(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 104168259 B
(45)授权公告日 2018.12.04

(21)申请号 201410160531.7

(22)申请日 2014.04.21

(65)同一申请的已公布的文献号
申请公布号 CN 104168259 A

(43)申请公布日 2014.11.26

(30)优先权数据
61/813,990 2013.04.19 US
14/254,465 2014.04.16 US

(73)专利权人 极进网络公司
地址 美国加利福尼亚

(72)发明人 H·V·曼迪拉塔 S·A·巴克 A·瓦克欧 S·R·杜尔尼 R·S·沃莱克 W·G·巴赫尔

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 冯玉清

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 101610487 A,2009.12.23,
CN 101449530 A,2009.06.03,
CN 101589607 A,2009.11.25,
CN 1549649 A,2004.11.24,
CN 1929633 A,2007.03.14,
US 6501754 B1,2002.12.31,
US 2008267081 A1,2008.10.30,

审查员 李珍珍

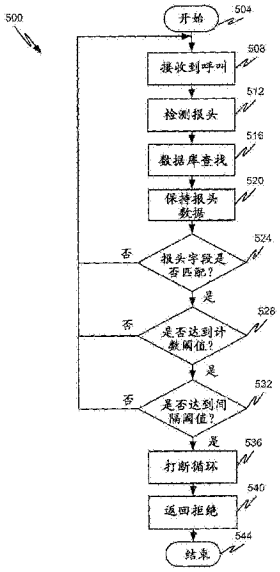
权利要求书2页 说明书9页 附图5页

(54)发明名称

会话管理器抗循环

(57)摘要

本公开涉及一种会话管理器抗循环，该会话管理器抗循环创建了作为针对循环的有效屏障的一个模型，其通过对于时间参数内的各个报头集合保持临时的各个单独的呼叫计数器而高效地识别出循环状况，并且在检测到循环状况时将其终止。所述系统为管理员提供了对应于循环检测计数和循环检测间隔的可调节参数，从而允许针对非刻意的和刻意的循环状况进行保护。



CN 104168259 B

1.一种用于针对会话发起协议SIP消息检测呼叫循环的方法,其包括:

通过微处理器保持对于通信服务器的循环计数阈值;

通过所述微处理器在通信服务器处接收第一SIP消息;

通过所述微处理器确定包含在第一SIP消息中的多个元素数值;

通过所述微处理器将包含在第一SIP消息中的所述多个元素数值与包括在先前在通信服务器处接收到的各条SIP消息中的历史元素数值进行比较;

基于比较步骤,通过所述微处理器确定包含在第一SIP消息中的所述多个元素数值与来自先前在通信服务器处接收到的SIP消息的多个元素数值相匹配,并且作为响应递增同样对于所述通信服务器所保持的循环计数数值,其中,所述微处理器对于包含在第一SIP消息中的所述多个元素数值的每一种独特组合保持临时的各个单独的循环计数数值;

通过所述微处理器确定循环计数数值已达到和超出循环计数阈值的至少其中一种情况;以及

响应于确定循环计数数值已达到和超出循环计数阈值的至少其中一种情况,通过所述微处理器确定已发生呼叫循环。

2.根据权利要求1所述的方法,其还包括:

通过所述微处理器在通信服务器处执行一项或多项功能以打断呼叫循环。

3.根据权利要求2所述的方法,其中,所述通信服务器通过拒绝第一SIP消息而打断呼叫循环。

4.根据权利要求2所述的方法,其中,所述通信服务器通过终止与第一SIP消息相关联的呼叫尝试而打断呼叫循环。

5.根据权利要求1所述的方法,其中包含在第一SIP消息中的所述多个元素数值对应于包含在第一SIP消息中的各个报头元素,其中在确定已发生呼叫循环之前需要第一SIP消息的每一个报头元素与先前在通信服务器处接收到的所述SIP消息的每一个报头元素相匹配。

6.根据权利要求1所述的方法,其还包括:

确定接收到第一SIP消息与先前在通信服务器处接收到的所述SIP消息之间的时间量;

将所确定的时间量与对于通信服务器保持的间隔阈值进行比较;以及

只有响应于确定所确定的时间量已达到和超出所述间隔阈值的至少其中一种情况,才确定已发生呼叫循环。

7.一种用于针对会话发起协议SIP消息检测呼叫循环的通信系统,其包括:

微处理器;和

与所述微处理器耦合并且包括微处理器可读和可执行指令的硬件计算机可读介质,所述微处理器可读和可执行指令对所述微处理器进行编程以执行:

保持对于通信服务器的循环计数阈值并且施行以下操作的SIP防火墙:

在通信服务器处接收第一SIP消息;

确定包含在第一SIP消息中的多个元素数值;

将包含在第一SIP消息中的所述多个元素数值与包括在先前在通信服务器处接收到的各条SIP消息中的历史元素数值进行比较;

基于比较步骤,确定包含在第一SIP消息中的所述多个元素数值与来自先前在通信服

务器处接收到的SIP消息的多个元素数值相匹配，并且作为响应递增同样由SIP防火墙对于所述通信服务器所保持的循环计数数值，其中，所述微处理器对于包含在第一SIP消息中的所述多个元素数值的每一种独特组合保持临时的各个单独的循环计数数值；

确定循环计数数值已达到和超出循环计数阈值的至少其中一种情况；

响应于确定循环计数数值已达到和超出循环计数阈值的至少其中一种情况，确定已发生呼叫循环；以及

在通信服务器处执行一项或多项功能以打断呼叫循环。

8.根据权利要求7所述的系统，其中，所述通信服务器通过拒绝第一SIP消息打断呼叫循环，并且其中所述通信服务器通过终止与第一SIP消息相关联的呼叫尝试打断呼叫循环。

9.根据权利要求7所述的系统，其中包含在第一SIP消息中的所述多个元素数值对应于包含在第一SIP消息中的各个报头元素，并且其中在确定已发生呼叫循环之前需要第一SIP消息的每一个报头元素与先前在通信服务器处接收到的所述SIP消息的每一个报头元素相匹配。

10.根据权利要求7所述的系统，其中，所述SIP防火墙还施行以下操作：

确定接收到第一SIP消息与先前在通信服务器处接收到的所述SIP消息之间的时间量；

将所确定的时间量与SIP防火墙对于通信服务器保持的间隔阈值进行比较；以及

只有响应于确定所确定的时间量已达到和超出所述间隔阈值的至少其中一种情况，才确定已发生呼叫循环。

会话管理器抗循环

[0001] 相关申请的交叉引用

[0002] 本申请要求Mendiratta等人2013年4月19日提交的序列号为61/813,990的美国临时申请的权益，通过该引用将其内容合并在此。

技术领域

[0003] 本公开内容总体上涉及企业通信，并且特别涉及用于识别及打断混合网络中的循环的方法。

背景技术

[0004] 在网络配置中，错误状况可能会导致严重问题。一种特别麻烦的错误状况被称作呼叫循环。呼叫循环的特征在于呼叫从未被连接也未被释放，从而会无限期地使用资源。呼叫循环可能由非刻意的配置问题导致，或者由旨在捣乱或者尝试损害网络的恶意人员刻意导致。经历一个或多个呼叫循环的网络可能产生性能问题，这是因为所述循环可能会一直占用资源。在没有足够资源可用的情况下，网络可能会变慢或者变得不可用。

[0005] 会话发起协议(SIP)是用在某些网络中的信令通信协议，其具有少数几项内建机制来打断所发生的呼叫循环。在包含全部具有SIP能力的元件的网络中，SIP可以在正创建请求的呼叫对话困在循环中时检测到并且打断循环。所述机制由用户代理(agent)客户端(UAC)把一个最大转发(Max-Forwards)报头(默认数值为70)插入在初始呼叫请求中。请求路径中的每一个SIP代理服务器(proxy)通常把Max-Forwards报头数值递减1。当Max-Forwards数值达到零时，所述请求被拒绝，并且呼叫循环被打断。作为一项可选的抗循环措施，SIP代理服务器还可以通过检察Via(经由)报头的内容来检查同一条请求是否重复。但是当在循环路径中存在背靠背用户代理(B2BUA)、协议互工作网关(IWG)和/或其他非SIP元件时，无法依赖于Max-Forwards和Via报头来检测循环，这是因为并非网络中的所有元件都是纯粹的SIP代理服务器。非SIP元件可能无法递减报头和/或检察报头的内容是否重复。当存在非SIP元件时，可能无法发现并打断呼叫循环，或者可能完全无法检测到呼叫循环。

发明内容

[0006] 通过本公开内容的各个方面、实施例和/或配置解决了前述和其他需求。本公开内容的实施例是针对一种识别及打断包括SIP和非SIP元件的混合网络中的呼叫循环的系统和方法。所述方法允许顾客调节包括定时器和计数器之类的参数以便精确地检测循环，从而在路由问题或攻击威胁到网络时保护网络资源。

[0007] 这里所使用的“呼叫循环”是来到代理服务器、被转发并且随后被递送回到相同的代理服务器的呼叫请求。当所述请求第二次到达时，被称作请求URI的SIP消息部分与该请求第一次被递送到该代理服务器时完全相同。所述代理服务器基于未发生改变的报头字段做出完全相同的处理决定。由于所述请求不断回到所述代理服务器并且呼叫从未被完整地处理、完成和/或终止，因此其变为呼叫循环。

[0008] 已循环或正在循环的呼叫请求被视为错误。在SIP网络中，通过以下情况辨识出呼叫循环：Max-Forwards计数递减到零，已经过去了到期时间，以及当服务器发现其自身处于所述请求的Via列表中时，其中包括分支参数。SIP呼叫循环可能对网络性能造成的负面影响包括代理服务器重启、呼叫失败、网络效率损失以及资源可用性降低，这是因为随着所述呼叫(或多个呼叫)被无限期地处理会消耗资源。SIP代理服务器的一个非限制性实例是Avaya Aura®会话管理器(SM)SIP防火墙(ASSET代理服务器特征)，其中通过两个新的字段而得到增强以便基于针对被称作INVITE(邀请)的SIP消息的管理来检测及打断呼叫循环的代理服务器。

[0009] 为管理员提供循环检测计数和循环检测间隔字段，从而提供针对呼叫循环的保护。在一个较短间隔内接收到的具有包括请求统一资源定位符(R-URI)、To(去往)、From(来自)和P-Asserted-Identiry(代理服务器声明身份)(PAI)报头字段的完全相同的报头集合的SIP INVITE请求被SIP防火墙检测到，并且被归类为已循环呼叫(PAI报头字段是可选的)。如果具有R-URI、To、From和PAI报头数值的相同组合的传入请求的数目在循环检测阈值间隔内达到循环检测阈值，则Avaya Aura®会话管理器(SM)可以拒绝所述INVITE请求。

[0010] 利用可调节的循环检测计数和循环检测间隔字段，可以针对非刻意和刻意的呼叫循环状况显著更好地保护包含SIP和非SIP元件的混合网络。

[0011] 通过本公开内容，前述和其他优点将会显而易见。

[0012] 在一些实施例中，提供一种方法，其总体上包括：

[0013] 保持对于通信服务器的循环计数阈值；

[0014] 在通信服务器处接收第一消息；

[0015] 确定包含在第一消息中的一个或多个元素数值；

[0016] 把包含在第一消息中的一个或多个元素数值与包括在先前在通信服务器处接收到的各条消息中的历史元素数值进行比较；

[0017] 基于所述比较步骤，确定包含在第一消息中的一个或多个元素数值与来自先前在通信服务器处接收到的一条消息的一个或多个元素数值相匹配，并且作为响应递增同样对于所述通信服务器所保持的循环计数数值；

[0018] 确定循环计数数值已达到和超出循环计数阈值的至少其中一种情况；

[0019] 响应于确定循环计数数值已达到和超出循环计数阈值的至少其中一种情况，确定已发生呼叫循环；以及

[0020] 在通信服务器处执行一项或多项功能以打断呼叫循环。

[0021] 这里使用的术语“自动”及其变型指的是任何处理或操作在其施行时是在没有任何实质性的人类输入的情况下而实现的。但是尽管某项处理或操作的施行使用了实质性或非实质性的人类输入，但是如果所述输入是在所述处理或操作的施行之前被接收的，则所述处理或操作仍可以是自动的。如果人类输入影响到所述处理或操作将被如何施行，则这样的输入被认为是实质性的。顺应所述处理或操作的施行的人类输入不被认为是“实质性的”。

[0022] 这里所使用的术语“计算机可读介质”指的是参与向处理器提供指令以供执行的任何存储和/或传输介质。这样的介质通常是有形且非瞬时性的，并且可以采取许多形式，其中包括而不限于非易失性介质、易失性介质和传输介质，并且包括而不限于随机存取存

储器(“RAM”)、只读存储器(“ROM”)等等。非易失性介质例如包括NVRAM或者磁盘或光盘。易失性介质包括例如主存储器之类的动态存储器。计算机可读介质的常见形式例如包括:软盘(其中包括而不限于Bernoulli卡盒、ZIP驱动器和JAZ驱动器),柔性盘,硬盘,磁带或卡带,或者任何其他磁介质,磁光介质,数字视频盘(例如CD-ROM),任何其他光学介质,打孔卡,纸带,任何其他具有孔洞模式的物理介质,RAM,PROM,以及EPROM,FLASH-EPROM,例如存储器卡之类的固态介质,任何其他存储器芯片或卡盒,后文中所描述的载波,或者可以由计算机从中进行读取的任何其他介质。电子邮件的数字文件附件或者其他整装式信息档案或档案集合被视为等效于有形存储介质的分发介质。当计算机可读介质被配置成数据库时,应当理解的是,所述数据库可以是任何类型的数据库,比如关系、分级、面向对象数据库等等。相应地,本公开内容被视为包括在其中存储本公开内容的软件实现方式的有形存储介质或分发介质以及现有技术认可的等效方案和后继介质。计算机可读存储介质通常排除瞬时性存储介质,特别是电、磁、电磁、光学、磁光信号。

[0023] 术语“用户”、“顾客”或“客户端”指代光顾联络中心和/或企业机构、由其服务或者以其他方式与之有业务往来的一方。

[0024] 短语“SIP用户代理(UA)”是被用来创建或接收SIP消息和管理SIP会话的逻辑网络端点。SIP UA可以施行发送SIP请求的用户代理客户端(UAC)以及接收请求并且返回SIP响应的用户代理服务器(UAS)的角色。

[0025] 这里所使用的“数据库”指的是保存在计算机中的有组织数据集合。对应于数据的组织架构或模型例如可以是分级、网络、关系、实体-关系、对象、文档、XML、实体-属性-数值模型、星型架构、对象-关系、关联、多维、多数值、语义和其他数据库设计。

[0026] 这里所使用的“确定”、“计算”等术语可互换使用,并且包括任何类型的方法、处理、数学运算或技术。

[0027] 这里所使用的术语“装置”应当根据35 U.S.C.第112节第6段给出其可能的最宽泛解释。相应地,合并有术语“装置”的权利要求应当涵盖这里所阐述的所有结构、材料或动作及其所有等效表述。此外,所述结构、材料或动作及其等效表述应当包括在发明内容部分、附图说明部分、具体实施方式部分、摘要和权利要求书本身当中所描述的全部所述结构、材料或动作及其等效表述。

[0028] 这里所使用的术语“模块”指代能够施行与该元件相关联的功能的任何已知的或后来开发的硬件、软件、固件、人工智能、模糊逻辑或者硬件与软件的组合。此外,虽然本公开内容是在示例性实施例方面给出的,但是应当认识到,本公开内容的各个单独方面可以被分别要求保护。

[0029] 前面给出了本公开内容的简化概要以便提供对于本公开内容的一些方面的理解。本概要不是关于本公开内容及其各个方面、实施例和/或配置的详尽或穷举性总览。本概要既不意图标识出本公开内容的关键性或决定性元素,也不意图界定本公开内容的范围,而是意图以简化形式给出本公开内容的一部分挑选出来的概念以作为针对后面给出的更加详细的描述的介绍。应当认识到,单独地或者组合地利用前面所阐述或者在后面详细描述的其中一项或多项特征,本公开内容的其他方面、实施例和/或配置也是可能的。

附图说明

[0030] 图1是根据本公开内容的实施例的通信系统的方块图；

[0031] 图2是根据本公开内容的实施例的SIP消息的一个实例；

[0032] 图3是根据本公开内容的实施例的呼叫循环的一个实例；

[0033] 图4是根据本公开内容的实施例的滑动窗口的一个实例；以及

[0034] 图5是根据本公开内容的实施例的对应于呼叫循环分析和终止的流程图。

具体实施方式

[0035] 图1是根据本公开内容的至少一些实施例的通信系统100的方块图。通信系统100被描绘成包括企业网络120，其经由通信网络104连接到一个或多个外部通信设备108。企业网络120的组件被描绘成包括：包含SIP防火墙128的通信服务器124，一个或多个通信设备108，企业网关112，以及企业数据库116。应当认识到，被描绘成处于企业网络120内部的其中一个或多个组件可以替换地或附加地被提供在企业网络120外部。

[0036] 根据本公开内容的至少一些实施例，通信网络104可以包括任何类型的已知通信介质或者通信介质的总集，并且可以使用任何类型的协议在端点之间传送消息。通信网络104可以包括有线和/或无线通信技术。因特网是构成互联网协议(IP)网络的通信网络104的一个实例，其由遍布全世界的许多计算机、计算网络和其他通信设备构成，并且通过许多电话系统和其他措施连接。通信网络104的其他实例包括而不限于：标准普通旧式电话系统(POTS)，综合服务数字网络(ISDN)，公共交换电话网(PSTN)，局域网(LAN)，广域网(WAN)，互联网协议语音(VoIP)网络，会话发起协议(SIP)网络，蜂窝网络，以及本领域内已知的任何其他类型的分组交换或电路交换网络。此外还可以认识到，通信网络104不需要被限制到任何一种网络类型，而是可以由若干不同的网络和/或网络类型构成。此外，通信网络104可以包括若干不同的通信介质，比如同轴电缆、铜电缆/电线、光纤线缆、用于发送/接收无线消息的天线及其组合。

[0037] 外部通信设备108通常被称为外部是因为其或者不处在管理企业网络120的企业的直接控制之下，或者与处在企业网络120内部的通信设备108相比对于企业网络120具有更低的信任水平。示例性的外部通信设备108类型包括而不限于蜂窝电话、膝上型计算机、平板电脑、个人计算机(PC)、数字电话、模拟电话、无线和Bluetooth设备等等。

[0038] 与外部通信设备108类似，企业网络120内部的通信设备108可以对应于用户通信设备，并且在一些实施例中可以包括而不限于电话、软件电话、蜂窝电话、多扬声器通信设备(例如会议电话)、视频电话、PC、膝上型计算机、平板电脑、智能电话、瘦客户端等等。应当认识到，通信设备108可以被配置成支持与企业网络120内部和外部的其他通信设备108的单用户或多用户交互，其对应于企业用户的单一用户代理(UA)和/或多个UA。

[0039] 通信设备108可以包括使得用户能够通过通信网络104和/或在企业网络120内部与彼此的通信设备交换媒体(例如语音、视频等等)、数据(例如电子邮件、短消息服务(SMS)消息、多媒体消息服务(MMS)消息、文件、演示、文档等等)的组件(硬件和软件)的任何总集。

[0040] 企业网络120可以对应于单一位置企业网络或多位置企业网络。单一位置企业网络可以包括局域网(LAN)，其包括有线(例如以太网)和/或无线(例如Wi-Fi)技术。多位置企业网络可以包括广域网(WAN)，其通过一个或多个不受信任的网络(例如通信网络104)连接多个LAN或类似网络位置。

[0041] 具体来说，虽然企业网络120被描绘成具有单一通信服务器124，但是应当认识到，一些企业网络120可以包括多台通信服务器124，并且这些服务器当中的每一台可以对于企业用户的一个子集具有权威(例如为之提供服务)。在这样的情形中，所接收到的消息将被路由到适当的通信服务器124。

[0042] 在一些实施例中，通信服务器124可以被用来帮助在企业网络120内部建立通信会话和/或移动信令路径、改变呼叫拓扑等等。具体来说，通信服务器124可以包括私有分支交换机(PBX)、企业交换机、企业服务器、前述各项的组合或者任何其他类型电信系统交换机或服务器。在一些实施例中，通信服务器124被配置成执行例如Avaya公司的Avaya Aura® 应用套装之类的电信功能，其中包括而不限于Communication Manager™(通信管理器)、Communication Manager Branch Edition™(通信管理器分支版本)、Avaya IP Offic™、Session Manager™(会话管理器)、System Manager™(系统管理器)、MultiVantage® Express™及其组合。

[0043] 根据至少一些实施例，通信服务器124可以接收呼叫请求。一旦通信服务器124接收到针对用户的呼叫请求，通信服务器124就向应用序列中的第一应用传递通信建立消息(例如INVITE消息)，从而允许第一应用确定通信会话的参数，将其自身插入到通信会话的控制和/或媒体流中，并且从而将其自身绑定到通信会话。通信服务器124可以包含或者连接到SIP防火墙128。SIP防火墙128可以是企业的应用层安全性的一个元件。SIP防火墙128可以允许或拒绝对于进入企业网络120的SIP消息的访问，并且可以跟踪报头和其他消息信息。

[0044] 附加的服务器124可以包括对于操作企业网络120所需要的任何其他类型的服务器或交换机。适当的其他服务器的实例包括而不限于存在服务器、即时消息传送(IM)服务器、电子邮件服务器、语音邮件服务器、虚拟机、web服务器、呼叫中心服务器、交互式语音响应(IVR)单元等等。

[0045] 企业数据库116可以是任何类型的数据库，比如关系、分级、面向对象等等。数据库116可以像所描绘的那样处在外部或者处在通信服务器124的内部。通信服务器124可以与数据库116通信。通信服务器124适于从通信设备108、网关112和其他服务器124获得请求。可以从通信服务器124向数据库116发送采取查询或订阅形式的请求。订阅和查询可以从数据库116取回数据，并且可以将结果返回到通信服务器124或其他服务器124。

[0046] 企业可能需要网关112来提供现场(on-premise)透明网络地址转换(NAT)控制。NAT转换是被用来允许多个企业设备连接到公共网络的一种网络协议。网关112可以把嵌入式私有地址转换成适当的公共地址(对于传入分组反之亦然)。网关112可以适于与企业网络120内部的任何元件通信，其中包括而不限于通信设备108、通信服务器124、企业数据库116等等。网关112可以把所有内部企业IP地址转换成公共地址，以便在与通信网络104或者任何其他公共或私有网络通信时使用。

[0047] 参照图2，其中根据本公开内容的实施例详细描述了说明性SIP消息200。SIP是具有两种类型的SIP消息(请求和响应)的基于文本的协议。请求204的起始或第一行可以包括方法、请求统一资源定位符(URI)以及协议版本标示(例如SIP/2.0)。方法可以定义请求的性质，其中可以包括例如REGISTER(登记)、INVITE(邀请)、ACK(确认)、CANCEL(取消)、BYE(再见)、OPTIONS(选项)、PRACK(临时确认)和INFO(信息)之类的方法。请求URI可以表明该

请求应当被发送到何处，其通常被用来标识出web资源(例如kat345@lake.com)。响应的起始或第一行可以包括相应代码(例如临时的1xx给出进展；最后的2xx、3xx、4xx、5xx、6xx终止事务)。

[0048] SIP消息的第二部分可以包含报头字段208。报头字段208可以通过<名称>:<数值>的形式传达属性以及修改消息含义(例如Via(经由)、Max-Forwards(最大转发)、To(去往)、From(来自)、Call-ID(呼叫ID)、CSeq(命令序列)、Contact(联系人)、Content-Type(内容类型)、Content Length(内容长度)等等)。各个报头字段可以在一则消息中出现一次或更多次。Via报头字段可以包含该消息已经过的先前元件的一个或多个地址。To报头字段可以表明或规定正被要求到会话的用户。From报头字段可以表明始发会话请求的用户。Call-ID报头字段可以包含对应于呼叫的全局唯一标识符。CSeq报头字段可以是标识出事务的命令序列。Contact报头字段可以表明对应于始发用户的位置。Content-Type和Content-Length报头字段可以分别规定主体的类型(例如会话描述协议-SDP)以及主体中的字节数目。

[0049] 一个空白行是可以表明SIP报头字段的结束和消息主体216的起始的分隔符212。在消息主体216内可以有消息内的一个或多个请求行，其中v可以表明SDP的版本(例如v＝0)，o可以表明所有者信息、会话ID、会话版本地址类型和地址(例如o＝-5894032 5894032 IN IP4 10.2.0.100)，并且媒体描述可以提供呼叫者可以发送和接收的类型、端口或可能格式(例如S＝SDP媒体会话)。关于SIP报头字段和字段数值的附加信息可以在RFC 3261中找到，其全部内容被合并在此以作参考。

[0050] 图3是呼叫循环300的一个实例，其中将根据本公开内容的至少一些实施例来描述呼叫循环检测和终止的特征。具体来说，图3描绘出第一呼叫拓扑，其中第一用户(例如用户A 304)涉及在与第二用户(用户B 308)的第一通信会话316中。可以建立第二通信会话324，并且可以尝试与用户C 312发起第三通信会话320。虽然没有描绘出，但是其他用户也可以涉及在第一通信会话316中，并且可以在用户A 304处、在用户B 308处或者通过集中式会议桥被转移到第一通信会话316中。

[0051] 在呼叫循环的一个非限制性实例中，用户A 304可以处在分机号1000处。用户A 304可以呼叫用户B 308，其中用户B 308可以处在分机号1002处。这可以是相同的通信服务器124上的内部呼叫，并且所述呼叫可以在没有问题的情况下被路由和连接。用户A 304可以决定向用户C 312询问一个问题，其中用户A 304无法为用户B 308回答该问题。用户C 312可以作为分机号1001在第二通信服务器124上被管理。当用户A 304呼叫用户C 312时，在1001上没有本地匹配，相反所述请求可以被匹配到第二通信管理器124上的1xxx。分机号1001可以在第二通信管理器124上找到，并且通信会话324可以在没有问题的情况下被正确地路由和连接。用户A 304向用户B 308告知他应当与用户C 312直接通话，并且提供对应于用户C 312的分机号而不是发起转移。然而不幸的是，用户B 308无意地把对应于用户C 312的分机号记为1003(而不是1001)。用户B 308可以向他所认为的对应于用户C 312的分机号发起呼叫，但是实际上该分机号并不存在。分机号1002(用户B)呼叫分机1003，并且没有本地匹配。所述请求可以被发送到下一台通信服务器124，并且可能没有匹配。第二通信服务器124可以把所述请求发送回到第一通信服务器124，从而产生循环。各台通信服务器124可能会来回发送所述请求，直到用户B 308终止呼叫。如果路径中的任何元件是非SIP元件，则传统的方法可能无法终止循环。当用户A 304、用户B 308和/或用户C 312处于企业网络120

外部时，相同的概念仍然适用。

[0052] 为了避免呼叫循环，管理员可以利用两个新参数来管理本公开内容的会话管理器抗循环检测，所述两个新参数即循环计数阈值和循环检测间隔。在通信系统100中，可以对于呼叫循环检测启用所述两个新字段，并且可以在通信服务器124上的管理用户接口上显示所述两个新字段以供管理员使用。如果循环计数阈值参数的默认数值是0，则表明循环检测被关闭。所允许的范围可以是0-10000。循环检测间隔参数的默认数值可以被设定到100msec。所允许的范围可以是10msec-10000msec。由于呼叫循环的频率是等待时间的函数并且取决于循环路径中的网络元件的数目，因此管理员可以对循环检测参数进行微调，以便满足特定于网络配置的企业的具体需求。

[0053] 管理员可以在每一台通信服务器124上修改这些参数，并且可以具有调节及测试循环计数阈值和循环检测间隔参数的选项以便适应网络120的具体需求。虽然管理员可以把循环检测间隔设定到低至10msec，但是可以预期管理员可以选择把所述间隔设定为100msec的倍数。如果设定了极小的循环检测，则可能会产生不必要的性能开销并且不会检测到循环。

[0054] 在管理循环检测间隔时的一项考虑可以是呼叫循环经过了多少元件，以及由每一个元件引入的传播延迟的总和。在一个非限制性实例中，呼叫循环以假设的25msec的积极(aggressive)间隔到达通信服务器124，其中中间跳跃的累积传播延迟是25msec或更少，并且管理员希望在相同呼叫的第五实例之后打断循环。管理员可以把配置设定到循环计数阈值＝5以及循环检测间隔＝200msec。如果管理员设定循环计数阈值＝2以及循环检测间隔≤50msec，则呼叫循环将不会被检测到。通常来说，最积极的呼叫循环速率是每秒12次循环尝试(～84msec)，管理员可以针对风险以及针对网络适当地设定所述参数。一旦设定了新的参数之后，可能有必要进行一些试错以便优化循环检测。

[0055] 为了识别出呼叫循环，SIP防火墙128可以对于传入请求的R-URI、To、From和PAI报头数值的每一种独特组合保持临时的各个单独的呼叫计数器。在接收到对话外(OOD)INVITE请求时，SIP防火墙128可以检查是否已经存在对应于所述报头数值组合的计数器。如果不是的话，则可以实例化新的计数器。可以对于每一条OOD INVITE请求递增循环计数器。如果循环计数器等于所管理的INVITE循环阈值，则可以拒绝OOD INVITE请求。

[0056] 为了使得两个URI相等，包括用户(user)、口令(password)、主机(host)和端口(port)在内的组成部分必须匹配。具体来说，SIP URI被定义为一个字符串，其中括号表明可选的组成部分：

[0057] sip:user[:password]@host[:port]

[0058] 用户组成部分是所述字符串的处在“sip”之后的第一个“:”与第二个“:”或者“@”字符之间的部分。出于比较目的可以不考虑包括检测参数在内的其他组成部分。当循环计数等于所管理的循环阈值计数并且/或者循环阈值间隔定时器到期时，应当去除循环呼叫计数器。

[0059] 利用所述新的参数，一旦达到循环计数阈值和循环检测间隔，就可以向用户B 308发送603拒绝(Decline)(目的地不希望参与呼叫或者无法参与呼叫，并且客户端知道没有替换的目的地(比如语音邮件服务器)希望接受呼叫)或604不存在于任何地方(Does Not Exit Anywhere)(服务器具有表明所请求的用户不存在于任何地方的权威信息)，并且可以

释放资源。

[0060] 图4是根据本公开内容的实施例使用的滑动窗口400的一个实例。滑动窗口协议可以被使用在基于分组的数据传输网络中。在需要按顺序的可靠分组递送时可以使用滑动窗口协议，比如在数据链路层(OSI模型)以及传输控制协议(TCP)中。

[0061] 在一个非限制性实例中，可以将分组1、分组2、分组3、分组4、分组5和分组6作为一条或多条SIP消息404从通信设备108发送。深黑方框描绘出窗口尺寸，其在本例中包含两个分组。所述窗口尺寸可以包括一定数目的分组(一个或多个)，其可以在接收到表明所述分组已被接收的确认(ACK)之前被发送。在滑动窗口模型中，可以在一个窗口408中发送针对多个分组的ACK(例如分组1和分组2)。ACK还可以包含关于缓冲器尺寸的信息，从而指导在下一次发送中应当有多少分组。如果太多分组同时到来并且缓冲器溢出，则可以减少同时发送的分组数目或者可以停止一段指定间隔。如果可以更快地处理分组，则可以请求并提供更大的窗口。

[0062] 当接收到SIP消息404的分组1和分组2时，可以由通信服务器124发送ACK。一旦接收到ACK，可以在一个窗口412中发送分组3和分组4。当接收到SIP消息404的分组3和分组4时，可以由通信服务器124发送ACK。一旦接收到ACK，可以在一个窗口416中发送分组5和分组6。当接收到SIP消息404的分组5和分组6时，可以由通信服务器124发送ACK。如图所示，滑动窗口可以移动，并且可选地可以在确认每一个先前分组集合时对其进行调节。通过使用滑动窗口机制，SIP防火墙128可以高效地检查计数阈值和间隔阈值，从而向通信服务器124提供该信息以供管理员使用来保护任何网络免于呼叫循环，而不管其是全SIP网络还是包含非SIP元件。

[0063] 在图5中示出了根据本公开内容的实施例的用于呼叫循环分析和终止的方法500。一般来说，方法500开始于开始操作504并且终止于结束操作544。虽然在图5中示出了方法500的各个步骤的一般顺序，但是方法500可以包括更多或更少步骤，或者可以按照不同于图5中所示的方式来安排各个步骤的顺序。方法500可以作为一个计算机可执行指令集合来执行，其由计算机系统执行并且被编码或存储在计算机可读介质上。此外，所述方法可以通过专用集成电路(ASIC)、现场可编程门阵列(FPGA)或者其他可配置硬件组件、模块或系统中的一组门或其他结构的集合来具体实现。在后文中将参照结合图1-4描述的系统、组件、模块、软件、数据结构等等来解释方法500。

[0064] 所述方法开始于步骤504，并且当在步骤508中由企业网络120接收到或者在企业网络120内部发起呼叫时继续。当所述呼叫由通信服务器124处理时，可以考虑各个通信元件。在一个非限制性实例中，SIP通信服务器124从通信设备108接收SIP呼叫。所述SIP呼叫包含标准SIP报头200组成部分。在步骤512中，通信服务器124检查SIP报头200。正如在图2中详细描述的那样，SIP报头200可以包含例如Via(经由)、Max-Forwards(最大转发)、To(去往)、From(来自)、Call-ID(呼叫ID)、CSeq(命令序列)、Contact(联系人)、Content-Type(内容类型)和Content-Length(内容长度)之类的元素数值。在步骤516中，通信服务器124内的SIP防火墙128可以发起数据库查找，以便查看是否有任何报头元素与来自先前呼叫请求的报头相匹配。SIP防火墙128可以记录并保持对应于当前呼叫的报头数据(步骤520)。在步骤524中，SIP防火墙128可以发起报头字段的比较，以便查看是否当前报头字段是否与任何先前呼叫报头字段相匹配。如果没有与先前呼叫请求的匹配，则所述方法返回开始，直到在步

骤508中接收到另一呼叫为止。

[0065] 如果SIP防火墙128在步骤524中确定有报头与一条或多条先前呼叫请求相匹配，则SIP防火墙128可以检查是否已达到由管理员设定的新的计数阈值(步骤528)。如果没有达到所述计数阈值，则所述方法返回开始，直到在步骤508中接收到另一呼叫为止。如果达到计数阈值，则SIP防火墙128可以检查是否已达到与操作系统所提供的系统时钟比较的由管理员设定的新的间隔阈值(步骤532)。如果没有达到所述间隔阈值，则所述方法返回开始，直到在步骤508中接收到另一呼叫为止。如果达到间隔阈值，则SIP防火墙128可以确定通过已达到计数阈值和间隔阈值而表明循环。SIP防火墙128可以在步骤536中打断循环。可以向呼叫始发者发送拒绝(例如603拒绝，604不存在)(步骤540)。一旦发送了拒绝消息，就可以终止呼叫尝试，从而释放由呼叫循环消耗的资源。所述方法在步骤544中结束。

[0066] 当网络包含混合的SIP和非SIP元件时，可以使用可调节的循环检测计数和循环检测间隔参数来精确地检测混合网络循环，从而在发生路由问题和/或恶意攻击时保护资源。

[0067] 虽然本公开内容参照特定标准和协议描述了在各个方面、实施例和/或配置中实施的组件和功能，但是所述方面、实施例和/或配置不限于这样的标准和协议。未在这里提到的其他类似标准和协议同样存在，并且被视为包括在本公开内容中。此外，这里所提到的标准和协议以及未在这里提到的其他类似标准和协议时时被具有基本上相同功能的更快或更有效的等效方案所取代。具有相同功能的此类替代标准和协议被视为包括在本公开内容中的等效方案。

[0068] 前面的讨论是出于说明和描述的目的而给出的。前述内容不意图把本公开内容限制到这里所公开的一种或多种形式。例如在前面的具体实施方式部分中，出于使得本公开内容顺畅的目的而在一个或多个方面、实施例和/或配置中将本公开内容的各项特征分组在一起。本公开内容的各个方面、实施例和/或配置的各项特征可以被组合在不同于前面所讨论的替换方面、实施例和/或配置中。这种公开方法不应被解释为反映出权利要求书要求多于在每一条权利要求中所明确引述的特征的意图。相反，正如后面的权利要求书所反映的那样，本发明的各个方面在于前面所公开的单一方面、实施例和/或配置的少于全部特征。因此，后面的权利要求书被合并到具体实施方式部分中，其中每一条权利要求独自作为本公开内容的一个单独的优选实施例。

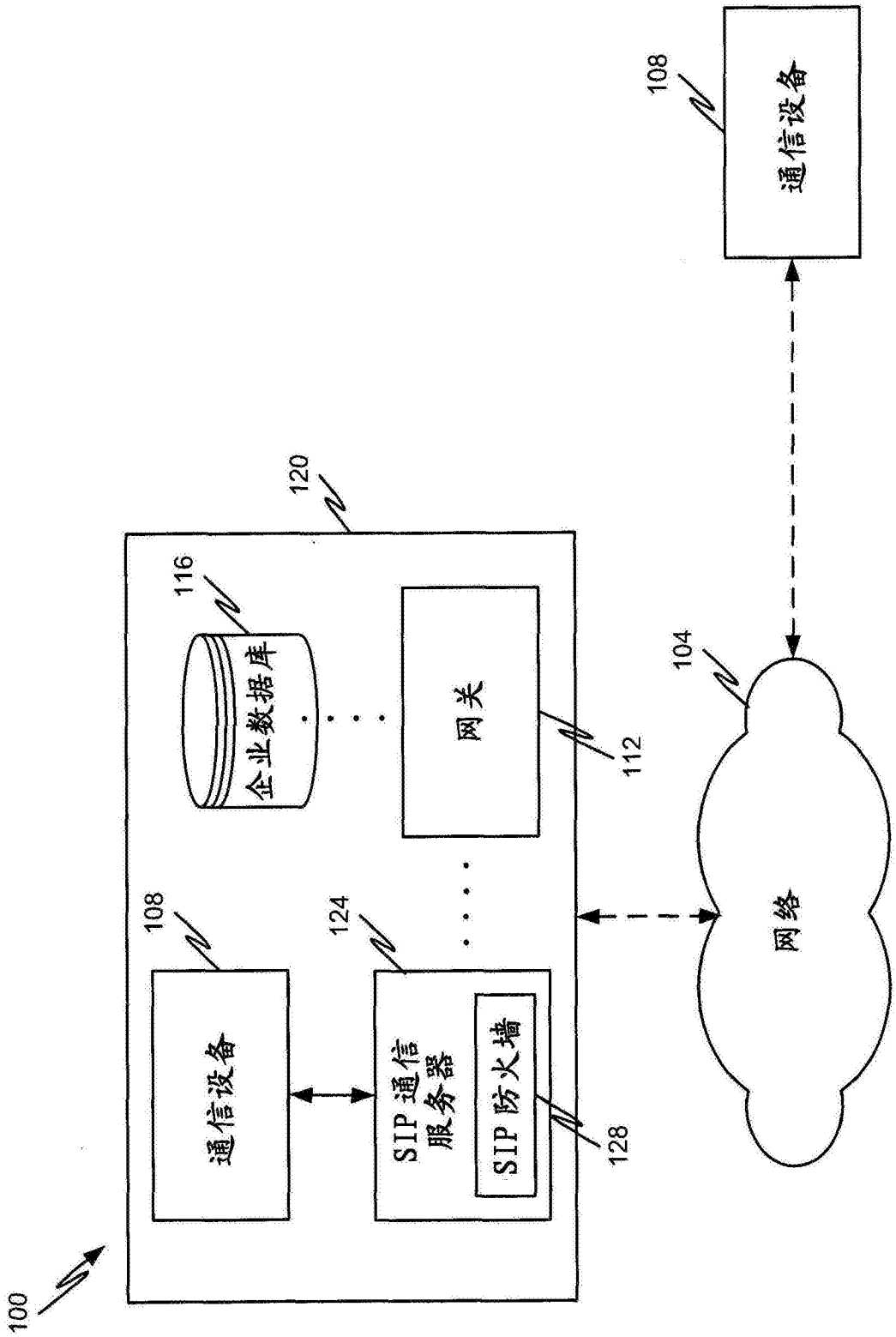

100
120
116
企业数据库
网关
112
108
通信设备
124
SIP 通信
服务器
SIP 防火墙
128
网络
104
108
通信设备

图1

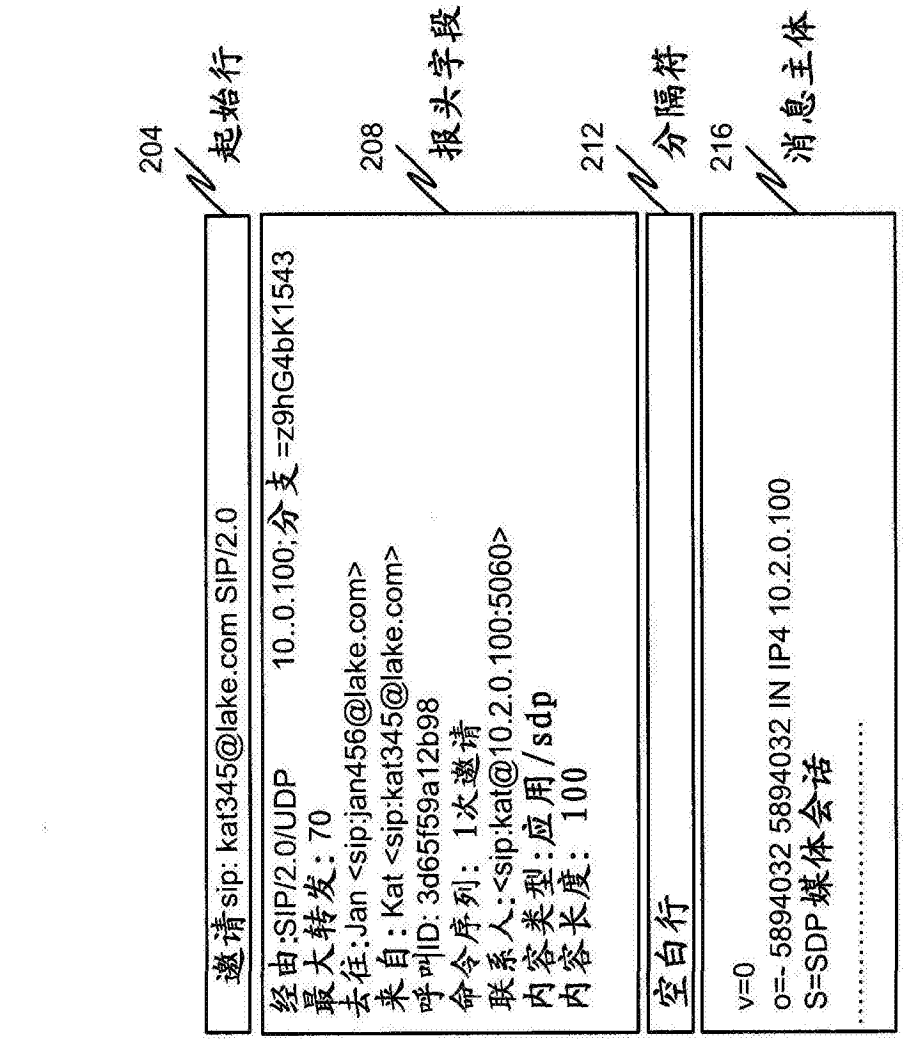

200
204
起始行
208
报头字段
212
分隔符
216
消息主体
邀请sip: kat345@lake.com SIP/2.0
经由:SIP/2.0/UDP 10..0.100;分支=z9hG4bK1543
最大转发: 70
去往:Jan <sip:jan456@lake.com>
来自: Kat <sip:kat345@lake.com>
呼叫ID: 3d65f59a12b98
命令序列: 1次邀请
联系人:<sip:kat@10.2.0.100:5060>
内容类型:应用/sdp
内容长度: 100
空白行
v=0
o=- 5894032 5894032 IN IP4 10.2.0.100
S=SDP 媒体会话
.....

图2

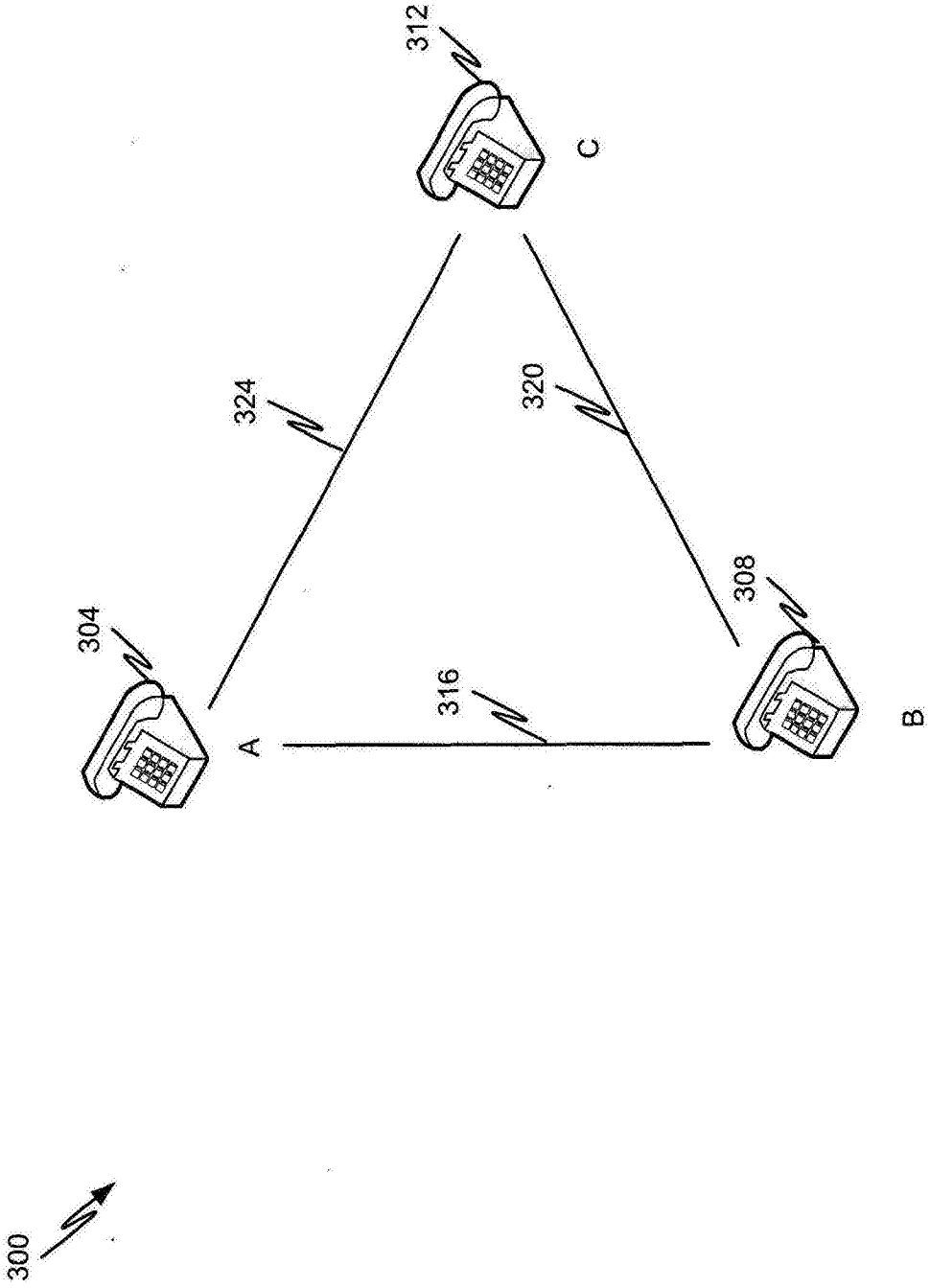


图3

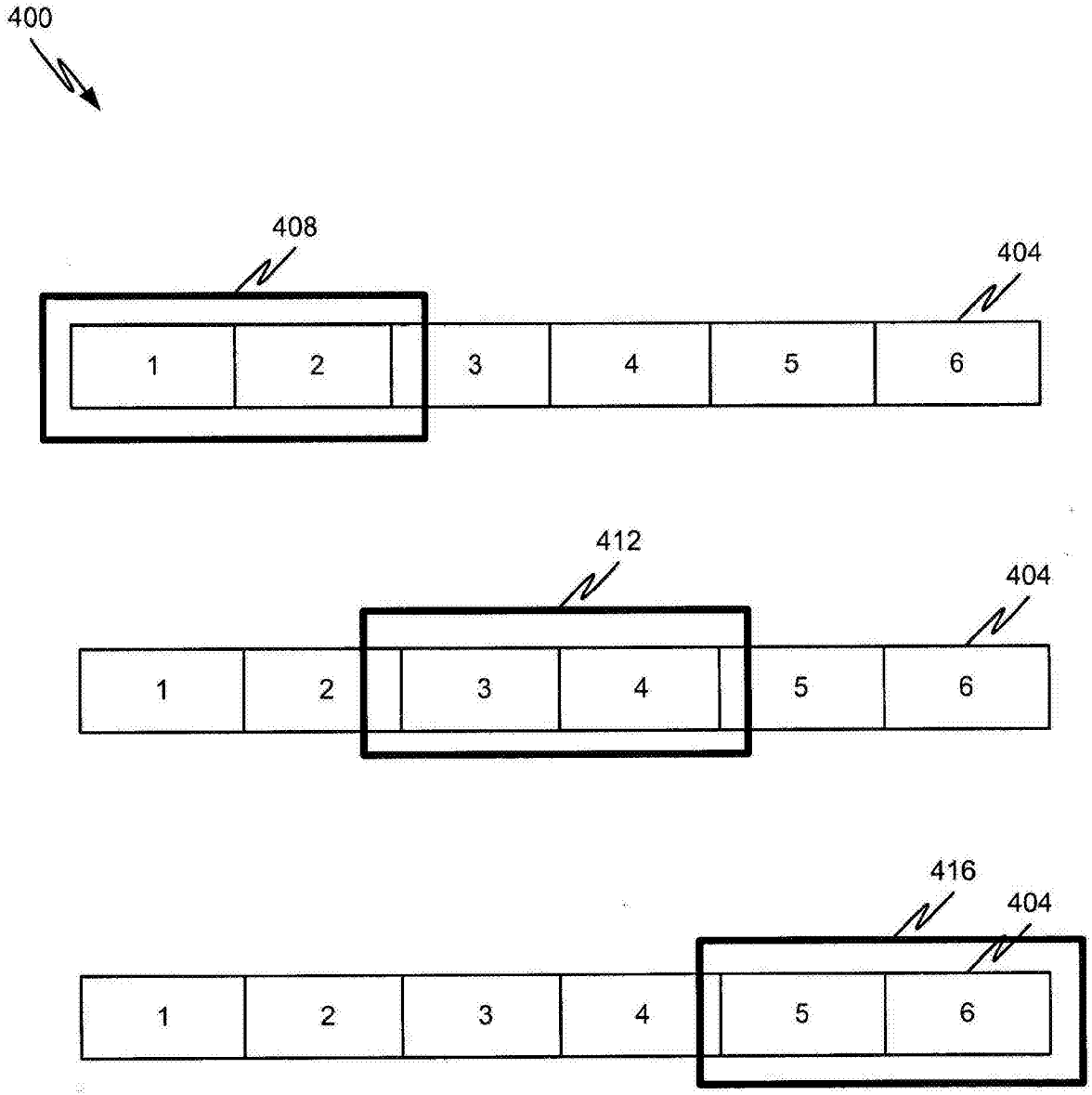


图4

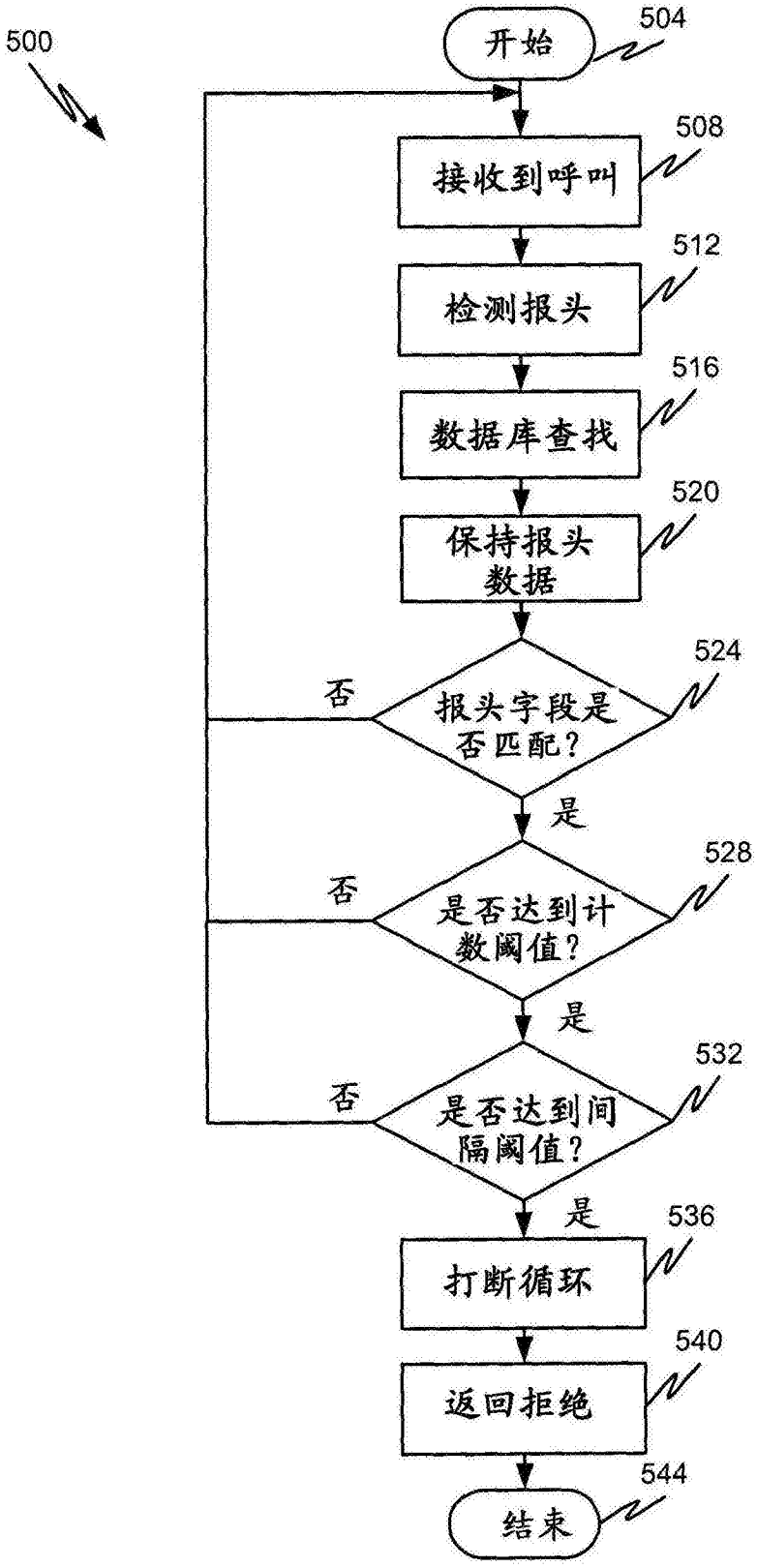

500
开始
504
接收到呼叫
508
检测报头
512
数据库查找
516
保持报头数据
520
报头字段是否匹配？
524
否
是
是否达到计数阈值？
528
否
是
是否达到间隔阈值？
532
否
是
打断循环
536
返回拒绝
540
结束
544

图5