(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 114363003 A
(43)申请公布日 2022.04.15

(21)申请号 202111499152.7

(22)申请日 2019.03.11

(62)分案原申请数据
201910181646.7 2019.03.11

(71)申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 庄顺万 王海波 顾钰楠 闫刚 李振斌

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

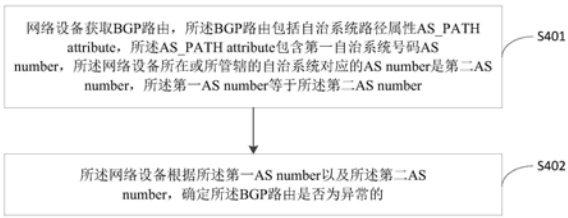
权利要求书3页 说明书29页 附图6页

(54)发明名称

BGP路由识别方法、装置及设备

(57)摘要

本申请实施例提供的BGP路由识别方法、装置及设备。网络设备获取BGP路由，所述BGP路由包括自治系统路径属性AS_PATH attribute，所述AS_PATH attribute包含第一自治系统号码AS number，所述网络设备所在或所管辖的自治系统对应的AS number是第二AS number，所述第一AS number等于所述第二AS number；所述网络设备根据所述第一AS number以及所述第二AS number，确定所述BGP路由是否为异常的，从而能够及时发现路由劫持等原因导致的异常环路路由，提高了网络安全性。



CN 114363003 A

1.一种边界网关协议BGP路由识别方法,其特征在于,包括:

网络设备获取BGP路由,所述BGP路由包括自治系统路径属性AS_PATH attribute和第一互联网协议IP前缀,所述AS_PATH attribute包含第一自治系统号码AS number,所述网络设备所在或所管辖的自治系统对应的AS number是第二AS number,所述第一AS number等于所述第二AS number;

所述网络设备确定所述网络设备没有发布或转发过包含所述第一IP前缀的路由;

响应于确定所述网络设备没有发布或转发过包含所述第一IP前缀的路由,所述网络确定所述BGP路由为劫持路由。

2.根据权利要求1所述的方法,其特征在于,所述第一AS number为所述AS_PATH attribute中的第一个元素element。

3.根据权利要求2所述的方法,其特征在于,所述网络设备发布过包含第二IP前缀的路由,所述第一IP前缀是所述第二IP前缀的子前缀。

4.根据权利要求2所述的方法,其特征在于,所述网络设备向特定AS发布过仅限于所述特定AS使用的包含所述第一IP前缀的路由,以及,所述AS_PATH attribute中不包括所述第二AS number。

5.根据权利要求1所述的方法,其特征在于,所述第一AS number不是所述AS_PATH attribute中的第一个元素element,所述网络设备所在或所管辖的自治系统与第四AS number对应的自治系统没有建立BGP会话,所述第四AS number是所述AS_PATH attribute中与所述第一AS number相邻的元素。

6.根据权利要求1所述的方法,其特征在于,所述第一AS number不是所述AS_PATH attribute中的第一个元素element,所述网络设备所在或所管辖的自治系统与左AS建立有BGP会话,所述网络设备所在或所管辖的自治系统与右AS建立有BGP会话,以及,所述网络设备没有接收过来自所述右AS的包含所述第一IP前缀的路由,或者,所述网络设备没有向所述左AS发布过包含所述第一IP前缀的路由;

所述右AS对应的AS number以及所述左AS对应的AS number是与所述AS_PATH attribute中与所述第一AS number相邻的两个元素,所述右AS对应的AS number位于所述第一AS number的右侧,所述左AS对应的AS number位于所述第一AS number的左侧。

7.一种边界网关协议BGP路由识别方法,其特征在于,包括:

网络设备获取BGP路由,所述BGP路由包括自治系统路径属性AS_PATH attribute和第一互联网协议IP前缀,所述AS_PATH attribute包含第一自治系统号码AS number,所述网络设备所在或所管辖的自治系统的邻居自治系统对应的AS number是第二AS number,所述第一AS number等于所述第二AS number;

所述网络设备确定所述网络设备没有发布或转发过包含所述第一IP前缀的路由,响应于确定所述网络设备没有发布或转发过包含所述第一IP前缀的路由,确定所述BGP路由为劫持路由。

8.根据权利要求7所述的方法,其特征在于,所述第一AS number是所述AS_PATH attribute中的第一个元素element,以及,所述邻居自治系统没有发布过包含所述第一IP前缀的路由。

9.根据权利要求8所述的方法,其特征在于,所述邻居自治系统发布过包含第二IP前缀

的路由,以及,所述邻居自治系统没有发布过包含所述第一IP前缀的路由,所述第一IP前缀是所述第二IP前缀的子前缀。

10.根据权利要求7所述的方法,其特征在于,

所述第一AS number不是所述AS_PATH attribute中的第一个元素element,以及,所述邻居自治系统与第三AS number对应的自治系统没有建立BGP会话,所述第三AS number是所述AS_PATH attribute中与所述第一AS number相邻的元素。

11.根据权利要求8所述的方法,其特征在于,所述第一AS number不是所述AS_PATH attribute中的第一个元素element,所述邻居自治系统与左AS建立有BGP会话,所述邻居自治系统与右AS建立有BGP会话,所述邻居自治系统接收过来自所述右AS的包含第一IP前缀的路由,以及,所述邻居自治系统没有向所述左AS发布过包含所述第一IP前缀的路由;

所述右AS对应的AS number以及所述左AS对应的AS number是与所述AS_PATH attribute中与所述第一AS number相邻的两个元素,所述右AS对应的AS number位于所述第一AS number的右侧,所述左AS对应的AS number位于所述第一AS number的左侧。

12.一种边界网关协议BGP路由识别装置,其特征在于,包括:

获取模块,用于获取BGP路由,所述BGP路由包括自治系统路径属性AS_PATH attribute和第一互联网协议IP前缀,所述AS_PATH attribute包含第一自治系统号码AS number,所述网络设备所在或所管辖的自治系统对应的AS number是第二AS number,所述第一AS number等于所述第二AS number;

识别模块,用于确定所述网络设备没有发布或转发过包含所述第一IP前缀的路由,响应于确定所述网络设备没有发布或转发过包含所述第一IP前缀的路由,确定所述BGP路由为劫持路由。

13.根据权利要求12所述的装置,其特征在于,

所述第一AS number是所述AS_PATH attribute中的第一个元素element,以及,所述网络设备没有发布过包含所述第一IP前缀的路由。

14.根据权利要求12所述的装置,其特征在于,

所述第一AS number是所述AS_PATH attribute中的第一个元素element,所述网络设备发布过包含第二IP前缀的路由,以及,所述网络设备没有发布过包含所述第一IP前缀的路由,所述第一IP前缀是所述第二IP前缀的子前缀。

15.根据权利要求13所述的装置,其特征在于,

所述网络设备向特定AS发布过仅限于所述特定AS使用的包含所述第一IP前缀的路由,以及,所述AS_PATH attribute中包括第三AS number或者不包括所述第二AS number。

16.根据权利要求12所述的装置,其特征在于,

所述第一AS number不是所述AS_PATH attribute中的第一个元素element,以及,所述网络设备所在或所管辖的自治系统与第四AS number对应的自治系统没有建立BGP会话,所述第四AS number是所述AS_PATH attribute中与所述第一AS number相邻的元素。

17.根据权利要求12所述的装置,其特征在于,所述第一AS number不是所述AS_PATH attribute中的第一个元素element,所述网络设备所在或所管辖的自治系统与左AS建立有BGP会话,所述网络设备所在或所管辖的自治系统与右AS建立有BGP会话,以及,所述网络设备没有接收过来自所述右AS的包含所述第一IP前缀的路由,或者,所述网络设备没有向所

述左AS发布过包含所述第一IP前缀的路由；

所述右AS对应的AS number以及所述左AS对应的AS number是与所述AS_PATH attribute中与所述第一AS number相邻的两个元素，所述右AS对应的AS number位于所述第一AS number的右侧，所述左AS对应的AS number位于所述第一AS number的左侧。

18.一种边界网关协议BGP路由识别装置，其特征在于，包括：

获取模块，用于获取BGP路由，所述BGP路由包括自治系统路径属性AS_PATH attribute和第一互联网协议IP前缀，所述AS_PATH attribute包含第一自治系统号码AS number，所述网络设备所在或所管辖的自治系统的邻居自治系统对应的AS number是第二AS number，所述第一AS number等于所述第二AS number；

识别模块，用于确定所述网络设备没有发布或转发过包含所述第一IP前缀的路由，响应于确定所述网络设备没有发布或转发过包含所述第一IP前缀的路由，确定所述BGP路由为劫持路由。

19.根据权利要求18所述的装置，其特征在于，所述第一AS number是所述AS_PATH attribute中的第一个元素element，以及，所述邻居自治系统没有发布过包含所述第一IP前缀的路由。

20.根据权利要求18所述的装置，其特征在于，所述第一AS number是所述AS_PATH attribute中的第一个元素element，所述邻居自治系统发布过包含第二IP前缀的路由，以及，所述邻居自治系统没有发布过包含所述第一IP前缀的路由，所述第一IP前缀是所述第二IP前缀的子前缀。

21.根据权利要求18所述的装置，其特征在于，所述第一AS number不是所述AS_PATH attribute中的第一个元素element，以及，所述邻居自治系统与第三AS number对应的自治系统没有建立BGP会话，所述第三AS number是所述AS_PATH attribute中与所述第一AS number相邻的元素。

22.根据权利要求18所述的装置，其特征在于，所述第一AS number不是所述AS_PATH attribute中的第一个元素element，所述邻居自治系统与左AS建立有BGP会话，所述邻居自治系统与右AS建立有BGP会话，所述邻居自治系统接收过来自所述右AS的包含第一IP前缀的路由，以及，所述邻居自治系统没有向所述左AS发布过包含所述第一IP前缀的路由；

所述右AS对应的AS number以及所述左AS对应的AS number是与所述AS_PATH attribute中与所述第一AS number相邻的两个元素，所述右AS对应的AS number位于所述第一AS number的右侧，所述左AS对应的AS number位于所述第一AS number的左侧。

23.一种网络设备，其特征在于，包括：存储器、处理器以及计算机程序，所述计算机程序存储在所述存储器中，所述处理器运行所述计算机程序执行如权利要求1至6任一项所述的方法，或者，如权利要求7至11任一项所述的方法。

24.一种芯片，其特征在于，包括：存储器、处理器以及计算机程序，所述计算机程序存储在所述存储器中，所述处理器运行所述计算机程序执行如权利要求1至6任一项所述的方法，或者，如权利要求7至11任一项所述的方法。

25.一种存储介质，其特征在于，所述存储介质包括计算机程序，所述计算机程序被处理器执行时实现如权利要求1至6任一项所述的方法，或者，如权利要求7至11任一项所述的方法。

BGP路由识别方法、装置及设备

[0001] 本申请是向中国国家知识产权局提交的申请日为2019年03月11日、申请号为201910181646.7、发明名称为“BGP路由识别方法、装置及设备”的申请的分案申请。

技术领域

[0002] 本申请实施例涉及通信技术领域，尤其涉及一种BGP路由识别方法、装置及设备。

背景技术

[0003] 自治系统(Autonomous System，AS)是可以自主决定在本系统内部采用何种路由协议的网络单位，每个自治系统对应一个全局唯一的自治系统号码(AS number)。不同自治系统之间传播路由信息时采用边界网关协议(Border Gateway Protocol，BGP)。每个自治系统中包括至少一个路由设备，其中一个路由设备作为该自治系统的BGP发言者(BGP Speaker)，用于与其他自治系统中的BGP Speaker建立BGP会话，通过BGP会话实现路由信息的传播。

[0004] 不同自治系统之间传播的BGP路由中包括自治系统路径属性(AS_PATH attribute)，AS_PATH attribute指示了从本地自治系统到该BGP路由的起源自治系统(Origin AS)所要经过的所有自治系统。示例性的，以AS1向AS2发送BGP路由为例，AS1中作为BGP Speaker的路由设备向AS2中作为BGP Speaker的路由设备发送BGP路由时，AS1将本地自治系统对应的AS number添加到AS_PATH attribute的最前面(最左边)，然后将BGP路由发送出去。

[0005] 现有技术中，为了避免形成路由环路，在AS2接收到BGP路由之后，会对其中的AS_PATH attribute进行检测，若AS_PATH attribute中包括本地自治系统对应的AS number，则直接将该BGP路由丢弃或者忽略；或者，在AS1生成BGP路由之后发送BGP路由之前，AS1对待发送的BGP路由进行环路检测，若AS_PATH attribute中包括对端自治系统对应的AS number，则直接将该BGP路由丢弃或者忽略。

[0006] 实际应用中，经常出现攻击者劫持BGP路由并对BGP路由进行伪造的情况，现有技术中的BGP路由传播机制，无法及时发现路由劫持情况，导致存在网络安全隐患。

发明内容

[0007] 本申请实施例提供一种BGP路由识别方法、装置及设备，以及时发现路由异常情况，提高网络安全性。

[0008] 第一方面，本申请实施例提供一种边界网关协议BGP路由识别方法，包括：

[0009] 网络设备获取BGP路由，所述BGP路由包括自治系统路径属性AS_PATH attribute，所述AS_PATH attribute包含第一自治系统号码AS number，所述网络设备所在或所管辖的自治系统对应的AS number是第二AS number，所述第一AS number等于所述第二AS number；

[0010] 所述网络设备根据所述第一AS number以及所述第二AS number，确定所述BGP路

由是否为异常的。

[0011] 可选的,所述BGP路由包括第一互联网协议IP前缀;

[0012] 所述网络设备根据所述第一AS number以及所述第二AS number,确定所述BGP路由是否为异常的,包括:

[0013] 所述网络设备根据所述第一AS number是所述AS_PATH attribute中的第一个元素element,以及,所述网络设备没有发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的。

[0014] 可选的,所述BGP路由包括第一互联网协议IP前缀;

[0015] 所述网络设备根据所述第一AS number以及所述第二AS number,确定所述BGP路由是否为异常的,包括:

[0016] 所述网络设备根据所述第一AS number是所述AS_PATH attribute中的第一个元素element,所述网络设备发布过包含第二IP前缀的路由,以及,所述网络设备没有发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的,所述第一IP前缀是所述第二IP前缀的子前缀。

[0017] 可选的,所述BGP路由包括第一互联网协议IP前缀;

[0018] 所述网络设备根据所述第一AS number以及所述第二AS number,确定所述BGP路由是否为异常的,包括:

[0019] 所述网络设备根据所述第一AS number是所述AS_PATH attribute中的第一个元素element,所述网络设备向特定AS发布过仅限于所述特定AS使用的包含所述第一IP前缀的路由,以及,所述AS_PATH attribute中包括第三AS number或者不包括所述第二AS number,确定所述BGP路由是异常的。

[0020] 可选的,所述网络设备根据所述第一AS number以及所述第二AS number,确定所述BGP路由是否为异常的,包括:

[0021] 所述网络设备根据所述第一AS number不是所述AS_PATH attribute中的第一个元素element,以及,所述网络设备所在或所管辖的自治系统与第四AS number对应的自治系统没有建立BGP会话,确定所述BGP路由是异常的,所述第四AS number是所述AS_PATH attribute中与所述第一AS number相邻的元素。

[0022] 可选的,所述BGP路由包括第一互联网协议IP前缀;

[0023] 所述网络设备根据所述第一AS number以及所述第二AS number,确定所述BGP路由是否为异常的,包括:

[0024] 所述网络设备根据所述第一AS number不是所述AS_PATH attribute中的第一个元素element,所述网络设备所在或所管辖的自治系统与左AS建立有BGP会话,所述网络设备所在或所管辖的自治系统与右AS建立有BGP会话,以及,所述网络设备没有接收过来自所述右AS的包含所述第一IP前缀的路由,或者,所述网络设备没有向所述左AS发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的;

[0025] 所述右AS对应的AS number以及所述左AS对应的AS number是与所述AS_PATH attribute中与所述第一AS number相邻的两个元素,所述右AS对应的AS number位于所述第一AS number的右侧,所述左AS对应的AS number位于所述第一AS number的左侧。

[0026] 第二方面,本申请实施例提供一种边界网关协议BGP路由识别方法,包括:

[0027] 网络设备获取BGP路由,所述BGP路由包括自治系统路径属性AS_PATH attribute,所述AS_PATH attribute包含第一自治系统号码AS number,所述网络设备所在或所管辖的自治系统的邻居自治系统对应的AS number是第二AS number,所述第一AS number等于所述第二AS number;

[0028] 所述网络设备根据所述第一AS number以及所述第二AS number,确定所述BGP路由是否为异常的。

[0029] 可选的,所述BGP路由包括第一互联网协议IP前缀;

[0030] 所述网络设备根据所述第一AS number以及所述第二AS number,确定所述BGP路由是否为异常的,包括:

[0031] 所述网络设备根据所述第一AS number是所述AS_PATH attribute中的第一个元素element,以及,所述邻居自治系统没有发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的。

[0032] 可选的,所述BGP路由包括第一互联网协议IP前缀;

[0033] 所述网络设备根据所述第一AS number以及所述第二AS number,确定所述BGP路由是否为异常的,包括:

[0034] 所述网络设备根据所述第一AS number是所述AS_PATH attribute中的第一个元素element,所述邻居自治系统发布过包含第二IP前缀的路由,以及,所述邻居自治系统没有发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的,所述第一IP前缀是所述第二IP前缀的子前缀。

[0035] 可选的,所述网络设备根据所述第一AS number以及所述第二AS number,确定所述BGP路由是否为异常的,包括:

[0036] 所述网络设备根据所述第一AS number不是所述AS_PATH attribute中的第一个元素element,以及,所述邻居自治系统与第三AS number对应的自治系统没有建立BGP会话,确定所述BGP路由是异常的,所述第三AS number是所述AS_PATH attribute中与所述第一AS number相邻的元素。

[0037] 可选的,所述BGP路由包括第一互联网协议IP前缀;

[0038] 所述网络设备根据所述第一AS number以及所述第二AS number,确定所述BGP路由是否为异常的,包括:

[0039] 所述网络设备根据所述第一AS number不是所述AS_PATH attribute中的第一个元素element,所述邻居自治系统与左AS建立有BGP会话,所述邻居自治系统与右AS建立有BGP会话,所述邻居自治系统接收过来自所述右AS的包含第一IP前缀的路由,以及,所述邻居自治系统没有向所述左AS发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的;

[0040] 所述右AS对应的AS number以及所述左AS对应的AS number是与所述AS_PATH attribute中与所述第一AS number相邻的两个元素,所述右AS对应的AS number位于所述第一AS number的右侧,所述左AS对应的AS number位于所述第一AS number的左侧。

[0041] 第三方面,本申请实施例提供一种边界网关协议BGP路由识别装置,包括:

[0042] 获取模块,用于获取BGP路由,所述BGP路由包括自治系统路径属性AS_PATH attribute,所述AS_PATH attribute包含第一自治系统号码AS number,所述网络设备所在

或所管辖的自治系统对应的AS number是第二AS number,所述第一AS number等于所述第二AS number;

[0043] 识别模块,用于根据所述第一AS number以及所述第二AS number,确定所述BGP路由是否为异常的。

[0044] 可选的,所述BGP路由包括第一互联网协议IP前缀,所述识别模块具体用于:

[0045] 根据所述第一AS number是所述AS_PATH attribute中的第一个元素element,以及,所述网络设备没有发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的。

[0046] 可选的,所述BGP路由包括第一互联网协议IP前缀,所述识别模块具体用于:

[0047] 根据所述第一AS number是所述AS_PATH attribute中的第一个元素element,所述网络设备发布过包含第二IP前缀的路由,以及,所述网络设备没有发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的,所述第一IP前缀是所述第二IP前缀的子前缀。

[0048] 可选的,所述BGP路由包括第一互联网协议IP前缀,所述识别模块具体用于:

[0049] 根据所述第一AS number是所述AS_PATH attribute中的第一个元素element,所述网络设备向特定AS发布过仅限于所述特定AS使用的包含所述第一IP前缀的路由,以及,所述AS_PATH attribute中包括第三AS number或者不包括所述第二AS number,确定所述BGP路由是异常的。

[0050] 可选的,所述识别模块具体用于:

[0051] 根据所述第一AS number不是所述AS_PATH attribute中的第一个元素element,以及,所述网络设备所在或所管辖的自治系统与第四AS number对应的自治系统没有建立BGP会话,确定所述BGP路由是异常的,所述第四AS number是所述AS_PATH attribute中与所述第一AS number相邻的元素。

[0052] 可选的,所述BGP路由包括第一互联网协议IP前缀,所述识别模块具体用于:

[0053] 根据所述第一AS number不是所述AS_PATH attribute中的第一个元素element,所述网络设备所在或所管辖的自治系统与左AS建立有BGP会话,所述网络设备所在或所管辖的自治系统与右AS建立有BGP会话,以及,所述网络设备没有接收过来自所述右AS的包含所述第一IP前缀的路由,或者,所述网络设备没有向所述左AS发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的;

[0054] 所述右AS对应的AS number以及所述左AS对应的AS number是与所述AS_PATH attribute中与所述第一AS number相邻的两个元素,所述右AS对应的AS number位于所述第一AS number的右侧,所述左AS对应的AS number位于所述第一AS number的左侧。

[0055] 第四方面,本申请实施例提供一种边界网关协议BGP路由识别装置,包括:

[0056] 获取模块,用于获取BGP路由,所述BGP路由包括自治系统路径属性AS_PATH attribute,所述AS_PATH attribute包含第一自治系统号码AS number,所述网络设备所在或所管辖的自治系统的邻居自治系统对应的AS number是第二AS number,所述第一AS number等于所述第二AS number;

[0057] 识别模块,用于根据所述第一AS number以及所述第二AS number,确定所述BGP路由是否为异常的。

[0058] 可选的,所述BGP路由包括第一互联网协议IP前缀,所述识别模块具体用于:

[0059] 根据所述第一AS number是所述AS_PATH attribute中的第一个元素element,以

及,所述邻居自治系统没有发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的。

[0060] 可选的,所述BGP路由包括第一互联网协议IP前缀,所述识别模块具体用于:

[0061] 根据所述第一AS number是所述AS_PATH attribute中的第一个元素element,所述邻居自治系统发布过包含第二IP前缀的路由,以及,所述邻居自治系统没有发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的,所述第一IP前缀是所述第二IP前缀的子前缀。

[0062] 可选的,所述识别模块具体用于:

[0063] 根据所述第一AS number不是所述AS_PATH attribute中的第一个元素element,以及,所述邻居自治系统与第三AS number对应的自治系统没有建立BGP会话,确定所述BGP路由是异常的,所述第三AS number是所述AS_PATH attribute中与所述第一AS number相邻的元素。

[0064] 可选的,所述BGP路由包括第一互联网协议IP前缀,所述识别模块具体用于:

[0065] 根据所述第一AS number不是所述AS_PATH attribute中的第一个元素element,所述邻居自治系统与左AS建立有BGP会话,所述邻居自治系统与右AS建立有BGP会话,所述邻居自治系统接收过来自所述右AS的包含第一IP前缀的路由,以及,所述邻居自治系统没有向所述左AS发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的;

[0066] 所述右AS对应的AS number以及所述左AS对应的AS number是与所述AS_PATH attribute中与所述第一AS number相邻的两个元素,所述右AS对应的AS number位于所述第一AS number的右侧,所述左AS对应的AS number位于所述第一AS number的左侧。

[0067] 第五方面,本申请实施例提供一种网络设备,其特征在于,包括:存储器、处理器以及计算机程序,所述计算机程序存储在所述存储器中,所述处理器运行所述计算机程序执行第一方面任一项所述的方法,或者,如第二方面任一项所述的方法。

[0068] 第六方面,本申请实施例提供一种芯片,包括:存储器、处理器以及计算机程序,所述计算机程序存储在所述存储器中,所述处理器运行所述计算机程序执行如第一方面任一项所述的方法,或者,如第二方面任一项所述的方法。

[0069] 第七方面,本申请实施例提供一种存储介质,所述存储介质包括计算机程序,所述计算机程序被处理器执行时实现如第一方面任一项所述的方法,或者,如第二方面任一项所述的方法。

[0070] 本申请实施例提供的BGP路由识别方法、装置及设备,网络设备获取BGP路由,所述BGP路由包括自治系统路径属性AS_PATH attribute,所述AS_PATH attribute包含第一自治系统号码AS number,所述网络设备所在或所管辖的自治系统对应的AS number是第二AS number,所述第一AS number等于所述第二AS number;所述网络设备根据所述第一AS number以及所述第二AS number,确定所述BGP路由是否为异常的,从而能够及时发现路由劫持等原因导致的异常环路路由,提高了网络安全性。

附图说明

[0071] 图1为本申请适用的网络架构的示意图一;

[0072] 图2为本申请适用的网络架构示意图二;

[0073] 图3为本申请实施例中BGP路由传播过程示意图；

[0074] 图4为本申请一实施例提供的BGP路由识别方法的流程示意图；

[0075] 图5为本申请实施例的应用场景示意图一；

[0076] 图6为本申请实施例的应用场景示意图二；

[0077] 图7为本申请另一实施例提供的BGP路由识别方法的流程示意图；

[0078] 图8为本申请实施例的应用场景示意图三；

[0079] 图9为本申请实施例的应用场景示意图四；

[0080] 图10为本申请一实施例提供的BGP路由识别装置的结构示意图；

[0081] 图11为本申请另一实施例提供的BGP路由识别装置的结构示意图；

[0082] 图12为本申请一实施例提供的网络设备的硬件结构示意图。

具体实施方式

[0083] 本申请实施例描述的网络架构以及业务场景是为了说明本申请实施例的技术方案，并不构成对于本申请实施例提供的技术方案的限定，本领域普通技术人员可知，随着网络架构的演变和新业务场景的出现，本申请实施例提供的技术方案对于类似的技术问题，同样适用。

[0084] 首先对本申请实施例中涉及的概念进行解释：

[0085] (1)自治系统(Autonomous System，AS)：在互联网中，一个AS是一个有权自主地决定在本系统中应采用何种路由协议的网络单位。这个网络单位可以是一个简单的网络也可以是由一个或多个普通的网络组成的网络群体，它是一个单独的可管理的网络单元(例如：一个运营商、一所大学、一个企业)。一个自治系统有时也被称为是一个路由选择域(routing domain)。在一个自治系统中的所有路由设备必须相互连接，运行相同的路由协议。一个自治系统对应一个唯一的自治系统号码(AS number)。

[0086] (2)内部网关协议(Interior Gateway Protocol，IGP)：在一个自治系统内部所使用的一种路由协议。一个自治系统内部包括多个路由设备，多个路由设备之间互相连接，各路由设备之间通过IGP协议传播路由。

[0087] (3)边界网关协议(Border Gateway Protocol，BGP)：用于在不同自治系统之间的传播路由。不同自治系统中作为BGP Speaker的路由设备之间建立BGP会话，通过BGP会话传播路由。示例性的，全国各大网络运营商多数都是通过BGP协议与自身的AS number来实现多线互联的，使用BGP协议互联后，网络运营商的所有骨干路由设备将会判断到互联网数据中心(Internet Data Center，IDC)的最佳路由，以保证不同网络运营商用户的高速访问。

[0088] 图1为本申请适用的网络架构的示意图一，该网络架构中包括至少两个AS，示例性的，图1中示出了包括5个AS的场景。不同AS之间传播BGP路由时采用边界网关协议(Border Gateway Protocol，BGP)。图1中，不同AS之间的连线表示BGP会话。一个BGP会话连接的两个AS可以互称为邻居AS。例如：图1中的AS1与AS2互为邻居AS，AS2与AS3互为邻居AS，AS1与AS4互为邻居AS，AS4与AS5互为邻居AS。

[0089] 图2为本申请适用的网络架构示意图二，图2示例了网络架构中包括AS1和AS2的场景。如图2所示，每个AS中均可以包括多个路由设备，AS内部的路由设备之间为IGP会话连接。每个AS中负责与其他AS进行BGP路由传播的AS称为BGP发言者(BGP Speaker)。如图2所

示,AS1内部的路由设备2为BGP Speaker,AS2内部的路由设备5为BGPSpeaker。

[0090] 一个BGP会话连接的两个AS中的各自的BGPSpeaker互为BGP对等体。例如:图2中的路由设备2与路由设备5互为BGP对等体。示例性的,当AS1向AS2发送BGP路由时,需要在路由设备2与路由设备5之间建立BGP会话,从而路由设备2通过BGP会话将BGP路由发送给路由设备5。

[0091] 图1和图2只是举例说明,并非限定,该网络架构中还可以包括更多的自治系统和路由设备。另外,路由设备可以是具有路由功能的任意设备,包括但不限于路由器、交换机等。另外,每个AS中除了路由设备之外,还可以包括其他设备,例如:控制器、服务器等。

[0092] 图3为本申请实施例中BGP路由传播过程示意图,如图3所示,示例性的,网络中包括4个AS,分别为AS100、AS200、AS300、AS500。其中,AS500与AS200之间建立BGP会话,AS200与AS100之间建立BGP会话,AS100与AS300之间建立BGP会话。

[0093] 对于一条BGP路由的传播过程而言,始发该BGP路由的自治系统称为起源AS(Origin AS),转发该BGP路由的自治系统称为转发AS(Transit AS)。例如,起源AS中的一个BGP speaker始发了BGP路由。该BGP路由中可以携带该BGP speaker产生的ORIGIN attribute。ORIGIN attribute是一种知名强制属性(a well-known mandatory attribute)。关于ORIGIN attribute,可以参考IETF发布的RFC4271定义的路径属性(Path Attributes)。

[0094] 示例性的,图3中示例了两条BGP路由。第一条BGP路由的传播过程为AS100->AS200->AS500,对于该条BGP路由,AS100称为起Origin AS,AS200和AS500称为Transit AS。第二条BGP路由的传播过程为AS100->AS300,对于该条BGP路由,AS100称为Origin AS,AS300称为Transit AS。

[0095] 不同自治系统之间传播的BGP路由中包括互联网协议(Internet Protocol,IP)前缀和自治系统路径属性AS_PATH attribute。

[0096] 其中,IP前缀表示该BGP路由对应的中Origin AS发布的网络地址集合。本申请实施例中,如无特殊说明,IP前缀均采用IP地址加掩码位数的方式进行表示,即:

[0097] A.B.C.D/X

[0098] 其中,A.B.C.D为IP地址,X为掩码位数。示例性的,10.10.0.0/16表示的是从10.10.10.0.0到10.10.255.255之间的所有网络地址;10.10.10.0/24表示的是从10.10.10.0至10.10.10.255之间的所有网络地址。

[0099] AS_PATH attribute包括该BGP路由所经过的各AS对应的自治系统号码(AS number)。AS_PATH attribute中记录的各AS number是按照从本地自治系统到始发自治系统(Origin AS)所要经过的各自治系统的顺序依次排列。AS_PATH attribute中的最右边第一个AS number表示的是BGP路由中Origin AS的号码,其余AS number表示的是BGP路由中Transit AS的号码。示例性的,某BGP路由的AS_PATH attribute为:100、200、300,则说明该BGP路由从AS300始发后,依次经过了AS200和AS100的转发。

[0100] 可以理解的,Origin AS在发布一条BGP路由时,在BGP路由中携带IP前缀和AS_PATH attribute,IP前缀指示的是该BGP路由所支持的网络地址集合,AS_PATH attribute指示的是到达Origin AS所要依次经过的各AS。当网络中其他AS接收到该BGP路由后,可以获知该BGP路由对应的Origin AS的网络地址集合,并获取达到Origin AS所要经过的各AS。

当其他AS需要向这些网络地址集合中的地址发送报文时，选择在该BGP路由上传递报文。

[0101] 下面结合图3描述BGP路由的传播过程。假设AS100根据自身业务需求，需要向其他AS发布BGP路由，该BGP路由包含的IP前缀为207.126.0.0/16。AS100将本地自治系统的AS number添加到AS_PATH attribute中，并通过Update消息将该BGP路由发送给AS100的邻居AS。如图3所示，AS100分别向AS200和AS300发送了BGP路由，该BGP路由的内容如表1所示。

[0102] 表1

[0103]

IP前缀	207.126.0.0/16
AS_PATH attribute	100

[0104] 继续参见图3，AS200接收到该BGP路由后，对该BGP路由进行学习，然后把本地自治系统的AS number添加到AS_PATH attribute的最前面(最左边)，并将BGP路由发送给AS200的邻居AS500。AS200发送给AS500的BGP路由的内容如表2所示。可以理解的，AS300接收到AS100发送的BGP路由后的处理过程与AS200类似，此处不再赘述。

[0105] 表2

[0106]

IP前缀	207.126.0.0/16
AS_PATH attribute	200,100

[0107] AS500接收到AS200发送的BGP路由后，对该BGP路由进行学习，然后把本地自治系统的AS number添加到AS_PATH attribute的最前面(最左边)，并将BGP路由发送给AS500的邻居自治系统。AS500发出的BGP路由的内容如表3所示。

[0108] 表3

[0109]

IP前缀	207.126.0.0/16
AS_PATH attribute	500,200,100

[0110] 由图3可知，每个自治系统接收到BGP路由后，根据其中的AS_PATH attribute，即可获知从本地自治系统去往AS100所要依次经过的AS，也就是说，按照AS_PATH attribute中从左向右的AS number的顺序即可到达AS100。

[0111] 在网络中进行BGP路由传播的过程中，有可能出现环路。例如:AS100发布一个BGP路由后，该BGP路由经过其他AS的转发后，又传播到了AS100;或者，AS100发布一个BGP路由后，经过AS200的转发传播到AS300，后续又经过一个或者多个AS的转发后，又传播到了AS200或AS300。为了避免在BGP路由传播过程中形成环路，需要在BGP路由传播过程中进行环路检测。

[0112] 一种技术中，作为接收端的自治系统在接收到BGP路由后，对BGP路由中的AS_PATH attribute进行检测。如果AS_PATH attribute中出现本地自治系统的AS number，则认为出现环路，将该BGP路由丢弃或者忽略，以免形成环路。

[0113] 另一种技术中，如果使能了自治系统之间的水平分割功能，则作为发送端的自治系统在向接收端自治系统发送BGP路由之前，对待发送的BGP路由进行检测。如果AS_PATH attribute中出现接收端自治系统对应的AS number，则认为出现环路，将该BGP路由丢弃或者忽略，以免该BGP路由发送到接收端AS后形成环路。

[0114] 然而，当前部署BGP的网络上，经常会发生伪造BGP路由的事件。具体的，路由劫持者劫持到BGP路由后，对BGP路由中的IP前缀或者AS_PATH attribute进行篡改，生成伪造的

BGP路由。

[0115] 路由劫持者可能有如下目的：

[0116] 1、路由劫持者试图使伪造后的路由看起来像是某些AS发布的路由，或者看起来像是传播过程中经过了某些AS，使路由看起来像一条正常的路由，避免引起别人的警觉；

[0117] 2、路由劫持者在BGP路由的AS_PATH attribute中加入某些自治系统的AS number，阻止这些使用这些AS number的系统接收该BGP路由。示例性的，BGP路由的AS_PATH attribute中有AS500之后，AS500接收到这条路由时，会认为是路由环路而将其丢弃，可见路由劫持者正是利用了现有BGP协议处理中环路检测处理的特点。

[0118] 下面结合具体的例子，分别描述上述两种技术下，路由劫持对网络安全的影响。

[0119] 假设网络中包括6个AS，分别为：AS100、AS200、AS300、AS400、AS500、AS600。某BGP路由的Origin AS为AS600，始发的IP前缀为10.10.0.0/16。该BGP路由从AS600始发后，经过AS500、AS400后传播到AS300，AS300再将该BGP路由传播给AS200。正常情况下，AS300向AS200发送的BGP路由的内容如表4所示。

[0120] 表4

[0121]

IP前缀	10.10.0.0/16
AS_PATH attribute	300,400,500,600

[0122] 一种可能的路由伪造场景中，该BGP路由传播到AS300后，位于AS300的路由劫持者对该路由的AS_PATH attribute进行篡改。篡改的BGP路由的内容如表5所示。AS200接收到篡改的BGP路由。该场景下，AS300将AS200伪造为该BGP路由的Origin AS，使得该BGP路由看起来像是AS200始发的。

[0123] 表5

[0124]

IP前缀	10.10.0.0/16
AS_PATH attribute	300,200

[0125] 另一种可能的路由伪造场景中，该BGP路由传播到AS300后，位于AS300的路由劫持者对该路由的AS_PATH attribute进行篡改。篡改的BGP路由的内容如表6所示。AS200接收到篡改的BGP路由。该场景下，AS300将AS200伪造为该BGP路由的Transit AS，使得该BGP路由看起来像是经过了AS200的转发。

[0126] 表6

[0127]

IP前缀	10.10.0.0/16
AS_PATH attribute	300,200,600

[0128] 需要说明的是，实际应用中，还会存在其他可能的路由伪造场景，本实施例不一一列举，上述两种路由伪造场景仅为示例性说明。

[0129] 基于上述的第一种技术，当AS200接收到如表5或者如表6所示的伪造路由时可以执行环路检测。在环路检测过程中，检测到AS_PATH attribute中包括本地自治系统的AS number(200)。因此，会认为该BGP路由为环路路由，AS200直接丢弃或者忽略该BGP路由。而实际上，针对表5所示的数据，AS200并未始发该BGP路由；针对表6所示的数据，AS200并未转发过该BGP路由。也就是说，该场景下的环路并非正常环路，而是由于路由劫持者的伪造导致的环路。

[0130] 基于上述的第二种技术，假设AS300将表5或者表6所示的路由作为待发送的BGP路由。AS300在向AS200发送之前，执行环路检测过程。环路检测过程中，检测到AS_PATH attribute包括接收端AS200的AS number(200)。进而，认为该BGP路由被发送到AS200后会形成环路。因此，AS300直接将该BGP路由丢弃或者忽略。而实际上，针对表5所示的数据，AS200实际并未始发过该BGP路由；针对表6所示的数据，AS200并未转发过该BGP路由，也就是说，该场景下的环路并非正常环路，而是由于路由劫持者的伪造导致的环路。

[0131] 可见，上述两种技术中，当自治系统中的网络设备检测到路由环路时，直接丢弃或者忽略该BGP路由。以上使得无法及时发现路由劫持情况，导致存在网络安全隐患。

[0132] 为了解决上述技术问题，本申请实施例提供一种BGP路由识别方法。当BGP路由中出现环路的情况下，能够进一步识别到该BGP路由是否是异常的。例如是否是伪造路由或者协议配置错误导致的路由异常。从而，能够及时发现网络中的路由传播异常情况，提高网络安全性。

[0133] 图4为本申请一实施例提供的BGP路由识别方法的流程示意图。如图4所示，本实施例的方法包括：S401以及S402。

[0134] S401：网络设备获取BGP路由，所述BGP路由包括自治系统路径属性AS_PATH attribute，所述AS_PATH attribute包含第一自治系统号码AS number，所述网络设备所在或所管辖的自治系统对应的AS number是第二AS number，所述第一AS number等于所述第二AS number。

[0135] 本实施例中，网络设备可以是自治系统内部的任意网络设备。例如：网络设备可以是自治系统内的路由设备，比如作为BGP Speaker的路由设备。另外，网络设备还可以是管辖自治系统的网络设备。例如：网络设备可以是用于控制和监控自治系统内部各路由设备的控制器或者服务器。

[0136] 本实施例中的网络设备所在或所管辖的自治系统，是在BGP路由传播过程中作为接收端的自治系统。为了描述方便，本实施例中将执行主体网络设备所在或所管辖的自治系统称为本地自治系统。将在BGP路由传播过程中作为发送端的自治系统，称为发送端自治系统。

[0137] 第一种可能的应用场景中，网络设备为本地自治系统内部作为BGP Speaker的路由设备。图5为本申请实施例的应用场景示意图一。如图5所示，在本地自治系统的路由设备中设置BGP路由识别装置，用于执行本实施例的方法。

[0138] 该场景下，S401中的网络设备获取BGP路由，包括：路由设备接收BGP路由。具体的，路由设备接收由发送端自治系统中的BGP Speaker发送的BGP路由。

[0139] 第二种可能的应用场景中，网络设备为管辖本地自治系统的控制器。图6为本申请实施例的应用场景示意图二。如图6所示，在管辖本地自治系统的控制器中设备BGP路由识别装置，用于执行本实施例的方法。

[0140] 该场景下，S401中的网络设备获取BGP路由，包括：控制器接收由路由设备发送的BGP路由。具体的，本地自治系统的路由设备(例如BGP Speaker)从发送端自治系统的BGP Speaker接收到BGP路由后，将该BGP路由转发给控制器。

[0141] 针对每个自治系统而言，控制器与该自治系统内部的路由设备通过BGP监测协议(BGP Monitoring Protocol，BMP)连接。控制器用于监控路由设备的BGP路由的接收情况。

为支持本实施例,BMP协议需要做一些扩展。当前BMP协议的RFC7854支持7种消息类型,包括下述的Type 0～6。本实施例中新增一种消息类型,即下述的Type＝TBD1:Diagnosis Message,该消息用于收集各路由设备的诊断信息。

[0142] Type＝0:Route Monitoring

[0143] Type＝1:Statistics Report

[0144] Type＝2:Peer Down Notification

[0145] Type＝3:Peer Up Notification

[0146] Type＝4:Initiation Message

[0147] Type＝5:Termination Message

[0148] Type＝6:Route Mirroring Message

[0149] Type＝TBD1:Diagnosis Message

[0150] 具体的,本地自治系统中BGP Speaker与控制器之间建立BMP会话。本地自治系统中BGP Speaker和发送端自治系统中的BGP Speaker之间建立BGP会话。本地自治系统中BGP Speaker接收到BGP路由信息后,将该BGP路由信息封装在上述新增的诊断消息中。然后,将该诊断消息转发给控制器。控制器通过解析该诊断消息,获取BGP路由,执行后续的BGP路由识别过程。

[0151] 本实施例中,网络设备获取的BGP路由中包括自治系统路径属性AS_PATH attribute,其中,AS_PATH attribute中可以包括一个或者多个自治系统号码(AS number)。本实施例对应的应用场景中,AS_PATH attribute中包括与本地自治系统的自治系统号码相同的AS number。为了描述方便,本实施例中将本地自治系统对应的AS number称为第二AS number,将AS_PATH attribute中与第二AS number相同的AS number称为第一AS number。也就是说,第一AS number等于第二AS number。

[0152] 当然,BGP路由除了AS_PATH attribute之外,还可以包括其他信息,例如:IP前缀。IP前缀可以携带在网络层可达信息(Network Layer ReachabilityInformation,NLRI)域。NLRI field可以携带在BGP update消息中。本申请中,IP前缀也可以称为IP地址前缀。

[0153] 下面结合举例进行说明。假设网络中包括四个自治系统,分别为:AS100、AS200、AS300、AS400。一条BGP路由从AS100始发(originated)后,经过AS200、AS300转发到AS400后,AS400接收的BGP路由中的内容如表7所示。

[0154] 表7

[0155]

IP前缀	10.10.0.0/16
AS_PATH attribute	300,200,100

[0156] 网络设备获取到该BGP路由。由于AS_PATH attribute中不包括本地自治系统对应的AS number(400),因此,可以按照已有的路由传播过程进行处理。例如,将本地自治系统的AS number(400)添加至AS_PATH attribute的最前面(最左边),并将BGP路由传播给AS400的邻居自治系统。本申请中,AS400是指AS number为400的AS。

[0157] 假设AS400接收到的BGP路由如表8或者如表9所示。由于AS_PATH attribute中包括本地自治系统的AS number(400),因此,执行步骤S402,从而确定该BGP路由是否是异常的。

[0158] 表8

[0159]

IP前缀	10.10.0.0/16
AS_PATH attribute	300,400

[0160] 表9

[0161]

IP前缀	10.10.0.0/16
AS_PATH attribute	300,400,100

[0162] S402:所述网络设备根据所述第一AS number以及所述第二AS number,确定所述BGP路由是否为异常的。

[0163] 本实施例中,异常可以是BGP路由是伪造的。另外,异常也可以是协议配置错误导致的BGP路由异常。

[0164] BGP路由伪造可以具体是路由劫持者对BGP路由进行篡改。例如,路由劫持者劫持到BGP路由后对BGP路由中的IP前缀和/或AS_PATH attribute进行篡改,使得篡改后的BGP路由看起来像是由某个AS始发的,或者看起来像是经过了某些AS的转发。

[0165] 协议配置错误导致的BGP路由异常是指,由于某个自治系统的配置错误导致BGP路由被传播到不应该接收该BGP路由的自治系统中。例如:AS1向AS2发布了一条BGP路由,并在该BGP路由的团体属性(community attribute)中指示该BGP路由是专供AS2使用的。例如,AS2接收到的BGP路由携带禁止输出团体属性(NO_EXPORTcommunities attribute)。NO_EXPORTcommunities attribute的值可以是0xFFFFFF01。AS2协议配置正确的情况下,AS2可以根据NO_EXPORTcommunities attribute确定该BGP路由是专供AS2使用的。由于AS2的协议配置错误,AS2将该BGP路由转发给了AS3。该场景中,AS3是不应该接收该BGP路由的AS。另一种场景中,AS2将该BGP路由转发至其他AS。其他AS将该BGP路由转发至AS1。该场景中,其他AS以及AS1是不应该接收该BGP路由的AS。本实施例中将该情况对应的BGP路由称为“由于协议配置错误导致的BGP路由异常”。

[0166] 本实施例中,网络设备获取到的BGP路由中,当AS_PATH attribute中包括与本地自治系统对应的AS number相等的第一AS number时,确定BGP路由是异常的。当AS_PATH attribute中不包括与本地自治系统对应的AS number相等的第一AS number时,确定BGP路由是正常的。

[0167] 一种可能的实施方式中,所述网络设备根据所述第一AS number、所述第二AS number以及所述第一AS number在所述AS_PATH attribute中的位置,确定所述BGP路由是否为异常的。

[0168] 本实施例中,在网络设备获取到的BGP路由的AS_PATH attribute中包括与本地自治系统的AS number相等的第一AS number时,可以进一步根据所述第一AS number在所述AS_PATH attribute中的位置,确定所述BGP路由是否为异常的。

[0169] 其中,AS_PATH attribute可以包括一个或者多个AS number。每个AS number可以称为AS_PATH attribute的一个元素(element)。本实施例中,第一AS number在所述AS_PATH attribute中的位置是指:第一AS number是AS_PATH attribute中第几个元素。

[0170] 可以理解的,第一AS number与本地自治系统对应的第二AS number相等。当第一AS number是AS_PATH attribute中第一个元素时,说明本地自治系统是BGP路由的Origin AS。当第一AS number不是AS_PATH attribute中第一个元素时,说明本地自治系统是BGP路由的Transit AS。

[0171] 其中,第一个元素是指位于AS_PATH attribute最右位置(rightmost position)的元素。

[0172] 当根据第一AS number在所述AS_PATH attribute中的位置确定出本地自治系统是BGP路由中的Origin AS或者Transit AS后,可以进一步根据AS_PATH attribute确定该BGP路由是否是异常的。

[0173] 一种可能的实施方式中,若第一AS number是AS_PATH attribute的第一个元素,说明本地自治系统是BGP路由的Origin AS。可以确定出AS_PATH attribute中与第一AS number左相邻的AS number。通过判断左相邻的AS number对应的自治系统是否与本地自治系统建立BGP会话,来确定该BGP路由是否为伪造的。例如:若所述左相邻的AS number对应的自治系统并未与本地自治系统建立BGP会话,则说明该BGP路由是伪造的。

[0174] 另一种可能的实施方式中,若第一AS number不是AS_PATH attribute的第一个元素,说明本地自治系统是BGP路由的Transit AS。可以确定出AS_PATH attribute中与第一AS number左相邻的AS number和右相邻的AS number,通过判断左相邻的AS number对应的自治系统和右相邻的AS number对应的自治系统是否与本地自治系统建立BGP会话,来确定该BGP路由是否为伪造的。例如:若左相邻的AS number对应的自治系统和右相邻的AS number对应的自治系统中,至少一个没有与本地自治系统建立BGP会话,则说明该BGP路由是伪造的。

[0175] 具体实施过程中,可以在本地自治系统的数据库中存储网络中各自治系统之间的实际连接关系,即各自治系统之间建立BGP会话的连接关系。当网络设备接收到如表8或者如表9所示的BGP路由时,可以根据BGP路由中的AS_PATH attribute以及数据库中存储的各自治系统之间的实际连接关系进行判断。

[0176] 需要说明的是,本实施例中的数据库,可以是设置在本地自治系统的路由设备上的数据库。也可以是设置在本地自治系统内部的其他网络设备的数据库。还可以是设置在管辖本地自治系统的控制器或者服务器中的数据库。本实施例对此不作具体限定。

[0177] 一种可能的实施方式中,在网络中设置全局控制器。全局控制器与网络中的各个自治系统连接,用于从各个自治系统中获取路由信息以及各自治系统之间的连接关系信息。同时,全局控制器还用于将收集到的信息同步至各个自治系统的本地数据库中。从而每个自治系统均可以从本地数据库中查询到各自治系统的路由信息以及各自治系统之间的连接关系信息。

[0178] 进一步的,在BGP路由中还包括IP前缀的情况下,在确定BGP路由是否异常时还可以结合IP前缀进行判断。下面结合几种具体的实施方式进行介绍。

[0179] 一种可能的实施方式中,所述BGP路由包括第一互联网协议IP前缀,所述网络设备根据所述第一AS number是所述AS_PATH attribute中的第一个元素element,以及,所述网络设备没有发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的。

[0180] 另一种表述方式为:若本地自治系统对应的AS number是所述AS_PATH attribute中的第一个元素element时,并且,本地自治系统没有发布过包含第一IP前缀的路由,则确定BGP路由是异常的。

[0181] 本申请中,“发布”包括:初始生成(originated)并发布,和,接收并发布。初始生成(originated)并发布指的是自治系统初始生成BGP路由并发布给其他AS。接收并发布指的

是自治系统从其他AS接收到BGP路由并发布给另外的AS。本实施例中，“初始生成并发布”可以称为始发，“接收并发布”可以称为转发。

[0182] “网络设备没有发布过包含第一IP前缀的路由”具体可以是网络设备在执行S402之前尚未发布过包含IP前缀的路由。“网络设备没有发布过包含第一IP前缀的路由”具体实现时可以是第一种情况或者第二种情况。第一种情况是网络设备没有初始生成并发布过包含第一IP前缀的路由。例如，网络设备没有生成包含第一IP前缀的路由。网络设备的数据库没有记录包含第一IP前缀的路由。第二种情况是网络设备没有接收并发布过包含第一IP前缀的路由。例如，网络设备没有从其他AS接收过包含第一IP前缀的路由并发布给另外的AS。

[0183] 具体实施过程中，本地自治系统的数据库用于记录本地自治系统发布的至少一个第二IP前缀，当BGP路由中的第一IP前缀与各第二IP前缀均不匹配，则确定BGP路由是异常的。

[0184] 需要说明的是，上述的匹配是指完全匹配，即IP地址和掩码位数完全匹配。

[0185] 下面举例说明，假设本地自治系统的数据库中记录了本地自治系统发布过两个IP前缀，分别为：10.1.0.0/16、10.2.0.0/16。

[0186] 一种情况下，路由设备获取的BGP路由中，本地自治系统对应的AS number是所述AS_PATH attribute中的第一个元素element，并且BGP路由中的IP前缀为10.3.0.0/16。该情况下，网络设备在进行BGP路由识别时，由于BGP路由中的IP前缀(10.3.0.0/16)与上述数据库中记录的两个IP前缀(10.1.0.0/16、10.2.0.0/16)均不匹配，因此，确定该BGP路由是伪造的。

[0187] 另一种情况下，路由设备获取的BGP路由中，本地自治系统对应的AS number是所述AS_PATH attribute中的第一个元素element，并且BGP路由中的IP前缀为10.2.1.0/24。该情况下，网络设备进行BGP路由识别时，由于BGP路由中的IP前缀(10.2.1.0/24)与上述数据库中记录的两个IP前缀(10.1.0.0/16、10.2.0.0/16)均不匹配，因此，确定BGP路由是伪造的。

[0188] 本实施方式对应的场景为：本地自治系统对应的AS number是所述AS_PATH attribute中的第一个元素element，但是，本地自治系统没有发布过包含第一IP前缀的路由。该场景下，说明是劫持者对BGP路由的IP前缀或AS_PATH attribute进行了伪造，使得伪造后的路由看起来像是该IP前缀是本地自治系统发布的，因此，这是纯粹的路由伪造事件，可以将该类型的路由伪造称为异常类型1。

[0189] 另一种可能的实施方式中，所述BGP路由包括第一互联网协议IP前缀，所述网络设备根据所述第一AS number是所述AS_PATH attribute中的第一个元素element，所述网络设备发布过包含第二IP前缀的路由，以及，所述网络设备没有发布过包含所述第一IP前缀的路由，确定所述BGP路由是异常的，所述第一IP前缀是所述第二IP前缀的子前缀。

[0190] 本申请中，网络设备发布过包含第二IP前缀的路由可以是网络设备执行S402之前发布过包含第二IP前缀的路由。

[0191] 另一种表述方式为：若本地自治系统对应的AS number是所述AS_PATH attribute中的第一个元素element，并且，所述第一IP前缀是本地自治系统发布过的某个第二IP前缀的子前缀，但是，本地自治系统没有发布过所述第一IP前缀，则确定所述BGP路由是异常的。

[0192] 其中，本实施例中“第一IP前缀是第二IP前缀的子前缀”是指：第一IP前缀所指示

的网络地址集合是第二IP前缀所指示的网络地址集合的子集，并且第一IP前缀所指示的网络地址集合不等于第二IP前缀所指示的网络地址集合。示例性的，假设第一IP前缀为10.10.192.0/24，第二IP前缀为10.10.128.0/17，由于第一IP前缀对应的网络地址集合为从10.10.192.0至10.10.192.255之间的网络地址，第二IP前缀对应的网络地址集合为从10.10.128.0至10.10.255.255之间的网络地址，第一IP前缀对应的网络地址集合是第二IP前缀对应的网络地址集合的子集，因此，认为第一IP前缀是第二IP前缀的子前缀。

[0193] 本实施方式对应的场景为：本地自治系统对应的AS number是所述AS_PATH attribute中的第一个元素element，并且，所述第一IP前缀是本地自治系统发布过的某个第二IP前缀的子前缀，但是本地自治系统没有发布过所述第一IP前缀。该场景下，说明是劫持者对BGP路由的IP前缀或AS_PATH attribute进行了伪造，使得伪造后的路由看起来像是本地自治系统发布过某个IP前缀的子前缀，因此，这是纯粹的路由伪造事件，可以将该类型的路由伪造称为异常类型2。

[0194] 又一种可能的实施方式中，所述网络设备根据第一AS number是所述AS_PATH attribute中的第一个元素element，以及，所述网络设备向所述AS_PATH attribute中与第一AS number相邻的元素对应的自治系统发布过包含所述第一IP前缀的路由，确定所述BGP路由是正常的。

[0195] 示例性的，假设本地自治系统的数据库中记录了AS100曾向AS200发布过一条BGP路由，IP前缀为10.10.10.0/24。若网络设备接收到的BGP路由的IP前缀为10.10.10.0/24，AS_PATH attribute为300、200、100，则确定该BGP路由为正常的。

[0196] 本实施例中，在确定BGP路由是正常的情况下，说明该BGP路由的环路类型为正常环路，可以按照现有技术中的处理方式，对该BGP路由丢弃或者忽略处理，以免造成路由环路。

[0197] 又一种可能的实施方式中，所述BGP路由包括第一互联网协议IP前缀，所述网络设备根据所述第一AS number是所述AS_PATH attribute中的第一个元素element，所述网络设备向特定AS发布过仅限于所述特定AS使用的包含所述第一IP前缀的路由，以及，所述AS_PATH attribute中包括第三AS number或者不包括所述第二AS number，确定所述BGP路由是异常的。

[0198] 其中，第三AS number不等于第一AS number，也不等于第二AS number。

[0199] 本申请中，网络设备向特定AS发布过仅限于所述特定AS使用的包含所述第一IP前缀的路由，可以是网络设置在执行S402之前发布过仅限于特定AS使用的包含第一IP前缀的路由。

[0200] 其中，网络设备向特定AS发布过仅限于特定AS使用的包含第一IP前缀的路由，可以具体是指网络设备在发布包含第一IP前缀的路由时，在该路由的团体属性(community attribute)中指示了该路由仅限于特定AS专用。例如，网络设备在发布包含第一IP前缀的路由时，在团体属性中携带禁止输出团体属性(NO_EXPORTcommunities attribute)。NO_EXPORTcommunities attribute的值可以是0xFFFFFF01。

[0201] 具体实施过程中，本地自治系统的数据库还用于记录本地自治系统发布(advertised)过的IP前缀，并且还记录各IP前缀发布给哪些AS，以及各IP前缀是否是某些特定AS专用等信息。当网络设备获取到BGP路由后，在判断BGP路由是否为异常路由时，通过

查询数据库中的相关信息进行判断。

[0202] 下面结合举例进行说明。假设本地自治系统的数据库中记录了AS100曾向AS200发布过一条BGP路由，IP前缀为10.10.10.0/24。并且，本地自治系统在发布该BGP路由时指定了该路由为AS200专用的路由。

[0203] 一种情况下，AS100获取到BGP路由后，发现BGP路由的内容如表10所示。BGP路由中的IP前缀为10.10.10.0/24，AS_PATH attribute为300、200、100。AS100的网络设备在进行路由识别时，通过查询数据库发现自己确实向AS200发布过前缀为10.10.10.0/24的路由，但是该路由是AS200专用的。而自己接收到的如表10所示的BGP路由中，AS200将该路由转发给了AS300。说明AS200在接收到AS100发送的专用路由后，没有按照协议配置进行使用，违反了路由使用约定。本实施例中，将该BGP路由的类型称为异常类型3。

[0204] 表10

[0205]

IP前缀	10.10.10.0/24
AS_PATH attribute	300、200、100

[0206] 另一种情况下，AS100获取到BGP路由后，发现BGP路由的内容如表11所示。BGP路由中的IP前缀为10.10.10.0/24，AS_PATH attribute为300、400、100。AS100的网络设备在进行路由识别时，通过查询数据库发现自己确实发布过前缀为10.10.10.0/24的路由，但是该路由是发布给AS200专用的。而自己接收到的如表10所示的BGP路由中AS_PATH attribute中不包括200，说明该路由可能是被劫持者劫持后对AS_PATH attribute进行伪造得到的。本实施例中，将该BGP路由的类型称为异常类型4。

[0207] 表11

[0208]

IP前缀	10.10.10.0/24
AS_PATH attribute	300,400,100

[0209] 又一种可能的实施方式中，所述网络设备根据所述第一AS number是所述AS_PATH attribute中的第一个元素element，所述网络设备向特定AS发布过仅限于所述特定AS使用的包含所述第一IP前缀的路由，以及，所述AS_PATH attribute中包括所述第二AS number且不包括第三AS number，确定所述BGP路由是正常的。其中，第三AS number不等于第一AS number，也不等于第二AS number。

[0210] 示例性的，假设本地自治系统的数据库中记录了AS100曾向AS200发布过一条BGP路由，IP前缀为10.10.10.0/24，并且该路由是AS200专用的。若网络设备接收到的BGP路由的IP前缀为10.10.10.0/24，AS_PATH attribute为200、100，即AS_PATH attribute中不包括除特定AS之前的其他AS，则确定该BGP路由为正常的。

[0211] 本实施例中，在确定BGP路由是正常的情况下，说明该BGP路由的环路类型为正常环路，可以按照现有技术中的处理方式，对该BGP路由丢弃或者忽略处理，以免造成路由环路。

[0212] 又一种可能的实施方式中，所述网络设备根据所述第一AS number不是所述AS_PATH attribute中的第一个元素element，以及，所述网络设备所在或所管辖的自治系统与第四AS number对应的自治系统没有建立BGP会话，确定所述BGP路由是异常的，所述第四AS number是所述AS_PATH attribute中与所述第一AS number相邻的元素。

[0213] 其中，第四AS number可以是一个AS number，也可以是两个AS number。

[0214] 也就是说，AS_PATH attribute中与第一AS number相邻的一个或者两个AS number中，至少一个对应的自治系统与本地自治系统没有建立BGP会话，则确定BGP路由为异常的。

[0215] 本申请中，本地自治系统与第四AS number对应的自治系统没有建立BGP会话，可以具体是在网络设备执行S402之前，本地自治系统与第四AS number对应的自治系统没有建立BGP会话。

[0216] 具体实施过程中，本地自治系统的数据库还用于存储各自治系统之间的连接关系，即存储各自治系统之间是否建立BGP会话。网络设备获取到BGP路由后，根据AS_PATH attribute确定出与第一AS number相邻的AS number后，可以通过查询数据库，确定这些相邻的AS number对应的自治系统与本地自治系统是否建立BGP会话。

[0217] 下面举例说明，假设本地自治系统AS100的数据库中记录了AS100与AS200建立了BGP会话，并且，AS100也与AS300建立了BGP会话。

[0218] 一种情况下，网络设备获取的BGP路由中AS_PATH attribute为200、100、400。通过查询数据库，由于AS400与AS100实际没有建立BGP会话，因此，确定该BPG路由为异常的。该情况下，本实施例中的第四AS number具体是指400。

[0219] 另一种情况下，网络设备获取的BGP路由中AS_PATH attribute为500、100、400。通过查询数据库，由于AS400与AS100实际没有建立BGP会话，且AS500与AS100实际也没有建立BGP会话，因此，确定该BPG路由为异常的。该情况下，本实施例中的第四AS number包括400和500。

[0220] 本实施方式对应的场景中，网络设备获取的BGP路由中，本地自治系统对应的AS number不是所述AS_PATH attribute中的第一个元素element，并且，所述AS_PATH attribute中与本地自治系统的AS number相邻的元素中，存在至少一个相邻的元素对应的自治系统与本地自治系统没有建立BGP会话。该场景下，说明是劫持者劫持到路由后，对路由中的AS_PATH attribute进行篡改，使得篡改后的路由看起来像是经过了本地自治系统，因此，该情况是纯粹的路由伪造事件，本实施例中，将该BGP路由的类型称为异常类型5。

[0221] 又一种可能的实施方式中，所述BGP路由包括第一互联网协议IP前缀，所述网络设备根据所述第一AS number不是所述AS_PATH attribute中的第一个元素element，所述网络设备所在或所管辖的自治系统与左AS建立有BGP会话，所述网络设备所在或所管辖的自治系统与右AS建立有BGP会话，以及，所述网络设备没有接收过来自所述右AS的包含所述第一IP前缀的路由，或者，所述网络设备没有向所述左AS发布过包含所述第一IP前缀的路由，确定所述BGP路由是异常的。

[0222] 其中，所述右AS对应的AS number以及所述左AS对应的AS number是与所述AS_PATH attribute中与所述第一AS number相邻的两个元素，所述右AS对应的AS number位于所述第一AS number的右侧，所述左AS对应的AS number位于所述第一AS number的左侧。

[0223] 具体实施过程中，本地自治系统的数据库除了存储各自治系统之间是否建立BGP会话之外，还用于存储本地自治系统转发的历史BGP路由信息。例如：本地自治系统从哪些自治系统接收过哪些IP前缀，以及向哪些自治系统发布过哪些IP前缀。网络设备获取到BGP路由后，根据AS_PATH attribute确定出与第一AS number相邻的AS number。然后，可以通过查询数据库，确定这些相邻的AS number对应的自治系统与本地自治系统是否建立BGP会

话。并确定本地自治系统是否从相邻的AS number对应的自治系统接收过BGP路由中的IP前缀，或者，本地自治系统是否向相邻的AS number对应的自治系统发布过BGP路由中的IP前缀。

[0224] 下面举例说明，假设本地自治系统为AS100。AS100中的网络设备获取的BGP路由中AS_PATH attribute为200、100、400，IP前缀为10.10.10.0/24。在网络设备进行路由识别时，若通过查询数据库发现，虽然AS400与本地自治系统AS100建立了BGP会话，并且，AS200与本地自治系统AS100也建立了BGP会话，但是，本地自治系统AS100并没有从AS400接收过包括IP前缀10.10.10.0/24的路由，则确定该BPG路由为异常的。

[0225] 或者，若通过查询数据库发现，虽然AS400与本地自治系统AS100建立了BGP会话，AS200与本地自治系统AS100也建立了BGP会话，并且，本地自治系统也从AS400接收过包括IP前缀10.10.10.0/24的路由，但是，本地自治系统AS100并没有向AS200发布过包括IP前缀10.10.10.0/24的路由，则确定该BPG路由为异常的。

[0226] 本实施方式对应的场景中，网络设备获取的BGP路由中，本地自治系统对应的AS number不是所述AS_PATH attribute中的第一个元素element，并且，所述AS_PATH attribute中与本地自治系统的AS number相邻的元素中，左相邻元素对应的自治系统和右相邻元素对应的自治系统均与本地自治系统建立BGP会话，但是，本地自治系统并没有从右相邻元素对应的自治系统中接收过包括该IP前缀的路由，或者，并没有向左相邻元素对应的自治系统中发布过包括该IP前缀的路由。该场景下，说明是劫持者劫持到路由后，对路由中的IP前缀或者AS_PATH attribute进行篡改，使得篡改后的路由看起来像是经过了本地自治系统，因此，该情况是纯粹的路由伪造事件，本实施例中，将该BGP路由的类型称为异常类型6。

[0227] 又一种可能的实施方式中，所述网络设备根据所述第一AS number不是所述AS_PATH attribute中的第一个元素element，所述网络设备所在或所管辖的自治系统与左AS建立有BGP会话，所述网络设备所在或所管辖的自治系统与右AS建立有BGP会话，所述网络设备接收过来自所述右AS的包含所述第一IP前缀的路由，以及，所述网络设备向所述左AS发布过包含所述第一IP前缀的路由，确定所述BGP路由是正常的。

[0228] 其中，所述右AS对应的AS number以及所述左AS对应的AS number是与所述AS_PATH attribute中与所述第一AS number相邻的两个元素，所述右AS对应的AS number位于所述第一AS number的右侧，所述左AS对应的AS number位于所述第一AS number的左侧。

[0229] 本实施例中，在确定BGP路由是正常的情况下，说明该BGP路由的环路类型为正常环路，可以按照现有技术中的处理方式，对该BGP路由丢弃或者忽略处理，以免造成路由环路。

[0230] 在上述各实施例的基础上，所述网络设备确定所述BGP路由为异常的之后，还包括：

[0231] 所述网络设备生成路由异常对应的日志信息和/或告警信息，通知所述AS_PATH attribute中的各AS number对应的自治系统进行路由修正。

[0232] 具体的，在识别出BGP路由异常之后，可以在网络设备本地生成BGP路由异常对应的日志信息，还可以向本地自治系统对应的网管服务器上报告警信息，使得用户能够及时发现网络中的异常路由传播，并及时进行路由修正，提高网络的安全性和稳定性。

[0233] 本实施例提供的BGP路由识别方法,包括:网络设备获取BGP路由,所述BGP路由包括自治系统路径属性AS_PATH attribute,所述AS_PATH attribute包含第一自治系统号码AS number,所述网络设备所在或所管辖的自治系统对应的AS number是第二AS number,所述第一AS number等于所述第二AS number;所述网络设备根据所述第一AS number以及所述第二AS number,确定所述BGP路由是否为异常的,从而能够及时发现路由劫持等原因导致的异常环路路由,提高了网络安全性。

[0234] 图7为本申请另一实施例提供的BGP路由识别方法的流程示意图。如图7所示,本实施例的方法,包括:S701以及S702。

[0235] S701:网络设备获取BGP路由,所述BGP路由包括自治系统路径属性AS_PATH attribute,所述AS_PATH attribute包含第一自治系统号码AS number,所述网络设备所在或所管辖的自治系统的邻居自治系统对应的AS number是第二AS number,所述第一AS number等于所述第二AS number。

[0236] 本实施例中,网络设备可以是自治系统内部的任意网络设备。例如:网络设备可以是自治系统内的路由设备,比如作为BGP Speaker的路由设备。另外,网络设备还可以是管辖自治系统的网络设备。例如:网络设备可以是用于控制和监控自治系统内部各路由设备的控制器或者服务器。

[0237] 本实施例中的网络设备所在或所管辖的自治系统,是在BGP路由传播过程中作为发送端的自治系统。为了描述方便,本实施例中将执行主体网络设备所在或所管辖的自治系统称为本地自治系统。将在BGP路由传播过程中作为接收端的自治系统,称为邻居自治系统(neighboring autonomous system)。

[0238] 第一种可能的应用场景中,网络设备为本地自治系统内部作为BGP Speaker的路由设备。图8为本申请实施例的应用场景示意图三。如图8所示,在本地自治系统的路由设备中设置BGP路由识别装置,用于执行本实施例的方法。

[0239] 该场景下,S701中的网络设备获取BGP路由,包括:路由设备生成BGP路由。其中,生成BGP路由具体是指生成待发送的BGP路由。具体的,在本地自治系统为Origin AS的情况下,路由设备根据待发布的IP前缀和本地自治系统对应的AS number生成待发送的BGP路由。在本地自治系统为Transit AS的情况下,路由设备从上一个邻居自治系统接收到的BGP路由后,将本地自治系统对应的AS number添加至AS_PATH attribute中,生成待发送的BGP路由。

[0240] 第二种可能的应用场景中,网络设备为管辖本地自治系统的控制器。图9为本申请实施例的应用场景示意图四。如图9所示,在管辖本地自治系统的控制器中设备BGP路由识别装置,用于执行本实施例的方法。

[0241] 该场景下,S401中的网络设备获取BGP路由,包括:控制器接收由路由设备发送的BGP路由。具体的,本地自治系统的路由设备(例如BGP Speaker)生成待发送的BGP路由后,将该BGP路由转发给控制器。

[0242] 针对每个自治系统而言,控制器与该自治系统内部的路由设备通过BGP监测协议(BGP Monitoring Protocol,BMP)连接。控制器用于监控路由设备的BGP路由的接收情况。为支持本实施例,BMP协议需要做一些扩展。当前BMP协议的RFC7854支持7种消息类型,包括下述的Type 0～6。本实施例中新增一种消息类型,即下述的Type＝TBD1:Diagnosis

Message,该消息用于收集各路由设备的诊断信息。

[0243] Type＝0:Route Monitoring

[0244] Type＝1:Statistics Report

[0245] Type＝2:Peer Down Notification

[0246] Type＝3:Peer Up Notification

[0247] Type＝4:Initiation Message

[0248] Type＝5:Termination Message

[0249] Type＝6:Route Mirroring Message

[0250] Type＝TBD1:Diagnosis Message

[0251] 具体的,本地自治系统中BGP Speaker与控制器之间建立BMP会话。本地自治系统中BGP Speaker和邻居自治系统中的BGP Speaker之间建立BGP会话。本地自治系统中BGP Speaker生成待发送的BGP路由后,将该BGP路由封装在上述新增的诊断消息中。然后将该诊断消息转发给控制器。控制器通过解析该诊断消息,获取BGP路由,执行后续的BGP路由识别过程。

[0252] 本实施例中,网络设备获取的BGP路由中包括自治系统路径属性AS_PATH attribute,其中,AS_PATH attribute中可以包括一个或者多个自治系统号码(AS number)。本实施例对应的应用场景中,AS_PATH attribute中包括与邻居自治系统的自治系统号码相同的AS number。为了描述方便,本实施例中将邻居自治系统对应的AS number称为第二AS number,将AS_PATH attribute中与第二AS number相同的AS number称为第一AS number。也就是说,第一AS number等于第二AS number。

[0253] 当然,BGP路由除了AS_PATH attribute之外,还可以包括其他信息,例如:IP前缀。IP前缀可以携带在网络层可达信息(Network Layer ReachabilityInformation,NLRI)域。NLRI field可以携带在BGP update消息中。本申请中,IP前缀也可以称为IP地址前缀。。

[0254] 下面结合举例进行说明。假设网络中包括四个自治系统,分别为:AS100、AS200、AS300、AS400。一条BGP路由从AS100始发(originated)后,经过AS200转发AS300后,AS300将本地自治系统对应的AS number添加至AS_PATH attribute的最前面(最左边),生成待发送给AS400的BGP路由,该待发送BGP路由中的内容如表12所示。

[0255] 表12

[0256]

IP前缀	10.10.0.0/16
AS_PATH attribute	300,200,100

[0257] AS300对应的网络设备获取到待发送BGP路由。由于AS_PATH attribute中不包括邻居自治系统对应的AS number(400),因此,不触发执行本实施例的BGP路由识别方法,按照现有的路由传播过程进行处理。例如,将BGP路由传播给AS400。本申请中,AS400是指AS number为400的AS。

[0258] 假设AS300生成的待发送BGP路由如表13或者如表14所示。由于AS_PATH attribute中包括邻居自治系统的AS number(400),因此,执行步骤S702,确定该BGP路由是否是异常的。

[0259] 表13

[0260]

IP前缀	10.10.0.0/16

AS_PATH attribute	300,400

[0261] 表14

[0262]

IP前缀	10.10.0.0/16
AS_PATH attribute	300,400,100

[0263] S702:所述网络设备根据所述第一AS number以及所述第二AS number,确定所述BGP路由是否为异常的。

[0264] 本实施例中,异常可以是BGP路由是伪造的。另外,异常也可以是由于协议配置错误导致的BGP路由异常。

[0265] BGP路由伪造是指路由劫持者劫持到BGP路由后对BGP路由中的IP前缀和/或AS_PATH attribute进行伪造,使得伪造后的BGP路由看起来像是由某个AS始发的,或者看起来像是经过了某些AS的转发。

[0266] 协议配置错误导致的BGP路由异常是指,由于某个自治系统的配置错误导致BGP路由被传播到不应该接收该BGP路由的自治系统中。例如:AS1向AS2发布了一条BGP路由,并在该BGP路由的团体属性(community attribute)中指示该BGP路由是专供AS2使用的。例如,AS2接收到的BGP路由携带禁止输出团体属性(NO_EXPORTcommunities attribute)。NO_EXPORTcommunities attribute的值可以是0xFFFFFF01。AS2协议配置正确的情况下,AS2可以根据NO_EXPORTcommunities attribute确定该BGP路由是专供AS2使用的。由于AS2的协议配置错误,AS2将该BGP路由转发给了AS3。该场景中,AS3是不应该接收该BGP路由的AS。另一种场景中,AS2将该BGP路由转发至其他AS。其他AS将该BGP路由转发至AS1。该场景中,其他AS以及AS1是不应该接收该BGP路由的AS。本实施例中将该情况对应的BGP路由称为“由于协议配置错误导致的BGP路由异常”。

[0267] 本实施例中,网络设备获取到的BGP路由中,当AS_PATH attribute中包括与邻居自治系统对应的AS number相等的第一AS number时,确定BGP路由是异常的。当AS_PATH attribute中不包括与邻居自治系统对应的AS number相等的第一AS number时,确定BGP路由是正常的。

[0268] 一种可能的实施方式中,所述网络设备根据所述第一AS number、所述第二AS number以及所述第一AS number在所述AS_PATH attribute中的位置,确定所述BGP路由是否为异常的。

[0269] 本实施例中,网络设备获取到BGP路由的AS_PATH attribute中包括与邻居自治系统的AS number相等的第一AS number时,可以进一步根据所述第一AS number在所述AS_PATH attribute中的位置,确定所述BGP路由是否为异常的。

[0270] 其中,AS_PATH attribute可以包括一个或者多个AS number。每个AS number可以称为AS_PATH attribute的一个元素(element)。本实施例中,第一AS number在所述AS_PATH attribute中的位置是指:第一AS number是AS_PATH attribute中第几个元素。

[0271] 可以理解的,第一AS number与邻居自治系统对应的第二AS number相等。当第一AS number是AS_PATH attribute中第一个元素时,说明邻居自治系统是BGP路由的Origin AS。当第一AS number不是AS_PATH attribute中第一个元素时,说明邻居自治系统是BGP路由的Transit AS。

[0272] 其中,第一个元素是指位于AS_PATH attribute最右位置(rightmost position)

的元素。

[0273] 当根据第一AS number在所述AS_PATH attribute中的位置确定出邻居自治系统是BGP路由中的Origin AS或者Transit AS后,可以进一步根据AS_PATH attribute确定该BGP路由是否是异常的。

[0274] 一种可能的实施方式中,若第一AS number是AS_PATH attribute的第一个元素,说明邻居自治系统是BGP路由的Origin AS。可以确定出AS_PATH attribute中与第一AS number左相邻的AS number。然后通过判断左相邻的AS number对应的自治系统是否与邻居自治系统建立BGP会话,来确定该BGP路由是否为伪造的。例如:若所述左相邻的AS number对应的自治系统并未与邻居自治系统建立BGP会话,则说明该BGP路由是伪造的。

[0275] 另一种可能的实施方式中,若第一AS number不是AS_PATH attribute的第一个元素,说明邻居自治系统是BGP路由的Transit AS。可以确定出AS_PATH attribute中与第一AS number左相邻的AS number和右相邻的AS number。然后通过判断左相邻的AS number对应的自治系统和右相邻的AS number对应的自治系统是否与邻居自治系统建立BGP会话,来确定该BGP路由是否为伪造的。例如:若左相邻的AS number对应的自治系统和右相邻的AS number对应的自治系统中,至少一个没有与邻居自治系统建立BGP会话,则说明该BGP路由是伪造的。

[0276] 具体实施过程中,可以在本地自治系统的数据库中存储网络中各自治系统之间的实际连接关系,即各自治系统之间建立BGP会话的连接关系。当网络设备获取到到如表8或者如表9所示的BGP路由时,可以根据BGP路由中的AS_PATH attribute以及数据库中存储的各自治系统之间的实际连接关系进行判断。

[0277] 需要说明的是,本实施例中的数据库,可以是设置在本地自治系统的路由设备上的数据库。也可以是设置在本地自治系统内部的其他网络设备的数据库。还可以是设置在管辖本地自治系统的控制器或者服务器中的数据库。本实施例对此不作具体限定。

[0278] 一种可能的实施方式中,在网络中设置全局控制器,全局控制器与网络中的各个自治系统连接,用于从各个自治系统中获取路由信息以及各自治系统之间的连接关系信息,同时,全局控制器还用于将收集到的信息同步至各个自治系统的本地数据库中,从而每个自治系统均可以从本地数据库中查询到各自治系统的路由信息以及各自治系统之间的连接关系信息。

[0279] 进一步的,在BGP路由中还包括IP前缀的情况下,在确定BGP路由是否异常时还可以结合IP前缀进行判断。下面结合几种具体的实施方式进行介绍。

[0280] 一种可能的实施方式中,所述网络设备根据所述第一AS number是所述AS_PATH attribute中的第一个元素element,以及,所述邻居自治系统没有发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的。

[0281] 另一种表述方式为:若邻居自治系统对应的AS number是所述AS_PATH attribute中的第一个元素element时,并且,邻居自治系统没有发布过包含第一IP前缀的路由,则确定BGP路由是异常的。

[0282] 本申请中,“发布”包括:初始生成(originated)并发布,和,接收并发布。初始生成(originated)并发布指的是自治系统初始生成BGP路由并发布给其他AS。接收并发布指的是自治系统从其他AS接收到BGP路由并发布给另外的AS。本实施例中,“初始生成并发布”可

以称为始发，“接收并发布”可以称为转发。

[0283] “网络设备没有发布过包含第一IP前缀的路由”具体可以是网络设备在执行S402之前尚未发布过包含IP前缀的路由。“邻居自治系统没有发布过包含第一IP前缀的路由”具体实现时可以是第一种情况或者第二种情况。第一种情况是邻居自治系统没有初始生成并发布过包含第一IP前缀的路由。例如，邻居自治系统没有生成包含第一IP前缀的路由。数据库没有记录邻居自治系统包含第一IP前缀的路由。第二种情况是邻居自治系统没有接收并发布过包含第一IP前缀的路由。例如，邻居自治系统没有从其他AS接收过包含第一IP前缀的路由并发布给另外的AS。

[0284] 具体实施过程中，本地自治系统的数据库用于记录邻居自治系统发布的至少一个第二IP前缀，当BGP路由中的第一IP前缀与各第二IP前缀均不匹配，则确定BGP路由是异常的。

[0285] 需要说明的是，上述的匹配是指完全匹配，即IP地址和掩码位数完全匹配。

[0286] 下面举例说明，假设数据库中记录了邻居自治系统发布过两个IP前缀，分别为：10.1.0.0/16、10.2.0.0/16。

[0287] 一种情况下，路由设备获取的BGP路由中，邻居自治系统对应的AS number是所述AS_PATH attribute中的第一个元素element，并且BGP路由中的IP前缀为10.3.0.0/16。该情况下，网络设备在进行BGP路由识别时，由于BGP路由中的IP前缀(10.3.0.0/16)与上述数据库中记录的两个IP前缀(10.1.0.0/16、10.2.0.0/16)均不匹配，因此，确定该BGP路由是伪造的。

[0288] 另一种情况下，路由设备获取的BGP路由中，邻居自治系统对应的AS number是所述AS_PATH attribute中的第一个元素element，并且BGP路由中的IP前缀为10.2.1.0/24。该情况下，网络设备进行BGP路由识别时，由于BGP路由中的IP前缀(10.2.1.0/24)与上述数据库中记录的两个IP前缀(10.1.0.0/16、10.2.0.0/16)均不匹配，因此，确定BGP路由是伪造的。

[0289] 本实施方式对应的场景为：邻居自治系统对应的AS number是所述AS_PATH attribute中的第一个元素element，但是，邻居自治系统没有发布过包含第一IP前缀的路由。该场景下，说明是劫持者对BGP路由的IP前缀或AS_PATH attribute进行了伪造，使得伪造后的路由看起来像是该IP前缀是邻居自治系统发布的，因此，这是纯粹的路由伪造事件，可以将该类型的路由伪造称为异常类型7。

[0290] 另一种可能的实施方式中，所述网络设备根据所述第一AS number是所述AS_PATH attribute中的第一个元素element，所述邻居自治系统发布过包含第二IP前缀的路由，以及，所述邻居自治系统没有发布过包含所述第一IP前缀的路由，确定所述BGP路由是异常的，所述第一IP前缀是所述第二IP前缀的子前缀。

[0291] 另一种表述方式为：若邻居自治系统对应的AS number是所述AS_PATH attribute中的第一个元素element，并且，所述第一IP前缀是邻居自治系统发布过的某个第二IP前缀的子前缀，但是邻居自治系统没有发布过所述第一IP前缀，则确定所述BGP路由是异常的。

[0292] 本申请中，邻居自治系统发布过包含第二IP前缀的路由可以是在网络设备执行S702之前，邻居自治系统发布过包含第二IP前缀的路由。

[0293] 其中，本实施例中“第一IP前缀是第二IP前缀的子前缀”是指：第一IP前缀所指示

的网络地址集合是第二IP前缀所指示的网络地址集合的子集。示例性的，假设第一IP前缀为10.10.192.0/24，第二IP前缀为10.10.128.0/17，由于第一IP前缀对应的网络地址集合为从10.10.192.0至10.10.192.255之间的网络地址，第二IP前缀对应的网络地址集合为从10.10.128.0至10.10.255.255之间的网络地址，第一IP前缀对应的网络地址集合是第二IP前缀对应的网络地址集合的子集，因此，认为第一IP前缀是第二IP前缀的子前缀。

[0294] 本实施方式对应的场景为：邻居自治系统对应的AS number是所述AS_PATH attribute中的第一个元素element，并且，所述第一IP前缀是邻居自治系统发布过的某个第二IP前缀的子前缀，但是邻居自治系统没有发布过所述第一IP前缀。该场景下，说明是劫持者对BGP路由的IP前缀或AS_PATH attribute进行了伪造，使得伪造后的路由看起来像是邻居自治系统发布过某个IP前缀的子前缀，因此，这是纯粹的路由伪造事件，可以将该类型的路由伪造称为异常类型9。

[0295] 又一种可能的实施方式中，所述网络设备根据第一AS number是所述AS_PATH attribute中的第一个元素element，以及，所述邻居自治系统向所述AS_PATH attribute中与第一AS number相邻的元素对应的自治系统发布过包含所述第一IP前缀的路由，确定所述BGP路由是正常的。

[0296] 示例性的，假设数据库中记录了邻居自治系统AS100曾向AS200发布过一条BGP路由，IP前缀为10.10.10.0/24。若网络设备接收到的BGP路由的IP前缀为10.10.10.0/24，AS_PATH attribute为300、200、100，则确定该BGP路由为正常的。

[0297] 本实施例中，在确定BGP路由是正常的情况下，说明该BGP路由的环路类型为正常环路，可以按照现有技术中的处理方式，对该BGP路由丢弃或者忽略处理，以免造成路由环路。

[0298] 又一种可能的实施方式中，所述网络设备根据所述第一AS number不是所述AS_PATH attribute中的第一个元素element，以及，所述邻居自治系统与第三AS number对应的自治系统没有建立BGP会话，确定所述BGP路由是异常的，所述第三AS number是所述AS_PATH attribute中与所述第一AS number相邻的元素。

[0299] 其中，第三AS number可以是一个AS number，也可以是两个AS number。

[0300] 也就是说，AS_PATH attribute中与第一AS number相邻的一个或者两个AS number中，至少一个相邻的AS number对应的自治系统与邻居自治系统没有建立BGP会话，则确定BGP路由为异常的。

[0301] 本申请中，邻居自治系统与第三AS number对应的自治系统没有建立BGP会话，可以具体是在网络设备执行S702之前，邻居自治系统与第三AS number对应的自治系统没有建立BGP会话。

[0302] 具体实施过程中，数据库还用于存储各自治系统之间的连接关系，即存储各自治系统之间是否建立BGP会话。网络设备获取到BGP路由后，根据AS_PATH attribute确定出与第一AS number相邻的AS number后，可以通过查询数据库，确定这些相邻的AS number对应的自治系统与本地自治系统是否建立BGP会话。

[0303] 下面举例说明，假设数据库中记录了AS100与AS200建立了BGP会话，并且，AS100也与AS300建立了BGP会话。

[0304] 一种情况下，假设AS200待向邻居AS100发送BGP路由，该待发送的BGP路由中AS_

PATH attribute为200、100、400。通过查询数据库，由于AS400与AS100实际没有建立BGP会话，因此，确定该BPG路由为异常的。该情况下，本实施例中的第三AS number具体是指400。

[0305] 另一种情况下，假设AS200待向邻居AS100发送BGP路由，该待发送BGP路由中AS_PATH attribute为500、100、400。通过查询数据库，由于AS400与AS100实际没有建立BGP会话，且AS500与AS100实际也没有建立BGP会话，因此，确定该BPG路由为异常的。该情况下，本实施例中的第三AS number包括400和500。

[0306] 本实施方式对应的场景中，网络设备获取的BGP路由中，邻居自治系统对应的AS number不是所述AS_PATH attribute中的第一个元素element，并且，所述AS_PATH attribute中与邻居自治系统的AS number相邻的元素中，存在至少一个相邻的元素对应的自治系统与本地自治系统没有建立BGP会话。该场景下，说明是劫持者劫持到路由后，对路由中的AS_PATH attribute进行篡改，使得篡改后的路由看起来像是经过了邻居自治系统，因此，该情况是纯粹的路由伪造事件，本实施例中，将该BGP路由的类型称为异常类型9。

[0307] 又一种可能的实施方式中，所述BGP路由包括第一互联网协议IP前缀，所述网络设备根据所述第一AS number不是所述AS_PATH attribute中的第一个元素element，所述邻居自治系统与左AS建立有BGP会话，所述邻居自治系统与右AS建立有BGP会话，所述邻居自治系统接收过来自所述右AS的包含第一IP前缀的路由，以及，所述邻居自治系统没有向所述左AS发布过包含所述第一IP前缀的路由，确定所述BGP路由是异常的。

[0308] 其中，所述右AS对应的AS number以及所述左AS对应的AS number是与所述AS_PATH attribute中与所述第一AS number相邻的两个元素，所述右AS对应的AS number位于所述第一AS number的右侧，所述左AS对应的AS number位于所述第一AS number的左侧。

[0309] 具体实施过程中，数据库除了存储各自治系统之间是否建立BGP会话之外，还用于存储邻居自治系统转发的历史BGP路由信息。例如：邻居自治系统从哪些自治系统接收过哪些IP前缀，以及向哪些自治系统发布过哪些IP前缀。网络设备获取到BGP路由后，根据AS_PATH attribute确定出与第一AS number相邻的AS number。然后可以通过查询数据库，确定这些相邻的AS number对应的自治系统与邻居自治系统是否建立BGP会话。并确定邻居自治系统是否从相邻的AS number对应的自治系统接收过BGP路由中的IP前缀，或者，邻居自治系统是否向相邻的AS number对应的自治系统发布过BGP路由中的IP前缀。

[0310] 下面举例说明，假设AS200待向邻居自治系统AS100发送BGP路由。待发送的BGP路由中AS_PATH attribute为200、100、400，IP前缀为10.10.10.0/24。在AS200中的网络设备在进行路由识别时，若通过查询数据库发现，虽然AS400与邻居自治系统AS100建立了BGP会话，并且，AS200与邻居自治系统AS100也建立了BGP会话，但是，邻居自治系统AS100并没有从AS400接收过包括IP前缀10.10.10.0/24的路由，则确定该BPG路由为异常的。

[0311] 或者，若通过查询数据库发现，虽然AS400与邻居自治系统AS100建立了BGP会话，AS200与邻居自治系统AS100也建立了BGP会话，并且，邻居自治系统AS100也从AS400接收过包括IP前缀10.10.10.0/24的路由，但是，邻居自治系统AS100并没有向AS200发布过包括IP前缀10.10.10.0/24的路由，则确定该BPG路由为异常的。

[0312] 本实施方式对应的场景中，网络设备获取的BGP路由中，邻居自治系统对应的AS number不是所述AS_PATH attribute中的第一个元素element，并且，所述AS_PATH attribute中与邻居自治系统的AS number相邻的元素中，左相邻元素对应的自治系统和右

相邻元素对应的自治系统均与邻居自治系统建立BGP会话，但是，邻居自治系统并没有从右相邻元素对应的自治系统中接收过包括该IP前缀的路由，或者，并没有向左相邻元素对应的自治系统中发布过包括该IP前缀的路由。该场景下，说明是劫持者劫持到路由后，对路由中的IP前缀或者AS_PATH attribute进行篡改，使得篡改后的路由看起来像是经过了邻居自治系统，因此，该情况是纯粹的路由伪造事件，本实施例中，将该BGP路由的类型称为异常类型10。

[0313] 又一种可能的实施方式中，所述网络设备根据所述第一AS number不是所述AS_PATH attribute中的第一个元素element，所述邻居自治系统与左AS建立有BGP会话，所述邻居自治系统与右AS建立有BGP会话，所述邻居自治系统接收过来自所述右AS的包含所述第一IP前缀的路由，以及，所述邻居自治系统向所述左AS发布过包含所述第一IP前缀的路由，确定所述BGP路由是正常的。

[0314] 其中，所述右AS对应的AS number以及所述左AS对应的AS number是与所述AS_PATH attribute中与所述第一AS number相邻的两个元素，所述右AS对应的AS number位于所述第一AS number的右侧，所述左AS对应的AS number位于所述第一AS number的左侧。

[0315] 本实施例中，在确定BGP路由是正常的情况下，说明该BGP路由的环路类型为正常环路，可以按照现有技术中的处理方式，对该BGP路由丢弃或者忽略处理，以免造成路由环路。

[0316] 在上述各实施例的基础上，所述网络设备确定所述BGP路由为异常的之后，还包括：

[0317] 所述网络设备生成路由异常对应的日志信息和/或告警信息，通知所述AS_PATH attribute中的各AS number对应的自治系统进行路由修正。

[0318] 具体的，在识别出BGP路由异常之后，可以在网络设备本地生成BGP路由异常对应的日志信息，还可以向本地自治系统对应的网管服务器上报告警信息，使得用户能够及时发现网络中的异常路由传播，并及时进行路由修正，提高网络的安全性和稳定性。

[0319] 本实施例提供的BGP路由识别方法，包括：网络设备获取BGP路由，所述BGP路由包括自治系统路径属性AS_PATH attribute，所述AS_PATH attribute包含第一自治系统号码AS number，所述网络设备所在或所管辖的自治系统的邻居自治系统对应的AS number是第二AS number，所述第一AS number等于所述第二AS number；所述网络设备根据所述第一AS number以及所述第二AS number，确定所述BGP路由是否为异常的，从而能够及时发现路由劫持等原因导致的异常环路路由，提高了网络安全性。

[0320] 图10为本申请一实施例提供的BGP路由识别装置的结构示意图。本实施例的BGP路由识别装置可设置于作为接收端的自治系统的网络设备中，该网络设备可以是作为接收端的自治系统内部的路由设备，还可以是管辖作为接收端的自治系统的控制器。如图10所示，本实施例的BGP路由识别装置100包括：获取模块101和识别模块102。

[0321] 其中，获取模块101，用于获取BGP路由，所述BGP路由包括自治系统路径属性AS_PATH attribute，所述AS_PATH attribute包含第一自治系统号码AS number，所述网络设备所在或所管辖的自治系统对应的AS number是第二AS number，所述第一AS number等于所述第二AS number；

[0322] 识别模块102，用于根据所述第一AS number以及所述第二AS number，确定所述

BGP路由是否为异常的。

[0323] 可选的,所述BGP路由包括第一互联网协议IP前缀,所述识别模块102具体用于:

[0324] 根据所述第一AS number是所述AS_PATH attribute中的第一个元素element,以及,所述网络设备没有发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的。

[0325] 可选的,所述BGP路由包括第一互联网协议IP前缀,所述识别模块102具体用于:

[0326] 根据所述第一AS number是所述AS_PATH attribute中的第一个元素element,所述网络设备发布过包含第二IP前缀的路由,以及,所述网络设备没有发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的,所述第一IP前缀是所述第二IP前缀的子前缀。

[0327] 可选的,所述BGP路由包括第一互联网协议IP前缀,所述识别模块102具体用于:

[0328] 根据所述第一AS number是所述AS_PATH attribute中的第一个元素element,所述网络设备向特定AS发布过仅限于所述特定AS使用的包含所述第一IP前缀的路由,以及,所述AS_PATH attribute中包括第三AS number或者不包括所述第二AS number,确定所述BGP路由是异常的。

[0329] 可选的,所述识别模块102具体用于:

[0330] 根据所述第一AS number不是所述AS_PATH attribute中的第一个元素element,以及,所述网络设备所在或所管辖的自治系统与第四AS number对应的自治系统没有建立BGP会话,确定所述BGP路由是异常的,所述第四AS number是所述AS_PATH attribute中与所述第一AS number相邻的元素。

[0331] 可选的,所述BGP路由包括第一互联网协议IP前缀,所述识别模块102具体用于:

[0332] 根据所述第一AS number不是所述AS_PATH attribute中的第一个元素element,所述网络设备所在或所管辖的自治系统与左AS建立有BGP会话,所述网络设备所在或所管辖的自治系统与右AS建立有BGP会话,以及,所述网络设备没有接收过来自所述右AS的包含所述第一IP前缀的路由,或者,所述网络设备没有向所述左AS发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的;

[0333] 所述右AS对应的AS number以及所述左AS对应的AS number是与所述AS_PATH attribute中与所述第一AS number相邻的两个元素,所述右AS对应的AS number位于所述第一AS number的右侧,所述左AS对应的AS number位于所述第一AS number的左侧。

[0334] 本实施例的BGP路由识别装置,可用于执行如图4所示的方法实施例,其实现原理和技术效果类似,此处不再赘述。

[0335] 图11为本申请另一实施例提供的BGP路由识别装置的结构示意图。本实施例的BGP路由识别装置可设置于作为发送端的自治系统的网络设备中,该网络设备可以是作为发送端的自治系统内部的路由设备,还可以是管辖作为发送端的自治系统的控制器。如图11所示,本实施例的BGP路由识别装置110包括:获取模块111和识别模块112。

[0336] 其中,获取模块111,用于获取BGP路由,所述BGP路由包括自治系统路径属性AS_PATH attribute,所述AS_PATH attribute包含第一自治系统号码AS number,所述网络设备所在或所管辖的自治系统的邻居自治系统对应的AS number是第二AS number,所述第一AS number等于所述第二AS number;

[0337] 识别模块112,用于根据所述第一AS number以及所述第二AS number,确定所述BGP路由是否为异常的。

[0338] 可选的,所述BGP路由包括第一互联网协议IP前缀,所述识别模块112具体用于:

[0339] 根据所述第一AS number是所述AS_PATH attribute中的第一个元素element,以及,所述邻居自治系统没有发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的。

[0340] 可选的,所述BGP路由包括第一互联网协议IP前缀,所述识别模块112具体用于:

[0341] 根据所述第一AS number是所述AS_PATH attribute中的第一个元素element,所述邻居自治系统发布过包含第二IP前缀的路由,以及,所述邻居自治系统没有发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的,所述第一IP前缀是所述第二IP前缀的子前缀。

[0342] 可选的,所述识别模块112具体用于:

[0343] 根据所述第一AS number不是所述AS_PATH attribute中的第一个元素element,以及,所述邻居自治系统与第三AS number对应的自治系统没有建立BGP会话,确定所述BGP路由是异常的,所述第三AS number是所述AS_PATH attribute中与所述第一AS number相邻的元素。

[0344] 可选的,所述BGP路由包括第一互联网协议IP前缀,所述识别模块112具体用于:

[0345] 根据所述第一AS number不是所述AS_PATH attribute中的第一个元素element,所述邻居自治系统与左AS建立有BGP会话,所述邻居自治系统与右AS建立有BGP会话,所述邻居自治系统接收过来自所述右AS的包含第一IP前缀的路由,以及,所述邻居自治系统没有向所述左AS发布过包含所述第一IP前缀的路由,确定所述BGP路由是异常的;

[0346] 所述右AS对应的AS number以及所述左AS对应的AS number是与所述AS_PATH attribute中与所述第一AS number相邻的两个元素,所述右AS对应的AS number位于所述第一AS number的右侧,所述左AS对应的AS number位于所述第一AS number的左侧。

[0347] 本实施例的BGP路由识别装置,可用于执行如图7所示的方法实施例,其实现原理和技术效果类似,此处不再赘述。

[0348] 图12为本申请一实施例提供的网络设备的硬件结构示意图。本实施例的网络设备可以是自治系统内的路由设备,还可以是管辖自治系统的控制器。如图12所示,该网络设备120包括:处理器121以及存储器122;其中,存储器122,用于存储计算机程序;处理器121,用于执行存储器存储的计算机程序,以实现上述实施例中网络设备所执行的方法。具体可以参见前述方法实施例中的相关描述。

[0349] 可选地,存储器122既可以是独立的,也可以跟处理器121集成在一起。

[0350] 当所述存储器122是独立于处理器121之外的器件时,所述网络设备120还可以包括:

[0351] 总线123,用于连接所述存储器122和处理器121。

[0352] 本实施例提供的网络设备,可用于执行上述任一方法实施例所示的网络设备所执行的方法,其实现原理和技术效果类似,本实施例此处不再赘述。

[0353] 本申请实施例还提供一种存储介质,所述存储介质包括计算机程序,所述计算机程序用于实现如上任一方法实施例中网络设备所执行的BGP路由识别方法。

[0354] 本申请实施例还提供一种芯片,包括:存储器、处理器以及计算机程序,所述计算机程序存储在所述存储器中,所述处理器运行所述计算机程序执行上述任一方法实施例中

网络设备所执行的BGP路由识别方法。

[0355] 在本申请所提供的几个实施例中，应该理解到，所揭露的设备和方法，可以通过其它的方式实现。例如，以上所描述的设备实施例仅仅是示意性的，例如，所述模块的划分，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，例如多个模块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，装置或模块的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0356] 所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块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模块来实现本实施例方案的目的。

[0357] 另外，在本申请各个实施例中的各功能模块可以集成在一个处理单元中，也可以是各个模块单独物理存在，也可以两个或两个以上模块集成在一个单元中。上述模块成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

[0358] 上述以软件功能模块的形式实现的集成的模块，可以存储在一个计算机可读取存储介质中。上述软件功能模块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(可以是个人计算机，服务器，或者网络设备等)或处理器(英文:processor)执行本申请各个实施例所述方法的部分步骤。

[0359] 应理解，上述处理器可以是中央处理单元(英文:Central Processing Unit，简称:CPU)，还可以是其他通用处理器、数字信号处理器(英文:Digital Signal Processor，简称:DSP)、专用集成电路(英文:Application Specific Integrated Circuit，简称:ASIC)等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合申请所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。

[0360] 存储器可能包含高速RAM存储器，也可能还包括非易失性存储NVM，例如至少一个磁盘存储器，还可以为U盘、移动硬盘、只读存储器、磁盘或光盘等。

[0361] 总线可以是工业标准体系结构(Industry Standard Architecture，ISA)总线、外部设备互连(Peripheral Component，PCI)总线或扩展工业标准体系结构(Extended Industry Standard Architecture，EISA)总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示，本申请附图中的总线并不限定仅有一根总线或一种类型的总线。

[0362] 上述存储介质可以是由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器(SRAM)，电可擦除可编程只读存储器(EEPROM)，可擦除可编程只读存储器(EPROM)，可编程只读存储器(PROM)，只读存储器(ROM)，磁存储器，快闪存储器，磁盘或光盘。存储介质可以是通用或专用计算机能够存取的任何可用介质。

[0363] 一种示例性的存储介质耦合至处理器，从而使处理器能够从该存储介质读取信息，且可向该存储介质写入信息。当然，存储介质也可以是处理器的组成部分。处理器和存储介质可以位于专用集成电路(Application Specific Integrated Circuits，简称:ASIC)中。当然，处理器和存储介质也可以作为分立组件存在于电子设备或主控设备中。

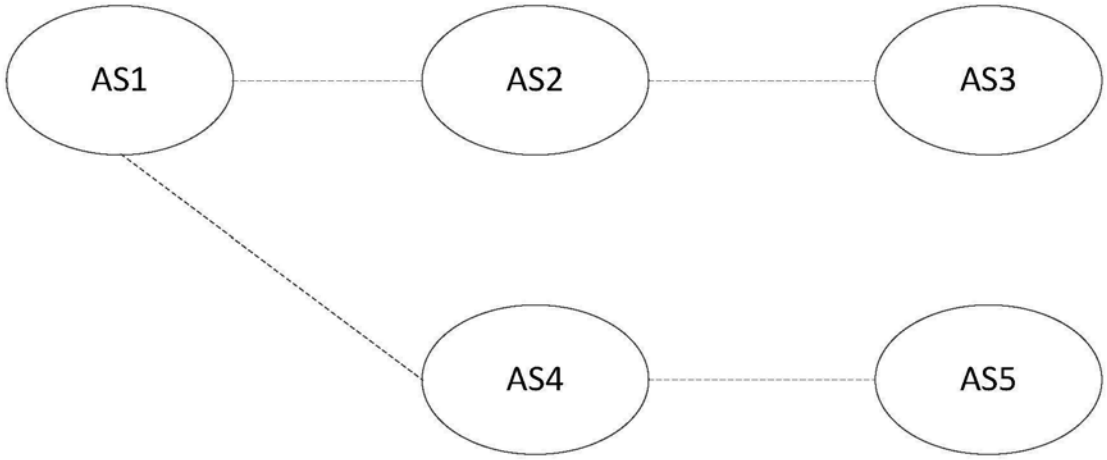

AS1
AS2
AS3
AS4
AS5

图1

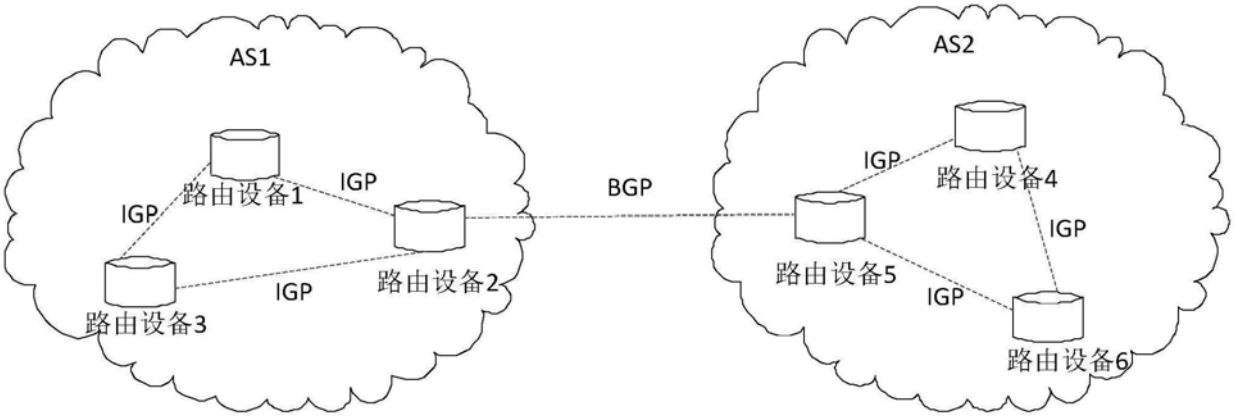

AS1
路由设备1
IGP
IGP
路由设备2
IGP
路由设备3
BGP
AS2
IGP
路由设备4
IGP
路由设备5
IGP
路由设备6

图2

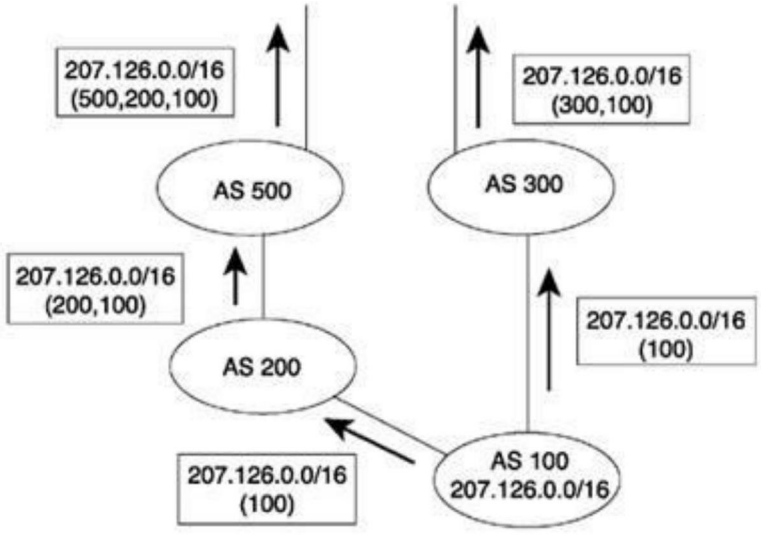

207.126.0.0/16
(500,200,100)
207.126.0.0/16
(300,100)
AS 500
AS 300
207.126.0.0/16
(200,100)
207.126.0.0/16
(100)
AS 200
AS 100
207.126.0.0/16
207.126.0.0/16
(100)

图3

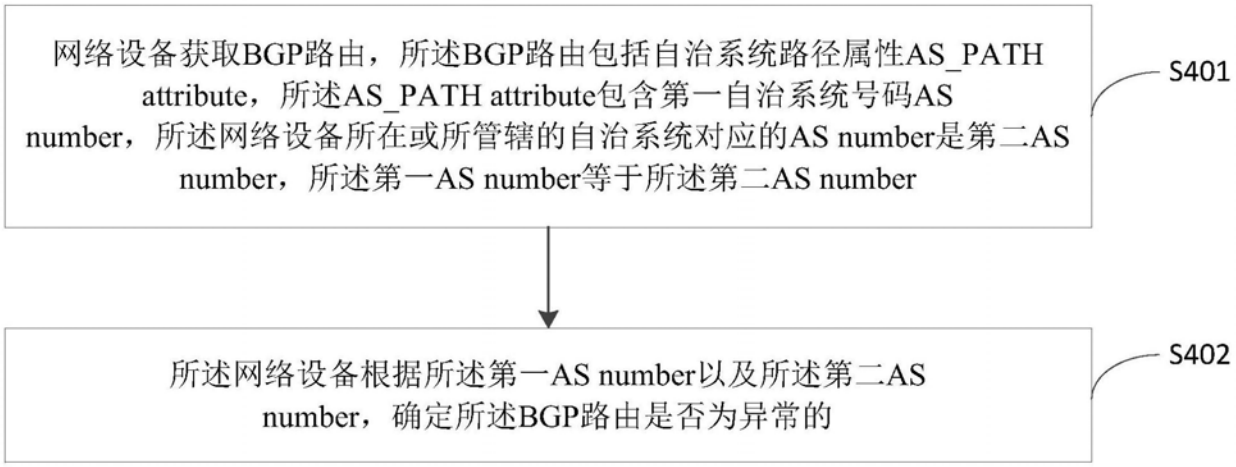

网络设备获取BGP路由，所述BGP路由包括自治系统路径属性AS_PATH attribute，所述AS_PATH attribute包含第一自治系统号码AS number，所述网络设备所在或所管辖的自治系统对应的AS number是第二AS number，所述第一AS number等于所述第二AS number
S401
所述网络设备根据所述第一AS number以及所述第二AS number，确定所述BGP路由是否为异常的
S402

图4

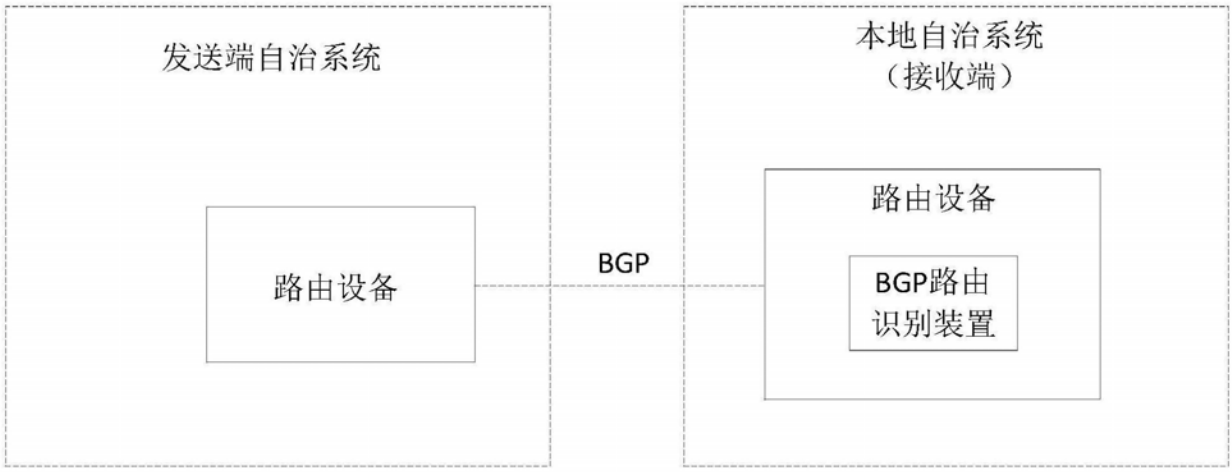

发送端自治系统
路由设备
BGP
本地自治系统
（接收端）
路由设备
BGP路由
识别装置

图5

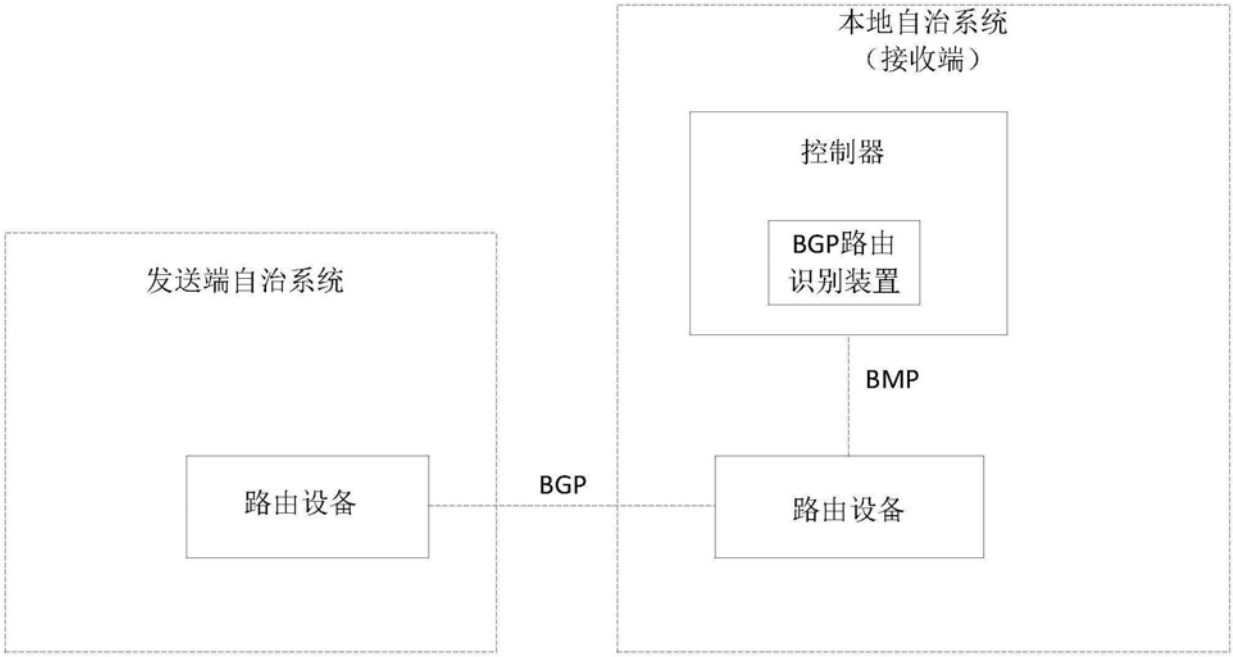

本地自治系统
（接收端）
控制器
BGP路由
识别装置
BMP
发送端自治系统
路由设备
BGP
路由设备

图6

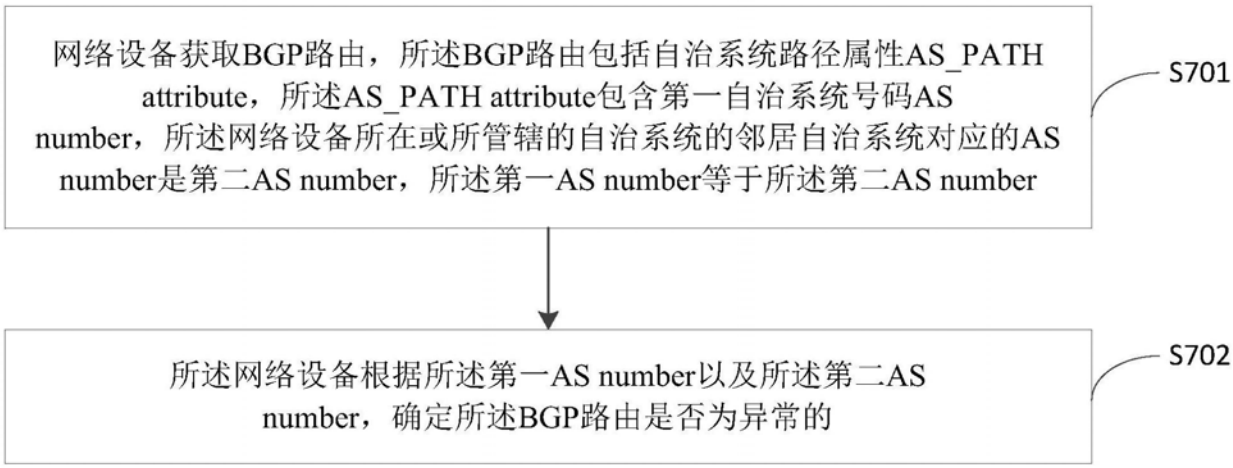

网络设备获取BGP路由，所述BGP路由包括自治系统路径属性AS_PATH attribute，所述AS_PATH attribute包含第一自治系统号码AS number，所述网络设备所在或所管辖的自治系统的邻居自治系统对应的AS number是第二AS number，所述第一AS number等于所述第二AS number
S701
所述网络设备根据所述第一AS number以及所述第二AS number，确定所述BGP路由是否为异常的
S702

图7

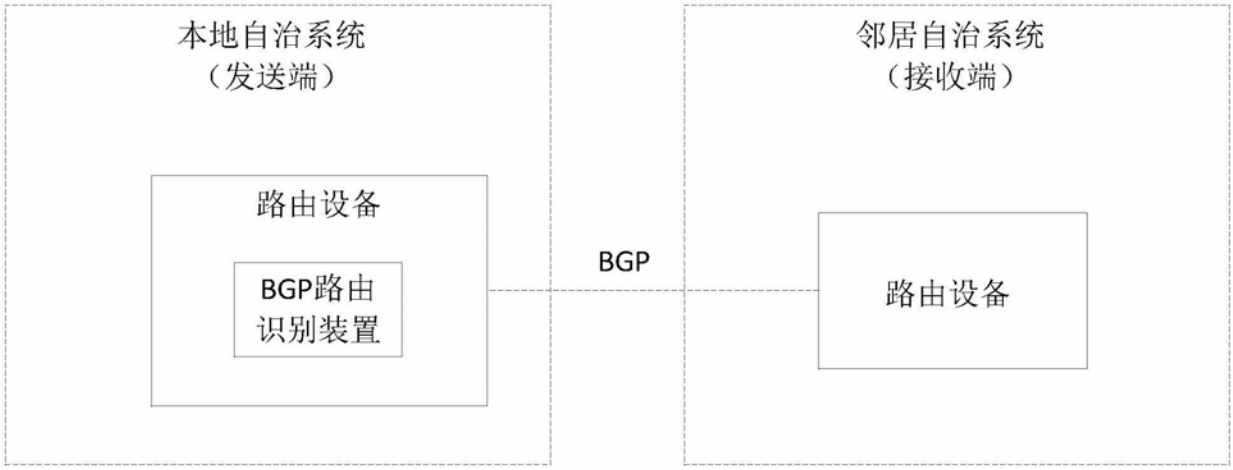

本地自治系统
（发送端）
路由设备
BGP路由
识别装置
BGP
邻居自治系统
（接收端）
路由设备

图8

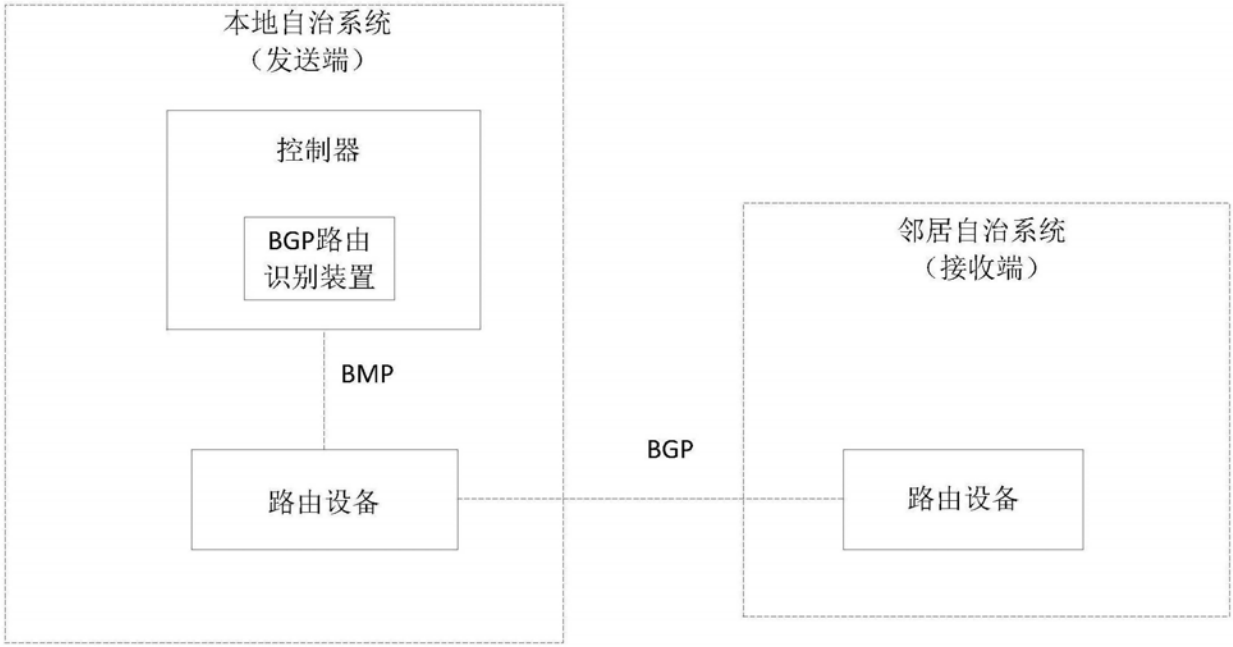

本地自治系统
（发送端）
控制器
BGP路由
识别装置
BMP
路由设备
BGP
邻居自治系统
（接收端）
路由设备

图9

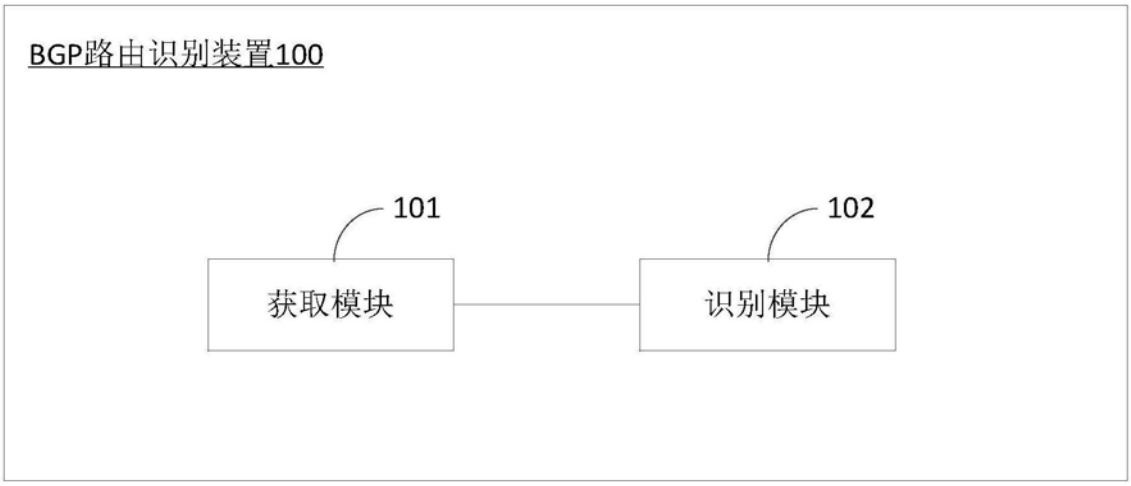

BGP路由识别装置100
101
102
获取模块
识别模块

图10

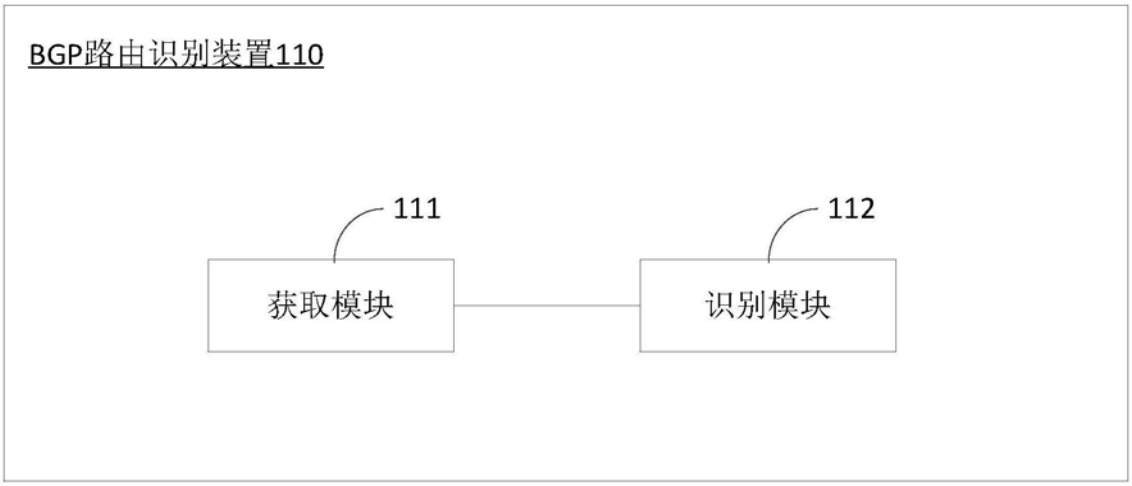

BGP路由识别装置110
111
112
获取模块
识别模块

图11

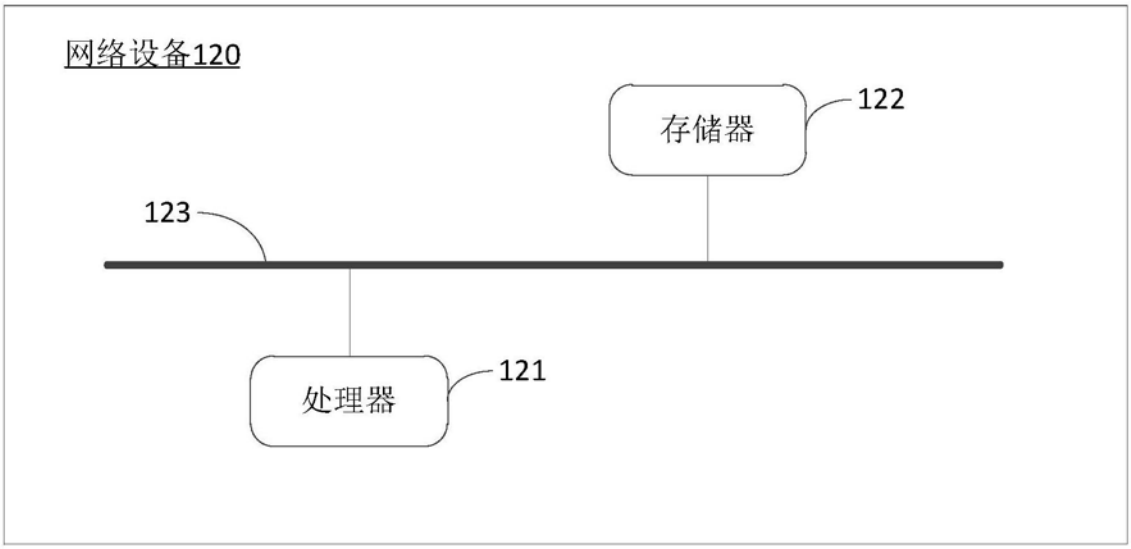


图12