(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101873259 B
(45)授权公告日 2013.01.09

(21)申请号 201010193624.1

(22)申请日 2010.06.01

(73)专利权人 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 刘华 周维军 段亮 潘能毅

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/801(2013.01)

(56)对比文件
WO 2007/067693 A2,2007.06.14,
CN 101094240 A,2007.12.26,
US 2006/0062203 A1,2006.03.23,

审查员 白雪慧

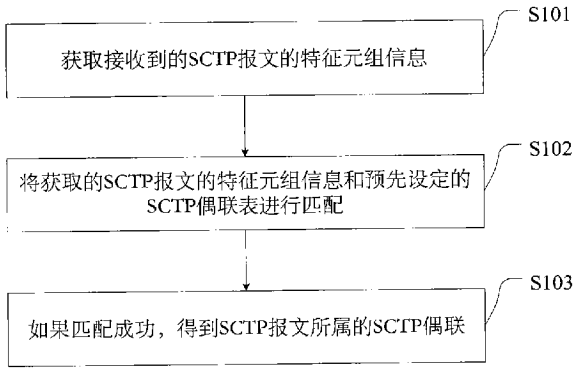
权利要求书 2 页 说明书 12 页 附图 9 页

(54)发明名称

SCTP报文识别方法和装置

(57)摘要

本发明实施例公开了一种SCTP报文识别方法,包括:获取接收到的SCTP报文的特征元组,所述特征元组包括源IP地址、目的IP地址和验证标签中的至少一项信息;将获取的SCTP报文的特征元组和预先设定的SCTP元组识别表进行匹配,SCTP元组识别表包括SCTP报文的特征集元组和SCTP偶联的对应关系,所述特征集元组包括源IP地址集、目的IP地址集和验证标签中的至少一项信息;如果匹配成功,得到SCTP报文所属的SCTP偶联。相应地,本发明实施例还公开了一种SCTP报文识别装置和系统以及建立SCTP元组识别表的方法,能减少SCTP流漏识别的情况。



CN 101873259 B

1. 一种流控制传输协议 SCTP 报文识别方法，其特征在于，包括：

获取接收到的 SCTP 报文的特征元组，所述特征元组包括源 IP 地址、目的 IP 地址和验证标签中的至少一项信息；

将获取的 SCTP 报文的特征元组和预先设定的 SCTP 元组识别表进行匹配，所述 SCTP 元组识别表包括所述 SCTP 报文的特征集元组和 SCTP 偶联的对应关系和关联关系，所述特征集元组包括源 IP 地址集、目的 IP 地址集和验证标签中的至少一项信息；所述关联关系用于将属于同一偶联的特征集元组的记录关联；

如果匹配成功，得到所述 SCTP 报文所属的 SCTP 偶联；

如果匹配不成功，解析本次 SCTP 握手消息的初始化消息报文，将解析到的信息作为一个记录添加到所述元组识别表中，所述解析到的信息包括所述初始化消息报文的 IP 地址集、端口和验证标签中的至少一项信息；

解析所述本次 SCTP 握手消息的初始化确认消息报文，获取所述初始化确认消息报文的 IP 地址集、端口和验证标签；

解析所述 SCTP 报文的公共分组头中的验证标签，利用所述公共分组头中的验证标签和所述 SCTP 元组识别表进行匹配，匹配到的记录为所述初始化消息报文对应的记录；

将解析所述本次 SCTP 握手消息的初始化确认消息报文得到的 IP 地址集、端口和验证标签作为另一个记录添加到所述 SCTP 元组识别表，建立和所述初始化消息报文对应的记录的关联关系；

识别所述 SCTP 报文所属的 SCTP 偶联所承载的应用类型；

用应用标识标记所述新的记录，所述应用标识和所述应用类型相对应。

2. 如权利要求 1 所述的 SCTP 报文识别方法，其特征在于，所述验证标签包括：

源端到目的端的验证标签和 / 或目的端到源端的验证标签。

3. 如权利要求 1 所述的 SCTP 报文识别方法，其特征在于，所述特征元组还包括源端口或目的端口；所述特征集元组还包括源端口号和目的端口号。

4. 如权利要求 1 所述的 SCTP 报文识别方法，其特征在于，所述 SCTP 偶联用偶联标识或者应用标识进行标记，所述偶联标识用于标记所述 SCTP 偶联的序号，所述应用标识用于标记所述 SCTP 偶联所承载的应用类型。

5. 如权利要求 1 所述的 SCTP 报文识别方法，其特征在于，还包括：

按照预定的周期对所述 SCTP 元组识别表进行老化处理，删除所述 SCTP 元组识别表中不再使用的记录；所述按照预定的周期对所述 SCTP 元组识别表进行老化处理，删除所述元组识别表中不再使用的记录，包括：

解析收到的 SCTP 报文，如果是 STCP 关闭报文，则从所述元组识别表中删除所述 SCTP 报文对应的记录；或者，

定期检查所述元组识别表中记录相应记录匹配成功的计数，删除计数没有增加的相应的记录；或者，

定期检查元组识别表中记录相应表项匹配成功的时间的时间戳，删除时间戳超过预置老化时间的记录。

6. 一种 SCTP 报文识别装置，其特征在于，包括：

第一获取模块，用于获取接收到的 SCTP 报文的特征元组，所述特征元组包括源 IP 地

址、目的 IP 地址和验证标签中的至少一项信息；

匹配模块，用于将获取的 SCTP 报文的特征元组和预先设定的 SCTP 元组识别表进行匹配，所述 SCTP 元组识别表包括所述 SCTP 报文的特征集元组和 SCTP 偶联的对应关系，所述特征集元组包括源 IP 地址集、目的 IP 地址集和验证标签中的至少一项信息；

第二获取模块，用于所述匹配模块匹配成功时，得到所述 SCTP 报文所属的 SCTP 偶联；

第三解析单元，用于解析本次 SCTP 握手消息的初始化消息报文，将解析到的信息作为一个记录添加到所述元组识别表中，所述解析到的信息包括所述初始化消息报文的 IP 地址集、端口和验证标签中的至少一项信息；

第四解析单元，用于解析所述本次 SCTP 握手消息的初始化确认消息报文，获取所述初始化确认消息报文的 IP 地址集、端口和验证标签；

解析匹配单元，用于解析所述 SCTP 报文的公共分组头中的验证标签，利用所述公共分组头中的验证标签和所述 SCTP 元组识别表进行匹配，匹配到的记录为所述初始化消息报文对应的记录；

关联建立单元，用于将解析所述本次 SCTP 握手消息的初始化确认消息报文得到的 IP 地址集、端口和验证标签作为另一个记录添加到所述 SCTP 元组识别表，建立和所述初始化消息报文对应的记录的关联关系；

应用识别模块，用于识别所述 SCTP 报文所属的 SCTP 偶联所承载的应用类型；

业务添加模块，用于用应用标识标记所述新的记录，所述应用标识和所述应用类型相对应。

7. 如权利要求 6 所述的 SCTP 报文识别装置，其特征在于，所述特征元组还包括源端口或目的端口；所述特征集元组还包括源端口号或目的端口号。

8. 如权利要求 6 或 7 所述的 SCTP 报文识别装置，其特征在于，所述装置还包括：

维护模块，用于按照预定的周期对所述 SCTP 元组识别表进行老化处理，删除所述 SCTP 元组识别表中不再使用的记录；所述维护模块包括第一维护单元、第二维护单元或第三维护单元；

所述第一维护单元，用于解析收到的 SCTP 报文，如果是 STCP 关闭报文，则从所述元组识别表中删除所述 SCTP 报文对应的记录；

所述第二维护单元，用于定期检查所述元组识别表中记录相应记录匹配成功的计数，删除计数没有增加的相应的记录；

所述第三维护单元，用于定期检查元组识别表中记录相应表项匹配成功的时间的时间戳，删除时间戳超过预置老化时间的记录。

SCTP 报文识别方法和装置

技术领域

[0001] 本发明涉及通信技术领域，特别涉及一种 SCTP 报文识别方法和装置。

背景技术

[0002] SCTP(Stream Control Transmission Protocol，流控制传输协议)，是在 IP 网络上使用的一种可靠的通用传输层协议。该协议最初是为发送电信信令而设计的，具有支持多归属、多流、初始化保护、消息分帧、可配置的无序发送、平滑关闭等特性，有很高的可靠性和安全性。基于此原因，很多主流操作系统（如 :Linux、BSD、Solaris 等）也开始支持 SCTP，所以现在网络上的使用该协议进行传输的业务逐渐增多。

[0003] 现有技术中使用五元组（源 IP、目的 IP、源 Port、目的 Port、传输层协议）来识别一个 TCP/UDP 报文，该数据流需要保存的信息和该五元组进行关联，数据流的后续报文使用五元组索引数据流保存的信息

[0004] 但是，由于 SCTP 支持多归属的特性，SCTP 的同一个偶联可能使用几个不同的五元组进行交互。由于偶联中的五元组有多个，如果识别 TCP/UDP 报文的五元组来识别 SCTP 偶联，只能识别出偶联中一个或少数几个五元组，使用偶联中其他五元组进行通信的报文则识别不出来，这样会造成大量的漏识别。

发明内容

[0005] 本发明实施例提供一种 SCTP 报文识别方法和装置，以减少现有技术中 SCTP 流漏识别的情况。

[0006] 本发明实施例提供一种流控制传输协议 SCTP 报文识别方法，包括 :

[0007] 获取接收到的 SCTP 报文的特征元组，所述特征元组包括源 IP 地址目的 IP 地址和验证标签中的至少一项信息 ;

[0008] 将获取的 SCTP 报文的特征元组和预先设定的 SCTP 元组识别表进行匹配，所述 SCTP 元组识别表包括所述 SCTP 报文的特征集元组和 SCTP 偶联的对应关系，所述特征集元组包括源 IP 地址集、目的 IP 地址集和验证标签中的至少一项信息 ;

[0009] 如果匹配成功，得到所述 SCTP 报文所属的 SCTP 偶联。

[0010] 本发明实施例提供一种 SCTP 报文识别装置，包括 :

[0011] 第一获取模块，用于获取接收到的 SCTP 报文的特征元组，所述特征元组包括源 IP 地址、目的 IP 地址和验证标签中的至少一项信息 ;

[0012] 匹配模块，用于将获取的 SCTP 报文的特征元组和预先设定的 SCTP 元组识别表进行匹配，所述 SCTP 元组识别表包括所述 SCTP 报文的特征集元组和 SCTP 偶联的对应关系，所述特征集元组包括源 IP 地址集、源端口号、目的 IP 地址集、目的端口号、验证标签中的至少一项信息 ;

[0013] 第二获取模块，用于所述匹配模块匹配成功时，得到所述 SCTP 报文所属的 SCTP 偶联。

[0014] 本发明实施例提供一种建立 SCTP 元组识别表的方法，

[0015] 获得 SCTP 偶联的 SCTP 握手消息，所述 SCTP 握手消息包括初始化消息报文和与所述初始化消息报文对应的初始化确认消息报文；

[0016] 从所述初始化消息报文和所述初始化确认消息报文对中获得所述 SCTP 偶联的 SCTP 特征集元组，所述 SCTP 特征集元组包括源 IP 地址集、目的 IP 地址集、源端口号、目的端口号、验证标签中的至少一项信息；

[0017] 建立所述特征集元组和 SCTP 偶联的关联关系。

[0018] 本发明实施例通过以上技术方案，针对 SCTP 支持多归属的特点，利用包包括所述 SCTP 报文的特征集元组和 SCTP 偶联的对应关系的 SCTP 元组识别表进行 SCTP 报文的识别，由于该 SCTP 特征集元组包括源 IP 地址集、目的 IP 地址集或者验证标签，包括了一个 SCTP 偶联中所有的交互。当 SCTP 报文的特征元组，如源 IP 地址、目的 IP 地址或者 SCTP 标签和上述特征集元组匹配成功时，就可以得到 SCTP 报文所属的 SCTP 偶联。与传统五元组识别 SCTP 数据流时存在的不能完整识别同一个偶联中所有交互的相比，在 SCTP 偶联中发生使用五元组切换后，本实施例中的方案根据 IP 地址集或者验证标签的匹配结果，仍能正确的识别出该交互的报文所属的 SCTP 偶联，减少了漏识别的情况。

附图说明

[0019] 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简单地介绍，显而易见地，下面描述中的附图仅仅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性的前提下，还可以根据这些附图获得其他的附图。

[0020] 图 1 本发明实施例提供一种 SCTP 报文识别方法流程图；

[0021] 图 2 本发明实施例提供一种 SCTP 报文识别方法流程图；

[0022] 图 3 本发明实施例提供一种 SCTP 报文识别方法流程图；

[0023] 图 4 本发明实施例提供一种 SCTP 元组识别表结构示意图；

[0024] 图 5 本发明实施例提供一种 SCTP 报文识别装置结构图；

[0025] 图 6 本发明实施例提供一种 SCTP 报文识别装置结构图；

[0026] 图 7 本发明实施例提供一种解析添加模块结构图；

[0027] 图 8 本发明实施例提供一种解析添加模块结构图；

[0028] 图 9 本发明实施例提供一种 SCTP 报文识别装置结构图；

[0029] 图 10 本发明实施例提供一种维护模块结构图；

[0030] 图 11 本发明实施例提供一种 SCTP 报文识别系统结构图；

[0031] 图 12 本发明实施例提供一种 SCTP 元组识别表结构示意图；

[0032] 图 13 本发明实施例提供一种建立 SCTP 元组识别表的方法流程图。

具体实施方式

[0033] 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，所描述的实施例仅仅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做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。

[0034] 如图 1 所示，本发明实施例提供一种 SCTP 报文识别方法，包括 ：

[0035] S101，获取接收到的 SCTP 报文的特征元组 ；

[0036] 在一个实施例中，SCTP 报文的特征元组包括 ：SCTP 报文中的源 IP 地址、目的 IP 地址和验证标签 (Verification Tag) 中的至少一项信息。在另一个实施例中，该 SCTP 报文的特征元组还可以包括源端口号或者目的端口号。在另一个实施例中，该 SCTP 报文的特征元组还可以包括源端口号和目的端口号。

[0037] 在一个实施例中，如果 SCTP 报文是源端发送到目的端的，那么验证标签为源端到目的端的验证标签。

[0038] 在一个实施例中，如果 SCTP 报文是目的端发送到源端的，那么验证标签为目的端到源端的验证标签。

[0039] S102，将获取的 SCTP 报文的特征元组和预先设定的 SCTP 元组识别表进行匹配，所述 SCTP 元组识别表包括所述 SCTP 报文的特征集元组和 SCTP 偶联的对应关系 ；

[0040] 需要说明的是，在一个实施例中，SCTP 元组识别表还可以包括关联关系，该关联关系用于指向属于同一偶联的特征集元组的记录。

[0041] 需要说明的是，在一个实施例中，在 SCTP 元组识别表中，上述 SCTP 偶联用偶联标识或者应用标识进行标记，偶联标识用于标记所述 SCTP 偶联的序号，应用标识用于标记所述 SCTP 偶联所承载的应用类型。

[0042] 在一个实施例中，上述 SCTP 元组识别表中的特征集元组包括源 IP 地址集、目的 IP 地址集和验证标签中的至少一项信息。在另一个实施例中，上述特征集元组还可以包括源端口号和目的端口号。

[0043] 需要说明的是，在本实施例以及本发明其它实施例中，源 IP 地址集包括该 SCTP 偶联中源端所有可用的 IP 地址，目的 IP 地址集包括该 SCTP 偶联中目的端所有可用的 IP 地址。验证标签 (Verification Tag) 专用于建立偶联，SCTP 两侧端点在建立偶联时会交换验证标签，验证标签的值在 SCTP 握手时第一次交换时确定，并且在以后的交互中保持不变。

[0044] 在一个实施例中，在进行匹配时，可以将获取的特征元组作为键 (key) 值，采用哈希 (hash) 查找的方法与 SCTP 元组识别表进行匹配。hash 查找的方法作为一个具体的查找方式具有迅速查找的优势，能提高匹配速度。可以理解的是 hash 查找的方法并不是匹配的唯一实现方式，故 hash 查找的方式作为一个举例不应理解为对本发明实施例的限定。

[0045] 如图 4 所示，本发明一个实施例提供一种 SCTP 元组识别表的结构示意图。根据图 4，该 SCTP 元组识别表包括验证标签 (V_tag)、端口 (Port)、应用标识 (Application)，IP 列表 (IP List) 和关联关系 (Relation)。本发明实施例中将 SCTP 元组识别表中每一个 SCTP 元组识别表的表项称为一个记录。如图 4 中，SCTP 表的每一个表项 (记录) 包括括验证标签、端口、应用，IP 列表和关联关系。在图 4 中，V_tag 用于标识 SCTP 报文。IP 列表通过一个指针来标识一个 IP 地址集，这个 IP 地址集可以是源 IP 地址集或者目的 IP 地址集。

[0046] 在本实施例中，在图 4 所示的 SCTP 元组识别表中，SCTP 报文的特征集元组和 SCTP 偶联的对应关系通过关联关系来表示。在表 4 中关联关系用于将属于同一偶联的特征集元组的记录关联，也就是说关联关系将两个记录关联起来，标识这两个记录同一个 SCTP 偶联。

[0047] 在图 4 中，本实施例是用应用标识来标记一个 SCTP 偶联，通过应用标识能获得偶该联所承载的应用类型。当然在另一个实施例中，也可以将应用标识替换为偶联标识来标记这个 SCTP 偶联，通过偶联标识能获得 SCTP 偶联的序号，这时在一个实施例中，可以再增加一个应用标识的信息表项，来标识这个 SCTP 偶联所承载的应用。

[0048] 当然，在另一个实施例中，也可以不使用指针，而直接将 IP 地址集放在 IP 列表项中。在另一个实施例中，还可以将两个具有关联关系的记录合并为一个记录，如图 12 所示，在图 12 中，SCTP 元组识别表的每一个记录包括了源 IP 地址集、目的 IP 地址集、源端口号、目的端口号、和验证标签（对于图 12 来说，在一个实施例中，也可以叫做验证标签对，即图 12 中的源端到目的端的验证标签和目的端到源端的验证标签）。在图 12 中，每一个记录就代表一个偶联的信息。图 4 和图 12 仅仅是作为本发明实施例一个 SCTP 元组识别表的举例，本发明实施例不对 SCTP 元组识别表进行特别的限定。

[0049] 在一个实施例中，验证标签为源端到目的端和 / 或目的端到源端的验证标签。例如，当采用图 4 所示的 SCTP 元组识别表的结构时，表中一个记录的验证标签可以为源端到目的端的验证标签，也可以为目的端到源端的验证标签。当采用图 12 所述的 SCTP 元组识别表的结构时，表中一个记录的验证标签为源端到目的端的验证标签和目的端到源端的验证标签。

[0050] 为了更为直观的说明两个记录的关联关系，在图 4 中将属于同一个 SCTP 偶联的记录用箭头连接示出。如图 4 所示，V_tag 为 1254932544 的 SCTP 报文与 V_tag 为 8941172325 的 SCTP 报文属于同一个 SCTP 偶联。V_tag 为 1254932544 的 SCTP 报文对应的记录中的 IP 列表通过一个指针来标识源 IP 地址集，V_tag 为 8941172325 的 SCTP 报文对应的记录中的 IP 列表通过一个指针来标识目的 IP 地址集。

[0051] 当接收到新的 SCTP 报文时，可以通过解析次 SCTP 报文获得此 SCTP 报文的特征元组。例如，在一个实施例中，通过解析接收到的新的 SCTP 报文得到此 SCTP 报文的源 IP 地址为 10.70.145.28，此时可以将得到的源 IP 地址与图 4 中的 SCTP 元组识别表进行匹配，得到该 SCTP 报文所属的 SCTP 偶联。

[0052] S 103，如果匹配成功，得到所述 SCTP 报文所属的 SCTP 偶联。

[0053] 在一个实施例中，如果上述 SCTP 报文的特征元组和 SCTP 元组识别表匹配成功，则说明该 SCTP 报文是属于 SCTP 元组识别表中已有的 SCTP 偶联，所以可以通过 SCTP 元组识别表中的 SCTP 报文的特征集元组和 SCTP 偶联的对应关系，获取该 SCTP 报文所属的 SCTP 偶联，即获取该 SCTP 报文所属的 SCTP 数据流。进一步，还可以通过 SCTP 元组识别表中的应用标识，获取该 SCTP 报文所属的 SCTP 偶联所承载的应用。由于一个 SCTP 偶联对应一个应用，所以当根据本实施例提供的方法识别出一个 SCTP 报文所属的偶联后，后续属于这个 SCTP 偶联的报文就都承载相同的应用。

[0054] 例如，在一个实施例中，将 IP 地址为 10.70.145.28 的 SCTP 报文的 IP 地址与图 4 中的 SCTP 元组识别表进行匹配，可以得到此 SCTP 报文对应的记录和与其具有关联关系的记录（在图 4 中为 V_tag 为 8941172325 的 SCTP 报文对应的记录），从而确定此 SCTP 报文所属的 SCTP 偶联。进一步通过应用标识，来得到该 SCTP 所属的偶联所承载的应用，后续如果识别出属于这个 SCTP 偶联的其它报文，直接可以得知这些其它报文都承载 HTTP 应用。

[0055] 例如，根据图 4，该 IP 地址为 10.70.145.28 的 SCTP 报文所属的 SCTP 偶联所承载

的应用为 HTTP 应用，在一个实施例中，IP 地址为 10.25.202.183 的报文经过匹配，发现该报文对应的记录和上述 IP 地址为 10.70.145.28 的 SCTP 报文对应的记录具有关联关系，属于同一个 SCTP 偶联，对应的应用为 HTTP 应用。

[0056] 需要说明的是，图 4 仅仅是本发明实施例一个元组识别表的举例，图 4 所示的 SCTP 元组识别表只是提供了元组识别表实现的一种典型方式，不是唯一的，可以在此表的基础上进行优化和完善。例如，在一个实施例中，如果不考虑误识别、漏识别、不需要获取对应的应用等因素，也可以只使用验证标签和关联关系来组织元组识别表。

[0057] 或者，在另一个实施例中也可以只使用 IP 列表和关联关系来组织元组识别表。由于 SCTP 元组识别表是预先设置的，所以此时就需要根据元组识别表中的记录来相应的提取 SCTP 报文的特征元组。例如，如果 SCTP 元组识别表只使用验证标签和关联关系来设定，那么就需要提取接收到的 SCTP 报文的验证标签；如果，SCTP 元组识别表只使用 IP 列表和关联关系来设定，那么就需要提取接收到的 SCTP 报文的源 IP 地址或者目的 IP 地址。

[0058] 本发明实施例通过以上技术方案，针对 SCTP 支持多归属的特点，利用包包括所述 SCTP 报文的特征集元组和 SCTP 偶联的对应关系的 SCTP 元组识别表进行 SCTP 报文的识别，由于该 SCTP 特征集元组包括源 IP 地址集、目的 IP 地址集或者验证标签，包括了一个 SCTP 偶联中所有的交互。当 SCTP 报文的特征元组，如源 IP 地址、目的 IP 地址或者 SCTP 标签和上述特征集元组匹配成功时，就可以得到 SCTP 报文所属的 SCTP 偶联。与传统五元组识别 SCTP 数据流时存在的不能完整识别同一个偶联中所有交互的相比，在 SCTP 偶联中发生使用五元组切换后，本实施例中的方案根据 IP 地址集或者验证标签的匹配结果，仍能正确的识别出该交互的报文所属的 SCTP 偶联，减少了漏识别的情况。

[0059] 如图 2 所示，本发明实施例提供一种 SCTP 报文识别方法，包括：

[0060] S110，判断接收到的报文的传输协议类型；

[0061] 在一个实施例中，可以通过判断接收到的报文的传输层协议的类型，来判断接收到的报文是否是 SCTP 报文。如果传输层协议的类型是 TCP/UDP 协议，则接收的报文是普通的报文，这时可以使用普通的五元组对该报文进行识别；如果传输层协议的类型是 SCTP 协议，则接收到的报文是 SCTP 报文。

[0062] S120，若传输协议类型为 SCTP 协议，则接收到的报文为 SCTP 报文，获取该 SCTP 报文的特征元组；

[0063] 在一个实施例中，SCTP 报文的特征元组包括：SCTP 报文中的源 IP 地址、目的 IP 地址和验证标签中的至少一项信息；在一个实施例中该特征元组还可以包括源端口号和目的端口号；在一个实施例中，该特征元组还可以全部包括源 IP 地址、目的 IP 地址、源端口号、目的端口号和验证标签这五项信息。

[0064] S130，将获取的 SCTP 报文的特征元组和预先设定的 SCTP 元组识别表进行匹配，所述 SCTP 元组识别表包括所述 SCTP 报文的特征集元组和 SCTP 偶联的对应关系；

[0065] 在一个实施例中，在进行匹配时，可以将获取的特征元组作为 key 值，采用 hash 查找的方法与 SCTP 元组识别表进行匹配。hash 查找的方法作为一个具体的查找方式具有迅速查找的优势，能提高匹配速度。可以理解的是 hash 查找的方法并不是匹配的唯一实现方式，故 hash 查找的方式作为一个举例不应理解为对本发明实施例的限定。

[0066] 在一个实施例中，上述特征集元组包括源 IP 地址集、目的 IP 地址集、源端口号、目

的端口号和验证标签中的至少一项信息。在一个实施例中，该特征集元组还可以包括源端口号和目的端口号；在一个实施例中，该特征集元组还可以全部包括源 IP 地址集、目的 IP 地址集、源端口号、目的端口号和验证标签这五项信息。关于验证标签具体类型，在前述实施例中已经详细描述，在此不再赘述。

[0067] S140，如果匹配成功，得到所述 SCTP 报文所属的 SCTP 偶联。

[0068] 在一个实施例中，进一步，还可以通过 SCTP 元组识别表中的应用标识，获取该 SCTP 报文所属的 SCTP 偶联所承载的应用。

[0069] S150，如果匹配不成功，解析本次 SCTP 握手消息得到新的具有关联关系的特征集元组，将上述特征集元组作为新的记录添加到所述 SCTP 元组识别表中。

[0070] 在一个实施例中，如果匹配不成功，说明该 SCTP 报文是 SCTP 建立新连接的握手消息，属于一个新的 SCTP 数据流，需要添加新的记录以标识此新的 SCTP 数据流。

[0071] 在一个实施例中，S150 可以包括：

[0072] S1501，获得 SCTP 的握手消息，所述握手消息包括属于同一新的 SCTP 偶联的 INIT（初始化消息）和 INIT ACK（初始化确认消息）报文；

[0073] 在一个实施例中可以通过 INIT 报文中的 IP 列表获得属于同一 SCTP 偶联握手消息对应的 INITACK 报文，从而获得 SCTP 的握手消息。具体地，在一个实施例中，可以解析 INIT 报文的 IP 列表，来获取 INIT ACK 报文的目的 IP，如果该目的 IP 在 INIT 报文的 IP 列表中，则可以确认 INIT ACK 报文和 INIT 报文是属于同一个 SCTP 偶联。

[0074] S1502，从该握手消息中的 INIT 报文解析，得到该 INIT 报文的特征元组，从该握手消息中 INIT ACK 报文解析得到该 INIT ACK 报文的特征元组；

[0075] S1503，根据解析得到的 INIT 报文和 INIT ACK 报文的特征元组，得到本次 SCTP 握手消息对应的新的 SCTP 偶联的源 IP 地址集、目的 IP 地址集、源端口号、目的端口号、验证标签；

[0076] S1504，将 S1503 中得到的源端数据和目的端数据进行关联，作为本次 SCTP 握手消息对应的新的 SCTP 偶联的记录；

[0077] S1505，将上述新的 SCTP 偶联的记录添加到 SCTP 元组识别表中。

[0078] 在另一个实施例中，S150 可以包括：

[0079] S1511，获得 SCTP 的握手消息，所述握手消息包括属于同一新的 SCTP 偶联的 INIT 和 INIT ACK 消息；

[0080] S1512，解析 INIT 报文，将解析到的信息作为一个记录添加到元组识别表，上述解析到的信息包括 INIT 报文的 IP 地址集、端口和验证标签中的至少一项信息；

[0081] 将解析 INIT 报文得到的信息作为一个记录添加到元组识别表后，此记录在 SCTP 元组识别表中并没有具有关联关系的记录，所以需要进行步骤 S1513。

[0082] S1513，解析 INITACK 报文，获取该报文的 IP 地址集、端口和验证标签；

[0083] S1514，解析 SCTP 报文的公共分组头中的验证标签，利用上述公共分组头中的验证标签匹配元组识别表，匹配到的记录为 S1512 中 INIT 报文对应的记录；

[0084] S1515，将 S1513 中解析到的信息作为另一个记录添加到元组识别表，建立和 S1514 中匹配到的记录的关联关系。

[0085] 由上述内容可知，在上述两个实施例中标识新的 SCTP 数据流，可以解析此次 SCTP

握手消息中的 INIT 和 INIT ACK 报文。在本发明的另一个实施例中，在 S150 中将新的记录添加到元组识别表中时，也可以只解析 INIT ACK 报文，INIT ACK 报文中携带了源端和目的端的验证标签和端口信息。通过解析 INIT ACK 报文获取两端的验证标签和端口信息，就将解析得到的两端的信息关联起来作为一个偶联的两个记录添加到元组识别表中。

[0086] 如图 13 所示，本发明实施例提供一种建立 SCTP 元组识别表的方法，包括：

[0087] S401，获得 SCTP 偶联的 SCTP 握手消息，所述 SCTP 握手消息包括初始化消息 (INIT) 报文和与所述初始化消息报文对应的初始化确认消息 (INITACK) 报文；

[0088] S402，从 INIT 报文和 INIT ACK 报文对中获得 SCTP 特征集元组，SCTP 特征集元组包括源 IP 地址集、目的 IP 地址集、源端口号、目的端口号、验证标签中的至少一项信息；

[0089] 具体地，在一个实施例中，S402 可以包括：

[0090] S4021，解析 INIT ACK 报文，得到此 SCTP 偶联的源 IP 地址集、目的 IP 地址、源端口号、目的端口号和源端到目的端的验证标签；

[0091] S4022，解析 INITACK 报文，得到此 SCTP 偶联的目的 IP 地址集、源 IP 地址、源端口号、目的端口号和目的端到源端的验证标签；

[0092] S4023，根据解析上述 INIT 报文和 INIT ACK 得到的信息，获得所述 SCTP 偶联特征集元组。

[0093] S403，建立所述特征集元组和 SCTP 偶联的关联关系。

[0094] 在一个实施例中，S403 可以包括：

[0095] 将 S402 中得到的源端数据和目的端数据进行关联，作为本次 SCTP 握手消息对应的新的 SCTP 偶联的记录。

[0096] 在一个实施例中，S403 可以包括：

[0097] S4031，将 S4021 解析得到的信息作为一个记录添加到元组识别表；

[0098] S4032，解析 SCTP 偶联中 SCTP 报文的公共分组头中的验证标签，利用上述公共分组头中的验证标签匹配元组识别表，匹配到的记录为 S4031 中 INIT 报文对应的记录；

[0099] S4033，将 S4022 中解析到的信息作为另一个记录添加到元组识别表，建立和 S4032 中匹配到的记录的关联关系。

[0100] 本发明实施例通过以上技术方案，针对 SCTP 支持多归属的特点，利用包包括所述 SCTP 报文的特征集元组和 SCTP 偶联的对应关系的 SCTP 元组识别表进行 SCTP 报文的识别，由于该 SCTP 特征集元组包括源 IP 地址集、目的 IP 地址集或者验证标签，包括了一个 SCTP 偶联中所有的交互。当 SCTP 报文的特征元组，如源 IP 地址、目的 IP 地址或者 SCTP 标签和上述特征集元组匹配成功时，就可以得到 SCTP 报文所属的 SCTP 偶联。与传统五元组识别 SCTP 数据流时存在的不能完整识别同一个偶联中所有交互的相比，在 SCTP 偶联中发生使用五元组切换后，本实施例中的方案根据 IP 地址集或者验证标签的匹配结果，仍能正确的识别出该交互的报文所属的 SCTP 偶联，减少了漏识别的情况。并且解析和元组识别表匹配不成功的报文，将解析到的结果作为记录更新到元组识别表中，方便后续属于同一个 SCTP 偶联的报文的识别。

[0101] 如图 3 所示，在基于图 2 对应的实施例的基础上，本发明实施例提供的 SCTP 数据流的识别方法还可以包括：

[0102] S160，在匹配不成功时，识别该 SCTP 报文所属的 SCTP 偶联所承载的应用类型；

[0103] 在一个实施例中，可以使用业务识别技术（例如，DPI(Deep PacketInspection)深度包检测）技术）识别 SCTP 数据流，即 SCTP 偶联所承载的应用类型。

[0104] S170，用应用标识标记所述新的记录，该应用标识和上述应用类型相对应。

[0105] 在一个实施例中，将识别出的应用类型和对应的偶联关联，并标识到 SCTP 元组识别表中的对应记录，便于该 SCTP 数据流的后续报文可以通过 SCTP 元组识别表直接查找到对应的表项，进一步可以获取该 SCTP 所承载的业务。

[0106] S180，按照预定的周期对上述元组识别表进行老化处理，删除上述元组识别表中不再使用的记录。

[0107] 在一个实施例中，可以解析收到的 SCTP 报文，如果是 STCP 关闭报文（如，SHUTDOWN、SHUTDOWN ACK 或 ABORT)，则从上述元组识别表中删除相应的记录；

[0108] 在一个实施例中，可以定期检查元组识别表中记录相应表项匹配成功的计数，如果相应表项的计数没有增加，在元组识别表中删除该记录。

[0109] 在一个实施例中，可以定期检查元组识别表中记录相应表项匹配成功的时间的时间戳，删除时间戳超过预置老化时间的记录。

[0110] 需要说明的是，在一个实施例中，在预先建立 SCTP 元组识别表时，采用的方法与步骤 S1501 ～ S1504 或者 S1511 ～ S1515 类似，在此不再赘述。在另一个实施例中，在预先建立 SCTP 元组识别表时，还可以进一步的采用步骤 S160 ～ S170 中的方法，识别出一个 SCTP 偶联所对应的应用，并利用对应的应用标识来标记此 SCTP 偶联，在此不再赘述。

[0111] 本发明实施例通过以上技术方案，针对 SCTP 支持多归属的特点，利用包包括所述 SCTP 报文的特征集元组和 SCTP 偶联的对应关系的 SCTP 元组识别表进行 SCTP 报文的识别，由于该 SCTP 特征集元组包括源 IP 地址集、目的 IP 地址集或者验证标签，包括了一个 SCTP 偶联中所有的交互。当 SCTP 报文的特征元组，如源 IP 地址、目的 IP 地址或者 SCTP 标签和上述特征集元组匹配成功时，就可以得到 SCTP 报文所属的 SCTP 偶联。与传统五元组识别 SCTP 数据流时存在的不能完整识别同一个偶联中所有交互的相比，在 SCTP 偶联中发生使用五元组切换后，本实施例中的方案根据 IP 地址集或者验证标签的匹配结果，仍能正确的识别出该交互的报文所属的 SCTP 偶联，减少了漏识别的情况。并且解析和元组识别表匹配不成功的报文，将解析到的结果作为记录更新到元组识别表中，方便后续属于同一个 SCTP 偶联的报文的识别。进一步，通过业务识别技术识别新的 SCTP 偶联所承载的应用，方便后续对所属同一个 SCTP 偶联的 SCTP 报文所承载的应用的识别，而且通过对元组识别表进行老化维护，及时删除元组识别表中不再使用的记录，提高了识别效率。

[0112] 如图 5 所示，本发明实施例提供一种 SCTP 报文识别装置，包括：

[0113] 第一获取模块 210，用于获取接收到的 SCTP 报文的特征元组；

[0114] 在一个实施例中，SCTP 报文的特征元组包括：SCTP 报文中的源 IP 地址、目的 IP 地址和验证标签中的至少一项信息；在一个实施例中，该特征元组还可以包括源端口号和目的端口号；在一个实施例中，该特征集元组还可以全部包括源 IP 地址、目的 IP 地址、源端口号、目的端口号和验证标签这五项信息。

[0115] 匹配模块 220，用于将获取的 SCTP 报文的特征元组和预先设定的 SCTP 元组识别表进行匹配，上述 SCTP 元组识别表包括上述 SCTP 报文的特征集元组和 SCTP 偶联的对应关系；

[0116] 在一个实施例中，上述特征集元组包括源 IP 地址集、目的 IP 地址集、源端口号、目的端口号和验证标签中的至少一项信息。在一个实施例中，该特征集元组还可以包括源端口号和目的端口号；在一个实施例中，该特征集元组还可以全部包括源 IP 地址集、目的 IP 地址集、源端口号、目的端口号和验证标签这五项信息。

[0117] 第二获取模块 230，用于在匹配模块 220 匹配成功时，得到所述 SCTP 报文所属的 SCTP 偶联。

[0118] 在一个实施例中，如果上述 SCTP 报文的特征元组和 SCTP 元组识别表匹配成功，则说明该 SCTP 报文是属于 SCTP 元组识别表中已有的 SCTP 偶联，所以第二获取模块 230 可以通过 SCTP 元组识别表中的 SCTP 报文的特征集元组和 SCTP 偶联的对应关系，获取该 SCTP 报文所属的 SCTP 偶联，即获取该 SCTP 报文所属的 SCTP 数据流。

[0119] 如图 5 中的虚线框所示，在一个实施例中，该装置还包括：

[0120] 第三获取模块 231，用于根据上述 SCTP 报文所属的 SCTP 偶联对应的应用标识，获取该 SCTP 报文所属的 SCTP 偶联所承载的应用。

[0121] 本发明实施例通过以上技术方案，针对 SCTP 支持多归属的特点，利用包包括所述 SCTP 报文的特征集元组和 SCTP 偶联的对应关系的 SCTP 元组识别表进行 SCTP 报文的识别，由于该 SCTP 特征集元组包括源 IP 地址集、目的 IP 地址集或者验证标签，包括了一个 SCTP 偶联中所有的交互。当 SCTP 报文的特征元组，如源 IP 地址、目的 IP 地址或者 SCTP 标签和上述特征集元组匹配成功时，就可以得到 SCTP 报文所属的 SCTP 偶联。与传统五元组识别 SCTP 数据流时存在的不能完整识别同一个偶联中所有交互的相比，在 SCTP 偶联中发生使用五元组切换后，本实施例中的方案根据 IP 地址集或者验证标签的匹配结果，仍能正确的识别出该交互的报文所属的 SCTP 偶联，减少了漏识别的情况。进一步地，还可以通过 SCTP 元组识别表中的业务标识，获取接收到的 SCTP 报文所承载的应用。

[0122] 如图 6 所示，在一个实施例中，该装置还可以包括：

[0123] 解析添加模块 240，用于在匹配模块 220 匹配不成功时，解析此次 SCTP 握手消息得到新的具有关联关系的特征集元组，将所述特征集元组作为新的记录添加到所述 SCTP 元组识别表中；

[0124] 应用识别模块 250，用于在匹配模块 220 匹配不成功时，识别该 SCTP 报文所属的 SCTP 数据流所承载的应用类型；

[0125] 在一个实施例中，可以使用 DPI 技术识别 SCTP 数据流所承载的应用类型。

[0126] 业务添加模块 260，用于用应用标识标记所述新的记录，所述应用标识和所述应用类型相对应。

[0127] 如图 7 所示，在一个实施例中，解析添加模块 240 可以包括：

[0128] 消息获取单元 2401，用于获得 SCTP 的握手消息，所述握手消息包括属于同一新的 SCTP 偶联的 INIT 和 INIT ACK 消息；

[0129] 在一个实施例中，消息获取单元 2401 可以通过 INIT 消息中的 IP 列表获得属于同一 SCTP 偶联握手消息对应的 INIT ACK，从而获得 SCTP 的握手消息。

[0130] 第一解析单元 2402，用于从上述握手消息中的 INIT 报文解析得到该 INIT 报文的特征元组；

[0131] 第二解析单元 2403，用于从握手消息中 INIT ACK 报文解析得到该 INITACK 报文的

特征元组；

[0132] 获取单元2404，用于根据解析得到的INIT报文和INIT ACK报文的特征元组，得到本次SCTP握手消息对应的新的SCTP偶联的源IP地址集、目的IP地址集、源端口号、目的端口号、验证标签；

[0133] 关联单元2405，用于将获取单元2404中得到的源端数据和目的端数据进行关联，作为上述新的SCTP偶联的记录；

[0134] 添加单元2406，用于将上述具有关联关系的记录添加到SCTP元组识别表中。

[0135] 如图8所示，在另一个实施例中，解析添加模块240可以包括：

[0136] 消息获取单元2401，用于获得SCTP的握手消息，所述握手消息包括属于同一新的SCTP偶联的INIT和INIT ACK消息；

[0137] 第三解析单元241，用于解析INIT报文，将解析到的信息作为一个记录添加到元组识别表中，所述解析到的信息包括所述初始化消息报文的IP地址集、端口和验证标签中的至少一项信息；

[0138] 第四解析单元242，用于解析INITACK报文，获取该报文的IP地址集、端口和验证标签；

[0139] 解析匹配单元243，用于解析SCTP报文的公共分组头中的验证标签，利用上述公共分组头中的验证标签匹配元组识别表，匹配到的记录为第一解析单元241中INIT报文对应的记录；

[0140] 关联建立单元244，用于将第二解析单元242中解析到的信息作为另一个记录添加到元组识别表，建立和解析匹配单元243中匹配到的记录的关联关系。

[0141] 本发明实施例通过以上技术方案，针对SCTP支持多归属的特点，利用包包括所述SCTP报文的特征集元组和SCTP偶联的对应关系的SCTP元组识别表进行SCTP报文的识别，由于该SCTP特征集元组包括源IP地址集、目的IP地址集或者验证标签，包括了一个SCTP偶联中所有的交互。当SCTP报文的特征元组，如源IP地址、目的IP地址或者SCTP标签和上述特征集元组匹配成功时，就可以得到SCTP报文所属的SCTP偶联。与传统五元组识别SCTP数据流时存在的不能完整识别同一个偶联中所有交互的相比，在SCTP偶联中发生使用五元组切换后，本实施例中的方案根据IP地址集或者验证标签的匹配结果，仍能正确的识别出该交互的报文所属的SCTP偶联，减少了漏识别的情况。并且解析和元组识别表匹配不成功的报文，将解析到的结果作为记录更新到元组识别表中，方便后续属于同一个SCTP偶联的报文的识别。进一步，通过业务识别技术识别新的SCTP偶联所承载的应用，方便后续对属于同一个SCTP偶联的SCTP报文所承载的应用的识别。

[0142] 如图9所示，在另一个实施例中，该装置还可以包括：

[0143] 维护模块270，用于按照预定的周期对上述元组识别表进行老化处理，删除上述元组识别表中不再使用的记录。

[0144] 如图10所示，在一个实施例中，所述维护模块270包括：

[0145] 第一维护单元271，用于解析收到的SCTP报文，如果是STCP关闭报文(SHUTDOWN、SHUTDOWN ACK或ABORT)，则从上述元组识别表中删除相应的记录；或者，

[0146] 第二维护单元272，用于定期检查元组识别表中记录相应记录匹配成功的计数，如果相应记录的计数没有增加，在元组识别表中删除该记录，即，删除计数没有增加的相应的

记录；或者，

[0147] 第三维护单元 273，用于定期检查元组识别表中记录相应记录匹配成功的时间的时间戳，删除时间戳超过预置老化时间的记录。

[0148] 本发明实施例通过以上技术方案，针对 SCTP 支持多归属的特点，利用包包括所述 SCTP 报文的特征集元组和 SCTP 偶联的对应关系的 SCTP 元组识别表进行 SCTP 报文的识别，由于该 SCTP 特征集元组包括源 IP 地址集、目的 IP 地址集或者验证标签，包括了一个 SCTP 偶联中所有的交互。当 SCTP 报文的特征元组，如源 IP 地址、目的 IP 地址或者 SCTP 标签和上述特征集元组匹配成功时，就可以得到 SCTP 报文所属的 SCTP 偶联。与传统五元组识别 SCTP 数据流时存在的不能完整识别同一个偶联中所有交互的相比，在 SCTP 偶联中发生使用五元组切换后，本实施例中的方案根据 IP 地址集或者验证标签的匹配结果，仍能正确的识别出该交互的报文所属的 SCTP 偶联，减少了漏识别的情况。并且解析和元组识别表匹配不成功的报文，将解析到的结果作为记录更新到元组识别表中，方便后续属于同一个 SCTP 偶联的报文的识别。进一步，通过业务识别技术识别新的 SCTP 偶联所承载的应用，方便后续对属于同一个 SCTP 偶联的 SCTP 报文所承载的应用的识别，而且通过对元组识别表进行老化维护，及时删除元组识别表中不再使用的记录，提高了识别效率。

[0149] 如图 11 所示，本发明实施例提供一种 SCTP 报文识别系统，包括：

[0150] 接收装置 10，用于接收报文；

[0151] SCTP 报文识别装置 20，用于接收装置 10 接受到 SCTP 报文时，获取接收到的 SCTP 报文的特征元组，所述特征元组包括源 IP 地址、目的 IP 地址和验证标签中的至少一项信息；将获取的 SCTP 报文的特征元组和预先设定的 SCTP 元组识别表进行匹配，所述 SCTP 元组识别表包括所述 SCTP 报文的特征集元组和 SCTP 偶联的对应关系，所述特征集元组包括源 IP 地址集、目的 IP 地址集和验证标签中的至少一项信息；如果匹配成功，得到所述 SCTP 报文所属的 SCTP 偶联。

[0152] 在一个实施例中，该特征元组还可以包括源端口号和目的端口号；在一个实施例中，该特征元组还可以全部包括源 IP 地址、目的 IP 地址、源端口号、目的端口号和验证标签这五项信息。

[0153] 在一个实施例中，该特征集元组还可以包括源端口号和目的端口号；在一个实施例中，该特征集元组还可以全部包括源 IP 地址集、目的 IP 地址集、源端口号、目的端口号和验证标签这五项信息。

[0154] SCTP 报文识别装置 20 的结构和功能如上述装置实施例所述，在此不再赘述。

[0155] 本发明实施例通过以上技术方案，针对 SCTP 支持多归属的特点，利用包包括所述 SCTP 报文的特征集元组和 SCTP 偶联的对应关系的 SCTP 元组识别表进行 SCTP 报文的识别，由于该 SCTP 特征集元组包括源 IP 地址集、目的 IP 地址集或者验证标签，包括了一个 SCTP 偶联中所有的交互。当 SCTP 报文的特征元组，如源 IP 地址、目的 IP 地址或者 SCTP 标签和上述特征集元组匹配成功时，就可以得到 SCTP 报文所属的 SCTP 偶联。与传统五元组识别 SCTP 数据流时存在的不能完整识别同一个偶联中所有交互的相比，在 SCTP 偶联中发生使用五元组切换后，本实施例中的方案根据 IP 地址集或者验证标签的匹配结果，仍能正确的识别出该交互的报文所属的 SCTP 偶联，减少了漏识别的情况。

[0156] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以

通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory，ROM）或随机存储记忆体（Random Access Memory，RAM）等。

[0157] 以上所述仅为本发明的几个实施例，本领域的技术人员依据申请文件公开的可以对本发明进行各种改动或变型而不脱离本发明的精神和范围。

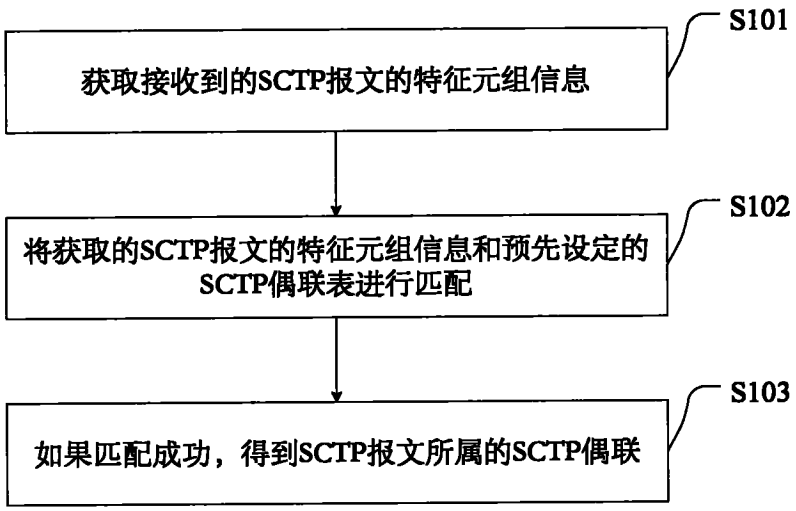

S101
获取接收到的SCTP报文的特征元组信息
S102
将获取的SCTP报文的特征元组信息和预先设定的SCTP偶联表进行匹配
S103
如果匹配成功，得到SCTP报文所属的SCTP偶联

图 1

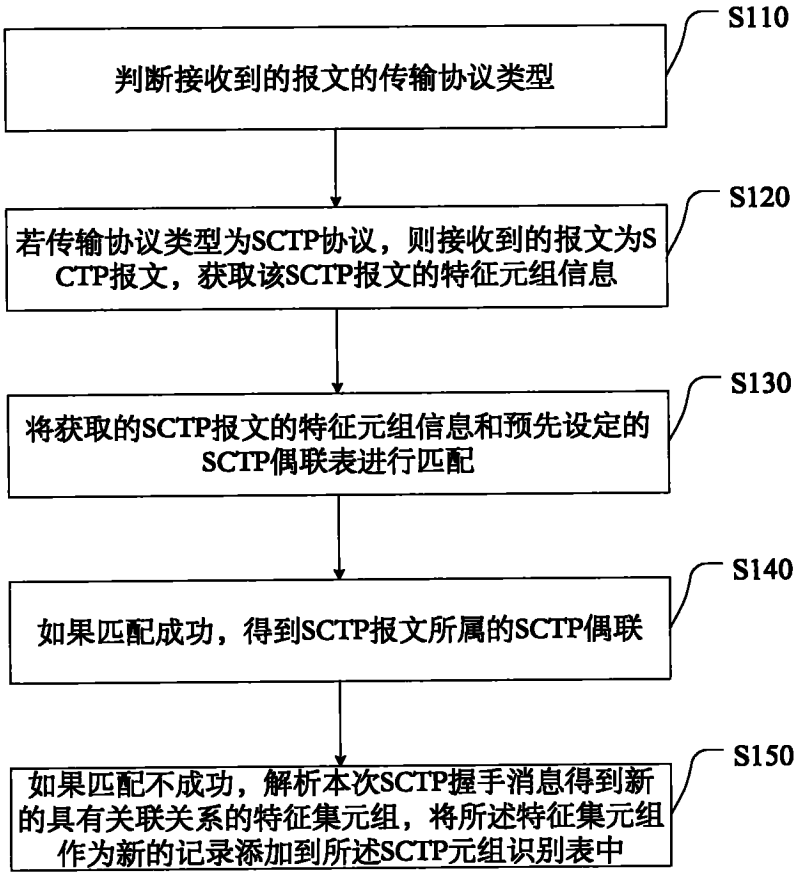

S110
判断接收到的报文的传输协议类型
S120
若传输协议类型为SCTP协议，则接收到的报文为SCTP报文，获取该SCTP报文的特征元组信息
S130
将获取的SCTP报文的特征元组信息和预先设定的SCTP偶联表进行匹配
S140
如果匹配成功，得到SCTP报文所属的SCTP偶联
S150
如果匹配不成功，解析本次SCTP握手消息得到新的具有关联关系的特征集元组，将所述特征集元组作为新的记录添加到所述SCTP元组识别表中

图 2

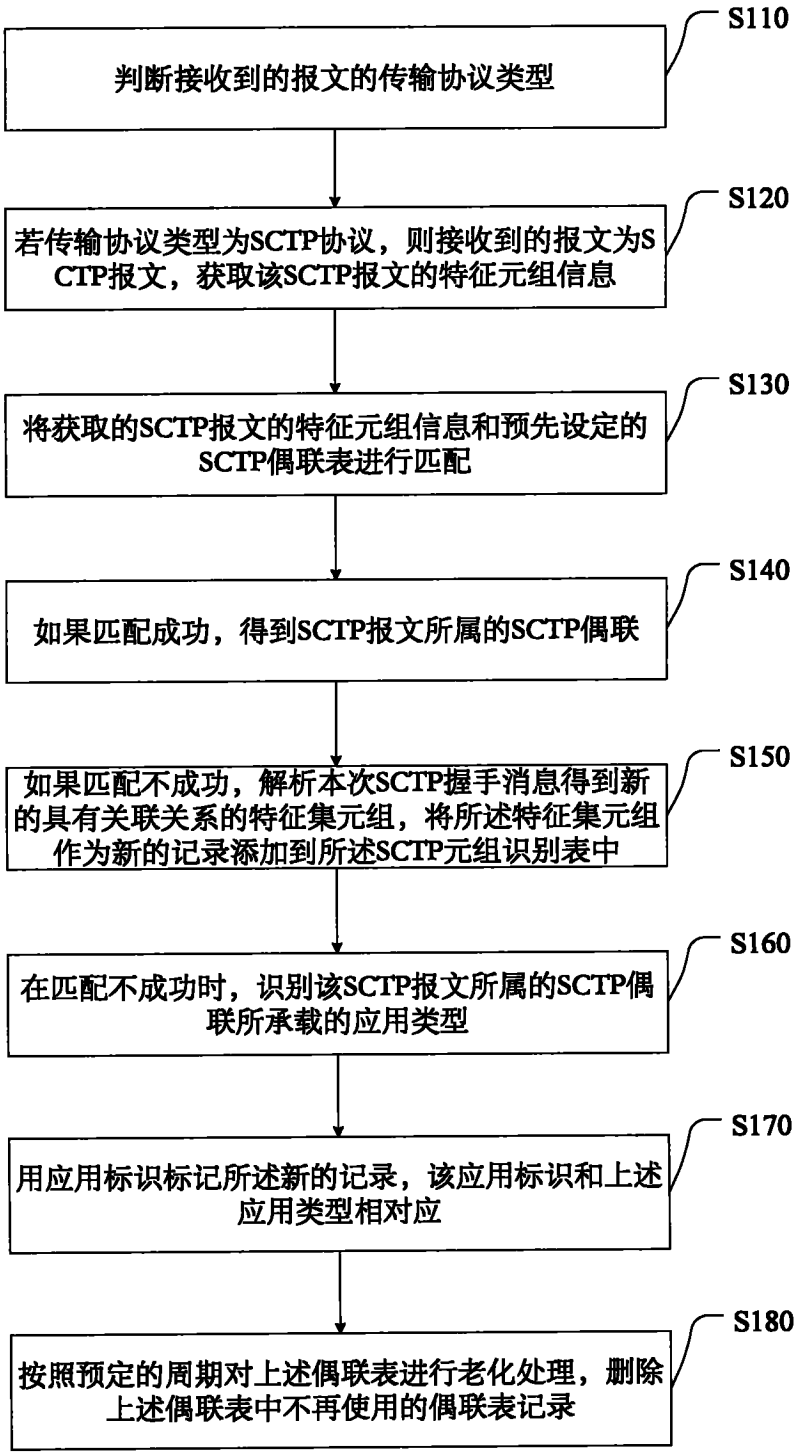

S110
判断接收到的报文的传输协议类型
S120
若传输协议类型为SCTP协议，则接收到的报文为SCTP报文，获取该SCTP报文的特征元组信息
S130
将获取的SCTP报文的特征元组信息和预先设定的SCTP偶联表进行匹配
S140
如果匹配成功，得到SCTP报文所属的SCTP偶联
S150
如果匹配不成功，解析本次SCTP握手消息得到新的具有关联关系的特征集元组，将所述特征集元组作为新的记录添加到所述SCTP元组识别表中
S160
在匹配不成功时，识别该SCTP报文所属的SCTP偶联所承载的应用类型
S170
用应用标识标记所述新的记录，该应用标识和上述应用类型相对应
S180
按照预定的周期对上述偶联表进行老化处理，删除上述偶联表中不再使用的偶联表记录

图 3

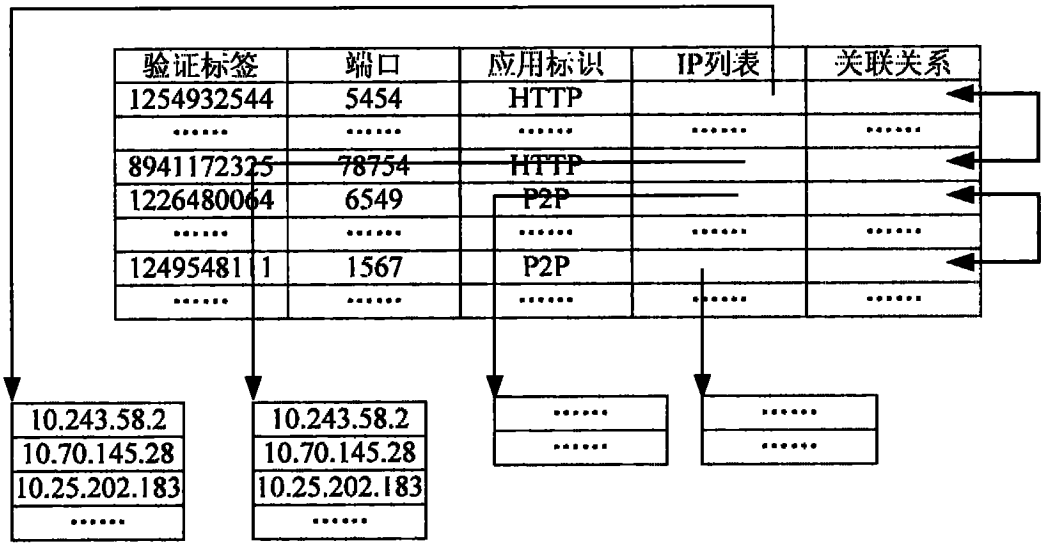

验证标签
端口
应用标识
IP列表
关联关系
1254932544
5454
HTTP
8941172325
78754
HTTP
1226480064
6549
P2P
12495481[illegible]1
1567
P2P
10.243.58.2
10.70.145.28
10.25.202.183
10.243.58.2
10.70.145.28
10.25.202.183

图 4

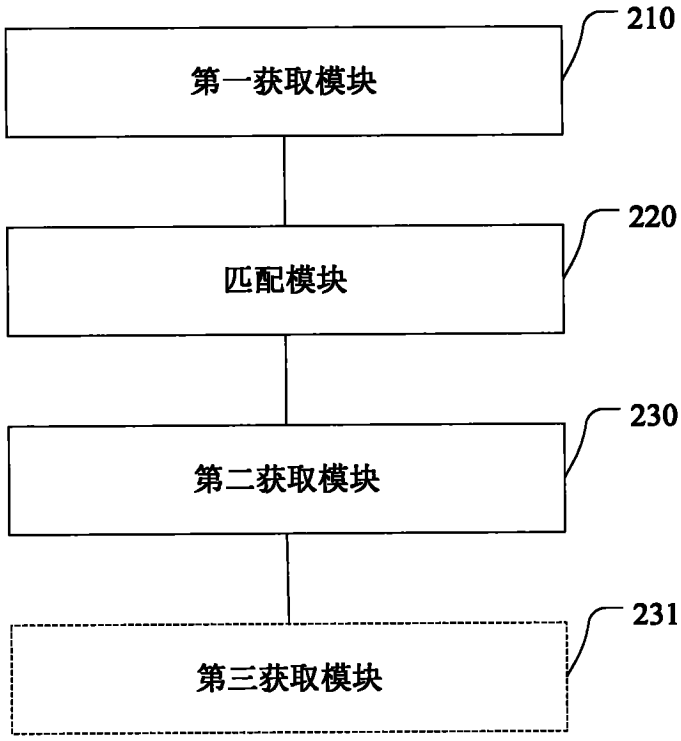

第一获取模块
210
匹配模块
220
第二获取模块
230
第三获取模块
231

图 5

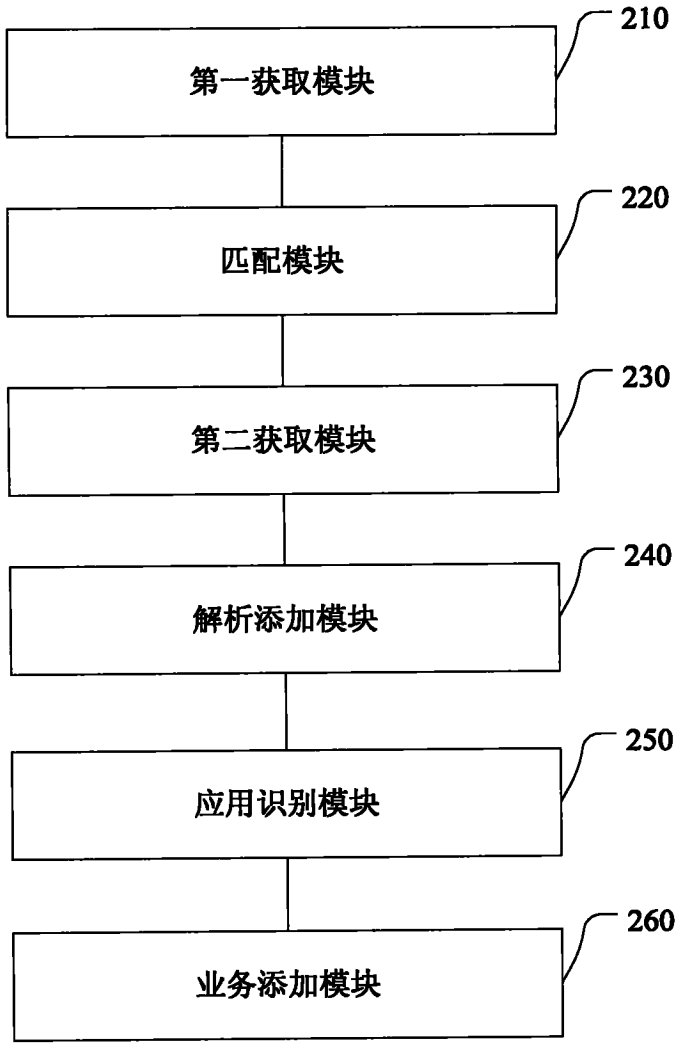

210
第一获取模块
220
匹配模块
230
第二获取模块
240
解析添加模块
250
应用识别模块
260
业务添加模块

图 6

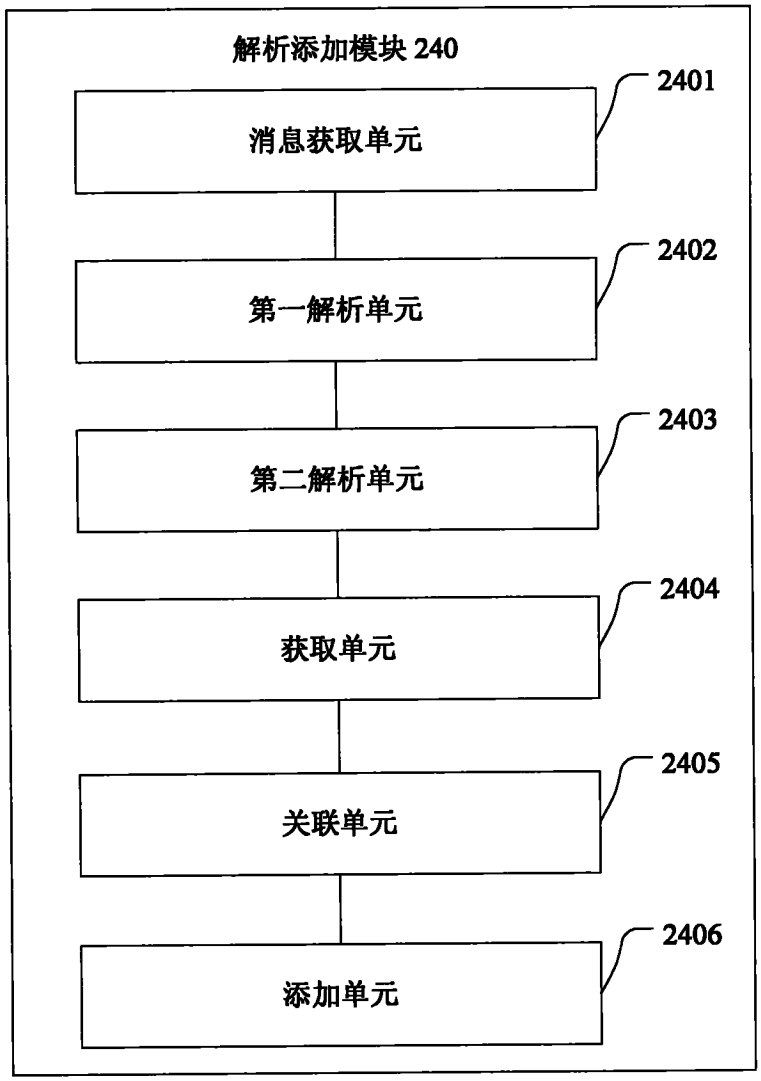

解析添加模块 240
2401
消息获取单元
2402
第一解析单元
2403
第二解析单元
2404
获取单元
2405
关联单元
2406
添加单元

图 7

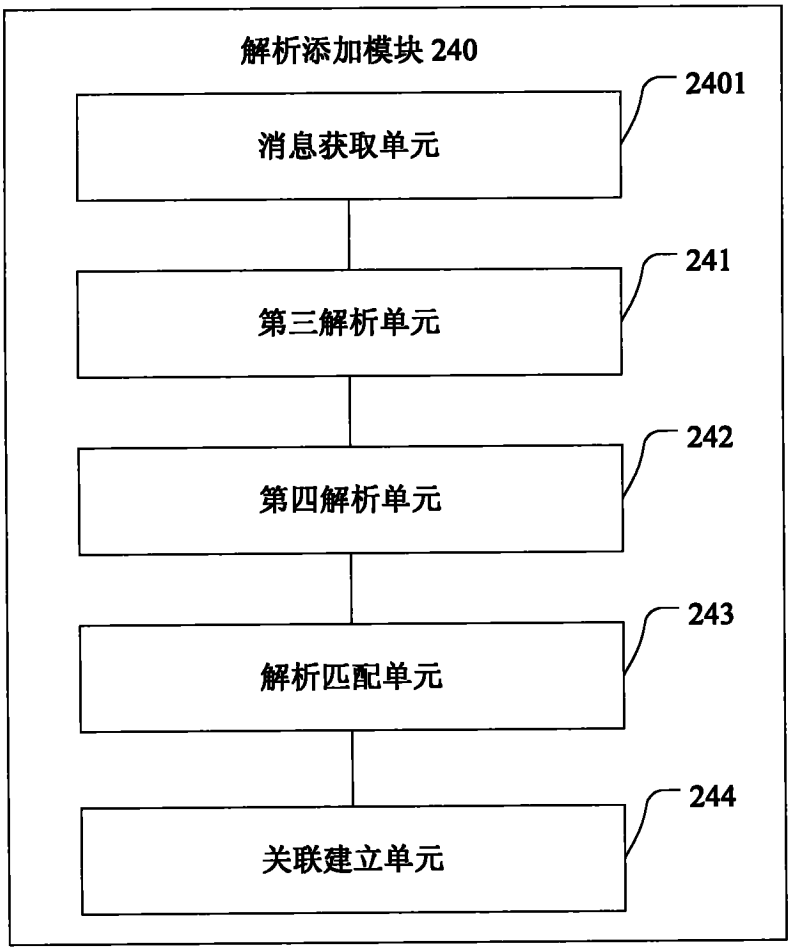

解析添加模块 240
2401
消息获取单元
241
第三解析单元
242
第四解析单元
243
解析匹配单元
244
关联建立单元

图 8

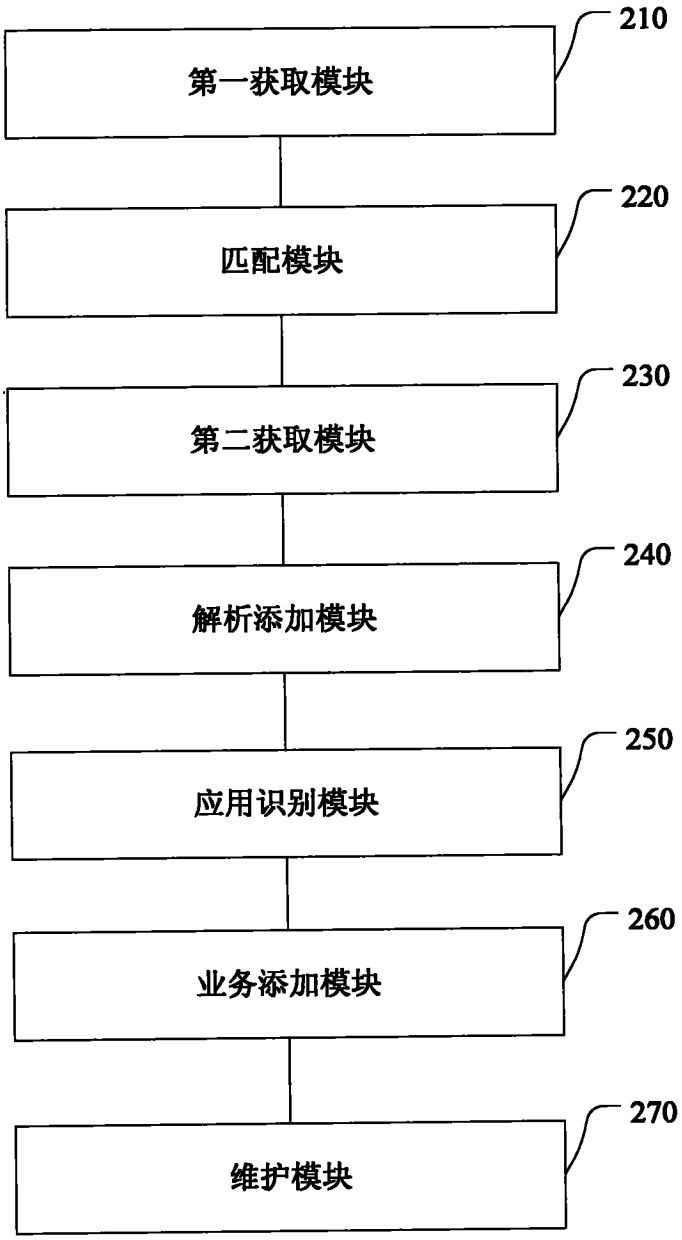

210
第一获取模块
220
匹配模块
230
第二获取模块
240
解析添加模块
250
应用识别模块
260
业务添加模块
270
维护模块

图 9

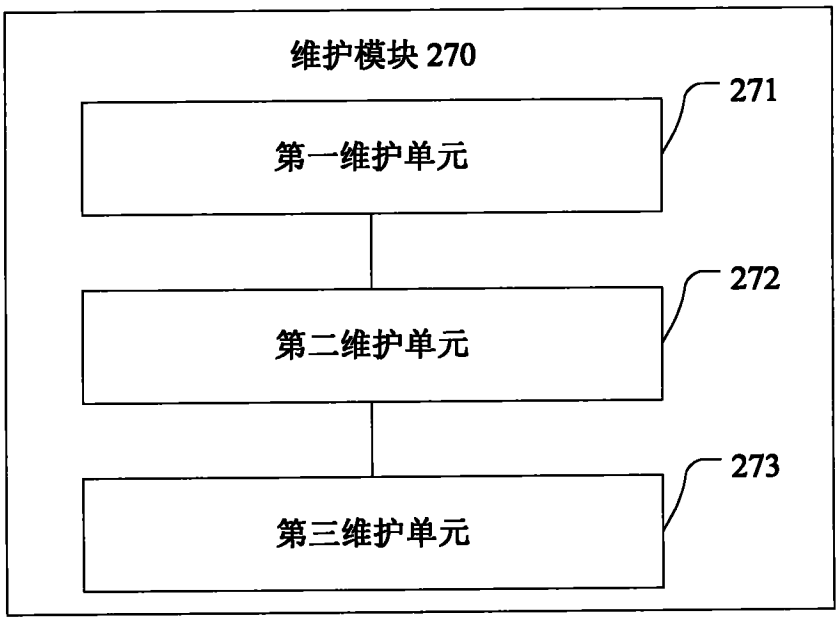


图 10

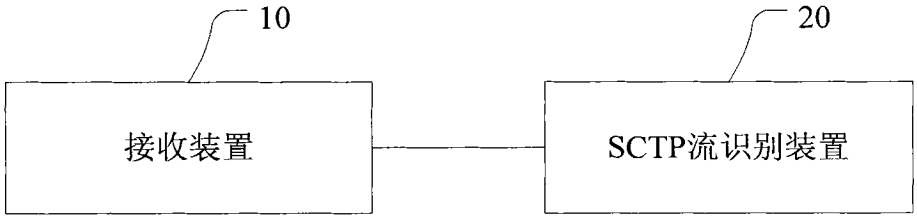


图 11

源端到目的端验证标签	源端口	应用标识	源IP列表	目的端到源端验证标签	目的端口	目的IP列表
1254932544	5454	HTTP		8941172325	78754	
……	……	……	……	……	……	……
1226480064	6549	HTTP		1249548111	1567	
……	……	P2P		……	……	
……	……	……	……	……	……	……
		P2P				
……	……	……	……	……	……	……

图 12

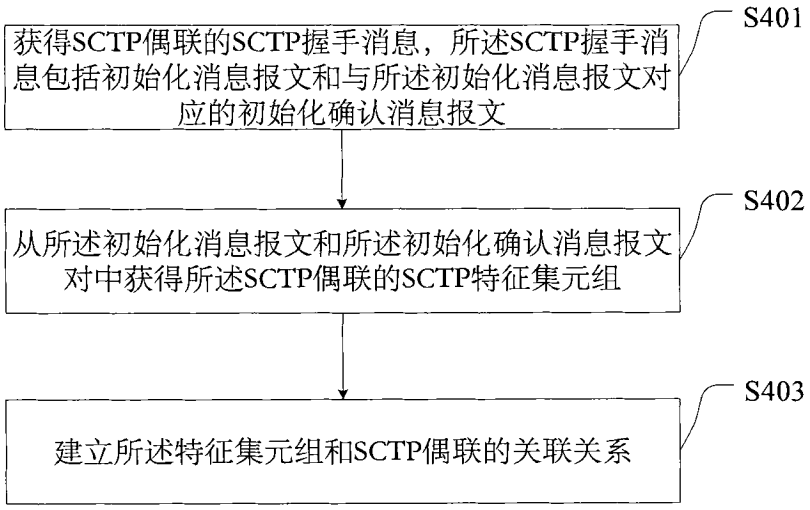

S401
获得SCTP偶联的SCTP握手消息，所述SCTP握手消息包括初始化消息报文和与所述初始化消息报文对应的初始化确认消息报文
S402
从所述初始化消息报文和所述初始化确认消息报文对中获得所述SCTP偶联的SCTP特征集元组
S403
建立所述特征集元组和SCTP偶联的关联关系

图 13