(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114915650 B
(45)授权公告日 2023.08.08

(21)申请号 202210430295.0

(22)申请日 2022.04.22

(65)同一申请的已公布的文献号
申请公布号 CN 114915650 A

(43)申请公布日 2022.08.16

(73)专利权人 国家计算机网络与信息安全管理中心
地址 100029 北京市朝阳区裕民路甲3号

(72)发明人 刘发强 揭真 石瑾 孙旭东 刘睿霖 李钊 段冬梅 杜梅婕

(74)专利代理机构 北京君尚知识产权代理有限公司 11200
专利代理师 李文涛

(51)Int.Cl.
H04L 67/14(2022.01)
H04L 65/1104(2022.01)
H04L 65/65(2022.01)

(56)对比文件
CN 101056283 A,2007.10.17
CN 101116296 A,2008.01.30
CN 102299962 A,2011.12.28
CN 102804744 A,2012.11.28
CN 105991856 A,2016.10.05
CN 107070741 A,2017.08.18
CN 110798379 A,2020.02.14
CN 111541645 A,2020.08.14
EP 3582467 A1,2019.12.18
US 2007030841 A1,2007.02.08
US 2010284288 A1,2010.11.11
“Security Status of VoIP Based on the Observation of Real-World Attacks on a Honeynet”.《2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing》.2012,全文.

审查员 张琳

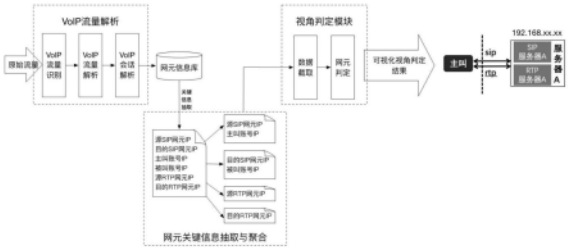
权利要求书2页 说明书5页 附图3页

(54)发明名称

基于网元信息聚合的VoIP服务观测视角的判定方法及系统

(57)摘要

本发明公开一种基于网元信息聚合的VoIP服务观测视角的判定方法及系统,涉及互联网语音传输服务领域,通过在单一观测点下对被动流量中VoIP网元信息进行聚合分析,进而判断其服务观测位置,可在全局观测点下提供各VoIP服务网元的相关信息,并为全局VoIP会话链路还原提供有效参考。



CN 114915650 B

1.一种基于网元信息聚合的VoIP服务观测视角的判定方法,其特征在于,包括以下步骤:

从流量观测点捕获VoIP流量,经过识别和解析,得到VoIP会话日志,对日志中的会话信息进行解析,建立VoIP网元信息库;

从VoIP网元信息库中抽取源SIP、目的SIP、源RTP和目的RTP这四类关键信息,其中源SIP包括源SIP网元IP和主叫账号IP,目的SIP包括目的SIP网元IP和被叫账号IP,源RTP包括源RTP网元IP,目的RTP包括目的RTP网元IP,对该四类关键信息进行聚合;

对聚合数据进行截取,截取的数据包含会话数据,设置一定数目的会话数据作为一个批次并进行一次判断,根据该截取的数据与该批次的倍数关系判断是否给出观测视角结果以及多少个观测视角结果;

对于给出了观测视角结果的情况,对整数倍部分的每个批次的数据进行以下处理:将数据中的源SIP网元IP、主叫账号IP、源RTP网元IP构成源IP集合,根据该源IP集合中的各个IP在上述截取数据中的占比,判断为源不定或源固定;将数据中的目的SIP网元IP、被叫账号IP、目的RTP网元IP构成目的IP集合,根据该目的IP集合中的各个IP在上述截取数据中的占比,判断为目的不定或目的固定;根据上述判断结果,记录SIP侧与RTP侧固定的网元IP信息;

比较记录的SIP侧与RTP侧固定的网元IP信息是否一致,如果一致,则判定该SIP侧与RTP侧共用一个服务器网元。

2.如权利要求1所述的方法,其特征在于,判断为源不定或源固定时,以占比50%为判断标准;如果源IP集合中,没有在截取数据中占比超过50%的单个IP,则判定为源不定,否则判定为源固定。

3.如权利要求1所述的方法,其特征在于,判断为目的不定或目的固定时,以占比50%为判断标准;如果目的IP集合中,没有在截取数据中占比超过50%的单个IP,则判定为目的不定,否则判定为目的固定。

4.如权利要求1所述的方法,其特征在于,根据截取的数据与批次的倍数关系判断是否给出观测视角结果以及多少个观测视角结果,具备包括以下几种情况:

设定n条会话数据为一个批次并判断一次,输出一个观测视角结果,则:

如果截取的数据为n的整数倍x时,给出x个观测视角结果;

如果截取的数据大于n但不足n的整数倍x时,给出(x-1)个观测视角结果;

如果截取的数据不足n时,不给出观测视角结果。

5.如权利要求1所述的方法,其特征在于,判断为源不定或源固定、目的不定或源目的固定的情况包括9种:

SIP侧源不定,目的固定;RTP侧源不定,目的固定;

SIP侧源固定,目的固定;RTP侧源固定,目的固定;

SIP侧源固定,目的不定;RTP侧源固定,目的不定;

SIP侧源不定,目的固定;RTP侧源固定,目的固定;

SIP侧源固定,目的固定;RTP侧源固定,目的不定;

SIP侧源固定,目的固定;RTP侧源不定,目的固定;

SIP侧源固定,目的不定;RTP侧源固定,目的固定;

SIP侧源不定,目的固定;RTP侧源固定,目的不定;

SIP侧源固定,目的不定;RTP侧源不定,目的固定。

6.一种基于网元信息聚合的VoIP服务观测视角的判定系统,其特征在于,包括:

VoIP流量解析模块,用于从流量观测点捕获VoIP流量,经过识别和解析,得到VoIP会话日志,对日志中的会话信息进行解析;

网元信息库存储模块,用于接收VoIP流量解析模块输出的数据,存储VoIP网元信息库;

数据聚合模块,用于从VoIP网元信息库中抽取源SIP、目的SIP、源RTP和目的RTP这四类关键信息,其中源SIP包括源SIP网元IP和主叫账号IP,目的SIP包括目的SIP网元IP和被叫账号IP,源RTP包括源RTP网元IP,目的RTP包括目的RTP网元IP,对该四类关键信息进行聚合;

视角判定模块,用于对聚合数据进行截取,截取数据包含若干条会话数据,根据该截取数据判断观测视角;由聚合数据中的源SIP网元IP、主叫账号IP、源RTP网元IP构成源IP集合,根据该源IP集合中的各个IP在上述截取数据中的占比,判断为源不定或源固定;由聚合数据中的目的SIP网元IP、被叫账号IP、目的RTP网元IP构成目的IP集合,根据该目的IP集合中的各个IP在上述截取数据中的占比,判断为目的不定或目的固定;根据上述判断结果,记录SIP侧与RTP侧固定的网元IP信息;比较记录的SIP侧与RTP侧固定的网元IP信息是否一致,如果一致,则判定该SIP侧与RTP侧共用一个服务器网元。

基于网元信息聚合的VoIP服务观测视角的判定方法及系统

技术领域

[0001] 本发明涉及互联网语音传输服务领域,具体涉及一种基于网元信息聚合的VoIP服务观测视角的判定方法。

背景技术

[0002] VoIP(Voice over Internet Protocol)是指在互联网上提供传输语音服务的技术。VoIP最基本的功能是提供基于Intemet、费用低廉的语音和传真服务。它还可以进一步扩展到基于IP的语音服务。因此VoIP就是一种提供IP电话业务和一些以此为基础的增值业务的技术。

[0003] 为了对VoIP流量进行测绘等深度分析,首先需对VoIP会话进行还原,而VoIP协议的控制信令与媒体数据是分离的,要从旁路还原出完整的VoIP会话信息,就必须将其控制信令和媒体数据关联起来。为了达到信令与数据关联的目的,需明确VoIP服务流量的观测位置,以便将同一个会话的上下游网元关联,从而进一步关联同一个会话的控制信令与媒体数据。与此同时,VoIP服务存在代理及多层转发的情况,这增加了确定流量中VoIP服务观测位置的困难性。

[0004] 确定VoIP服务的观测位置是指明确流量观测点所连接的承载VoIP服务的网元之间的路由信息和网元所提供的服务类型。单一观测点是指在完整的VoIP会话闭环中只有一个流量观测点,即该观测点下不包含该会话中的全局网元信息。一个完整的VoIP会话简化模型如图1所示,主叫网元与被叫网元之间有一个或多个SIP、RTP服务器网元,其中SIP服务器转发信令消息,RTP服务器转发媒体数据,且存在同一个服务器同时提供SIP和RTP服务的情况。由于实际应用中的互联网十分复杂,即使流量观测点位置不变,该点下也存在多层关联或无关联的VoIP服务网络,即该单一观测点下可能存在多个关联或无关联的图1所示VoIP通话网络。而在不同的VoIP通话网络中,该点可能位于不同提供不同服务的网元之间,即该单一观测点下的不同VoIP网络中观测视角可能不同。目前业界是在获取全局流量的前提下针对物理层和网络层判定网元之间的拓扑连接关系,但都未涉及单一观测点下VoIP服务观测视角的判定问题,而在实际应用场景中,很难获取完整VoIP会话闭环的全局流量,因此本发明提出的方法具有很强的现实意义。

[0005] 已有方法是在获取完备的全局流量的前提下针对物理层和网络层判定网元之间的拓扑连接关系,而不能解决单一观测点下VoIP服务观测视角的判定问题。与已有方法中涉及的网络层和物理层协议相比,VoIP网络在协议消息的格式和网元实体的鉴别方法上均不同,且VoIP网络中的网元之间存在逻辑连接关系,这与物理层和网络层的连接关系不同,其中VoIP网络的信令消息在网元实体之间的传递路径与物理层和网络层不在一个层次,原有的物理层和网络层路由不能表示。因此,已有的方法不能应用到VoIP网络中。

发明内容

[0006] 本发明的目的是提供一种基于网元信息聚合的VoIP服务观测视角的判定方法及

系统，通过在单一观测点下对被动流量中VoIP网元信息进行聚合分析，进而判断其服务观测位置，可在全局观测点下提供各VoIP服务网元的相关信息，并为全局VoIP会话链路还原提供有效参考。

[0007] 为实现上述目的，本发明采用以下技术方案：

[0008] 一种基于网元信息聚合的VoIP服务观测视角的判定方法，包括以下步骤：

[0009] 从流量观测点捕获VoIP流量，经过识别和解析，得到VoIP会话日志，对日志中的会话信息进行解析，建立VoIP网元信息库；

[0010] 从VoIP网元信息库中抽取源SIP、目的SIP、源RTP和目的RTP这四类关键信息，其中源SIP包括源SIP网元IP和主叫账号IP，目的SIP包括目的SIP网元IP和被叫账号IP，源RTP包括源RTP网元IP，目的RTP包括目的RTP网元IP，对该四类关键信息进行聚合；

[0011] 对聚合数据进行截取，截取的数据包含会话数据，设置一定数目的会话数据作为一个批次并进行一次判断，根据该截取的数据与该批次的倍数关系判断是否给出观测视角结果以及多少个观测视角结果；

[0012] 对于给出了观测视角结果的情况，对整数倍部分的每个批次的数据进行以下处理：将数据中的源SIP网元IP、主叫账号IP、源RTP网元IP构成源IP集合，根据该源IP集合中的各个IP在上述截取数据中的占比，判断为源不定或源固定；将数据中的目的SIP网元IP、被叫账号IP、目的RTP网元IP构成目的IP集合，根据该目的IP集合中的各个IP在上述截取数据中的占比，判断为目的不定或目的固定；根据上述判断结果，记录SIP侧与RTP侧固定的网元IP信息；

[0013] 比较记录的SIP侧与RTP侧固定的网元IP信息是否一致，如果一致，则判定该SIP侧与RTP侧共用一个服务器网元。

[0014] 进一步地，判断为源不定或源固定时，以占比50％为判断标准；如果源IP集合中，没有在截取数据中占比超过50％的单个IP，则判定为源不定，否则判定为源固定。

[0015] 进一步地，判断为目的不定或目的固定时，以占比50％为判断标准；如果目的IP集合中，没有在截取数据中占比超过50％的单个IP，则判定为目的不定，否则判定为目的固定。

[0016] 进一步地，根据截取的数据与批次的倍数关系判断是否给出观测视角结果以及多少个观测视角结果，具备包括以下几种情况：

[0017] 设定n条会话数据为一个批次并判断一次，输出一个观测视角结果，则：

[0018] 如果截取的数据为n的整数倍x时，给出x个观测视角结果；

[0019] 如果截取的数据大于n但不足n的整数倍x时，给出(x-1)个观测视角结果；

[0020] 如果截取的数据不足n时，不给出观测视角结果。

[0021] 进一步地，判断为源不定或源固定、目的不定或源目的固定的情况包括9种：

[0022] SIP侧源不定，目的固定；RTP侧源不定，目的固定；

[0023] SIP侧源固定，目的固定；RTP侧源固定，目的固定；

[0024] SIP侧源固定，目的不定；RTP侧源固定，目的不定；

[0025] SIP侧源不定，目的固定；RTP侧源固定，目的固定；

[0026] SIP侧源固定，目的固定；RTP侧源固定，目的不定；

[0027] SIP侧源固定，目的固定；RTP侧源不定，目的固定；

[0028] SIP侧源固定,目的不定;RTP侧源固定,目的固定;

[0029] SIP侧源不定,目的固定;RTP侧源固定,目的不定;

[0030] SIP侧源固定,目的不定;RTP侧源不定,目的固定。

[0031] 一种基于网元信息聚合的VoIP服务观测视角的判定系统,包括:

[0032] VoIP流量解析模块,用于从流量观测点捕获VoIP流量,经过识别和解析,得到VoIP会话日志,对日志中的会话信息进行解析;

[0033] 网元信息库存储模块,用于接收VoIP流量解析模块输出的数据,存储VoIP网元信息库;

[0034] 数据聚合模块,用于从VoIP网元信息库中抽取源SIP、目的SIP、源RTP和目的RTP这四类关键信息,其中源SIP包括源SIP网元IP和主叫账号IP,目的SIP包括目的SIP网元IP和被叫账号IP,源RTP包括源RTP网元IP,目的RTP包括目的RTP网元IP,对该四类关键信息进行聚合;

[0035] 视角判定模块,用于对聚合数据进行截取,截取数据包含若干条会话数据,根据该截取数据判断观测视角;由聚合数据中的源SIP网元IP、主叫账号IP、源RTP网元IP构成源IP集合,根据该源IP集合中的各个IP在上述截取数据中的占比,判断为源不定或源固定;由聚合数据中的目的SIP网元IP、被叫账号IP、目的RTP网元IP构成目的IP集合,根据该目的IP集合中的各个IP在上述截取数据中的占比,判断为目的不定或目的固定;根据上述判断结果,记录SIP侧与RTP侧固定的网元IP信息;比较记录的SIP侧与RTP侧固定的网元IP信息是否一致,如果一致,则判定该SIP侧与RTP侧共用一个服务器网元。

[0036] 较之于现有技术,本发明在没有全局VoIP会话流量的情况下,对单一观测点下的VoIP服务流量中的网元信息进行聚合分析,定义了若干有效的网元关键信息要素及各要素之间的关联关系,包括所在观测点关联网元提供的服务信息、收发数据的链路方向、VoIP服务属性、可能的拓扑关系等,从而给出与观测点相关网元的上下游链路、拓扑关系和所提供的服务类型等信息;并可据此还原观测位置两侧的网元信息和链路方向等信息,即可将一个会话的上下游网元关联,从而可进一步关联同一个会话的控制信令与媒体数据,实现对VoIP会话进行还原、对VoIP资源进行测绘等深度分析,最终实现对VoIP服务的规范化管理,达到打击私搭乱建、恶意服务滋生等监管目的。

附图说明

[0037] 图1是完整VoIP通话路径示意图。

[0038] 图2是本发明实施例中的一种VoIP服务观测视角的判定流程图。

[0039] 图3是本发明实施例中的VoIP服务9种观测视角示意图。

[0040] 图4是本发明实例中对可能的拓扑关系举例的示意图。

具体实施方式

[0041] 为使本发明的上述特征和优点能更明显易懂,下文特举实施例,并配合所附图作详细说明如下。

[0042] 本实施例提供一种基于网元信息聚合的VoIP服务观测视角的判定方法,如图2所示,包括以下步骤:

[0043] 步骤1:先对流量观测点捕获的原始流量中的VoIP流量进行识别与解析,可得到VoIP会话日志,对日志中的会话信息进一步解析,可建立丰富的VoIP网元信息库;

[0044] 步骤2:从中可对网元的关键信息进行抽取,并以源SIP(源SIP网元IP和主叫账号IP)、目的SIP(目的SIP网元IP和被叫账号IP)、源RTP(源RTP网元IP)、目的RTP(目的RTP网元IP)四类对关键信息聚合;

[0045] 步骤3:将聚合后的数据作为输入传给视角判定模块,最后直接由该模块输出视角判定的可视化结果。视角判定模块的逻辑如下:

[0046] (1)设定数据截取的范围:可设每n=50条会话数据作为一个批次并判定一次,输出一个可能的观测视角结果;

[0047] 如果截取数据为n的整数倍x时,给出x个观测视角结果;

[0048] 如果截取数据大于n但不足n的整数倍x时,给出(x-1)个观测视角结果;

[0049] 如果截取数据不足n时,不给出观测视角结果。

[0050] 数据截取的范围和n值应依据当时网络的复杂程度灵活选择。在简单网络中,网元数量较少,截取较少的数据也能得到较可靠的结果;在复杂网络中,网元数量较多,需截取更多的数据才能得到可靠的结果。

[0051] 总体原则是:一定时间内所截取的会话数越多,则判定的可靠性增加;截取的会话数确定时,n的值越接近所截取的全部会话数据则判定的可靠性增加;n相对所截取的全部会话数据量越小,则判定的可靠性降低,但可得到多个可能的结果进行辅助判断。

[0052] 本方法不采纳以会话数据产生的时间段为数据截取范围的方法,理由是:若截取某时间段的会话,时间区间过大会使判定的精度不够,因为在海量数据下足够宽的时间区间内,各IP的百分比可能都比较均匀,一般不会有单个IP超过50%;同时VoIP通话活跃时间跨度波动大(有的网元节点一天会话数据达到千条,有的网元节点一个月数据达到千条),难以衡量如何截取时间范围。

[0053] (2)判定SIP/RTP侧源或目的网元是否固定:

[0054] 对于步骤(1)中给出了观测视角结果的情况,将整数倍部分的每个批次的数据分别进行以下处理。该整数倍部分的每个批次的含义是,如果截取的数据大于n但不足n的整数倍x时,则对(x-1)个批次进行判断,比如截取的数据为120条,而设定的每个批次的会话数据量为50条,则截取的数据显然是每个批次的2.4倍,则只对2倍部分的批次(即两个50条会话数据的批次)进行处理,不对非整数部分的批次(即剩下的20条部分的非完整批次)进行处理。处理过程如下:

[0055] 源网元是否固定:如果聚合后的源IP集合各数据分布均匀,数据截取的范围内的数据没有占比超过50%的单个IP的情况,则定义该情况为“源不定”;如果数据聚合模块聚合后的源IP集合各数据分布不均匀,数据截取的范围内的有某IP占比超过50%的情况,则定义该情况为“源固定”。

[0056] 目的网元是否固定:如果数据聚合模块聚合后的目的IP集合各数据分布均匀,数据截取的范围内的没有占比超过50%的单个IP的情况,则定义该情况为“目的不定”;如果数据聚合模块聚合后的目的IP集合各数据分布不均匀,数据截取的范围内的有某IP占比超过50%的情况,则定义该情况为“目的固定”。

[0057] 基于前述的视角判定逻辑,在单一流量观测点下的VoIP服务不外乎以下9种观测

视角结果(如图3所示)：

[0058] 视角①:SIP侧源不定,目的固定;RTP侧源不定,目的固定。

[0059] 视角②:SIP侧源固定,目的固定;RTP侧源固定,目的固定。

[0060] 视角③:SIP侧源固定,目的不定;RTP侧源固定,目的不定。

[0061] 视角④:SIP侧源不定,目的固定;RTP侧源固定,目的固定。

[0062] 视角⑤:SIP侧源固定,目的固定;RTP侧源固定,目的不定。

[0063] 视角⑥:SIP侧源固定,目的固定;RTP侧源不定,目的固定。

[0064] 视角⑦:SIP侧源固定,目的不定;RTP侧源固定,目的固定。

[0065] 视角⑧:SIP侧源不定,目的固定;RTP侧源固定,目的不定。

[0066] 视角⑨:SIP侧源固定,目的不定;RTP侧源不定,目的固定。

[0067] 根据上述的判断结果,分别记录SIP侧与RTP侧固定的网元IP信息。

[0068] (3)找出网元固定的某侧进行比较,若该侧SIP与RTP网元信息一致,则判定该侧SIP/RTP共用一个服务器网元。

[0069] 本发明在没有全局VoIP会话流量的情况下,对单一观测点下的VoIP服务流量中的网元信息进行聚合分析,定义了若干有效的网元关键信息要素及各要素之间的关联关系,包括所在观测点关联网元提供的服务信息(SIP服务或RTP服务)、收发数据的链路方向(源SIP/RTP为发送数据侧、目的SIP/RTP为接受数据侧)、VoIP服务属性(VoIP服务是服务器类型或移动端类型,图3中两端的“主叫”和“被叫”在本方法中默认为移动端类型)、可能的拓扑关系(例如图4所示,根据本方法判定虚线为观测视角,结合聚合的6种网元服务信息和链路方向,可得到两种拓扑关系。拓扑①为两台服务器之间通信,且源、目的两侧的SIP服务与RTP服务均共用一台服务器;拓扑②为三台服务器之间通信,且源SIP服务与RTP服务共用一台服务器,目的SIP服务与RTP服务不共用)等,从而给出与观测点相关网元的上下游链路、拓扑关系和所提供的服务类型等信息;并可据此还原观测位置两侧的网元信息和链路方向等信息,即可将一个会话的上下游网元关联,从而可进一步关联同一个会话的控制信令与媒体数据,实现对VoIP会话进行还原、对VoIP资源进行测绘等深度分析,最终实现对VoIP服务的规范化管理,达到打击私搭乱建、恶意服务滋生等监管目的。

[0070] 虽然本发明已以实施例公开如上,然其并非用以限定本发明,本领域的普通技术人员对本发明的技术方案进行的适当修改或者等同替换,均应涵盖于本发明的保护范围内,本发明的保护范围以权利要求所限定者为准。

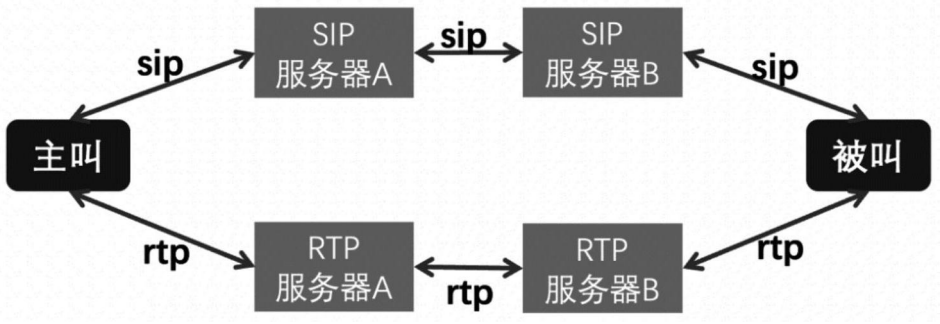

SIP
服务器A
sip
SIP
服务器B
sip
主叫
被叫
rtp
RTP
服务器A
rtp
RTP
服务器B
rtp

图1

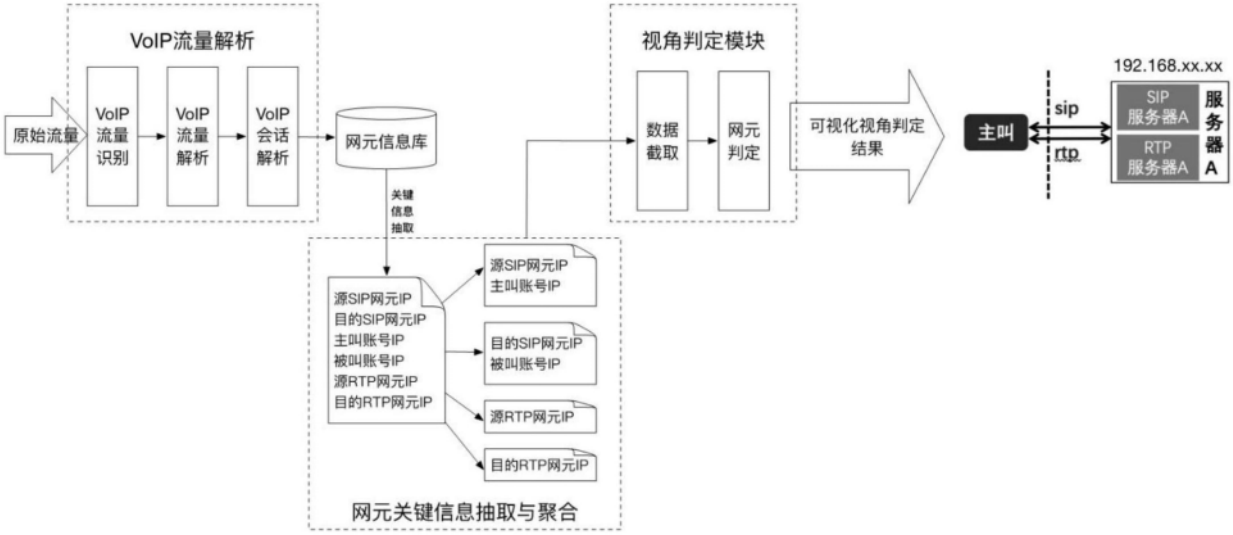

VoIP流量解析
原始流量
VoIP
流量
识别
VoIP
流量
解析
VoIP
会话
解析
网元信息库
关键
信息
抽取
源SIP网元IP
目的SIP网元IP
主叫账号IP
被叫账号IP
源RTP网元IP
目的RTP网元IP
源SIP网元IP
主叫账号IP
目的SIP网元IP
被叫账号IP
源RTP网元IP
目的RTP网元IP
网元关键信息抽取与聚合
视角判定模块
数据
截取
网元
判定
可视化视角判定
结果
主叫
sip
rtp
192.168.xx.xx
SIP
服务器A
RTP
服务器A
服务器A

图2

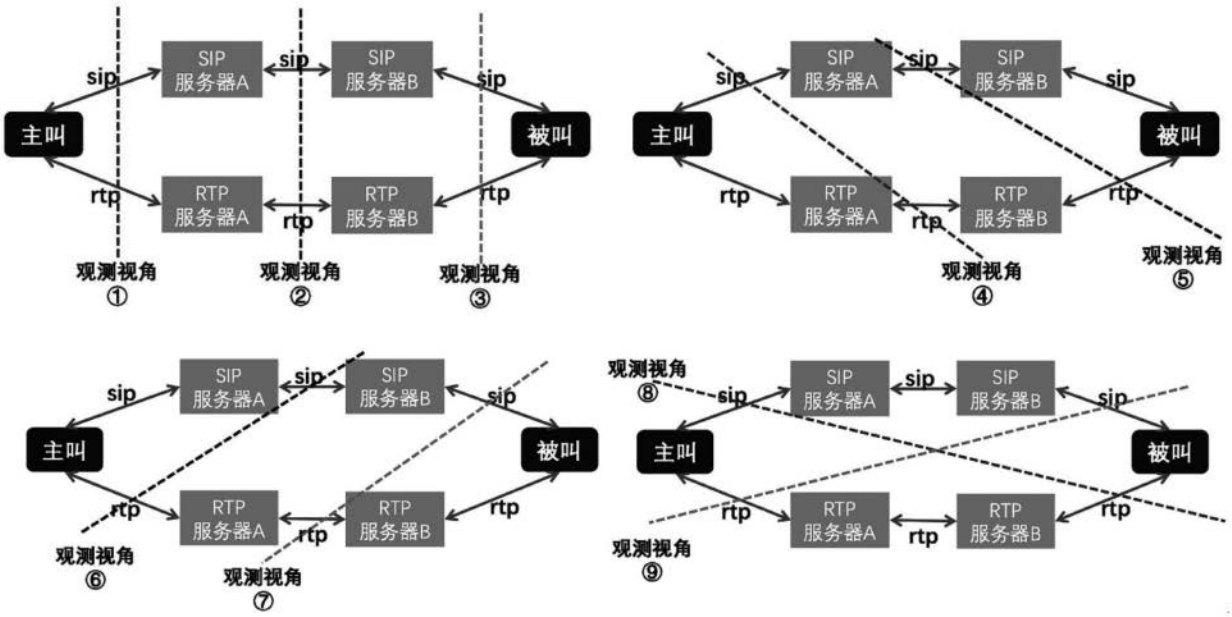

SIP
服务器A
SIP
服务器B
主叫
被叫
RTP
服务器A
RTP
服务器B
sip
rtp
观测视角
①
观测视角
②
观测视角
③
观测视角
④
观测视角
⑤
观测视角
⑥
观测视角
⑦
观测视角
⑧
观测视角
⑨

图3

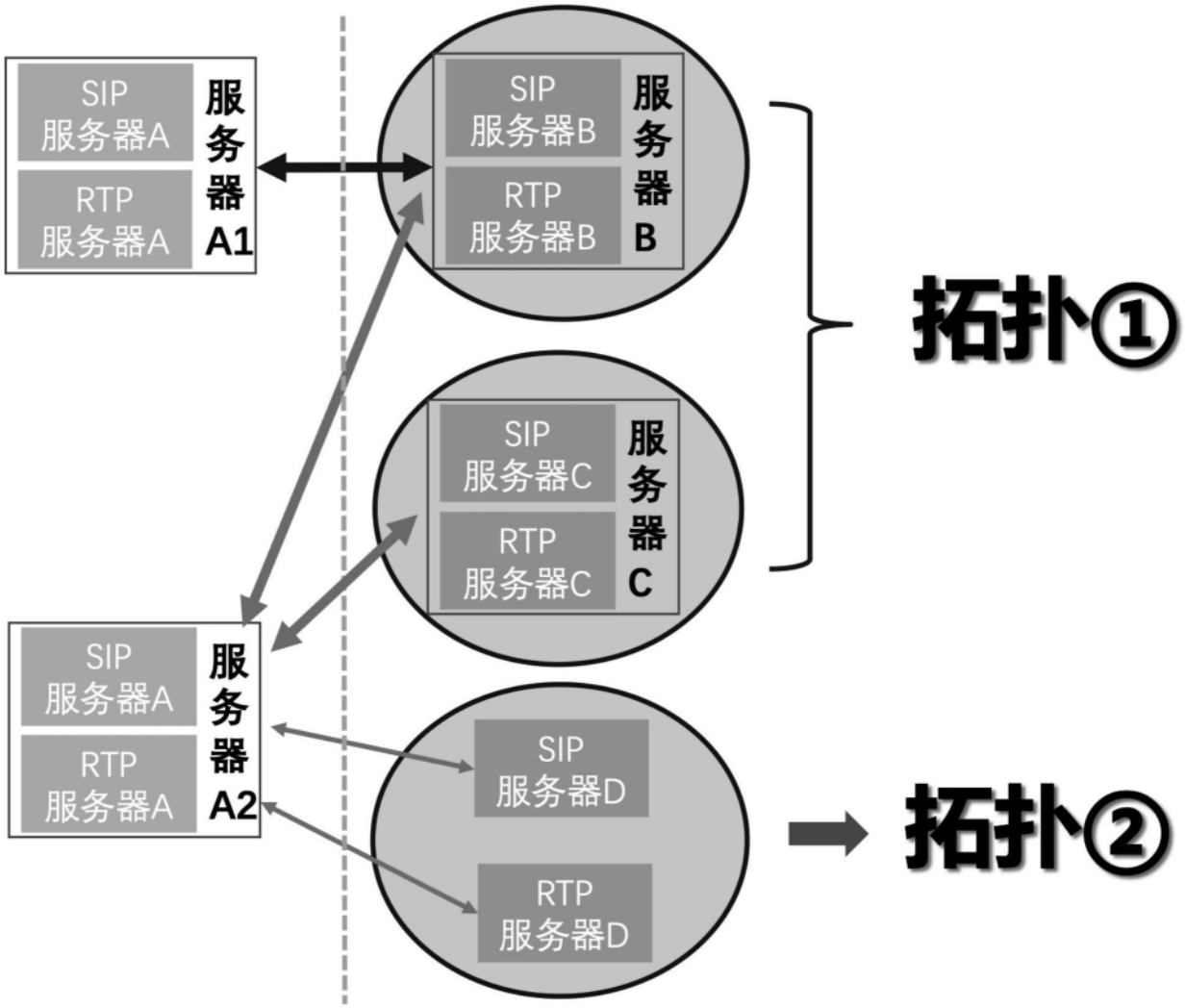

SIP
服务器A
RTP
服务器A
服务器A1
SIP
服务器B
RTP
服务器B
服务器B
SIP
服务器C
RTP
服务器C
服务器C
拓扑①
SIP
服务器A
RTP
服务器A
服务器A2
SIP
服务器D
RTP
服务器D
拓扑②

图4