括：

[0110] 第三流量转移操作子模块，用于在所述第一段列表所属的优选路径和备选路径中的所有段列表均发生通信故障且所述头结点的报文中段列表不存在所述候选路径的绑定标识的情况下，根据所述拓扑信息配置第二段列表，并执行第三流量转移操作，以使所述优选路径和备选路径中的流量转移到所述第二段列表所对应的候选路径中。

[0111] 可选地，所述装置还可以包括：

[0112] 设备信息获取模块，用于获取所述第一网络节点对应的设备信息；

[0113] 攻击溯源策略查询模块，用于根据所述设备信息在预设的网络安全库中查询与所述设备信息相关的攻击溯源策略；

[0114] 溯源模块，用于根据所述溯源策略进行溯源，找到导致所述第一网络节点发生故障的攻击源。

[0115] 可选地，所述攻击溯源策略查询模块可以包括：

[0116] 第一溯源策略查询子模块，用于根据所述设备信息在预设的网络安全库中查询与所述设备信息相关的第一溯源策略；

[0117] 子溯源策略查询子模块，用于若所述第一溯源策略为关联溯源策略，则以所述第一溯源策略为输入，利用所述网络安全库查询所述第一溯源策略的子溯源策略；

[0118] 相应地，所述溯源模块可以包括：

[0119] 子溯源策略执行子模块，用于执行所述子溯源策略，得到子溯源结果；

[0120] 逻辑运算子模块，用于按照预设的所述第一溯源策略的关联规则，对所述子溯源结果进行逻辑运算，得到最终溯源结果；

[0121] 攻击源定位子模块，根据所述最终溯源结果定位导致所述第一网络节点发生故障的攻击源。

[0122] 可选地，所述装置还可以包括：

[0123] 故障信息获取模块，用于获取所述第一网络节点的故障信息，所述故障信息包括攻击源地址、攻击源端口、故障地址、故障端口和协议信息；

[0124] 五元组构建模块，用于根据所述攻击源地址、攻击源端口、故障地址、故障端口和协议信息构建五元组；

[0125] 攻击类型确定模块，用于根据所述五元组确定攻击所述第一网络节点的攻击类型；

[0126] 第一网络节点定位模块，用于利用多维数据关联和威胁分析模型库确定并执行所述攻击类型对应的攻击溯源策略，定位被攻击的所述第一网络节点。

[0127] 本发明还提供了一种电子设备，参见图6，包括：处理器601、存储器602以及存储在所述存储器上并可在所述处理器上运行的计算机程序6021，所述处理器执行所述程序时实现前述实施例的故障处理方法。

[0128] 本发明还提供了一种可读存储介质，当所述存储介质中的指令由电子设备的处理器执行时，使得电子设备能够执行前述实施例的头结点的故障处理。

[0129] 对于装置实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0130] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其他设备固有相关。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0131] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0132] 类似地，应当理解，为了精简本发明并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图，或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0133] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地

改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0134] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器(DSP)来实现根据本发明的排序设备中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0135] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

[0136] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0137] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所做的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

[0138] 以上所述，仅为本发明的具体实施方式，但本发明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发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以权利要求的保护范围为准。

[0139] 需要说明的是，本发明实施例中获取各种数据相关过程，都是在遵照所在地国家相应的数据保护法规政策的前提下，并获得由相应装置所有者给予授权的情况下进行的。

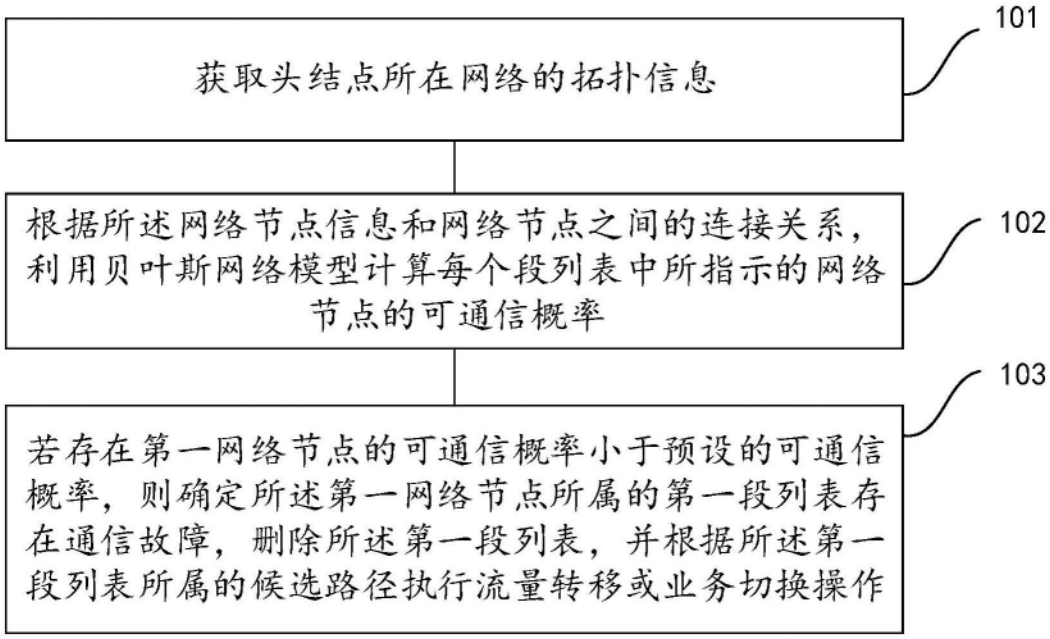

101
获取头结点所在网络的拓扑信息
102
根据所述网络节点信息和网络节点之间的连接关系，利用贝叶斯网络模型计算每个段列表中所指示的网络节点的可通信概率
103
若存在第一网络节点的可通信概率小于预设的可通信概率，则确定所述第一网络节点所属的第一段列表存在通信故障，删除所述第一段列表，并根据所述第一段列表所属的候选路径执行流量转移或业务切换操作

图1

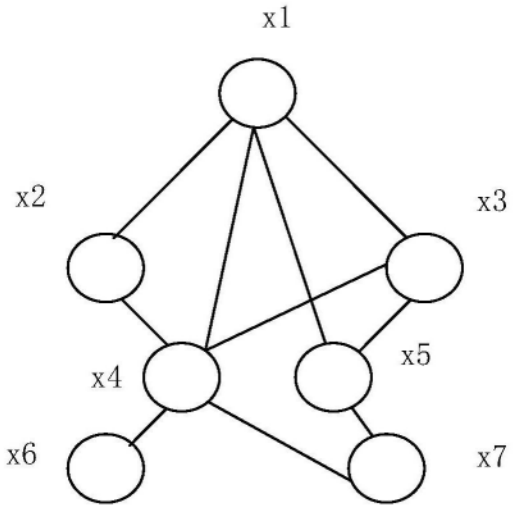

x1
x2
x3
x4
x5
x6
x7

图2

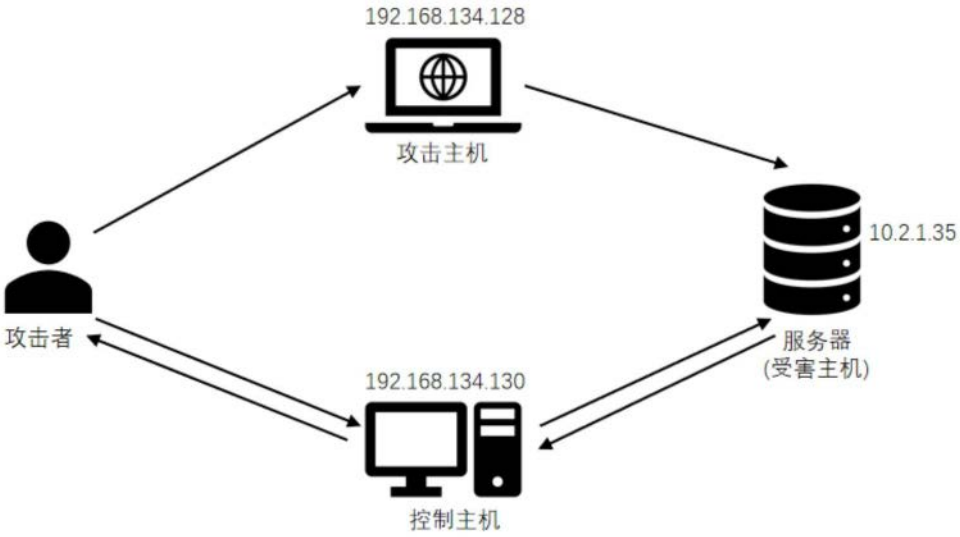

192.168.134.128
攻击主机
10.2.1.35
攻击者
服务器
(受害主机)
192.168.134.130
控制主机

图3

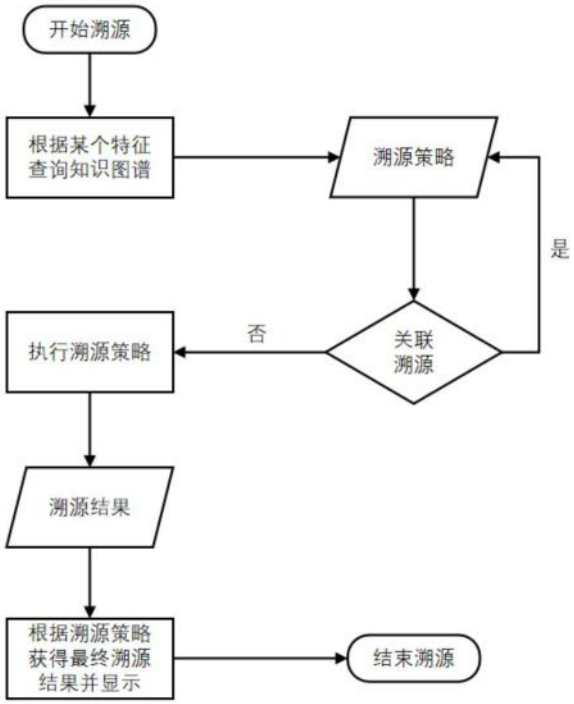

开始溯源
根据某个特征
查询知识图谱
溯源策略
是
否
执行溯源策略
关联
溯源
溯源结果
根据溯源策略
获得最终溯源
结果并显示
结束溯源

图4


故障处理装置500
拓扑信息获取模块501
贝叶斯网络模型模块502
调度模块503

图5

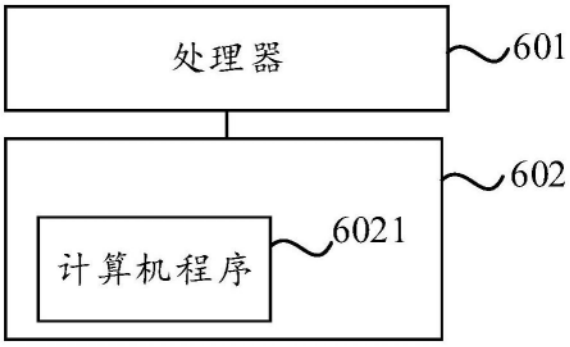

处理器
601
602
计算机程序
6021

图6