(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111416806 B
(45)授权公告日 2022.05.10

(21)申请号 202010174652.2

(22)申请日 2020.03.13

(65)同一申请的已公布的文献号
申请公布号 CN 111416806 A

(43)申请公布日 2020.07.14

(73)专利权人 首都师范大学
地址 100037 北京市海淀区西三环北路105号

(72)发明人 陈文龙 王晓林 唐晓岚 王晓亮

(74)专利代理机构 北京清亦华知识产权代理事务所(普通合伙) 11201
专利代理师 王艳斌

(51)Int.Cl.
H04L 9/40(2022.01)

(56)对比文件
CN 108494769 A,2018.09.04
CN 109120602 A,2019.01.01
CN 106506274 A,2017.03.15
CN 105915505 A,2016.08.31
CN 110290234 A,2019.09.27
CN 105337951 A,2016.02.17
US 2006028996 A1,2006.02.09
宋宇波等.一种基于拓扑分析的网络攻击流量分流和阻断方法.《信息网络安全》.2020,(第03期),

审查员 吴超

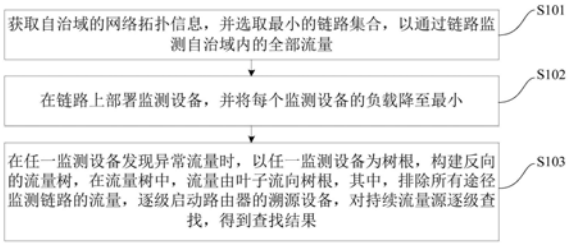
权利要求书2页 说明书6页 附图2页

(54)发明名称

骨干网匿名攻击流量的IP地址溯源方法及装置

(57)摘要

本发明公开了一种骨干网匿名攻击流量的IP地址溯源方法及装置,其中,方法包括以下步骤:获取自治域的网络拓扑信息,并选取最小的链路集合,以通过链路监测自治域内的全部流量;在链路上部署监测设备,并将每个监测设备的负载降至最小;在任一监测设备发现异常流量时,以任一监测设备为树根,构建反向的流量树,在流量树中,流量由叶子流向树根,其中,排除所有途径监测链路的流量,逐级启动路由器的溯源设备,对持续流量源逐级查找,得到查找结果。该方法可以完成匿名攻击流量的真实地址范围定位,简单易实现。



CN 111416806 B

1.一种骨干网匿名攻击流量的IP地址溯源方法,其特征在于,包括以下步骤:

获取自治域的网络拓扑信息,并选取最小的链路集合,以通过链路监测所述自治域内的全部流量,其中,所述选取最小的链路集合,包括:

计算独享路径集合$S_P_{single}=\{P_1,P_2,\cdots,P_s\}$,$S\_P_{single}\in\omega$,计算独占链路集合$S_E_{single}=\{L_1,L_2,\cdots,L_n\}$,其中$\forall L_i,\ \exists P_j\in\omega, L_i\in P_j, L_i\notin\omega-P_j$,则共享路径集合$S_P_{intersect}=\omega-S_P_{single}$,共享链路集合$S_E_{intersect}=\varepsilon-S_E_{single}$;$S_E_{min}$中,将P'从$S_P_{single}$移除,直到$S_P_{single}$为空;对$S_P_{intersect}=\{P_1,P_2,\cdots,P_n\}$,任意$P_i\in S_P_{intersect}$,$i\in\{1,2,\cdots,n\}$,得到路径所包含的链路集合,即$P_i=\{L_{i1},L_{i2},\cdots,L_{in}\}$;对$S_E_{intersect}=\{L_1,L_2,\cdots,L_n\}$,任意$L_i$,$L_i\in S\_E_{intersect}$,$i\in\{1,2,\cdots,n\}$,得到链路可以监测的路径集合,$S\_P(L_i)=\{P_1',P_2',\cdots,P_m'\}$,其中,ω表示连接两个不同边缘路由器之间最短路径集合,P_{i-j}表示从R_i到R_j的路径,$P_{i-j}\in\omega$,i<j,不考虑具体边缘路由器时可以将路径表示为P_i,$P_i\in\omega$,$i\in\{1,2,\cdots,n\}$,L_i为P_{i-j}的链路,P为路径,P'是平行路径;

在所述链路上部署监测设备,并将每个监测设备的负载降至最小;

在任一监测设备发现异常流量时,以所述任一监测设备为树根,构建反向的流量树,在所述流量树中,流量由叶子流向所述树根,其中,排除所有途径监测链路的流量,逐级启动路由器的溯源设备,对持续流量源逐级查找,得到查找结果。

2.根据权利要求1所述的方法,其特征在于,在获取所述自治域的网络拓扑信息之后,还包括:

对拓扑中的链路和路径进行分类。

3.根据权利要求2所述的方法,其特征在于,所述路径包括独享路径、共享路径,且所述链路包括独享链路和共享链路。

4.根据权利要求1所述的方法,其特征在于,所有监测设备监测静态流量,并以动态平衡的方式由链路分配监测静态流量。

5.一种骨干网匿名攻击流量的IP地址溯源装置,其特征在于,包括:

获取模块,用于获取自治域的网络拓扑信息,并选取最小的链路集合,以通过链路监测所述自治域内的全部流量,其中,所述选取最小的链路集合,包括:

计算独享路径集合$S_P_{single}=\{P_1,P_2,\cdots,P_s\}$,$S\_P_{single}\in\omega$,计算独占链路集合$S_E_{single}=\{L_1,L_2,\cdots,L_n\}$,其中$\forall L_i,\ \exists P_j\in\omega, L_i\in P_j, L_i\notin\omega-P_j$,则共享路径集合$S_P_{intersect}=\omega-S_P_{single}$,共享链路集合$S_E_{intersect}=\varepsilon-S_E_{single}$;$S_E_{min}$中,将P'从$S_P_{single}$移除,直到$S_P_{single}$为空;对$S_P_{intersect}=\{P_1,P_2,\cdots,P_n\}$,任意$P_i\in S_P_{intersect}$,$i\in\{1,2,\cdots,n\}$,得到路径所包含的链路集合,即$P_i=\{L_{i1},L_{i2},\cdots,L_{in}\}$;对$S_E_{intersect}=\{L_1,L_2,\cdots,L_n\}$,任意$L_i$,$L_i\in S\_E_{intersect}$,$i\in\{1,2,\cdots,n\}$,得到链路可以监测的路径集合,$S\_P(L_i)=\{P_1',P_2',\cdots,P_m'\}$;求出所述最小的链路集合$S_E_{min}=\{L_1'',L_2'',\cdots,L_n''\}$,使得$\forall P_i\in\omega,\ \exists L_i\in S_E_{min}$且$L_i\in P_i$,$P_{i-j}\in\omega$,i<j,不考虑具体边缘路由器时可以将路径表示为$P_i$,$P_i\in\omega$,$i\in\{1,2,\cdots,n\}$,$L_i$为$P_{i-j}$的链路,P为路径,P'是平行路径;

部署模块,用于在所述链路上部署监测设备,并将每个监测设备的负载降至最小;

构建模块,用于在任一监测设备发现异常流量时,以所述任一监测设备为树根,构建反向的流量树,在所述流量树中,流量由叶子流向所述树根,其中,排除所有途径监测链路的

流量，逐级启动路由器的溯源设备，对持续流量源逐级查找，得到查找结果。

6.根据权利要求5所述的装置，其特征在于，还包括：

分类模块，用于在获取所述自治域的网络拓扑信息之后，对拓扑中的链路和路径进行分类。

7.根据权利要求6所述的装置，其特征在于，所述路径包括独享路径、共享路径，且所述链路包括独享链路和共享链路。

8.根据权利要求5所述的装置，其特征在于，所有监测设备监测静态流量，并以动态平衡的方式由链路分配监测静态流量。

骨干网匿名攻击流量的IP地址溯源方法及装置

技术领域

[0001] 本发明涉及计算机网络技术领域，特别涉及一种骨干网匿名攻击流量的IP地址溯源方法及装置。

背景技术

[0002] 互联网自治域内匿名攻击流量溯源检测技术中，如何提到溯源成本和效率是关键问题之一，基于动态包标记的溯源往往存在计算开销大等问题，一种实时动态的溯源方案，不需要对包进行标记，主要针对持续性匿名攻击，通过可插拔的路由器流量检测设备，逐级溯源，可避免由打标签所带来的额外计算，此外只有在攻击发生时才启动检测，不会影响正常的路由效率，然而，该方案存在的不足是只能在攻击发生时且持续才能有效溯源。

发明内容

[0003] 本发明旨在至少在一定程度上解决相关技术中的技术问题之一。

[0004] 为此，本发明的一个目的在于提出一种骨干网匿名攻击流量的IP地址溯源方法，该方法可以完成匿名攻击流量的真实地址范围定位，简单易实现。

[0005] 本发明的另一个目的在于提出一种骨干网匿名攻击流量的IP地址溯源装置。

[0006] 为达到上述目的，本发明一方面实施例提出了一种骨干网匿名攻击流量的IP地址溯源方法，包括以下步骤：获取自治域的网络拓扑信息，并选取最小的链路集合，以通过链路监测所述自治域内的全部流量；在所述链路上部署监测设备，并将每个监测设备的负载降至最小；在任一监测设备发现异常流量时，以所述任一监测设备为树根，构建反向的流量树，在所述流量树中，流量由叶子流向所述树根，其中，排除所有途径监测链路的流量，逐级启动路由器的溯源设备，对持续流量源逐级查找，得到查找结果。

[0007] 本发明实施例的骨干网匿名攻击流量的IP地址溯源方法，将监测流量的工作由旁路监测设备负责，不影响网络开销，溯源过程由监测设备和路由器配合完成，路由器只需要付出很小的开销即可完成溯源，从而可以完成匿名攻击流量的真实地址范围定位，简单易实现。

[0008] 另外，根据本发明上述实施例的骨干网匿名攻击流量的IP地址溯源方法还可以具有以下附加的技术特征：

[0009] 进一步地，在本发明的一个实施例中，在获取所述自治域的网络拓扑信息之后，还包括：对拓扑中的链路和路径进行分类。

[0010] 进一步地，在本发明的一个实施例中，所述路径包括独享路径、共享路径，且所述链路包括独享链路和共享链路。

[0011] 进一步地，在本发明的一个实施例中，所述选取最小的链路集合，包括：

[0012] 计算独享路径集合$S_P_{single}=\{P_1,P_2,\cdots,P_s\}$，$S\_P_{single}\in\omega$，计算独占链路集合$S_E_{single}=\{L_1,L_2,\cdots,L_n\}$，其中$\forall L_i,\ \exists P_j\in\omega, L_i\in P_j, L_i\notin\omega-P_j$，则共享路径集合$S_P_{intersect}=\omega-S_P_{single}$，共享链路集合$S_E_{intersect}=\varepsilon-S_E_{single}$；

[0013] S_E_{min}中，将P'从S_P_{single}移除，直到S_P_{single}为空；

[0014] 对$S_P_{intersect}=\{P_1,P_2,\cdots,P_n\}$，任意$P_i\in S_P_{intersect}$，$i\in\{1,2,\cdots,n\}$，得到路径所包含的链路集合，即$P_i=\{L_{i1},L_{i2},\cdots,L_{in}\}$；对$S_E_{intersect}=\{L_1,L_2,\cdots,L_n\}$，任意$L_i$，$L_i\in S\_E_{intersect}$，$i\in\{1,2,\cdots,n\}$，得到链路可以监测的路径集合，$S\_P(L_i)=\{P_1',P_2',\cdots,P_m'\}$；

[0015] 求出所述最小的链路集合$S_E_{min}=\{L_1'',L_2'',\cdots,L_n''\}$，使得$\forall P_i\in\omega,\exists L_i\in S_E_{min}$且$L_i\in P_i$。

[0016] 进一步地，在本发明的一个实施例中，所有监测设备监测静态流量，并以动态平衡的方式由链路分配监测静态流量。

[0017] 为达到上述目的，本发明另一方面实施例提出了一种骨干网匿名攻击流量的IP地址溯源装置，包括：获取模块，用于获取自治域的网络拓扑信息，并选取最小的链路集合，以通过链路监测所述自治域内的全部流量；部署模块，用于在所述链路上部署监测设备，并将每个监测设备的负载降至最小；构建模块，用于在任一监测设备发现异常流量时，以所述任一监测设备为树根，构建反向的流量树，在所述流量树中，流量由叶子流向所述树根，其中，排除所有途径监测链路的流量，逐级启动路由器的溯源设备，对持续流量源逐级查找，得到查找结果。

[0018] 本发明实施例的骨干网匿名攻击流量的IP地址溯源装置，将监测流量的工作由旁路监测设备负责，不影响网络开销，溯源过程由监测设备和路由器配合完成，路由器只需要付出很小的开销即可完成溯源，从而可以完成匿名攻击流量的真实地址范围定位，简单易实现。

[0019] 另外，根据本发明上述实施例的骨干网匿名攻击流量的IP地址溯源装置还可以具有以下附加的技术特征：

[0020] 进一步地，在本发明的一个实施例中，还包括：分类模块，用于在获取所述自治域的网络拓扑信息之后，对拓扑中的链路和路径进行分类。

[0021] 进一步地，在本发明的一个实施例中，所述路径包括独享路径、共享路径，且所述链路包括独享链路和共享链路。

[0022] 进一步地，在本发明的一个实施例中，所述选取最小的链路集合，包括：

[0023] 计算独享路径集合$S_P_{single}=\{P_1,P_2,\cdots,P_s\}$，$S\_P_{single}\in\omega$，计算独占链路集合$S_E_{single}=\{L_1,L_2,\cdots,L_n\}$，其中$\forall L_i,\ \exists P_j\in\omega,L_i\in P_j,L_i\notin\omega-P_j$，则共享路径集合$S_P_{intersect}=\omega-S_P_{single}$，共享链路集合$S_E_{intersect}=\varepsilon-S_E_{single}$；

[0024] S_E_{min}中，将P'从S_P_{single}移除，直到S_P_{single}为空；

[0025] 对$S_P_{intersect}=\{P_1,P_2,\cdots,P_n\}$，任意$P_i\in S_P_{intersect}$，$i\in\{1,2,\cdots,n\}$，得到路径所包含的链路集合，即$P_i=\{L_{i1},L_{i2},\cdots,L_{in}\}$；对$S_E_{intersect}=\{L_1,L_2,\cdots,L_n\}$，任意$L_i$，$L_i\in S\_E_{intersect}$，$i\in\{1,2,\cdots,n\}$，得到链路可以监测的路径集合，$S\_P(L_i)=\{P_1',P_2',\cdots,P_m'\}$；

[0026] 求出所述最小的链路集合$S_E_{min}=\{L_1'',L_2'',\cdots,L_n''\}$，使得$\forall P_i\in\omega,\exists L_i\in S_E_{min}$且$L_i\in P_i$。

[0027] 进一步地，在本发明的一个实施例中，所有监测设备监测静态流量，并以动态平衡的方式由链路分配监测静态流量。

[0028] 本发明附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变

得明显,或通过本发明的实践了解到。

附图说明

[0029] 本发明上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解,其中:

[0030] 图1为根据本发明实施例的骨干网匿名攻击流量的IP地址溯源方法的流程图;

[0031] 图2为根据本发明一个实施例的骨干网匿名攻击流量的IP地址溯源方法的流程图;

[0032] 图3为根据本发明实施例的监测链路发现异常带宽时启动溯源的流程图;

[0033] 图4为根据本发明实施例的骨干网匿名攻击流量的IP地址溯源装置的结构示意图。

具体实施方式

[0034] 下面详细描述本发明的实施例,所述实施例的示例在附图中示出,其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的,旨在用于解释本发明,而不能理解为对本发明的限制。

[0035] 下面参照附图描述根据本发明实施例提出的骨干网匿名攻击流量的IP地址溯源方法及装置,首先将参照附图描述根据本发明实施例提出的骨干网匿名攻击流量的IP地址溯源方法。

[0036] 图1是本发明一个实施例的骨干网匿名攻击流量的IP地址溯源方法的流程图。

[0037] 如图1所示,该骨干网匿名攻击流量的IP地址溯源方法包括以下步骤:

[0038] 在步骤S101中,获取自治域的网络拓扑信息,并选取最小的链路集合,以通过链路监测自治域内的全部流量。

[0039] 可以理解的是,获取自治域网络拓扑信息,选取最小的链路集合,使得这些链路可以监测到自治域内全部的流量,

[0040] 进一步地,在本发明的一个实施例中,在获取自治域的网络拓扑信息之后,还包括:对拓扑中的链路和路径进行分类,其中,路径包括独享路径、共享路径,且链路包括独享链路和共享链路。

[0041] 具体而言,对拓扑中的链路和路径进行分类,定义路径为一个边缘路由器到另一个边缘路由器的最短路径,对拓扑和链路进行分类的主要目的是为了简化最有检测链路集合的计算量,如果存在两条路径,且包含至少一条相同的链路,则这两条路径划分为共享路径,反之,如果一条路径与其他路径没有相同链路,划分为独享路径。如果一条链路只存在于一条路径中,则划分为独享链路,反之划分为共享链路。

[0042] 在步骤S102中,在链路上部署监测设备,并将每个监测设备的负载降至最小。

[0043] 可以理解的是,在这些链路上部署监测设备,并且尽可能均衡每个监测设备的负载。

[0044] 具体而言,选取最优监测链路集合,部署监测设备和溯源设备,可以将选取最优监测链路过程看成覆盖集问题模型,利用近似贪心算法可以求出解,这个解不一定是最优解,但是,是近似最优解。监测设备用于监测全部的流量,溯源设备则负责在溯源的时候查询流

量上一跳路由地址。

[0045] 其中，在所有节点上部署溯源设备，平时处于待机状态，低功耗运行，只有在需要溯源的时候再启动溯源设备。

[0046] 在步骤S103中，在任一监测设备发现异常流量时，以任一监测设备为树根，构建反向的流量树，在流量树中，流量由叶子流向树根，其中，排除所有途径监测链路的流量，逐级启动路由器的溯源设备，对持续流量源逐级查找，得到查找结果。

[0047] 可以理解的是，某个监测设备一旦发现异常流量，以该监测设备为树根，构建一个反向的流量树，该流量树中，流量由叶子流向树根。首先排除所有途径监测链路的流量，然后逐级启动路由器的溯源设备，对持续流量源逐级查找。

[0048] 具体而言，监测链路发现异常带宽，启动溯源流程。监测设备发现持续的异常流量，以流量的目的地址作为树根，构造反向的流量树，监测设备根据流量树查找到异常流量的上一个节点1，由该节点启动溯源，检测到持续异常流量，查看流量的上一个节点2，并发出溯源请求，节点2重复节点1操作，直到真正的源边缘路由器，即可确定匿名流量所在区域。

[0049] 下面将通过具体实施例对骨干网匿名攻击流量的IP地址溯源方法进行进一步阐述，如图2所示，具体包括：

[0050] 1、获取自治域物理拓扑结构，用于计算所要部署监测点的监测链路。

[0051] 2、对拓扑中的链路和路径进行分类。

[0052] ω表示连接两个不同边缘路由器之间最短路径集合(边缘路由器至少连接一个子网)，R_i表示自治域内所有连接子网的边缘路由器，$R_i \in v$，$i \in \{1,2,3,\cdots,n\}$，R_i连接子网个数为$NR_{i(Subnet)}$。

[0053] P_{i-j}表示从R_i到R_j的路径(Dijkstra)，$P_{i-j} \in \omega$，$i<j$，不考虑具体边缘路由器时可以将路径表示为P_i，$P_i \in \omega$，$i \in \{1,2,\cdots,n\}$。若L_i为P_{i-j}的链路，$i \in \{1,2,\cdots,m\}$，则$P_{i-j}=\{L_1, L_2, L_3, \ldots, L_m\}$；按照IP前缀对一条路径$P_{i-j}$上的流量进行划分，则$P_{i-j}$之间的流量条数可表示为$NFP_{i-j}=NR_{i_Subnet} \times NR_{j_Subnet}$。

[0054] 独享路径，对于路径P，P'是平行路径当且仅当，$\forall L_i \in P'$，$P' \in \omega$，$\forall P_i \in \omega$，$P_i \neq P'$，$L_i \notin P_i$。平行路径P'，$\forall L_i \in P'$，L_i可作为监测链路。其中，平行路径上每条链路都是独享链路，反之错误。

[0055] 共享路径，$\forall P_i \in \omega$，$\forall P_j \in \omega$，$\exists L_i \in P_i, P_j$，则P_i，P_j均为交叉路径。

[0056] 独享链路，链路L_i，$i \in \{1,2,\cdots,n\}$为独享链路当且仅当，$L_i \in P'$，$P' \in \omega$，$L_i \notin \omega - P'$。

[0057] 共享链路，链路L_i，$i \in \{1,2,\cdots,n\}$为共享链路当且仅当，$L_i \in P_j$，$P_j \in \omega$，$j>1$。

[0058] 3、选取最优监测链路集合，部署监测设备和溯源设备。

[0059] 计算独享路径集合$S_P_{single}=\{P_1, P_2, \cdots, P_s\}$，$S\_P_{single} \in \omega$。计算独占链路集合$S_E_{single}=\{L_1, L_2, \cdots, L_n\}$，其中$\forall L_i$，$\exists P_j \in \omega$，$L_i \in P_j$，$L_i \notin \omega - P_j$。则共享路径集合$S_P_{intersect}=\omega - S_P_{single}$，共享链路集合$S_E_{intersect}=\varepsilon - S_E_{single}$。

[0060] S_E_{min}初始化为空，对于P'，若$P' \in S_P_{single}$，则任取$L' \in P'$，添加到S_E_{min}中，将P'从S_P_{single}移除，直到S_P_{single}为空。

[0061] 对$S_P_{intersect}=\{P_1, P_2, \cdots, P_n\}$，任意$P_i \in S_P_{intersect}$，$i \in \{1,2,\cdots,n\}$，可以得到路

径所包含的链路集合，即$P_i=\{L_{i1},L_{i2},\cdots,L_{in}\}$。对$S_E_{intersect}=\{L_1,L_2,\cdots,L_n\}$，任意$L_i,L_i\in S_E_{intersect}$，$i\in\{1,2,\cdots,n\}$，可以得到链路可以监测的路径集合，$S\_P(L_i)=\{P_1',P_2',\cdots,P_m'\}$。

[0062] 求出最小监测链路集合$S_E_{min}=\{L_1'',L_2'',\cdots,L_n''\}$，使得$\forall P_i\in\omega$，$\exists L_i\in S_E_{min}$且$L_i\in P_i$。

[0063] 静态流量：监测链路和路径的关系里，一对一关系，路径P只能由唯一的监测L链路监测，因此P上所有的流量是L必须监测的。一对多关系中，路径集合{P1,P2,…,Pn}中所有的路径只能由唯一的链路L监测，因此该集合中路径上的所有流量必须由L监测，这些必须监测的流量称为必要监测流量，这个概念是对任意一个监测链路而言的。

[0064] 调整流量：监测链路和路径的关系里，多对一和多对多关系中，一条路径上有多个监测链路，因此流经此路径的流量不是某一监测链路的必须监测的流量，即可以调整是否检测或监测多少的流量，称为调整流量。

[0065] 优化方案：所有监测设备必须监测静态流量，对于动态流量，则以动态平衡的方式由链路分配监测。

[0066] 4、在所有节点上部署溯源设备。

[0067] 5、监测链路发现异常带宽，启动溯源流程。

[0068] 如图3所示，监测链路发现异常带宽，启动溯源流程。监测设备发现持续的异常流量，以监测点为树根，路由器为节点，构造反向的流量树，监测设备根据流量树查找到异常流量的上一个节点1，由该节点启动溯源，检测到持续异常流量，查看流量的上一个节点2，并发出溯源请求，节点2重复节点1操作，直到真正的源边缘路由器，即可确定匿名流量所在区域。

[0069] 根据本发明实施例提出的骨干网匿名攻击流量的IP地址溯源方法，将监测流量的工作由旁路监测设备负责，不影响网络开销，溯源过程由监测设备和路由器配合完成，路由器只需要付出很小的开销即可完成溯源，从而可以完成匿名攻击流量的真实地址范围定位，简单易实现。

[0070] 其次参照附图描述根据本发明实施例提出的骨干网匿名攻击流量的IP地址溯源装置。

[0071] 图4是本发明一个实施例的骨干网匿名攻击流量的IP地址溯源装置的结构示意图。

[0072] 如图4所示，该骨干网匿名攻击流量的IP地址溯源装置10包括：获取模块100、部署模块200和构建模块300。

[0073] 其中，获取模块100用于获取自治域的网络拓扑信息，并选取最小的链路集合，以通过链路监测自治域内的全部流量；部署模块200用于在链路上部署监测设备，并将每个监测设备的负载降至最小；构建模块300用于在任一监测设备发现异常流量时，以任一监测设备为树根，构建反向的流量树，在流量树中，流量由叶子流向树根，其中，排除所有途径监测链路的流量，逐级启动路由器的溯源设备，对持续流量源逐级查找，得到查找结果。本发明实施例的装置10可以完成匿名攻击流量的真实地址范围定位，简单易实现。

[0074] 进一步地，在本发明的一个实施例中，本发明实施例的装置10还包括：分类模块。其中，分类模块用于在获取自治域的网络拓扑信息之后，对拓扑中的链路和路径进行分类。

[0075] 进一步地，在本发明的一个实施例中，路径包括独享路径、共享路径，且链路包括独享链路和共享链路。

[0076] 进一步地，在本发明的一个实施例中，选取最小的链路集合，包括：

[0077] 计算独享路径集合$S_P_{single}=\{P_1,P_2,\cdots,P_s\}$，$S\_P_{single}\in\omega$。计算独占链路集合$S_E_{single}=\{L_1,L_2,\cdots,L_n\}$，其中$\forall L_i,\ \exists P_j\in\omega, L_i\in P_j, L_i\notin\omega-P_j$，则共享路径集合$S_P_{intersect}=\omega-S_P_{single}$，共享链路集合$S_E_{intersect}=\varepsilon-S_E_{single}$；

[0078] S_E_{min}中，将P'从S_P_{single}移除，直到S_P_{single}为空；

[0079] 对$S_P_{intersect}=\{P_1,P_2,\cdots,P_n\}$，任意$P_i\in S_P_{intersect}$，$i\in\{1,2,\cdots,n\}$，得到路径所包含的链路集合，即$P_i=\{L_{i1},L_{i2},\cdots,L_{in}\}$；对$S_E_{intersect}=\{L_1,L_2,\cdots,L_n\}$，任意$L_i,L_i\in S_E_{intersect}$，$i\in\{1,2,\cdots,n\}$，得到链路可以监测的路径集合，$S\_P(L_i)=\{P_1',P_2',\cdots,P_m'\}$；

[0080] 求出最小的链路集合$S_E_{min}=\{L_1'',L_2'',\cdots,L_n''\}$，使得$\forall P_i\in\omega,\ \exists L_i\in S_E_{min}$且$L_i\in P_i$。

[0081] 进一步地，在本发明的一个实施例中，所有监测设备监测静态流量，并以动态平衡的方式由链路分配监测静态流量。

[0082] 需要说明的是，前述对骨干网匿名攻击流量的IP地址溯源方法实施例的解释说明也适用于该实施例的骨干网匿名攻击流量的IP地址溯源装置，此处不再赘述。

[0083] 根据本发明实施例提出的骨干网匿名攻击流量的IP地址溯源装置，将监测流量的工作由旁路监测设备负责，不影响网络开销，溯源过程由监测设备和路由器配合完成，路由器只需要付出很小的开销即可完成溯源，从而可以完成匿名攻击流量的真实地址范围定位，简单易实现。

[0084] 此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。在本发明的描述中，“多个”的含义是至少两个，例如两个，三个等，除非另有明确具体的限定。

[0085] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外，在不相互矛盾的情况下，本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

[0086] 尽管上面已经示出和描述了本发明的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本发明的限制，本领域的普通技术人员在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。

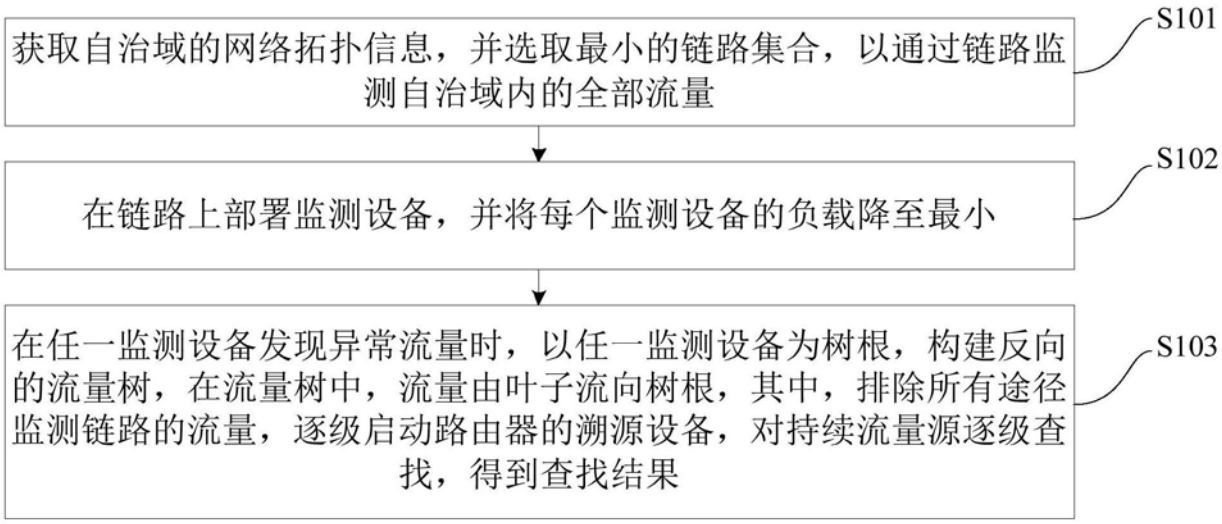

获取自治域的网络拓扑信息，并选取最小的链路集合，以通过链路监测自治域内的全部流量
S101
在链路上部署监测设备，并将每个监测设备的负载降至最小
S102
在任一监测设备发现异常流量时，以任一监测设备为树根，构建反向的流量树，在流量树中，流量由叶子流向树根，其中，排除所有途径监测链路的流量，逐级启动路由器的溯源设备，对持续流量源逐级查找，得到查找结果
S103

图1

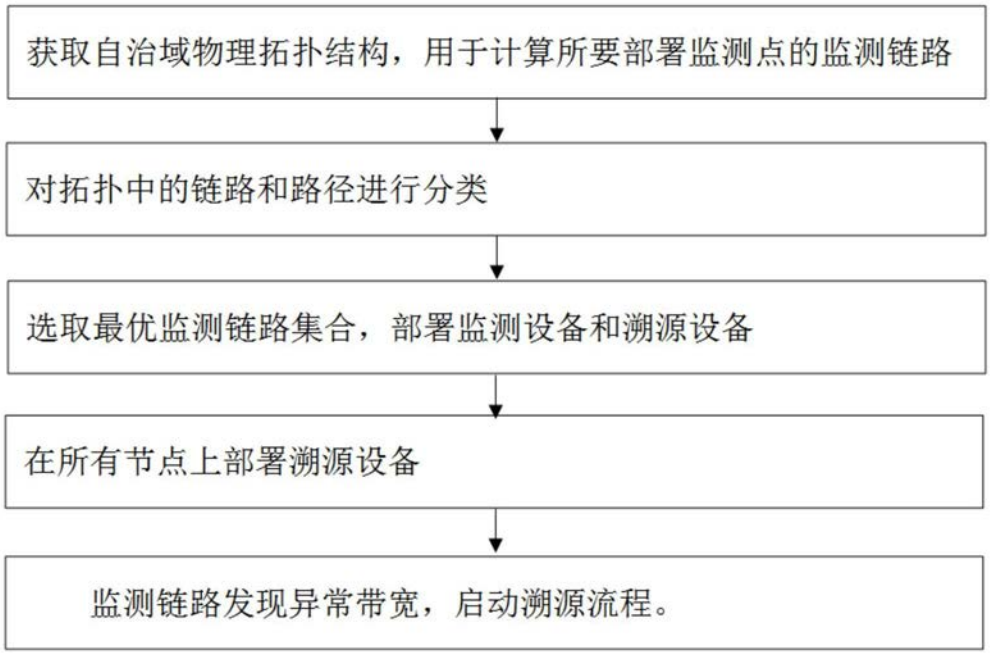

获取自治域物理拓扑结构，用于计算所要部署监测点的监测链路
对拓扑中的链路和路径进行分类
选取最优监测链路集合，部署监测设备和溯源设备
在所有节点上部署溯源设备
监测链路发现异常带宽，启动溯源流程。

图2

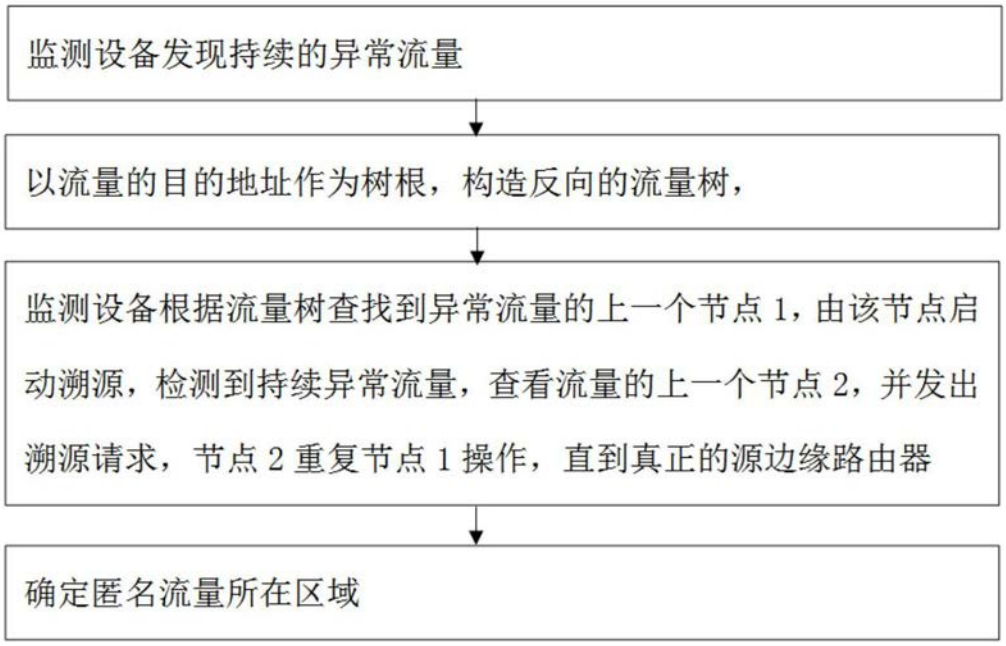

监测设备发现持续的异常流量
以流量的目的地址作为树根，构造反向的流量树，
监测设备根据流量树查找到异常流量的上一个节点 1，由该节点启动溯源，检测到持续异常流量，查看流量的上一个节点 2，并发出溯源请求，节点 2 重复节点 1 操作，直到真正的源边缘路由器
确定匿名流量所在区域

图3

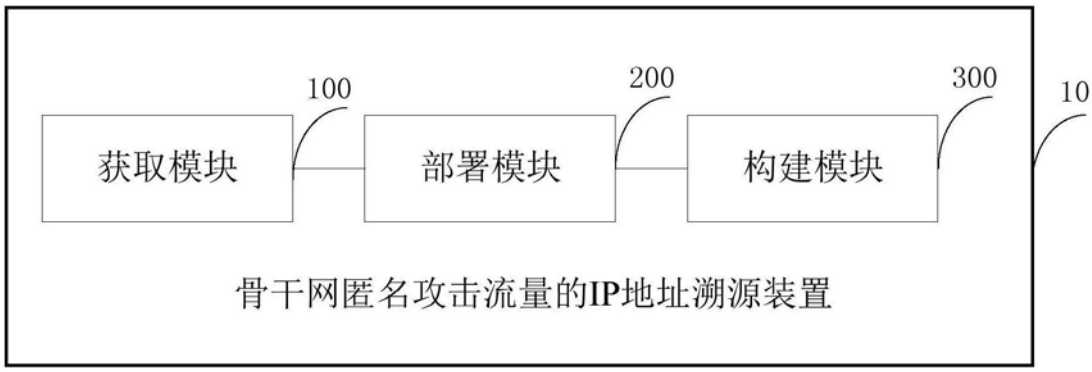

100
200
300
10
获取模块
部署模块
构建模块
骨干网匿名攻击流量的IP地址溯源装置

图4