



(12)发明专利

(10)授权公告号 CN 103546442 B

(45)授权公告日 2018.10.23

(21)申请号 201210246779.6

(22)申请日 2012.07.17

(65)同一申请的已公布的文献号

申请公布号 CN 103546442 A

(43)申请公布日 2014.01.29

(73)专利权人 中兴通讯股份有限公司

地址 518057 广东省深圳市南山区科技南路55号

(72)发明人 游世林

(74)专利代理机构 北京康信知识产权代理有限

责任公司 11240

代理人 余刚 梁丽超

(51)Int.Cl.

H04L 29/06(2006.01)

(56)对比文件

CN 1406005 A, 2003.03.26,

CN 101282250 A, 2008.10.08,

CN 101282250 A, 2008.10.08,

CN 102055585 A, 2011.05.11,

US 2010002880 A1, 2010.01.07,

CN 102223356 A, 2011.10.19,

CN 1602611 A, 2005.03.30,

审查员 冯慧婷

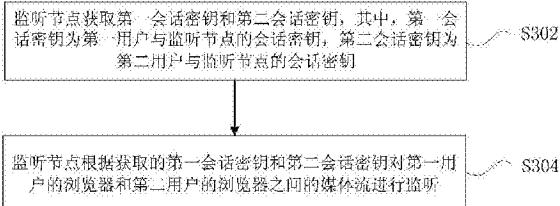
权利要求书2页 说明书11页 附图5页

(54)发明名称

浏览器的通讯监听方法及装置

(57)摘要

本发明提供了一种浏览器的通讯监听方法及装置，其中，上述方法通过在主叫浏览器和被叫浏览器之间新增的监听节点实现，该方法包括：监听节点获取第一会话密钥和第二会话密钥，其中，第一会话密钥为第一用户与监听节点的会话密钥，第二会话密钥为第二用户与监听节点的会话密钥；监听节点根据获取的第一会话密钥和第二会话密钥对第一用户的浏览器和第二用户的浏览器之间的媒体流进行监听。采用本发明提供的上述技术方案，解决了相关技术中，不能对两个浏览器的通讯进行监听等技术问题，从而实现了对浏览器之间的通讯内容进行监听的效果。



1. 一种浏览器的通讯监听方法,其特征在于,通过在主叫浏览器和被叫浏览器之间新增的监听节点实现,所述方法包括:

所述监听节点获取第一会话密钥和第二会话密钥,其中,所述第一会话密钥为第一用户与所述监听节点的会话密钥,所述第二会话密钥为第二用户与所述监听节点的会话密钥;

所述监听节点根据获取的所述第一会话密钥和所述第二会话密钥对所述第一用户的浏览器和所述第二用户的浏览器之间的媒体流进行监听;

所述监听节点根据获取的所述第一会话密钥和所述第二会话密钥对所述第一用户的浏览器和所述第二用户的浏览器之间的媒体流进行监听之前,包括:在所述第一用户为主叫时,所述监听节点接收所述第一用户的信令服务器转发的来自于所述第一用户的浏览器的业务请求;所述监听节点将所述业务请求经由所述第二用户的信令服务器转发给所述第二用户的浏览器,以建立所述第一用户的浏览器和所述第二用户的浏览器之间的媒体流传输。

2. 根据权利要求1所述的方法,其特征在于,所述监听节点获取第一会话密钥和第二会话密钥,包括:

所述监听节点向密钥管理服务器发送密钥生成信息,其中,所述密钥生成信息携带有生成所述第一会话密钥和所述第二会话密钥所需要的信息;

所述监听节点获取所述密钥管理服务器生成的所述第一会话密钥和所述第二会话密钥。

3. 根据权利要求2所述的方法,其特征在于,所述信息包括:所述第一用户的标识、所述第二用户的标识和所述监听节点的标识。

4. 根据权利要求1所述的方法,其特征在于,所述监听节点获取第一会话密钥和第二会话密钥,包括:

所述监听节点接收所述第一用户的信令服务器和所述第二用户的信令服务器上报的信息;

所述监听节点将上报的所述信息发送给所述密钥管理服务器,其中,上报的所述信息为所述密钥管理服务器生成所述第一会话密钥和所述第二会话密钥的依据;

所述监听节点获取所述密钥管理服务器生成的所述第一会话密钥和所述第二会话密钥。

5. 根据权利要求1所述的方法,其特征在于,在所述监听节点接收所述第一用户的信令服务器转发的来自于所述第一用户的浏览器的业务请求之后,包括:

所述监听中心从所述密钥管理服务器中获取所述第一会话密钥。

6. 根据权利要求1所述的方法,其特征在于,所述监听节点根据获取的所述第一会话密钥和所述第二会话密钥对所述第一用户的浏览器和所述第二用户的浏览器之间的媒体流进行监听之前,还包括:

在所述第二用户为被叫时,所述监听节点接收所述第二用户的信令服务器转发的来自于所述第二用户的浏览器的业务请求;

所述监听节点将接收的所述第二用户的浏览器的业务请求转发给所述第一用户的浏览器,以建立所述第一用户的浏览器和所述第二用户的浏览器之间的媒体流传输。

7. 根据权利要求6所述的方法,其特征在于,

所述监听节点将接收的所述第二用户的浏览器的业务请求转发给所述第一用户的浏览器之前,包括:所述监听中心从所述密钥管理服务器中获取所述第二会话密钥;

所述监听节点将接收的所述第二用户的浏览器的业务请求转发给所述第一用户的浏览器之后,包括:所述监听中心从所述密钥管理服务器中获取所述第一会话密钥。

8. 一种浏览器的通讯监听装置,其特征在于,位于主叫浏览器和被叫浏览器之间新增的监听节点中,包括:

获取模块,用于获取第一会话密钥和第二会话密钥,其中,所述第一会话密钥为第一用户与所述监听节点的会话密钥,所述第二会话密钥为第二用户与所述监听节点的会话密钥;

监听模块,用于根据获取的所述第一会话密钥和所述第二会话密钥对所述第一用户的浏览器和所述第二用户的浏览器之间的媒体流进行监听;

所述装置在根据获取的所述第一会话密钥和所述第二会话密钥对所述第一用户的浏览器和所述第二用户的浏览器之间的媒体流进行监听之前,还用于:在所述第一用户为主叫时,接收所述第一用户的信令服务器转发的来自于所述第一用户的浏览器的业务请求;将所述业务请求经由所述第二用户的信令服务器转发给所述第二用户的浏览器,以建立所述第一用户的浏览器和所述第二用户的浏览器之间的媒体流传输。

9. 根据权利要求8所述的装置,其特征在于,所述获取模块包括:

第一发送单元,用于向密钥管理服务器发送密钥生成信息,其中,所述密钥生成信息携带有生成所述第一会话密钥和所述第二会话密钥所需要的信息;

第一获取单元,用于获取所述密钥管理服务器生成的所述第一会话密钥和所述第二会话密钥。

10. 根据权利要求8所述的装置,其特征在于,所述获取模块,包括:

接收单元,用于接收所述第一用户和所述第二用户的信令服务器上报的信息;

第二发送单元,用于将上报的所述信息发送给所述密钥管理服务器,其中,上报的所述信息为所述密钥管理服务器生成所述第一会话密钥和所述第二会话密钥的依据;

第二获取单元,用于获取所述密钥管理服务器生成的所述第一会话密钥和所述第二会话密钥。

浏览器的通讯监听方法及装置

技术领域

[0001] 本发明涉及网络通信安全技术领域,尤其涉及一种浏览器的通讯监听方法和装置。

背景技术

[0002] 随着通信网络和互联网的日益融合,各方对沟通的需求越来越复杂,沟通不仅仅是单一的音频,可能还有视频和其他媒体的混合形式,而且沟通有时还具有时效性要求。

[0003] 目前浏览器为客户端/服务器(Client/Server,简称为C/S)结构,而且现在一般在网页上提供音频(audio),或者视频(video)等实时媒体服务的,基本上是通过插件技术(plus-in)或者下载来实现的,现在的网页技术,甚至现在的超文本传输协议(Hypertext Transfer Protocol,简称为HTTP)技术,不能很好的支持流方式的媒体下发。这些都导致了基于浏览器的实时通信是存在缺陷的,都要通过插件/外挂应用程序/或者下载来实现,来加速浏览器的效率。

[0004] 针对上述技术问题,对等(Peer-to-Peer,简称为P2P)的浏览器技术作为浏览器之间对等的通信技术,让浏览器可以实时运用P2P的特性传送内容,包括视频、音频和用于实时通信的“补充”。

[0005] 而目前出现的实时通信(Real-Time Communications,简称为RTC)网络(web)研究课题,实质也就是一项直接让浏览器和浏览器之间对等通信的标准,而不需要中央服务器。该标准可以减少人为干扰和嗅探,提高互联网络通信的可靠性,通过客户端应用程序编程接口(Application Programming Interface,简称为API)的方式实现这个新的实时通信概念,该API可以直接被浏览器厂商调用,无须额外下载插件和应用程序即可使用。

[0006] 标准组织IETF中RTCweb工作组于2011年7月成立,主要目标是配合万维网联盟(World Wide Web Consortium,简称为W3C)的WebRTC工作组实现通过浏览器直接实现实时的视频和音频通讯,而不需要插件的支持。

[0007] IETF涉及的标准化部分包含:数据传输协议,包含网络地址转换(NAT, Network Address Translation简称为NAT)穿越等等;媒体传输协议,实时传输协议(Real-time Transport Protocol,简称为RTP)/安全实时传输协议(Secure Real-time Transport Protocol,简称为SRTP)的运用上的规定),会话连接和控制(重点,包含如何建立会话,如何进行媒体协商等等),媒体数据格式(包括必选和可选的编码格式等),浏览器本地支持(包括基础的本地设备控制,如音量,摄像头焦距等等)。

[0008] RTCweb工作组刚成立就吸引了许多互联网巨头以及传统电信业的爱立信等公司。多家公司实现了RTCweb的原型并进行了展示。

[0009] 图1为现有RTCWeb业务基本架构图,主要包括如下网元:

[0010] 信令服务器,主要负责浏览器(Browser)用户注册,用户寻址,会话状态维护;

[0011] Browser浏览器(A,B),主要负责用户终端界面显示,负责发起和接受会话,与目标Browser之间建立媒体连接;

[0012] 当浏览器A准备与浏览器B建立实时通讯会话,浏览器A首先通过超文本传输协议(HTTP)或者Web插口协议(WebSocket)向它注册的信令服务器A发送会话请求,请求消息中携带目标浏览器B的身份标识ID,及自身的媒体地址信息;信令服务器A根据浏览器B的身份标识ID分析,发现用户在信令服务器B进行注册登记,于是采用会话启动协议(Session Initiation Protocol,简称为SIP)向信令服务器B发送会话请求;信令服务器B根据浏览器B用户注册的地址,向浏览器B通过HTTP协议发送会话请求消息,消息中携带浏览器A的媒体端口IP地址及端口信息;浏览器B接受本次会话,返回应答消息,返回本端的媒体地址和端口信息。

[0013] 此时,浏览器A和浏览器B建立实时通讯。

[0014] 图2是MIKEY-TICKET中定义的三个密钥协商交互流程示意图,包括步骤1-5(详见图2,此处不再赘述)。MIKEY-TICKET是基于密钥管理服务器(Key Management Servicer,简称为KMS)的安全通信技术方案是一种保护媒体流端到端的技术方案,其是针对与信令和传输网络无关的具有更高要求的安全需求而提出的。该种技术方案是基于使用密钥管理服务器(KMS)和一个“票据(ticket)”的概念来实现的,其中,密钥管理服务器KMS用于负责提供安全、用户鉴权以及密钥生成等功能。

[0015] 所述基于密钥管理服务器的安全通信技术方案主要是针对具有较高安全需求的用户,基于KMS的方案可以完全不依赖于信令面的安全,即使信令面的数据被窃取,攻击者也无法获取通话双方的媒体密钥。但该基于密钥管理服务器的技术方案需要增加新的网元,即增加一个密钥管理服务器KMS。

[0016] MIKEY-Ticket密钥协商机制是用来扩充MIKEY(RFC3830)协议的一种新的模式,这个新的模式使用了密钥管理服务器(KMS)和票据(Ticket)的概念。MIKEY-TICKET对MIKEY协议的扩展的需求来源于爱立信公司的TBS方案,该方案中使用的“ticket(票据)”概念,而实际中,该“ticket”实体没有一个具体的协议来承载,使之能在信令中传输。在RFC4568的SDP的密钥协商协议扩展中,SDP已经能支持传输MIKEY,让MIKEY支持“ticket”,则问题迎刃而解。

[0017] MIKEY-TICKET机制中包含三次交互,如图2所示,分别为:票据请求(Ticket Requests),票据传输(Ticket Transfer)和票据解决(Ticket Resolve)。在图2中,用户A表示发起会话用户,用户B表示应答会话用户,KMS表示密钥管理服务器。下面针对上述三种交互过程分别进行详细说明,其中在交互参数中可分为三类表示方式,即*[]表示该参数可选,()表示可含一个或超过一个该类参数,{}表示不含或含超过零个该类参数。

[0018] 票据请求(Ticket Request)

[0019] 首先会话发起方即用户A向KMS发送一个请求触发(REQUEST_INIT)消息,用于向KMS请求一个票据,该REQUEST_INIT消息中包含了会话信息(例如,被呼叫者的标识),并且这个REQUEST_INIT消息由基于用户A和KMS的共享密钥的消息认证码(MAC)来保护。

[0020] Ticket Request分为两种模式:1.共享密钥2.公私钥机制。由于公私钥机制需要PKI的支持而不被采用,这里只介绍共享密钥模式。该REQUEST_INIT消息中所带的参数包括:HDR,T,RAND,[IDi],[IDkms],(IDre),{SP},IDtp,[KEMAC],[IDpsk],V,其中:

[0021] HDR表示消息头,T表示时间戳,RAND表示随机数;

[0022] IDi包含发送方的标识,这个标识一般存在票据(ticket)中的“发送到”字段,由于

发送方的标识可以从消息的发送方字段读取到,所以在REQUEST_INIT消息中该参数有时可以省去;

[0023] IDkms应包含在该消息中,但如果KMS只有一个惟一标识的时候可省;

[0024] IDre为接收方的标识,可为单个用户或者一组用户。如果超过一个接受方时,每个接收方的标识都必需放在一个单独的ID载荷中;

[0025] IDtp是所希望采用的票据(ticket)策略的标识;SP为安全策略载荷;

[0026] KEMAC为密钥数据传输载荷,简单说就是用来存放传输各个密钥的地方,这里KEMAC=E(encr_key,[MPK] || {TGK|TEK}),其中MPK(MIKEY Protection Key)为MIKEY消息保护密钥,即用encr_key将MPK,TGK或者TEK加密,TGK可以不止一个,encr_key即由PSK生成,该参数可选;

[0027] IDpsk不是必需参数,只有当PSK超过一个,需要指定是使用哪个PSK时使用;V是验证载荷,存放相应MAC值。

[0028] 如果发起方被认证合法发起这个请求,那么KMS产生所需要的密钥,并将这些密钥进行编码放在票据(ticket)中,在REQUEST_RESP消息中返回票据(ticket)给发起方用户A,该消息中的具体参数包括:HDR,T,[IDkms],[IDtp],[TICKET],[KEMAC],V,其中有[]的参数均为可选,其中TICKET包含ticket类型以及ticket数据,ticket类型和数据均取决于IDtp。

[0029] 票据请求(Ticket Request)这一交互流程是可选的,当用户自身有能力产生ticket而无需和KMS进行交互时,ticket request步骤可省略。

[0030] 票据传输(Ticket Transfer)

[0031] 收到KMS发回的REQUEST_RESP消息后,用户A将ticket放在传输触发(TRANSFER_INIT)消息中发给被叫方用户B,即图2中步骤3所示。如果用户B检查策略为可接受,它就把ticket放在解析触发(RESOLVE_INIT)消息中转发给KMS,让KMS返回包含在ticket中的密钥信息,见图2中的步骤4,其中RESOLVE_INIT消息也采用基于用户B和KMS的共享密钥的MAC保护。基于ticket的类型,步骤4也是可选的,仅在用户B离开KMS的协助无法或者ticket中所包含信息时使用。TRANSFER_INIT和RESOLVE_INIT消息中具体参数分别如下:

[0032] TRANSFER_INIT消息中的IDI与IDr参数在有其他途径可以获取发送方和接收方的标识时,在该消息中可不包含。在最后面的验证载荷中,验证密钥auth_key由MPK生成。由于发送方和接收方此时并没有共享密钥,接收方不能在ticket在处理前验证自己从接收方收到的消息,所以接收方首先需要检查自己接受的策略,如果所收到的消息中的IDtp自己不能接受,则拒绝该消息,不再与KMS进行交互。这也是提前预防对KMS的DoS攻击的一个方法。

[0033] 票据解析(Ticket Resolve)

[0034] 在(解析触发)RESOLVE_INIT消息中,TICKET载荷携带需要被KMS解密的ticket, IDtp和IDI载荷必需和TRANSFER_INIT中相应参数一致。V是验证载荷,验证密钥auth_key由PSK生成。

[0035] KMS收到RESOLVE_INIT消息后,验证用户B是否是合法接受者,如果是,则KMS取回在ticket中的密钥和其他信息,并给用户B发送(解析响应)RESOLVE_RESP消息,如果KMS不能正确解析收到的消息或者发送RESOLVE_INIT的用户B未通过验证,则KMS应该返回相应的错误消息。KMS在RESOLVE_RESP消息中将相关密钥和其他附加信息一起发给用户R,参见图2

中的步骤5。

[0036] 该RESOLVE_RESP消息中的具体参数:其中HDR除了消息类型,下一个载荷以及V标签外,其他头部载荷需和RESOLVE_INIT消息中的头一致,时间戳类型和值需和RESOLVE_INIT消息中一致,KEMAC=E($\text{encr_key}, \text{MPK} || [\text{MPK}] || \{\text{TGK} | \text{TEK}\}$)。如果是Forking情况,KMS则需要两个分叉MPK和多个TGK。这种情况下,第一个MPK用来保护TRANSFER_INIT消息,而第二个MPK用来保护TRANSFER_RESP消息。用来生成不同分叉密钥的修改因子包含在IDmod载荷中。

[0037] 用户B收到该RESOLVE_RESP消息后,发送TRANSFER_RESP消息给用户A作为确认,见图2中的步骤6,在TRANSFER_RESP消息中可能包含用于密钥生成的一些信息。实际中的信令流程需要依赖具体的ticket类型和KMS域的策略而定,其中,ticket的类型由ticket的策略决定。

[0038] RTCWeb为了保证通讯安全,在媒体面采用媒体流加密技术来保证通讯的安全,该技术在媒体面中直接传输会话密钥,这就保证了浏览器A和浏览器B的安全。

[0039] 然而各国法律都有规定,执法部门必须要能够对任何通话进行合法监听,如果采用媒体流加密技术的RTCweb实现监听,由于现有技术只能侦听到使用了会话密钥加密后的媒体流,并且由于会话密钥在媒体流传输,不容易获取该会话密钥,导致监听不顺畅。

[0040] 针对相关技术中的上述问题,目前尚未提出有效的解决方案。

发明内容

[0041] 针对相关技术中,浏览器间媒体面传递会话密钥不能监听即不能对两个浏览器的通讯进行监听等技术问题,本发明提供了一种浏览器的通讯监听方法和装置,以至少解决上述问题。

[0042] 根据本发明的一个方面,提供了一种浏览器的通讯监听方法,通过在主叫浏览器和被叫浏览器之间新增的监听节点实现,该方法包括:监听节点获取第一会话密钥和第二会话密钥,其中,第一会话密钥为第一用户与监听节点的会话密钥,第二会话密钥为第二用户与监听节点的会话密钥;监听节点根据获取的第一会话密钥和第二会话密钥对第一用户的浏览器和第二用户的浏览器之间的媒体流进行监听。

[0043] 上述监听节点获取第一会话密钥和第二会话密钥,包括:监听节点向密钥管理服务器发送密钥生成信息,其中,密钥生成信息携带有生成第一会话密钥和第二会话密钥所需要的信息;监听节点获取密钥管理服务器生成的第一会话密钥和第二会话密钥。

[0044] 上述信息包括:第一用户的标识、第二用户的标识和监听节点的标识。

[0045] 上述监听节点获取第一会话密钥和第二会话密钥,包括:监听节点接收第一用户的信令服务器和第二用户的信令服务器上报的信息;监听节点将上报的信息发送给密钥管理服务器,其中,上报的信息为密钥管理服务器生成第一会话密钥和第二会话密钥的依据;监听节点获取密钥管理服务器生成的第一会话密钥和第二会话密钥。

[0046] 上述监听节点根据获取的第一会话密钥和第二会话密钥对第一用户的浏览器和第二用户的浏览器之间的媒体流进行监听之前,包括:在第一用户为主叫时,监听节点接收第一用户的信令服务器转发的来自于第一用户的浏览器的业务请求;监听节点将业务请求经由第二用户的信令服务器转发给第二用户的浏览器,以建立第一用户的浏览器和第二用

户的浏览器之间的媒体流传输。

[0047] 在监听节点接收第一用户的信令服务器转发的来自于第一用户的浏览器的业务请求之后,包括:监听中心从密钥管理服务器中获取第一会话密钥。

[0048] 上述监听节点根据获取的第一会话密钥和第二会话密钥对第一用户的浏览器和第二用户的浏览器之间的媒体流进行监听之前,还包括:在第二用户为被叫时,监听节点接收第一用户的信令服务器转发的来自于第二用户的浏览器的业务请求;监听节点将接收的第二用户的浏览器的业务请求转发给第一用户的浏览器,以建立第一用户的浏览器和第二用户的浏览器之间的媒体流传输。

[0049] 上述监听节点将接收的第二用户的浏览器的业务请求转发给第一用户的浏览器之前,包括:监听中心从密钥管理服务器中获取第二会话密钥。

[0050] 上述监听节点将接收的第二用户的浏览器的业务请求转发给第一用户的浏览器之后,包括:监听中心从密钥管理服务器中获取第一会话密钥。

[0051] 根据本发明的另一个方面,提供了一种浏览器的通讯监听装置,位于主叫浏览器和被叫浏览器之间新增的监听节点中,包括:获取模块,用于获取第一会话密钥和第二会话密钥,其中,第一会话密钥为第一用户与监听节点的会话密钥,第二会话密钥为第二用户与监听节点的会话密钥;监听模块,用于根据获取的第一会话密钥和第二会话密钥对第一用户的浏览器和第二用户的浏览器之间的媒体流进行监听。

[0052] 上述获取模块包括:第一发送单元,用于向密钥管理服务器发送密钥生成信息,其中,密钥生成信息携带有生成第一会话密钥和第二会话密钥所需要的信息;第一获取单元,用于获取密钥管理服务器生成的第一会话密钥和第二会话密钥。

[0053] 上述获取模块,包括:接收单元,用于接收第一用户和第二用户的信令服务器上报的信息;第二发送单元,用于将上报的信息发送给密钥管理服务器,其中,上报的信息为密钥管理服务器生成第一会话密钥和第二会话密钥的依据;第二获取单元,用于获取密钥管理服务器生成的第一会话密钥和第二会话密钥。

[0054] 通过本发明,采用新增的监听节点根据获取的第一用户与监控节点的会话密钥以及第二用户与监控节点的会话密钥对第一用户的浏览器和第二用户的浏览器之间的媒体流进行监听的技术手段,解决了相关技术中,不能对两个浏览器的通讯进行监听等技术问题,从而实现了对浏览器之间的通讯内容进行监听的效果。

附图说明

[0055] 此处所说明的附图用来提供对本发明的进一步理解,构成本申请的一部分,本发明的示意性实施例及其说明用于解释本发明,并不构成对本发明的不当限定。在附图中:

[0056] 图1为根据相关技术的RTCWeb的架构图;

[0057] 图2为根据相关技术的MIKEY-TICKET中定义的三个密钥协商交互流程示意图;

[0058] 图3为根据本发明实施例的浏览器的通讯监听方法的流程图;

[0059] 图4为根据本发明实施例的浏览器的通讯监听装置的结构框图;

[0060] 图5为根据本发明优选实施例的浏览器的通讯监听装置的结构框图;

[0061] 图6为根据本发明实施例的基于实时通讯浏览器监听系统的架构示意图;

[0062] 图7为根据本发明实施例的基于实时通讯浏览器监听系统的架构密钥协商交换流

程示意图；

[0063] 图8为根据本发明实施例的基于实时通讯浏览器监听系统实现方式设置监听流程示意图；

[0064] 图9为根据本发明实施例的基于实时通讯浏览器监听系统实现方式主叫监听流程示意图；

[0065] 图10为根据本发明实施例的基于实时通讯浏览器监听系统实现方式被叫监听流程示意图。

具体实施方式

[0066] 下文中将参考附图并结合实施例来详细说明本发明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

[0067] 考虑到相关技术浏览器间媒体面传递会话密钥不能监听即不能对两个浏览器的通讯进行监听等技术问题，以下实施例提供了相应的对媒体流进行监听的解决方案。具体如下：

[0068] 实施例1

[0069] 本实施例提供的通讯监听方案通过在主叫浏览器和被叫浏览器之间新增的监听节点实现。图3为根据本发明实施例的浏览器的通讯监听方法的流程图。如图3所示，该方法包括：

[0070] 步骤S302，监听节点获取第一会话密钥和第二会话密钥，其中，第一会话密钥为第一用户与监听节点的会话密钥，第二会话密钥为第二用户与监听节点的会话密钥；

[0071] 步骤S304，监听节点根据获取的第一会话密钥和第二会话密钥对第一用户的浏览器和第二用户的浏览器之间的媒体流进行监听。

[0072] 无论浏览器间的传输的是否为媒体流，均可以通过上述处理步骤对浏览器间的通信内容进行监控，尤其适用于媒体流的监控。由于上述处理步骤采用新增的监听节点根据获取的第一用户与监控节点的会话密钥以及第二用户与监控节点的会话密钥对第一用户的浏览器和第二用户的浏览器之间的媒体流进行监听，因此。可以解决不能对两个浏览器的通讯进行监听等技术问题，实现了对浏览器之间的通讯内容进行监听。

[0073] 上述监听节点获取第一会话密钥和第二会话密钥的方式有多种，例如可以通过向密钥管理服务器发送请求实现，也可以通过监听用户的信令服务器上报的内容实现。

[0074] 对于前一种处理方式，可以采用以下过程实现：监听节点向密钥管理服务器发送密钥生成信息，其中，密钥生成信息携带有生成第一会话密钥和第二会话密钥所需要的信息；监听节点获取密钥管理服务器生成的第一会话密钥和第二会话密钥。此时上述生成第一会话密钥和第二会话密钥所需要的信息可以包括但不限于：第一用户的标识、第二用户的标识和监听节点的标识。对于后一种处理方式，可以采用以下处理过程实现：监听节点接收第一用户和第二用户的信令服务器上报的信息；监听节点将上报的信息发送给密钥管理服务器，其中，上报的信息为密钥管理服务器生成第一会话密钥和第二会话密钥的依据；监听节点获取密钥管理服务器生成的第一会话密钥和第二会话密钥。

[0075] 在本实施例中，当上述第一用户为主叫时，在监听节点根据获取的第一会话密钥和第二会话密钥对第一用户的浏览器和第二用户的浏览器之间的媒体流进行监听之前，可

以包括以下处理过程：监听节点接收第一用户的信令服务器转发的来自于第一用户的浏览器的业务请求；监听节点将业务请求经由第二用户的信令服务器转发给第二用户的浏览器，以建立第一用户的浏览器和第二用户的浏览器之间的媒体流传输。

[0076] 在本实施例中，在监听节点接收第一用户的信令服务器转发的来自于第一用户的浏览器的业务请求之后，监听中心需要从密钥管理服务器中获取第一会话密钥。

[0077] 对于第一用户为主叫，在第二用户为被叫时，相应地流程为：监听节点接收第一用户的信令服务器转发的来自于第二用户的浏览器的业务请求；监听节点将接收的第二用户的浏览器的业务请求转发给第一用户的浏览器，以建立第一用户的浏览器和第二用户的浏览器之间的媒体流传输。此时，监听节点将接收的第二用户的浏览器的业务请求转发给第一用户的浏览器之前，监听中心需要从密钥管理服务器中获取第二会话密钥。监听节点将接收的第二用户的浏览器的业务请求转发给第一用户的浏览器之后，包括：监听中心从密钥管理服务器中获取第一会话密钥。

[0078] 在本实施例中还提供了一种浏览器的通讯监听装置，该装置位于主叫浏览器和被叫浏览器之间新增的监听节点中，用于实现上述实施例及优选实施方式，已经进行过说明的不再赘述，下面对该装置中涉及到的模块进行说明。如以下所使用的，术语“模块”可以实现预定功能的软件和/或硬件的组合。尽管以下实施例所描述的装置较佳地以软件来实现，但是硬件，或者软件和硬件的组合的实现也是可能并被构想的。图4为根据本发明实施例的浏览器的通讯监听装置的结构框图。如图4所示，该装置包括：

[0079] 获取模块40，连接至监听模块42，用于获取第一会话密钥和第二会话密钥，其中，第一会话密钥为第一用户与监听节点的会话密钥，第二会话密钥为第二用户与监听节点的会话密钥；

[0080] 监听模块42，用于根据获取的第一会话密钥和第二会话密钥对第一用户的浏览器和第二用户的浏览器之间的媒体流进行监听。

[0081] 通过上述处理模块实现的功能，同样可以解决不能对两个浏览器的通讯进行监听等技术问题，实现了对浏览器之间的通讯内容进行监听。详见上述方法实施例中的描述，此处不再赘述。

[0082] 如图5所示，获取模块40包括：第一发送单元400，用于向密钥管理服务器发送密钥生成信息，其中，密钥生成信息携带有生成第一会话密钥和第二会话密钥所需要的信息；第一获取单元402，用于获取密钥管理服务器生成的第一会话密钥和第二会话密钥。

[0083] 如图5所示，上述获取模块40还可以包括：接收单元404，用于接收第一用户和第二用户的信令服务器上报的信息；第二发送单元406，用于将上报的信息发送给密钥管理服务器，其中，上报的信息为密钥管理服务器生成第一会话密钥和第二会话密钥的依据；第二获取单元408，用于获取密钥管理服务器生成的第一会话密钥和第二会话密钥。

[0084] 实施例2

[0085] 本实施例的目的在于解决现有监听技术媒体面传递会话密钥不能监听的问题。为了解决上述问题，本实施例提出了一种实时通讯浏览器监听方法，包括：

[0086] 监听中心，作为实时通讯浏览器一种浏览器节点，设置用户为监听对象，将监听状态保存在被监听用户的信令服务器中，当被监听用户的信令服务器发现被监听用户触发业务，将业务转发到监听中心，监听中心代替发起业务主叫，向被叫发起相同的业务，同时监

听中心携带监听用户的监听状态、监听中心标识以及主被叫标识到密钥管理服务器，密钥管理服务器根据收到信息计算出监听服务器与主叫侧的会话密钥，并重新计算出新的票证，其中包含监听服务器与被叫侧会话密钥。

[0087] 本实施例还提供一种实时通讯浏览器监听系统，包括：密钥管理服务器，监听设备，其中：

[0088] 相对于实时通讯浏览器系统增加了监听中心和密钥管理服务器，监听中心类似一个浏览器与用户的信令服务器相连，同样采用HTTP/Socket与信令服务器通讯，其主要功能就是监听中心向信令服务器设置用户的监听状态，所述监听状态包含监听中心标识和用户被监听的状态，同时信令服务器还增加了当用户触发业务时，将转发呼叫业务到监听中心或者向监听中心汇报用户的行为（比如：注册等），监听中心能够监听信令服务器的汇报，或者代替主叫向被叫重新发起呼叫业务。同时监听中心与密钥管理服务器相连，监听中心在收到转发呼叫时，携带主叫和被叫标识，以及用于认证的票据和监听中心标识和监听标识到密钥管理服务器获取主叫到监听中心的会话密钥和重新生成新的票据，密钥管理服务器根据携带的参数生成主叫到监听中心的会话密钥，所述会话密钥由被叫标识根据密钥生成器生成，密钥管理服务器则根据主叫标识或者监听中心标识与被叫标识生成新的票据，密钥管理中心将获取的会话密钥和新的票据传送到监听中心，监听中心使用的会话密钥加解密主叫到监听中心的媒体流，监听中心还将新生成的票据发送到被叫，被叫通过被叫标识向密钥管理服务器获得监听中心到被叫侧的会话密钥。

[0089] 实施例3

[0090] 本实施例的基于实时通讯浏览器合法监听方法及系统，本实施例的核心网思想是：监听中心，作为实时通讯浏览器一种浏览器节点，设置用户为监听对象，将监听状态保存在被监听用户的信令服务器中，当被监听用户的信令服务器发现被监听用户触发业务，将业务转发到监听中心，监听中心代替发起业务主叫，向被叫发起相同的业务，同时监听中心携带监听用户的监听状态、监听中心标识以及主被叫标识到密钥管理服务器，密钥管理服务器根据收到信息计算出监听服务器与主叫侧的会话密钥，并重新计算出新的票证，其中包含监听服务器与被叫侧会话密钥。

[0091] 如图6所示，本实施例提供的实时通讯浏览器监听系统，相对于相关技术中的实时通讯浏览器系统增加了监听中心64和密钥管理服务器66，监听中心64（可以为浏览器）类似一个浏览器与用户的信令服务器62和信令服务器68相连，同样采用HTTP/Socket与信令服务器62或信令服务器68通讯，其主要功能就是监听中心64向信令服务器62或信令服务器68设置用户的监听状态，所述监听状态包含监听中心标识和用户被监听的状态，同时信令服务器62或信令服务器68还增加了当用户触发业务时，将转发呼叫业务到监听中心64或者向监听中心64汇报用户的行为（比如：注册等），监听中心64能够监听信令服务器68的汇报，或者代替主叫（在本实施例中为浏览器60）向被叫（在本实施例中为浏览器70）重新发起呼叫业务。同时监听中心64与密钥管理服务器66相连，监听中心在收到转发呼叫时，携带主叫和被叫标识，以及用于认证的票据和监听中心标识和监听标识到密钥管理服务器66获取主叫到监听中心的会话密钥和重新生成新的票据，密钥管理服务器66根据携带的参数生成主叫到监听中心的会话密钥，所述会话密钥由被叫标识根据密钥生成器生成，密钥管理服务器66则根据主叫标识或者监听中心标识与被叫标识生成新的票据，密钥管理服务器66将获取

的会话密钥和新的票据传送到监听中心64，监听中心64使用的会话密钥加解密主叫到监听中心的媒体流，监听中心64还将新生成的票据发送到被叫，被叫通过被叫标识向密钥管理服务器66获得监听中心到被叫侧的会话密钥。

[0092] 如图7所示，本实施例中的基于实时通讯浏览器监听系统的架构密钥协商交换流程包括：

[0093] 步骤S702、步骤S704、和步骤S706与背景技术图2中的步骤1,2和3描述一致；

[0094] 步骤S708，监听中心还携带监听中心标识和监听号码到密钥管理，

[0095] 步骤S710，和背景技术中图2中的步骤5一致，密钥管理服务器向监听中心发送了监听中心到主叫的密钥和新产生的票据；

[0096] 步骤S712，与背景技术中图2的步骤3一致；

[0097] 步骤S714和S716与背景技术中的S708和S710描述一致；

[0098] 步骤S718和步骤S720与背景技术中图2的步骤6描述一致。因此相对于现有技术，密钥管理服务器能够识别监听中心，给监听中心下发会话密钥和产生新的票据，监听中心代替主叫重新发起了一次票据请求。

[0099] 为了方便说明，以下的实施例以监听中心将用户A设置为监听对象。

[0100] 如图8所示，本实施例基于实时通讯浏览器监听系统实现方式设置监听流程：

[0101] 步骤S802，监听中心操作人员在监听中心操作台上设置用户A的标识为监听对象；

[0102] 步骤S804，监听中心通过设置监听对象消息向用户A的信令服务器设置监听对象，所述消息携带监听中心号码和用户A的标识，所述监听中心通过用户A的标识发现用户A的信令服务器，所述用户A的信令服务器完成监听设置后，向监听中心响应设置监听对象成功；

[0103] 步骤S806，用户A的信令服务器认证监听中心为合法监听中心，保存监听中心标识，并将用户A标识为监听对象；

[0104] 步骤S808，监听中心设置监听对象成功后，可选地向密钥管理服务器获取标识A对应的密钥，所述消息携带监听中心标识，所述密钥管理服务器根据A的标识和监听中心的标识产生票据和密钥，所述密钥管理服务器讲产生的票据和密钥发送到监听中心；

[0105] 步骤S810，监听中心保存监听对象A的票据和密钥。

[0106] 如图9所示，本实施例基于实时通讯浏览器监听系统实现方式主叫监听流程：

[0107] 步骤S902，用户A的浏览器携带用户A和被叫号码标识B按照图7步骤S702和S704向密钥管理服务器获取密钥和票据；

[0108] 步骤S904，用户A的浏览器向用户A的信令服务器发起业务请求，所述消息携带被叫号码B和票据；

[0109] 步骤S906，用户A的信令服务器检查到用户A被设置为监听对象，根据保存的监听中心号码将所述业务请求转发到监听中心，所述消息携带被叫号码B和票据；

[0110] 步骤S908，监听中心按照图7中步骤S708和步骤S710向密钥管理中心获取用户A到监听中心的会话密钥，以及密钥管理服务器根据所述用户A标识或者监听中心标识和被叫标识产生新的票据，监听中心保存会话密钥；

[0111] 步骤S910，监听中心根据被叫用户B的标识向用户B的信令服务器发起业务请求，所述消息携带被叫用户B的标识和新产生的票据；

[0112] 步骤S912,用户B的信令服务器向用户的浏览器转发业务请求,所述消息携带被叫用户B的标识和新产生的票据;

[0113] 步骤S914,用户B的浏览器按照图7中的S714和步骤S716向密钥管理服务器获取监听中心到用户B的浏览器的会话密钥;

[0114] 步骤S916-S922,用户B同意本次会话后,用户B的浏览器通过用户B的信令服务器,监听中心、用户A的信令服务器向用户A的浏览器回送业务响应消息,所述监听中心收到业务响应消息后将两段媒体进行关联,并同时实现监听。

[0115] 至此,在不影响业务的情况下,用户A实现了合法监听的主叫业务。

[0116] 如图10所示,本实施例基于实时通讯浏览器监听系统实现方式被叫监听流程:

[0117] 步骤S1002,用户B的浏览器携带用户B和被叫号码标识A按照图7步骤S702和步骤S704向密钥管理服务器获取密钥和票据;

[0118] 步骤S1004,用户B的浏览器向用户B的信令服务器发起业务请求,所述消息携带被叫号码A和票据;

[0119] 步骤S1006,用户B的信令服务器根据被叫号码A路由到用户A的信令服务器,所述消息携带被叫号码A和票据;

[0120] 步骤S1008,用户A的信令服务器检查到用户A被设置为监听对象,根据保存的监听中心号码将所述业务请求转发到监听中心,所述消息携带被叫号码A和票据;

[0121] 步骤S1010,监听中心按照图7中步骤S708和步骤S710向密钥管理中心获取用户B到监听中心的会话密钥,以及密钥管理服务器根据所述用户B标识或者监听中心标识和被叫标识A产生新的票据,监听中心保存会话密钥;

[0122] 步骤S1012,监听中心根据被叫用户A的标识向用户A的信令服务器发起业务请求,所述消息携带被叫用户A的标识和新产生的票据;

[0123] 步骤S1014,用户A的信令服务器向用户的浏览器转发业务请求,所述消息携带被叫用户A的标识和新产生的票据;

[0124] 步骤S1016,用户A的浏览器按照图7中的步骤S714和S716向密钥管理服务器获取监听中心到用户A的浏览器的会话密钥;

[0125] 步骤S1018-步骤S1026,用户A同意本次会话后,用户A的浏览器通过用户A的信令服务器,监听中心、用户B的信令服务器向用户B的浏览器回送业务响应消息,所述监听中心收到业务响应消息后将两段媒体进行关联,并同时实现监听。

[0126] 至此,在不影响业务的情况下,用户A实现了合法监听的被叫业务。

[0127] 在另外一个实施例中,还提供了一种软件,该软件用于执行上述实施例及优选实施方式中描述的技术方案。

[0128] 在另外一个实施例中,还提供了一种存储介质,该存储介质中存储有上述软件,该存储介质包括但不限于:光盘、软盘、硬盘、可擦写存储器等。

[0129] 显然,本领域的技术人员应该明白,上述的本发明的各模块或各步骤可以用通用的计算装置来实现,它们可以集中在单个的计算装置上,或者分布在多个计算装置所组成的网络上,可选地,它们可以用计算装置可执行的程序代码来实现,从而,可以将它们存储在存储装置中由计算装置来执行,并且在某些情况下,可以以不同于此处的顺序执行所示出或描述的步骤,或者将它们分别制作成各个集成电路模块,或者将它们中的多个模块或

步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。
[0130] 以上仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

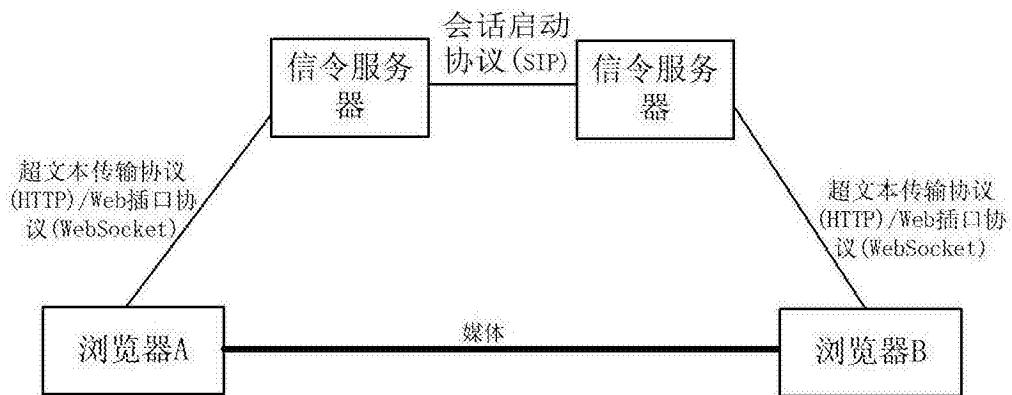


图1

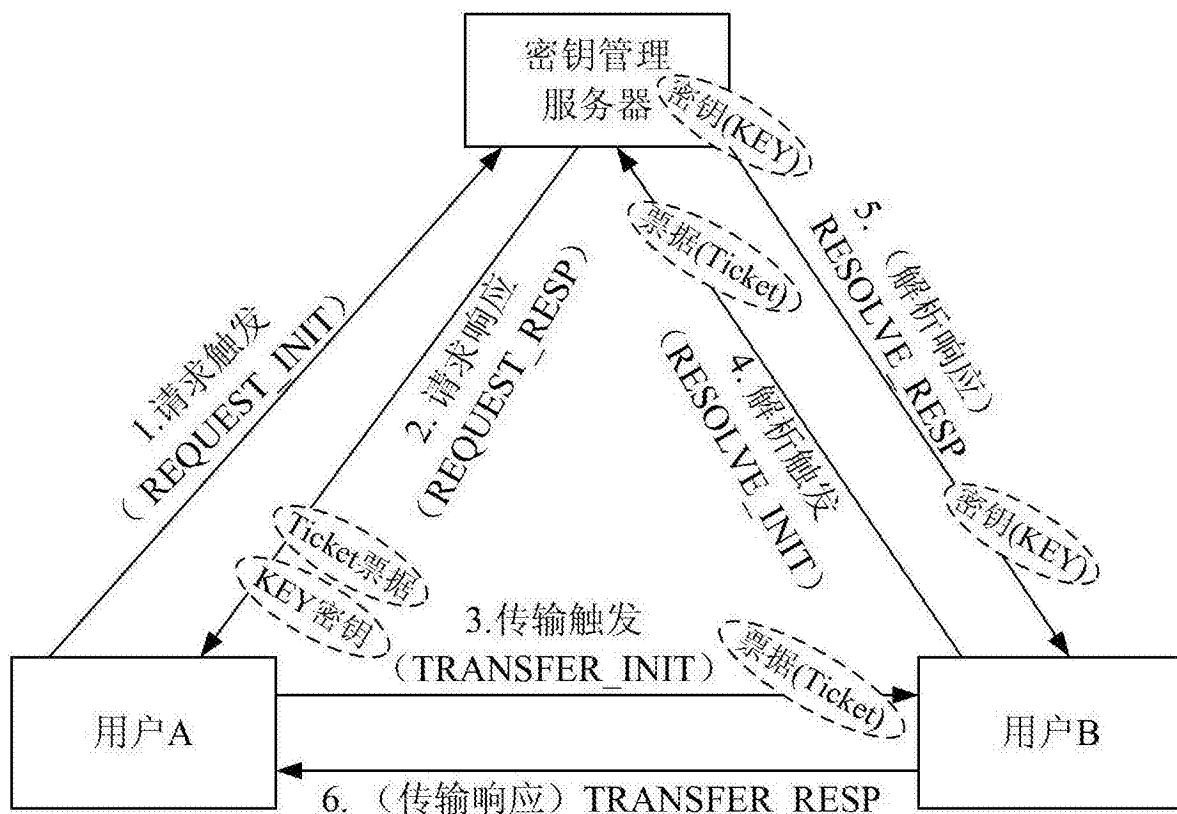


图2

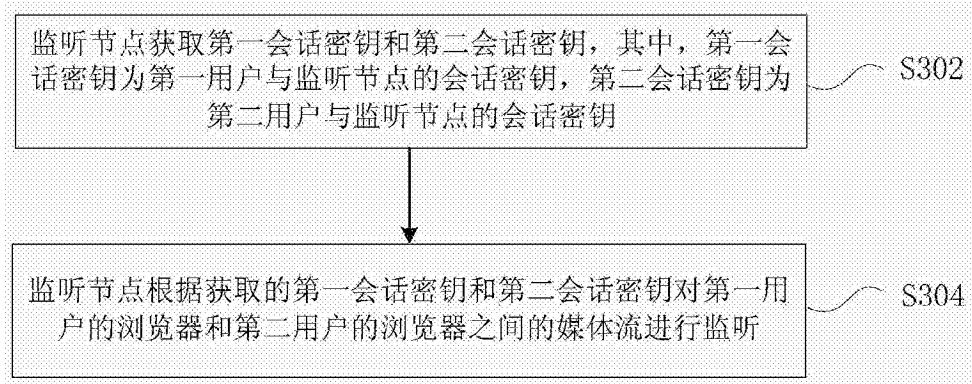


图3

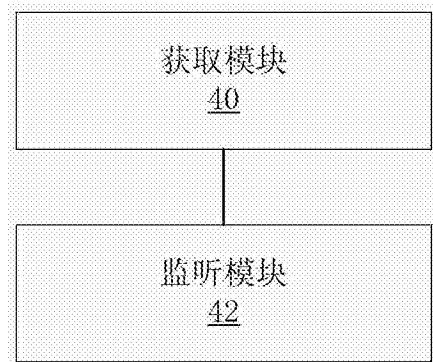


图4

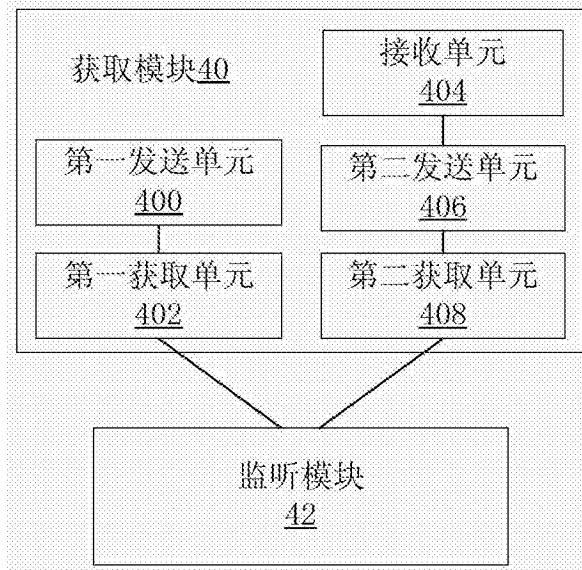


图5

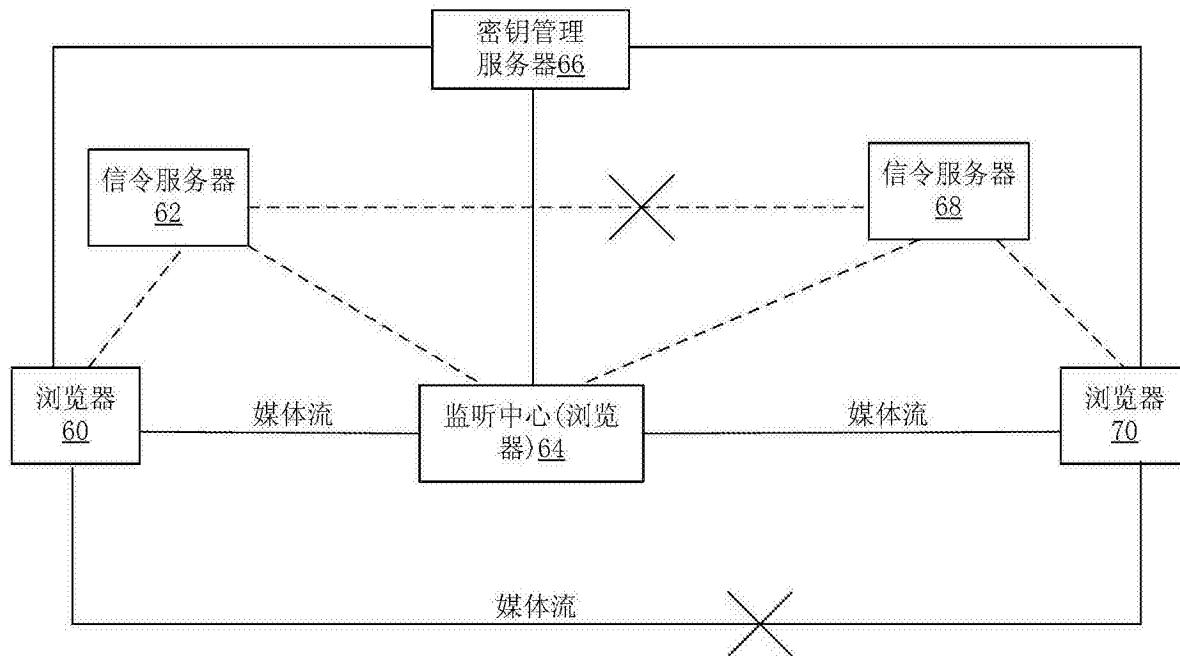


图6

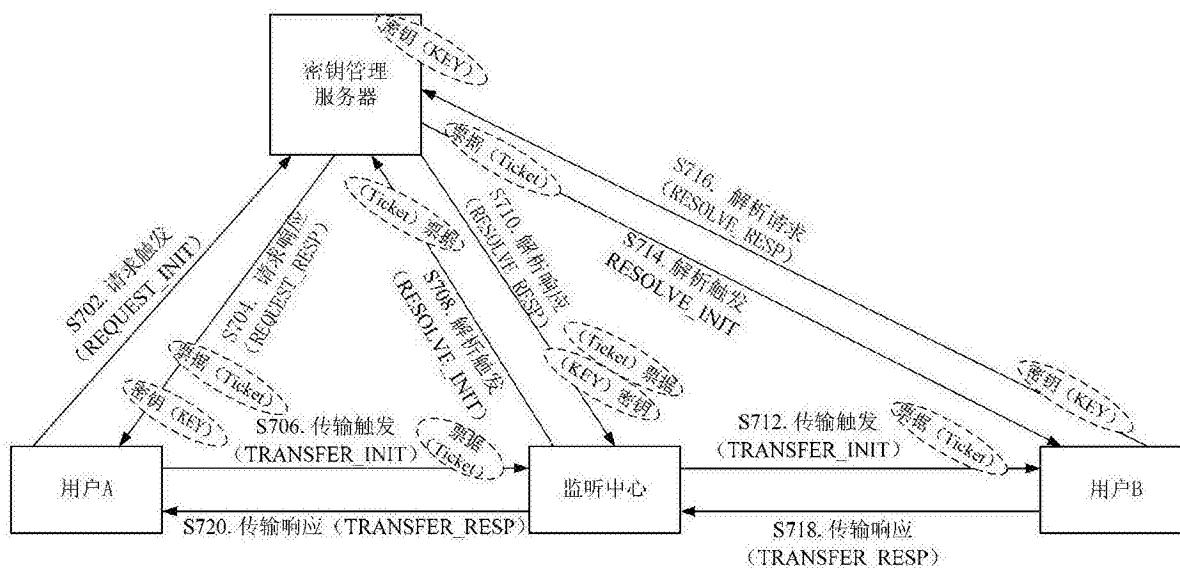


图7

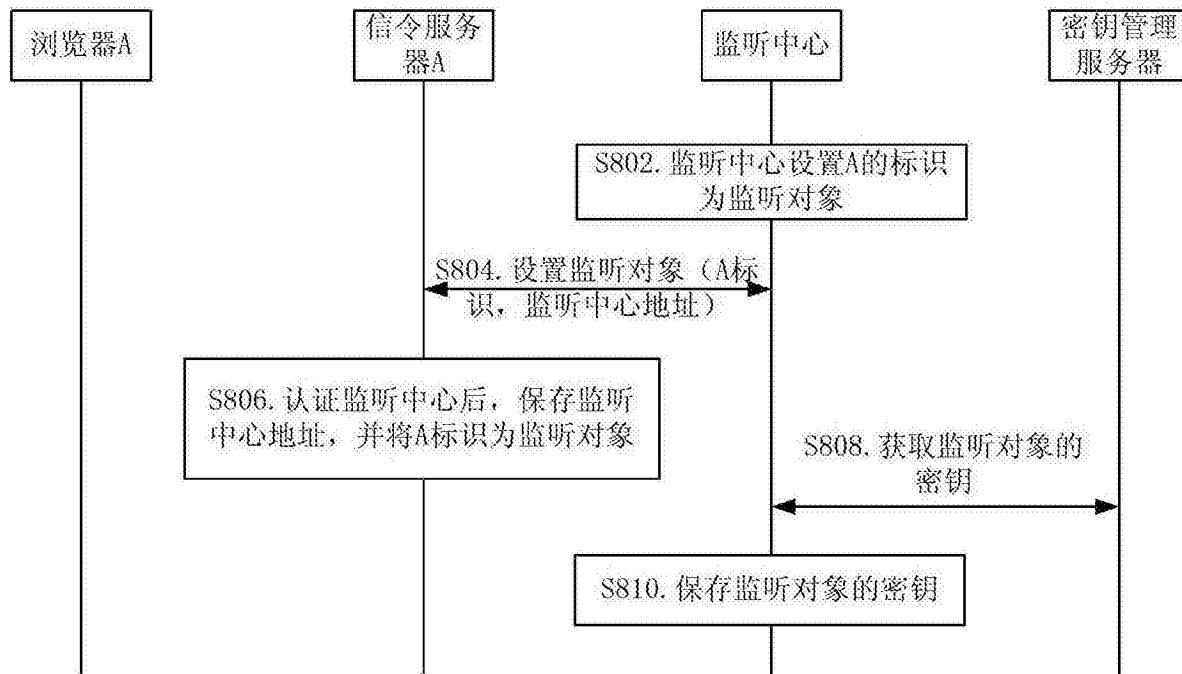


图8

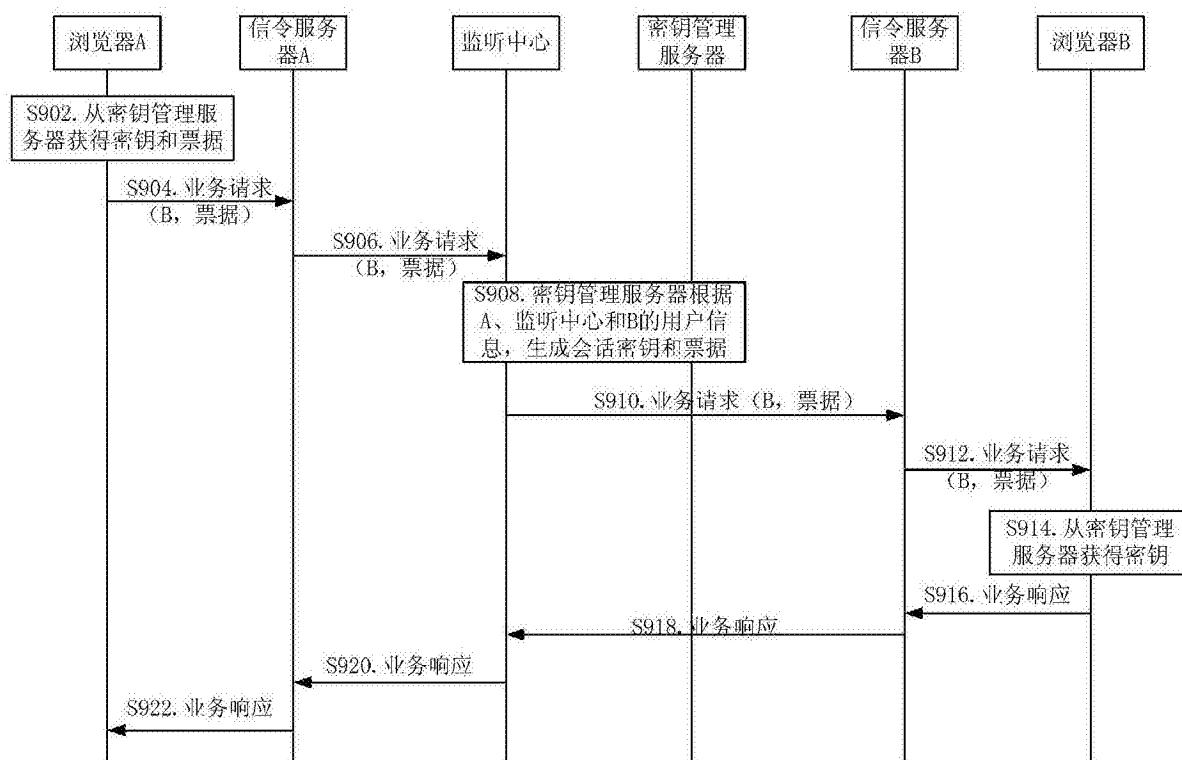


图9

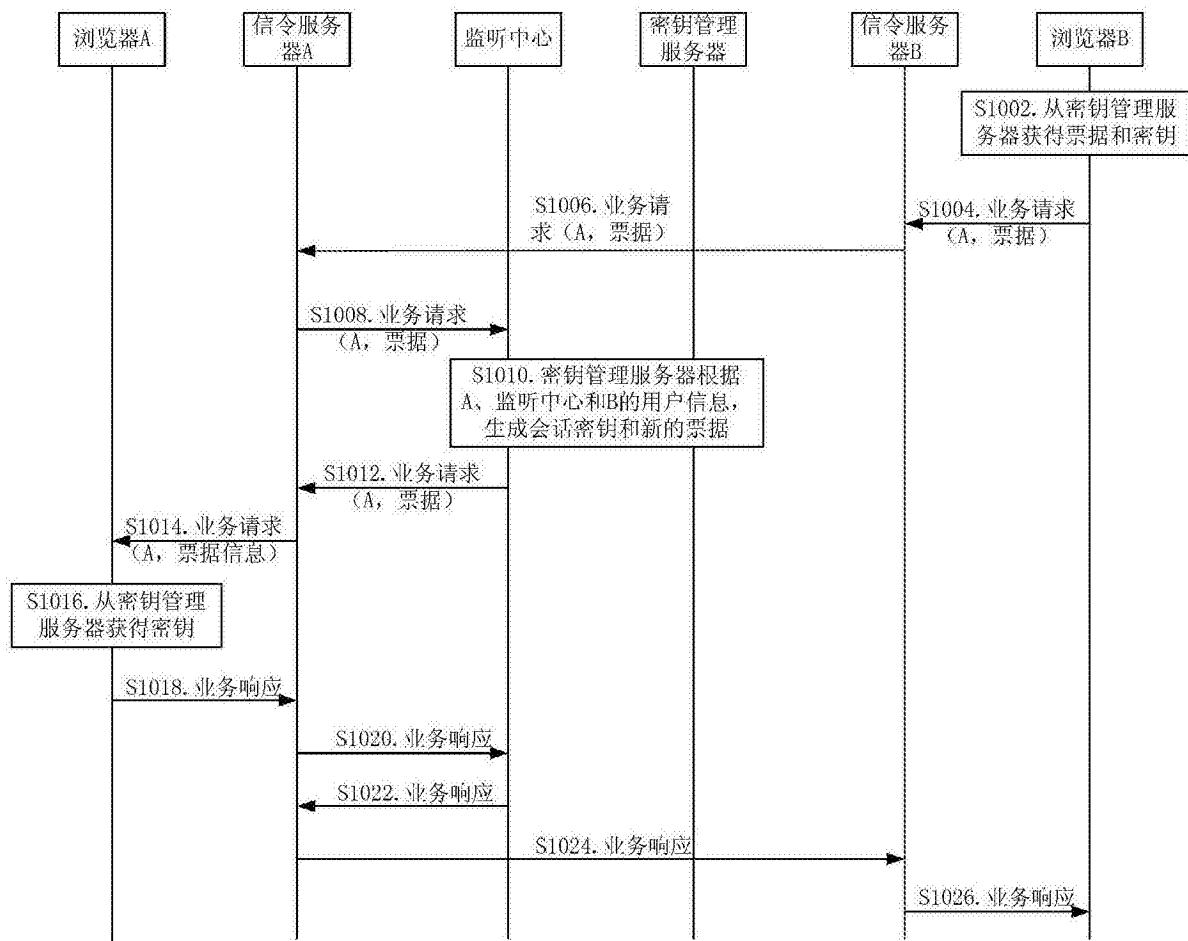


图10