(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 103795966 B
(45)授权公告日 2017.12.26

(21)申请号 201410018109.8

(22)申请日 2014.01.15

(65)同一申请的已公布的文献号
申请公布号 CN 103795966 A

(43)申请公布日 2014.05.14

(73)专利权人 北京明朝万达科技股份有限公司
地址 100097 北京市海淀区蓝靛厂南路25号嘉友国际大厦北区二层

(72)发明人 赵海洋 高百善 喻波 何晋昊 王志海 王志华

(51)Int.Cl.
H04N 7/15(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 1859081 A,2006.11.08,
CN 102497581 A,2012.06.13,
CN 101958907 A,2011.01.26,
CN 101094394 A,2007.12.26,
CN 102833246 A,2012.12.19,
US 2002002674 A1,2002.01.03,

审查员 程时文

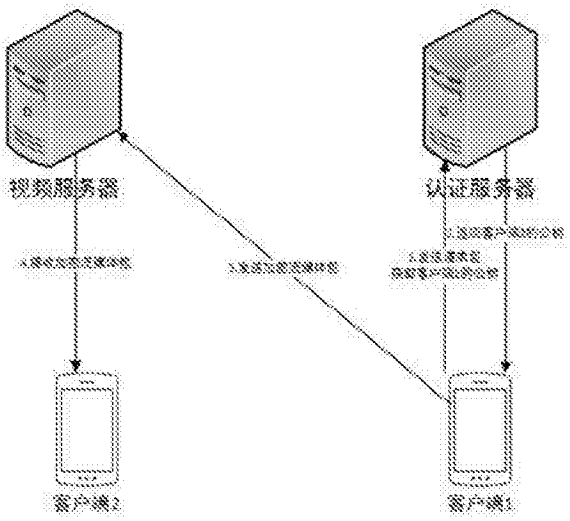
权利要求书2页 说明书5页 附图4页

(54)发明名称

一种基于数字证书的安全视频通话实现方法及系统

(57)摘要

本发明公开了一种基于数字证书的安全视频通话实现方法和系统，该系统包括：发送客户端，接收客户端，认证服务器，视频服务器；其中，发送客户端向认证服务器发送获取视频加密公钥的请求，所述认证服务器接收到所述请求后，向发送客户端返回信息，所述发送客户端接收到所述返回信息后，确认该返回信息是否正确，如果不正确，则结束本次视频通话，否则，所述发送客户端对本地流媒体数据进行加密，并将加密后的数据发送到视频服务器，所述视频服务器接收所述加密后的数据后转发至接收客户端，所述接收客户端对接收到的所述流媒体数据进行解密并显示，通过本发明，保证了视频通话内容的安全。



CN 103795966 B

1.一种基于数字证书的安全视频通话实现方法，该方法包括如下步骤：

1)发送客户端向认证服务器发送获取视频加密公钥的请求；

2)所述认证服务器接收到所述请求后，向发送客户端返回信息；

3)所述发送客户端接收到所述返回信息后，确认该返回信息是否正确，如果正确则跳至步骤4)，否则，跳至步骤8)；

4)所述发送客户端对本地流媒体数据进行对称和/或非对称加密，并将加密后的数据发送到视频服务器；

5)所述视频服务器接收所述加密后的数据后转发至接收客户端；

6)所述接收客户端对接收到的所述流媒体数据进行对称和/或非对称解密并显示；

7)判断视频通话是否结束，如果否，跳转至步骤4)，否则跳至步骤8)；

8)视频通话结束；

其中，所述步骤2)中所述认证服务器接收到所述请求后，判断该请求是否为合法请求，如果是则向发送客户端返回视频加密公钥，否则返回错误信息；

所述步骤4)中所述发送客户端对本地流媒体数据进行对称和/或非对称加密的具体步骤为：开启视频会话线程，随机生成对称密钥，使用该对称密钥将本地流媒体数据进行加密，同时使用所述返回信息中的公钥对所述对称密钥进行加密，并将所述加密后的对称密钥及流媒体数据发送到所述视频服务器。

2.根据权利要求1所述的方法，所述加密公钥为接收客户端的公钥。

3.根据权利要求1所述的方法，所述步骤6)中所述接收客户端对接收到的所述流媒体数据进行对称和/或非对称解密并显示的具体步骤为：

接收客户端接收到加密的流媒体数据及对称密钥后，首先使用私钥将加密的对称密钥进行解密，之后接收客户端使用解密后的对称密钥，将加密的流媒体数据进行解密，最后显示给用户。

4.一种基于数字证书的安全视频通话实现系统，该系统包括：发送客户端，接收客户端，认证服务器，视频服务器；

其中，发送客户端向认证服务器发送获取视频加密公钥的请求，所述认证服务器接收到所述请求后，判断该请求是否为合法请求，如果是则向发送客户端返回视频加密公钥，否则返回错误信息，所述发送客户端接收到返回信息后，确认该返回信息是否正确，如果不正确，则结束本次视频通话，否则，所述发送客户端对本地流媒体数据进行对称和/或非对称加密，并将 加密后的数据发送到视频服务器，所述视频服务器接收所述加密后的数据后转发至接收客户端，所述接收客户端对接收到的所述流媒体数据进行对称和/或非对称解密并显示；

其中，所述发送客户端在每完成一次向所述视频服务器发送加密数据后，判断视频通话是否结束，如果是，结束本次视频通话，否则，准备下一次向所述视频服务器发送数据；

所述发送客户端对本地流媒体数据进行对称和/或非对称加密的具体步骤为：

开启视频会话线程，随机生成对称密钥，使用该对称密钥将本地流媒体数据进行加密，同时使用所述返回信息中的公钥对所述对称密钥进行加密，并将所述加密后的对称密钥及流媒体数据发送到所述视频服务器。

5.根据权利要求4所述的系统，所述加密公钥为接收客户端的公钥。

6.根据权利要求4所述的系统，所述接收客户端对接收到的所述流媒体数据进行对称和/或非对称解密并显示的具体步骤为：

接收客户端接收到加密的流媒体数据及对称密钥后，首先使用私钥将加密的对称密钥进行解密，之后接收客户端使用解密后的对称密钥，将加密的流媒体数据进行解密，最后显示给用户。

一种基于数字证书的安全视频通话实现方法及系统

技术领域

[0001] 本发明涉及一种通信领域，尤其涉及安全视频通话的方法和系统。

背景技术

[0002] 缩略语和关键术语定义

[0003] PKI:Public Key Infrastructure即“公钥基础设施”，是一种遵循标准的利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范。

[0004] SSL:Secure Socket Layer即“安全套接层协议”，可以在Internet上提供秘密性传输。其目标是保证两个应用间通信的保密性和可靠性，可在服务器端和用户端同时实现支持。

[0005] OpenSSL：为网络通信提供安全及数据完整性的一种安全协议，囊括了主要的密码算法、常用的密钥和证书封装管理功能以及SSL协议，并提供了丰富的应用程序供测试或其它目的使用。

[0006] 随着移动终端的不断普及，以及4G时代的到来，网络通讯技术必将进入一个新的时代。企业发展也将进入全信息化时代。伴随而来的将是越来越多的电话会议，视频会议。就个人而言，与亲友间的联系也将被视频电话所取代，因为视频通讯有着廉价、实时性高、方便快捷的特点。

[0007] 在人们不断享受高科技技术所带来的视觉享受以及成本降低的同时，视频通话所产生的安全问题也将接踵而至。

[0008] 目前软件市场中，各种加密软件也是应有尽有：手机通话可以被加密、文件传输可以被加密，但是很多厂商却很难做到或没有想到将视频通话时的视频进行加密，所以视频通话加密技术必将会为信息传递的可靠性及安全性提供新的保障。

[0009] 目前手机软件市场中视频聊天软件多种多样，但是大多数视频软件只是在登录时进行简单的用户名及密码认证，一旦认证通过即可进行视频聊天，但是在聊天过程中所发送的时时视频图像却鲜有软件进行加密处理，即使有加密处理也是非常简单的加解密，此时如果有黑客在传输过程中拦截视频信息的话很容易会被泄密，没有达到真正的加密、防泄密效果。

[0010] 比如悠米(UM)视频聊天软件的安全性与个人隐私方面，采用用户名与密码登录的第四代密码保护机制；并沿用了即时通讯软件一贯采取的“黑名单”与“我的好友”，可拒绝陌生人视频邀请与开启免打扰模式，杜绝恶意视频邀请。

[0011] 图1-2展示了现有技术中的视频通话技术，图1展示了现有技术中视频通话的系统架构，图2展示了现有技术中视频通话的方法流程。

[0012] 现有视频通话技术中，视频通话系统主要包括视频通话服务器，发送客户端和接收客户端。视频通话服务器完成发送客户端与接收客户端之间视频数据的传送，发送客户端实现用户视频数据的采集和发送，并实现发送客户端用户身份的简单认证，比如通过用户名和密码；接收客户端从视频通话服务器接收视频数据，并显示给接收客户端用户，并实

现对接收客户端用户身份的简单认证，比如通过用户名和密码进行认证。

[0013] 现有视频通话技术中，视频的通话的流程如下：

[0014] 1）客户端连接\重新连接视频服务器；

[0015] 2）如果连接\重新连接不成功，跳至步骤1），否则跳至步骤3）；

[0016] 3）如果连接\重新连接成功，输入\重新输入用户名和密码；

[0017] 4）判断用户名和密码是否正确，如果不正确则跳至步骤3），否则，如果是发送用户跳至步骤51），如果是接收用户跳至步骤61）；

[0018] 51）发起视频聊天；

[0019] 52）跳至步骤7）；

[0020] 61）收到视频聊天申请；

[0021] 62）判断是否“我的好友”发起，如果是，跳至步骤63），否则跳至步骤65）；

[0022] 63）开始视频聊天；

[0023] 64）跳至步骤7）；

[0024] 65）如果是黑名单用户，跳至步骤7），否则跳至步骤66）；

[0025] 66）是否允许接收陌生人发起的视频请求，如果是，跳至步骤63），否则跳至步骤7）；

[0026] 7）视频通话结束。

[0027] 根据上述现有技术的视频通话，由于仅进行用户名及密码的认证方式，用户名密码认证方式是最简单的也是最普遍的认证方式，一旦认证通过后，用户进行视频通话传输时将不再进行加密操作，在视频传输过程中很容易被黑客截取网络中传输的视频资料，一些重要的以及一些包含隐私的视频资料将被泄密。

发明内容

[0028] 为了解决目前存在的视频传输安全问题，本发明考虑通过密钥认证方式，保证视频通话可靠性、安全性。从而从根本上解决视频传输过程中引起的泄密等安全问题。

[0029] 为解决上述技术问题，本发明提出了一种基于数字证书的安全视频通话实现方法，该方法包括如下步骤：

[0030] 1）发送客户端向认证服务器发送获取视频加密公钥的请求；

[0031] 2）所述认证服务器接收到所述请求后，向发送客户端返回信息；

[0032] 3）所述发送客户端接收到所述返回信息后，确认该返回信息是否正确，如果正确则跳至步骤4），否则，跳至步骤8）；

[0033] 4）所述发送客户端对本地流媒体数据进行加密，并将加密后的数据发送到视频服务器；

[0034] 5）所述视频服务器接收所述加密后的数据后转发至接收客户端；

[0035] 6）所述接收客户端对接收到的所述流媒体数据进行解密并显示；

[0036] 7）判断视频通话是否结束，如果否，跳转至步骤4），否则跳至步骤8）；

[0037] 8）视频通话结束。

[0038] 进一步，所述步骤2）中所述认证服务器接收到所述请求后，判断该请求是否为合法请求，如果是则向发送客户端返回视频加密公钥，否则返回错误信息。

[0039] 进一步，所述加密公钥为接收客户端的公钥。

[0040] 进一步，所述步骤4)中所述发送客户端对本地流媒体数据进行加密，并将加密后的数据发送到所述视频服务器的具体步骤为：

[0041] 开启视频会话线程，随机生成对称密钥，使用该对称密钥将本地流媒体数据进行加密，同时使用所述返回信息中的公钥对所述对称密钥进行加密，并将所述加密后的对称密钥及流媒体数据发送到所述视频服务器。

[0042] 进一步，所述步骤6)中所述接收客户端对接收到的所述流媒体数据进行解密并显示的具体步骤为：

[0043] 接收客户端接收到加密的流媒体数据及对称密钥后，首先使用私钥将加密的对称密钥进行解密，之后接收客户端使用解密后的对称密钥，将加密的流媒体数据进行解密，最后显示给用户。

[0044] 为解决上述技术问题，本发明提出了一种基于数字证书的安全视频通话实现系统，该系统包括：发送客户端，接收客户端，认证服务器，视频服务器；

[0045] 其中，发送客户端向认证服务器发送获取视频加密公钥的请求，所述认证服务器接收到所述请求后，向发送客户端返回信息，所述发送客户端接收到所述返回信息后，确认该返回信息是否正确，如果不正确，则结束本次视频通话，否则，所述发送客户端对本地流媒体数据进行加密，并将加密后的数据发送到视频服务器，所述视频服务器接收所述加密后的数据后转发至接收客户端，所述接收客户端对接收到的所述流媒体数据进行解密并显示。

[0046] 其中，所述发送客户端在每完成一次向所述视频服务器发送加密数据后，判断视频通话是否结束，如果是，结束本次视频通话，否则，准备下一次向所述视频服务器发送数据。

[0047] 进一步，所述认证服务器接收到所述请求后，判断该请求是否为合法请求，如果是则向发送客户端返回视频加密公钥，否则返回错误信息。

[0048] 进一步，所述加密公钥为接收客户端的公钥。

[0049] 进一步，所述发送客户端对本地流媒体数据进行加密，并将加密后的数据发送到所述视频服务器的具体步骤为：

[0050] 开启视频会话线程，随机生成对称密钥，使用该对称密钥将本地流媒体数据进行加密，同时使用所述返回信息中的公钥对所述对称密钥进行加密，并将所述加密后的对称密钥及流媒体数据发送到所述视频服务器。

[0051] 进一步，所述接收客户端对接收到的所述流媒体数据进行解密并显示的具体步骤为：

[0052] 接收客户端接收到加密的流媒体数据及对称密钥后，首先使用私钥将加密的对称密钥进行解密，之后接收客户端使用解密后的对称密钥，将加密的流媒体数据进行解密，最后显示给用户。

[0053] 通过本发明，可以有效预防视频通话中的数据被非法截取后从而导致的泄密情况，发送视频的客户端和接收视频的客户端使用同一公钥，随机生成对称密钥方式，采取一对一的加密技术，双重加密手段，即使装有相同客户端，没有接收者公钥也不会产生泄密。即使视频被非法截取，也不会有泄密情况产生。

[0054] 使用本技术有效提高了视频通话的安全性、可靠性，加密安全系数高、加密稳定性高，降低因视频通话引起的泄密现象，

附图说明

[0055] 图1是现有技术中视频通话的系统架构。

[0056] 图2是现有技术中视频通话的方法流程图。

[0057] 图3是本发明视频通话的整体系统架构图。

[0058] 图4是本发明视频通话的方法流程流程图。

具体实施方式

[0059] 图3是公开了本发明中安全视频通话技术的总体架构图。

[0060] 该安全视频通话系统除了包括现有技术中的发送客户端1、接收客户端2和视频服务器之外，还包括一个认证服务器，用于对客户端用户身份进行认证，以及向发送客户端和接收客户端提供流媒体数据加/解密使用的公钥/私钥，当然也可以从接收客户端2接收接收客户端2的私钥和公钥，并在发送客户端1发起请求时，将接收客户端公钥发送给发送客户端1。

[0061] 当发送客户端1发现有视频传输时，将发送请求发送至认证服务器，获取接收客户端2的公钥；

[0062] 认证服务器收到请求信息后，将接收客户端公钥返回给发送客户端1；

[0063] 发送客户端1收到认证服务器返回的接收客户端2的公钥后，随机生成对称密钥对流媒体数据进行加密，并使用接收客户端公钥将对称密钥进行加密，并发送到视频服务器；

[0064] 接收客户端2接收到带有公钥加密对称密钥及使用对称密钥加密的流媒体数据后，使用自己的私钥对加密的对称密钥进行解密，并使用解密后的对称密钥对加密的流媒体数据进行解密。

[0065] 其中，所述发送客户端1在每完成一次向所述视频服务器发送加密数据后，判断视频通话是否结束，如果是，结束本次视频通话，否则，准备下一次向所述视频服务器发送数据。

[0066] 如图4所示，其展示了本发明安全视频通话的方法流程图。

[0067] 1)发送客户端开始视频聊天后，向视频服务器发送获取视频接收客户端公钥的请求；

[0068] 2)视频服务器接收到请求后，判断其合法性，并将结果返回到发送客户端，如果为合法请求则返回接收客户端公钥，不合法请求则返回错误信息；

[0069] 在视频服务器向发送客户端发送接收客户端公钥的同时，向接收客户端发送私钥；当然也可以在开启视频通话之前，接收客户端已经保存了私钥，并向视频服务器发送了公钥，在发送客户端请求时，由视频服务器发送接收客户端的公钥；

[0070] 3)发送客户端接收到视频服务器的返回信息，确认返回信息是否正确，如果信息正确则正常开启视频会话，如果发现结果不正确，结束本次视频通话；

[0071] 4)发送客户端接收到正确的接收客户端公钥后，开启视频会话线程，随机生成对称密钥，使用随机生成的对称密钥将本地流媒体数据进行加密，同时使用接收客户端公钥

将随机生成的对称密钥进行加密，并将加密后的对称密钥及加密后的流媒体数据发送到视频服务器；

[0072] 5)视频服务器接收到加密的流媒体数据及加密后的对称密钥，转发至接收客户端；

[0073] 6)接收客户端接收到加密的流媒体数据及加密的对称密钥后，首先使用私钥将加密的对称密钥进行解密；

[0074] 7)接收客户端使用解密后的对称密钥，将加密的流媒体数据进行解密，送给用户观看；

[0075] 8)同时判断视频通话是否结束，如果没有结束则跳转至步骤5)，由发送客户端继续发送加密的流媒体数据，否则结束视频通话。

[0076] 所述客户端可以为移动终端，笔记本电脑，PDA，PC机等各种可实现网络通信的设备。

[0077] 使用本发明公开的技术方案后，可以有效预防视频通话中的数据被非法截取后从而导致的泄密情况，发送视频的客户端和接收视频的客户端使用同一公钥，随机生成对称密钥方式，采取一对一的加密技术，双重加密手段，即使装有相同客户端，没有接收者公钥也不会产生泄密。即使视频被非法截取，也不会有泄密情况产生。

[0078] 使用本技术有效提高了视频通话的安全性、可靠性，加密安全系数高、加密稳定性高，降低因视频通话引起的泄密现象。

[0079] 以上所述仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内，所作的任何修改、等同替换以及改进等，均应保护在本发明的保护范围之内。

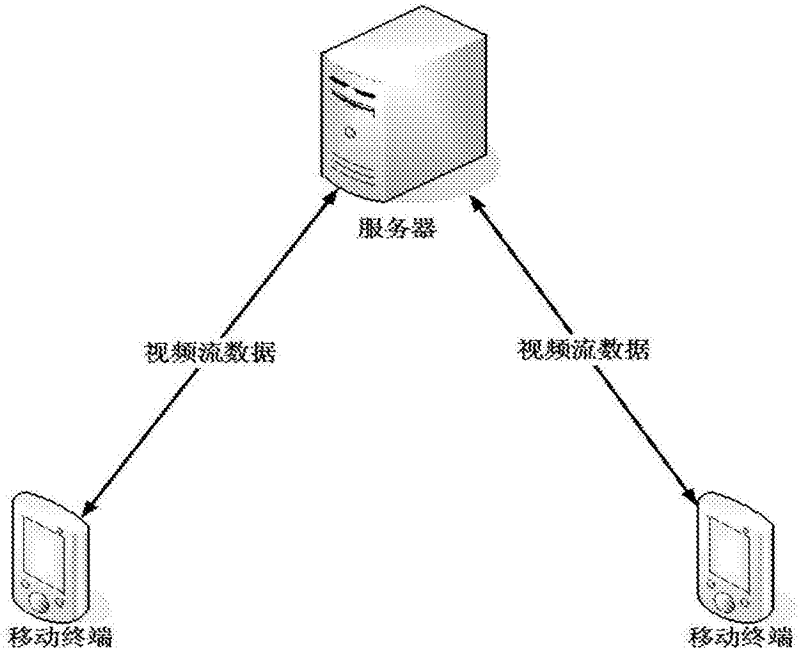


图1

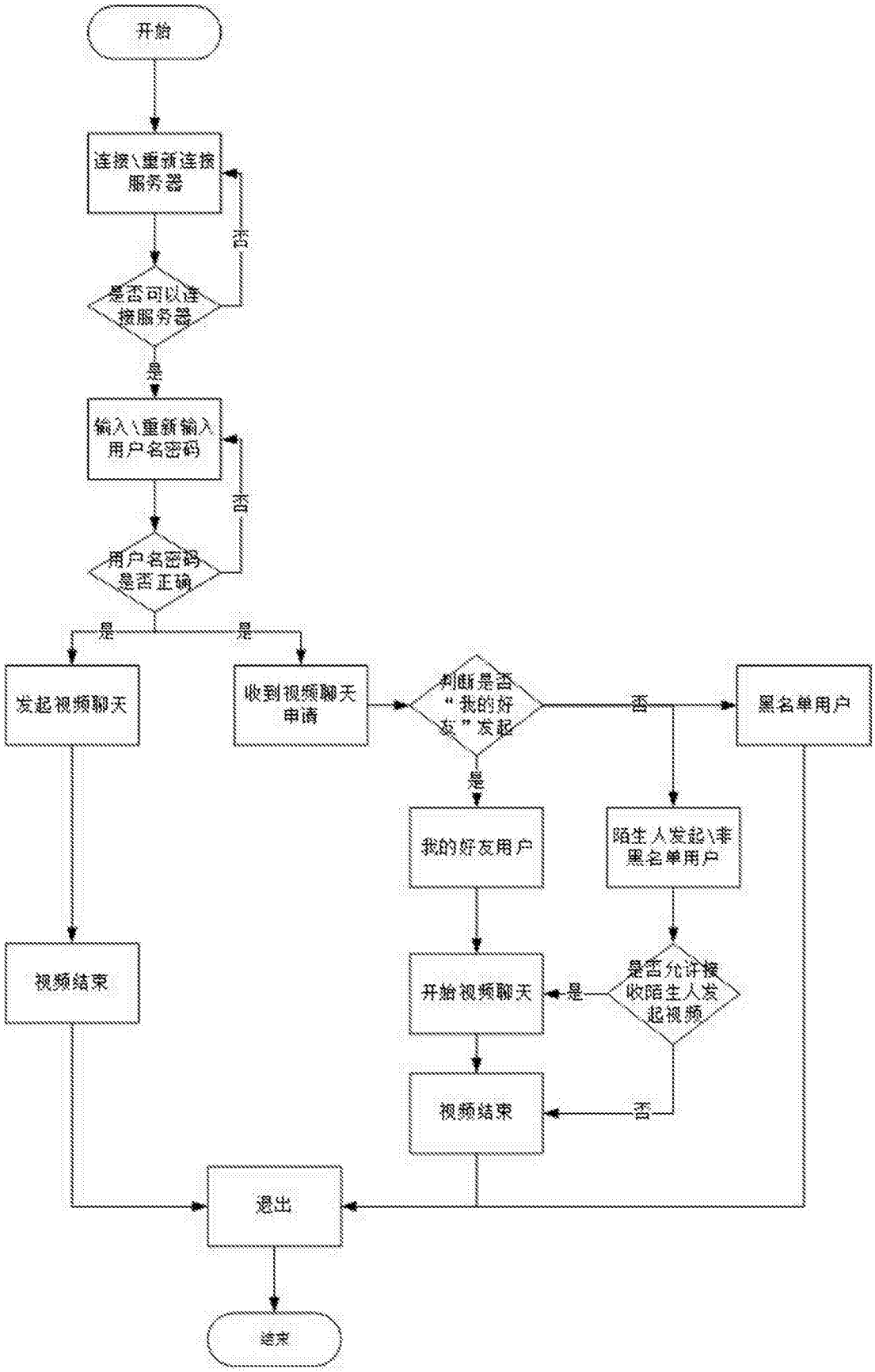

开始
连接\重新连接服务器
否
是否可以连接服务器
是
输入\重新输入用户名密码
否
用户名密码是否正确
是
是
发起视频聊天
收到视频聊天申请
判断是否“我的好友”发起
否
黑名单用户
是
我的好友用户
陌生人发起\非黑名单用户
视频结束
开始视频聊天
是
是否允许接收陌生人发起视频
视频结束
否
退出
结束

图2

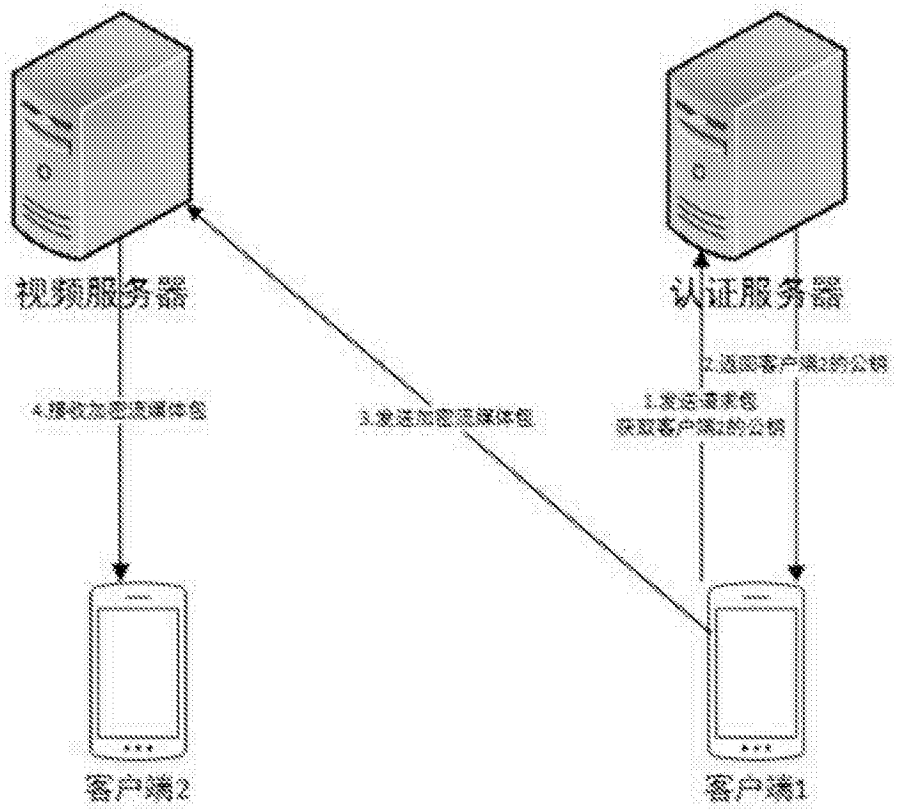


图3

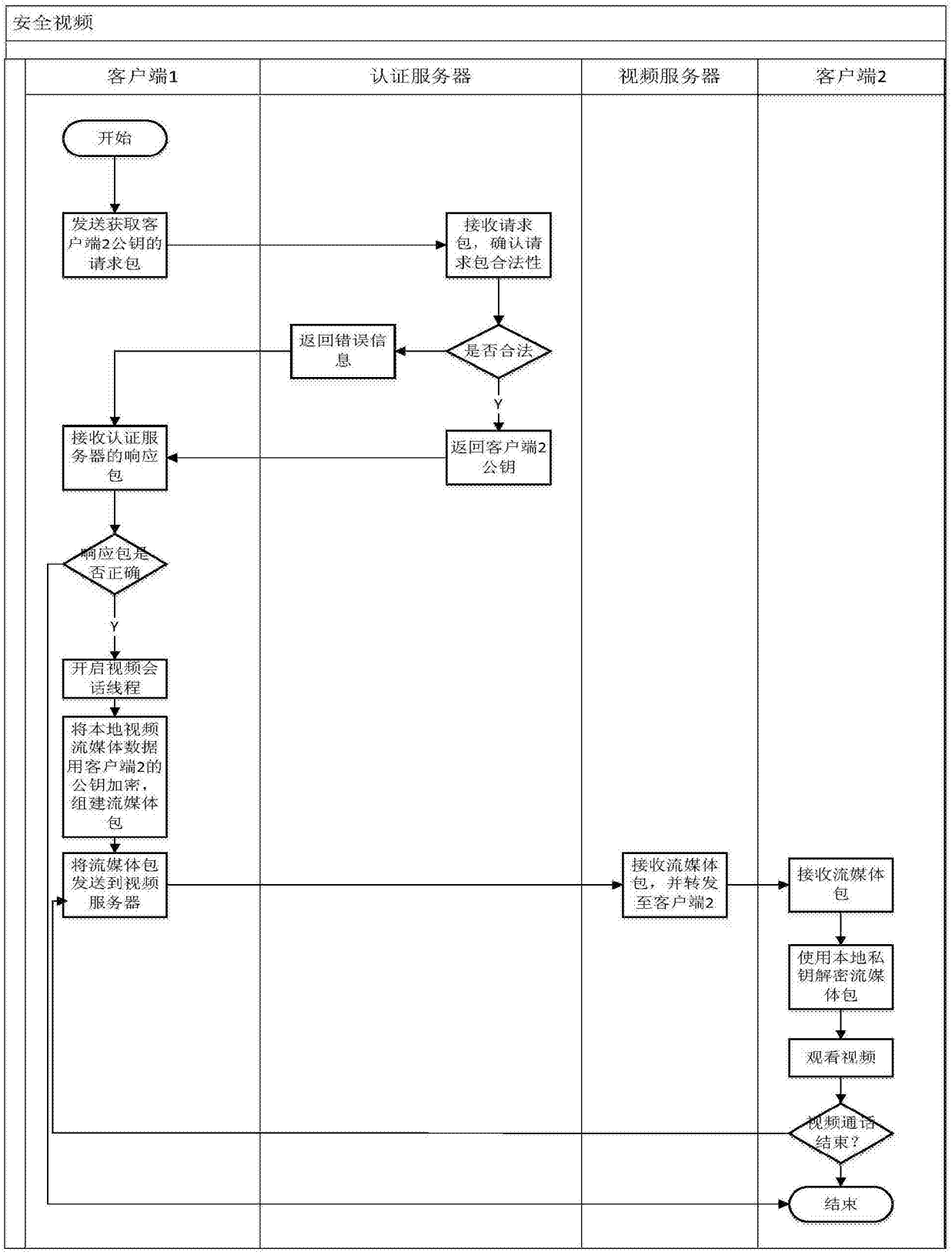

安全视频
客户端1
认证服务器
视频服务器
客户端2
开始
发送获取客户端2公钥的请求包
接收请求包，确认请求包合法性
是否合法
返回错误信息
Y
返回客户端2公钥
接收认证服务器的响应包
响应包是否正确
Y
开启视频会话线程
将本地视频流媒体数据用客户端2的公钥加密，组建流媒体包
将流媒体包发送到视频服务器
接收流媒体包，并转发至客户端2
接收流媒体包
使用本地私钥解密流媒体包
观看视频
视频通话结束？
结束

图4