



(12)发明专利申请

(10)申请公布号 CN 107770219 A

(43)申请公布日 2018.03.06

(21)申请号 201610693802.4

(22)申请日 2016.08.19

(71)申请人 中兴通讯股份有限公司

地址 518057 广东省深圳市南山区高新技术
产业园科技南路中兴通讯大厦

(72)发明人 魏国强

(74)专利代理机构 深圳鼎合诚知识产权代理有
限公司 44281

代理人 江婷 李发兵

(51)Int.Cl.

H04L 29/08(2006.01)

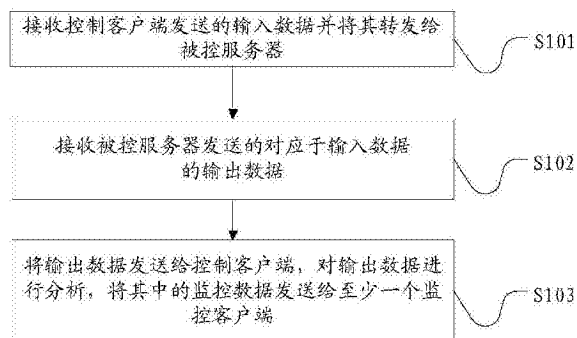
权利要求书2页 说明书9页 附图3页

(54)发明名称

一种视窗窗口的共享方法、网关服务器和系统

(57)摘要

本发明公开了一种视窗窗口的共享方法、网关服务器和系统,利用设置在控制客户端和被控服务器之间的网关服务器,可以接收控制客户端的输入发送给被控服务器以便控制被控服务器操作,接收被控服务器的反馈的输出数据并发给控制至少一个客户端,由于输出数据中存在反映控制客户端对被控服务器的操作的监控数据,将监控数据发送给监控客户端,监控客户端可以实时监控控制客户端对被控服务器的操作,实现将某用户访问被控服务器的操作实时分享给一个或多个用户。相对于现有技术,本发明对远程桌面服务的应用模式没有限制,且在被控服务器上不需要额外安装共享软件,共享过程的传输效率得到了提高,用户体验度更好,具有更高的实用性和更好的适应性。



1. 一种视窗窗口的共享方法,包括:

接收控制客户端发送的输入数据并将其转发给被控服务器;所述输入数据用于控制所述被控服务器的操作;

接收被控服务器发送的对应于所述输入数据的输出数据;

将所述输出数据发送给控制客户端,对所述输出数据进行分析,将其中的监控数据发送给至少一个监控客户端;所述监控数据用于反映所述控制客户端对所述被控服务器的操作。

2. 如权利要求1所述的视窗窗口的共享方法,其特征在于,所述监控数据包括图像数据;所述对所述输出数据进行分析,将其中的监控数据发送给至少一个监控客户端包括:对所述输出数据进行分析,将所述输出数据中的图像数据发送给至少一个监控客户端。

3. 如权利要求1任一项所述视窗窗口的共享方法,其特征在于,还包括:

若接收到所述监控客户端的输入数据,则丢弃所述输入数据。

4. 如权利要求1-3任一项所述视窗窗口的共享方法,其特征在于,在接收控制客户端发送的输入数据并将其转发给被控服务器前,还包括:

接收所述控制客户端输入的第一连接请求,根据所述第一连接请求携带的被控服务器的信息与所述控制客户端进行协议要求的协商;

使用所述控制客户端的第一连接请求携带的信息发起与被控服务器的连接,进行协议要求的协商。

5. 如权利要求1-3任一项所述视窗窗口的共享方法,其特征在于,在对所述输出数据进行分析,将其中的监控数据发送给至少一个监控客户端前,还包括:

接收所述至少一个监控客户端输入的第二连接请求,所述第二连接请求包括用户名;所述用户名包括所述控制客户端和所述被控服务器的会话的会话ID;

根据所述第二连接请求建立与所述监控客户端的连接。

6. 一种网关服务器,包括:

接收模块,用于接收控制客户端发送的输入数据以及接收被控服务器发送的对应于所述输入数据的输出数据;所述输入数据用于控制所述被控服务器的操作;

分析模块,用于对所述输出数据进行分析,识别出其中的监控数据;所述监控数据用于反映所述控制客户端对所述被控服务器的操作;

发送模块,用于将所述输出数据发送给控制客户端,将所述分析模块分析出的监控数据发送给至少一个监控客户端。

7. 如权利要求6所述的网关服务器,其特征在于,所述分析模块用于对所述输出数据进行分析,将其中的图像数据识别出来作为所述监控数据。

8. 如权利要求6所述的网关服务器,其特征在于,所述接收模块还用于接收所述监控客户端的输入数据;所述分析模块还用于对所述接收模块接收的所述输入数据进行分析,识别出所述监控客户端的输入数据,并将其丢弃。

9. 如权利要求6-8任一项所述的网关服务器,其特征在于,还包括连接模块;

所述接收模块还用于在所述发送模块将监控数据发送给至少一个监控客户端前,接收所述至少一个监控客户端输入的第二连接请求,所述第二连接请求包括用户名;所述用户名包括所述控制客户端和所述被控服务器的会话的会话ID;

所述连接模块用于根据所述第二连接请求建立与所述监控客户端的连接。

10. 一种视窗窗口的共享系统, 其特征在于, 包括控制客户端、被控服务器、监控客户端以及如权利要求6-9任一项所述的网关服务器; 所述控制客户端、被控服务器、监控客户端分别与所述网关服务器连接;

所述控制客户端用于向所述网关服务器发送输入数据, 接收所述网关服务器发送的输出数据; 所述输入数据用于控制所述被控服务器的操作;

所述被控服务器用于接收所述网关服务器转发的所述输入数据; 向所述网关服务器发送对应于所述输入数据的输出数据;

所述监控客户端用于接收所述网关服务器的监控数据。

一种视窗窗口的共享方法、网关服务器和系统

技术领域

[0001] 本发明涉及通信领域,具体涉及一种视窗窗口的共享方法、网关服务器和系统。

背景技术

[0002] 桌面共享是在互联网上一种常用的远程交流、协作的方式,能够将一方对于桌面的情况实时传递到远端的另一方。常用的软件有VNC(Virtual Network Computing,虚拟网络计算机)和TeamViewer,其中VNC是点对点的模式,而TeamViewer是通过中心节点转发的模式。中心节点模式可以穿过防火墙,使两个内网客户都可以共享桌面,但是缺点是需要到中心节点注册。国内的QQ软件的共享也是类似的工作模式。至于点对点的VNC,则需要在服务器上运行VNC的服务器软件,并且VNC是通过桌面截屏的方式传输,传输效率没有RDP协议高。

[0003] 此外,Windows系统自带的远程桌面服务上有一个共享(shadow)功能,通常在用户同意的情况下才可以将用户的桌面共享给另外一个用户,或者只有管理员才有权限不经某用户同意共享该用户的桌面。但是无论哪种方式,该共享功能只能在桌面模式下使用,在RemoteApp(windows远程桌面服务的另外一种应用模式)的模式下没有办法进行共享。

发明内容

[0004] 本发明实施例要解决的主要技术问题是,提供一种视窗窗口的共享方法、网关服务器和系统,解决现有技术中需要额外安装共享软件或者远程桌面服务只能在桌面模式下使用共享功能带来的传输效率低,共享功能受远程桌面服务的应用模式限制的问题。

[0005] 为解决上述技术问题,本发明实施例提供一种视窗窗口的共享方法,包括:

[0006] 接收控制客户端发送的输入数据并将其转发给被控服务器;输入数据用于控制被控服务器的操作;

[0007] 接收被控服务器发送的对应于输入数据的输出数据;

[0008] 将输出数据发送给控制客户端,对输出数据进行分析,将其中的监控数据发送给至少一个监控客户端;监控数据用于反映控制客户端对被控服务器的操作。

[0009] 为解决上述技术问题,本发明实施例还提供一种网关服务器,包括:

[0010] 接收模块,用于接收控制客户端发送的输入数据以及接收被控服务器发送的对应于输入数据的输出数据;输入数据用于控制被控服务器的操作;

[0011] 分析模块,用于对输出数据进行分析,识别出其中的监控数据;监控数据用于反映控制客户端对被控服务器的操作;

[0012] 发送模块,用于将输出数据发送给控制客户端,将分析模块分析出的监控数据发送给至少一个监控客户端。

[0013] 为解决上述技术问题,本发明实施例还提供一种视窗窗口的共享系统,包括控制客户端、被控服务器、监控客户端以及如权利要求6-8任一项的网关服务器;控制客户端、被控服务器、监控客户端分别与网关服务器连接;

[0014] 控制客户端用于向网关服务器发送输入数据,接收网关服务器发送的输出数据;输入数据用于控制被控服务器的操作;

[0015] 被控服务器用于接收网关服务器转发的输入数据;向网关服务器发送对应于输入数据的输出数据;

[0016] 监控客户端用于接收网关服务器的监控数据。

[0017] 本发明实施例公开了一种视窗窗口的共享方法、网关服务器和系统,利用设置在控制客户端和被控服务器之间的网关服务器,可以接收控制客户端的输入发送给被控服务器,接收被控服务器的反馈的输出数据并发给控制客户端,由于输入数据是用来控制被控服务器操作的数据,所以本发明实施例的输出数据中必然能存在反映控制客户端对被控服务器的操作的监控数据,再将输出数据中的监控数据发送给监控客户端,监控客户端可以实时监控控制客户端如何控制被控服务器的操作,实现将一个用户访问被控服务器的操作情况实时分享到一个或其他多个用户终端上。现有技术中,虽然远程桌面服务也有共享功能,但是该功能只能在桌面模式下使用,本发明实施例的对远程桌面服务的应用模式没有限制,且在被控服务器上不需要额外安装如VNC等共享软件,只需要Windows自带的远程桌面服务,使用RDP协议传输,传输效率得到了提高,用户体验度更好,此外还提高了对现有资源的有效利用,具有更高的实用性和更好的适应性。

附图说明

[0018] 图1为本发明实施例一提供的一种视窗窗口的共享方法的流程图;

[0019] 图2为本发明实施例二提供的另一种视窗窗口的共享方法的流程图;

[0020] 图3为本发明实施例三提供的一种网关服务器的模块示意图。

具体实施方式

[0021] 下面通过具体实施方式结合附图对本发明作进一步详细说明。

[0022] 实施例一:

[0023] 参见图1,示出了一种视窗窗口的共享方法,可以在用户使用控制客户端远程操控被控服务器的情况下,通过对控制客户端和被控服务端之间传输的数据进行拦截,并对被控服务器向控制客户端反馈的输出数据进行分析,从中识别出能反映控制客户端对被控服务器的操作的监控数据,通过将监控数据发送给监控客户端,可以使得监控客户端实现监控控制客户端对被控服务器的操作,达到在监控客户端上实时监控用户操作的目的。

[0024] 本实施例的视窗窗口的共享方法包括:

[0025] S101、接收控制客户端发送的输入数据并将其转发给被控服务器;输入数据用于控制被控服务器的操作;

[0026] S102、接收被控服务器发送的对应于输入数据的输出数据;

[0027] S103、将输出数据发送给控制客户端,对输出数据进行分析,将其中的监控数据发送给至少一个监控客户端;监控数据用于反映控制客户端对被控服务器的操作。

[0028] 由上述的步骤其实可以得到,在本实施例中,控制客户端是用来对被控服务器进行远程控制的客户端,其功能可以由软件程序来实现,当然,控制客户端也可以是安装了远程控制软件的终端,包括电脑、平板、甚至手机等电子设备。

[0029] 可以预见,为了控制客户端和被控服务器之间的远程控制能实现,被控服务器上也需要安装有与监控客户端对应的实现远程控制的软件。

[0030] 本实施例的上述步骤可以由设置在控制客户端以及被控服务器之间的网关服务器实现,网关服务器分别与控制客户端和被控服务器连接,可以对它们之间传输的数据进行拦截、分析、分流传输。本实施例的控制客户端与被控服务器之间可以基于RDP(Remote Desktop Protocol,远程桌面协议)进行通信。为了控制客户端与被控服务器之间可以正确交流,实现控制客户端对被控服务器的远程控制,控制客户端和被控服务器传输的数据的压缩和解压需要满足协议(RDP)要求。本实施例中,控制客户端和监控客户端是满足RDP协议的客户端。

[0031] 控制客户端可以通过windows自带的远程桌面(mstsc.exe)或RemoteApp模式远程连接到被控服务器上,当然,在本实施例中,也可以采用其他的可行的远程控制的软件实现控制客户端与被控服务器的远程连接,不局限于远程桌面(mstsc.exe)或RemoteApp模式。

[0032] 为了使得控制客户端的输入数据可以发送到被控服务器,并且能接收到被控服务器反馈的输出数据,在S101之前,需要在控制客户端、被控服务器、网关服务器之间进行相应的设置。

[0033] 一般,用户操作的是控制客户端,用户可以通过控制客户端向网关服务器发起连接,控制客户端发起连接的地址是网关服务器的地址。具体的,控制客户端可以向网关服务器发送第一连接请求,第一连接请求中可以携带控制客户端欲控制的被控服务器的信息。

[0034] 所以在本实施例中S101前,还包括:其接收控制客户端的第一连接请求,根据第一连接请求中的信息实现与控制客户端的连接。其中,第一连接请求携带需要控制的被控服务器的相关信息,此相关信息可以帮助网关服务器确定控制客户端需要控制的服务器具体是哪一个,然后根据被控服务器的信息与控制客户端进行相关协议(例如RDP协议)需要的协商,完成控制客户端到网关服务器之间的连接。其中,如果被控服务器设置有登录用户名和登录密码,第一连接请求中可以携带被控服务器的登录用户名和登录密码,便于与被控服务器的连接时,完成被控服务器的解锁。本实施例中,在与控制客户端完成协议协商后,可以使用控制客户端发送的第一连接请求携带的信息发起与被控服务器的连接,并进行相关协议(例如RDP协议)需要的协商,如用户名和登录密码的认证等等。

[0035] 与控制客户端和被控服务器的协议协商过程均完成后,被控服务器就可以输出包含自身当前操作界面的图像数据和其他的协议规定的通道数据如语音数据等给网关服务器,网关服务器接收到这些输出的协议数据后,可以解压这些协议数据,然后按照RDP协议在对这些数据进行压缩,之后将压缩的数据转发到控制客户端上,上述是被控服务器的数据到达控制客户端的过程。控制客户端的数据到达被控服务器的过程类似。

[0036] 其中,可以预见,在被控服务器上可能有多个客户端在使用,也就会造成被控服务器上同时存在多个会话,一般为了对多个会话进行区分,被控服务器上的多个会话均有各自对应的会话ID(SESSION ID),在被控服务器发送给网关服务器的协议数据中也包括会话ID,网关服务器在将被控服务器输出的协议数据解压后,可以将其中的会话ID识别出来并保存,在监控客户端需要接入网关服务器对某一对控制客户端和被控服务器进行监控时,将会话ID作为区别监控对象(区别监控客户端具体连接哪一个会话)的标识。

[0037] 其中,协议协商完成后,控制客户端接收用户通过键盘和鼠标等输入工具的输入,

生成并发送输入数据给网关服务器,被控服务器根据网关服务器转发给自身的输入数据进行相应的操作,然后返回对应的输出数据到网关服务器。

[0038] 可以预见,当监控客户端欲监控控制客户端对被控服务器的操作时,需要先完成与网关服务器的连接。即在S103中网关服务器向监控客户端发送数据之前。还需要接收至少一个监控客户端的第二连接请求,根据第二连接请求携带的信息建立与监控客户端的连接。其中,当监控客户端通过第二连接请求向网关服务器发起连接时,输入的服务器的地址即为网关服务器的地址,连接请求中还包括了监控客户端自身需要监控的会话的会话ID,该会话ID是监控客户端需要监控的控制客户端与被控服务器的会话的会话ID。

[0039] 接收到监控客户端的第二连接请求后,根据会话ID确定监控客户端需要监控的被控服务器具体是哪一个,再根据被控服务器的信息与监控客户端进行相关协议(RDP协议)需要的协商。

[0040] 进一步地,为了避免其他客户端非法连接网关服务器,造成用户的隐私泄露,本实施例中,可以对监控客户端的进行身份认证,认证通过,才完成协议协商。其中,监控客户端可以在第二连接请求中写入自身与网关服务器的认证信息,例如采用令牌作为监控客户端与网关服务器的认证信息。网关服务器根据第二连接请求中的认证信息进行认证,认证通过,则认为监控客户端是合法的监控客户端。

[0041] 其中,网关服务器可以在从第二连接请求中取出会话ID,根据会话ID确定共享的会话的过程之前,先进行上述的认证过程,进一步确保监控客户端的监控行为的合法。

[0042] 在网关服务器与监控客户端的协议协商完成后,当网关服务器接收到被控服务器的输出数据,就可以对其中的监控数据进行识别,发送给监控客户端。

[0043] 可以预见,S102中,被控服务器发送的输出数据中一般包含了图像数据,这些图像数据是由被控服务器根据自身的界面获取到的图像数据,可以准确反映被控服务器在控制客户端的控制下的操作,被控服务器获取图像数据的方式包括但不限于截屏,可以预见,为了在监控客户端和控制客户端上呈现被控服务器的界面,输出数据中的图像数据至少包含一张图片。所以,在S103中,对输出数据进行分析,将其中的监控数据发送给至少一个监控客户端的过程包括:对输出数据进行分析,将输出数据中的图像数据发送给至少一个监控客户端。当然,除了图像数据之外,也可以将其他可以反映控制客户端对被控服务器的操作的数据作为监控数据发送给监控客户端。

[0044] 在本实施例S103中,收到被控服务器的输出数据后,可以先将输出数据发送给控制客户端,再对输出数据进行分析得到图像数据发送给监控客户端;也可以先对输出数据进行分析得到图像数据发送给监控客户端,再将输出数据发送给控制客户端;或者较优的,在网关服务器将输出数据发送给控制客户端的同时,对输出数据进行分析,将其中的监控数据发送给至少一个监控客户端。

[0045] 在本实施例中,监控客户端只是监控控制客户端的操作,因此通常不会有任何输入的要求。但是监控客户端一般也是具有如键盘、鼠标等输入工具的,为了防止监控客户端输入对被控服务器造成影响,以及用户在监控客户端的误操作。在网关服务器上需要对监控客户端的输入进行过滤,即在本实施例中,在网关服务器已经完成与监控客户端的协议协商后,若接收到监控客户端发送的输入数据(包括但不限于键盘输入和鼠标输入),则丢弃该输入数据。

[0046] 采用本实施例的视窗窗口的共享方法,可以接收控制客户端的输入发送给被控服务器,接收被控服务器的反馈的输出数据并发给控制客户端,由于输入数据是用来控制被控服务器操作的数据,所以本发明实施例的输出数据中必然能存在反映控制客户端对被控服务器的操作的监控数据,再将输出数据中的监控数据发送给监控客户端,监控客户端可以实时监控控制客户端如何监控被控服务器,实现将一个用户访问被控服务器的操作情况实时分享到一个或其他多个用户终端上。现有技术中,虽然远程桌面服务也有共享功能,但是该功能只能在桌面模式下使用,本发明实施例的对远程桌面服务的应用模式没有限制,且在被控服务器上不需要安装其他的共享软件,只需要Windows自带的远程桌面服务功能即可,不仅提高了对现有资源的有效利用,还具有更高的实用性和更好的适应性。

[0047] 实施例二:

[0048] 参见图2,本实施例提出了一种视窗窗口的共享方法,在本实施例中,客户端A是监控客户端,客户端B是监控客户端,服务器S是被控服务器,本实施例的视窗窗口的共享方法包括:

[0049] S201、客户端A连接网关服务器G。

[0050] 客户端A是满足RDP协议要求客户端,如Windows系统自带的“远程桌面连接”。客户端A发起连接的地址是网关服务器G的地址。在连接的过程中,客户端A需要向网关服务器告知自身需要控制的服务器S是哪一个,告知的方式可以通过在连接请求中携带服务器S的信息实现。网关服务器G根据服务器S的信息与客户端A进行RDP协议要求的协商。

[0051] 其中,如果远程桌面连接使用的是RemoteApp的模式,就是窗口的共享,否则就是桌面的共享。本实施例的远程桌面连接只是一种示例,并不作为对客户端A的限制。

[0052] S202、网关服务器G连接服务器S。

[0053] 网关服务器G使用客户端A的请求信息发起与服务器S连接,并进行RDP协议要求的协商。如用户名和密码的认证等。

[0054] S203、网关服务器G接收服务器S的输出数据。

[0055] RDP协商过程完毕后,服务器S就会输出图形数据和其他协议规定的通道数据,如语音等。网关服务器G接收这些协议输出数据,然后解压这些协议数据。

[0056] S204、网关服务器G转发输出数据到客户端A。

[0057] 网关服务器再将解压后的数据进行压缩,转发到客户端A上。

[0058] 在这些协议数据中会有会话ID数据,网关服务器G需要保存会话ID数据。由于服务器S上可能会多个客户端使用,会存在多个会话,因此这个会话ID可以作为客户端B监控具体哪个会话的标识。

[0059] S205、网关服务器G接收客户端A的输入数据。

[0060] 服务器S将远程桌面或者RemoteApp呈现给用户后,用户在客户端A上就可以通过鼠标和键盘操作服务器S。客户端A连接的是网关服务器G,网关服务器G接收到客户端的输入数据。

[0061] S206、网关服务器G转发输入数据到服务器G。

[0062] 网关服务器将接收到得输入数据进行压缩,作为一个客户端将数据发到服务器S。

[0063] 以上是网关服务器G正常转发服务器S的输出和客户端A的输入的过程。

[0064] S207、客户端B接入网关服务器G。

[0065] 客户端B也是满足RDP协议要求客户端。客户端B输入连接的服务器地址为网关服务器G的地址,连接的用户名会包含会话ID以及客户端B与网关服务器G的认证信息,如可以采用令牌作为客户端B与网关服务器G的认证信息。认证通过,就认为是合法的监控客户端。并从用户名中取出会话ID,根据会话ID来定位需要共享哪个会话。

[0066] S208、网关服务器G接收服务器S的输出数据。

[0067] 由于已经接入客户端B,网关服务器G需要分析输出数据中那些是图像数据,那些是非图像数据。对于客户端A,全部数据都需要转发过去,流程同S204。

[0068] S209、网关服务器G转发输出数据中的图像数据到客户端B。

[0069] 网关服务器分析出图像数据之后,只将图像输出部分的数据转发到客户端B,这样客户端B就可以看到客户端A的操作情况。

[0070] S210、若网关服务器G接收到客户端B的输入,则丢弃客户端B的输入。

[0071] 客户端B只是监控客户端A的操作,因此通常不会有任何输入的要求。如果有意外的输入,被网关服务器G收到之后,网关服务器G将其丢弃。对于客户端A,所有的输出都需要转发到服务器S。

[0072] 采用本实施例,可以利用设置在控制客户端和被控服务器之间的网关服务器建立控制客户端和被控服务器的远程控制连接,在控制客户端和被控服务器均连接上网关服务器之后,网关服务器可以接收控制客户端的输入并发送给被控服务器,接收被控服务器的输出并发送给控制客户端,由此,实现了控制客户端和被控服务器的远程控制,同时,由于网关服务器接收的被控服务器的输出中含有可以反映被控服务器被控制客户端操作的数据,网关服务器可以将这些数据发送给监控客户端,由监控客户端根据这些数据监控控制客户端对被控服务器的操作。本实施例的方法不受远程桌面连接的应用模式的限制,也无需在应用服务器上另外安装共享软件如VNC等,本实施例方法的适应性和实用性更强。

[0073] 实施例三:

[0074] 参见图3,本实施例提出了一种网关服务器,包括:

[0075] 接收模块31,用于接收控制客户端发送的输入数据以及接收被控服务器发送的对应于输入数据的输出数据;输入数据用于控制被控服务器的操作;

[0076] 分析模块32,用于对输出数据进行分析,识别出其中的监控数据;监控数据用于反映控制客户端对被控服务器的操作;

[0077] 发送模块33,用于将输出数据发送给控制客户端,将分析模块分析出的监控数据发送给至少一个监控客户端。

[0078] 在本实施例中,接收模块31和发送模块33可以由网关服务器中的天线和相应的硬件模块实现,分析模块32可以由网关服务器中的处理器实现。

[0079] 在本实施例中的网关服务器分别与控制客户端和被控服务器连接,可以对控制客户端和被控服务器之间传输的数据进行拦截、分析、分流传输。本实施例的控制客户端与被控服务器之间可以基于RDP(Remote Desktop Protocol,远程桌面协议)进行通信。为了控制客户端与被控服务器之间可以正确交流,实现控制客户端对被控服务器的远程控制,控制客户端和被控服务器传输的数据的压缩和解压需要满足协议(RDP)要求。本实施例中,控制客户端和监控客户端是满足RDP协议的客户端。

[0080] 在本实施例中,控制客户端是用来对被控服务器进行远程控制的客户端,其功能

可以由软件程序来实现,当然,控制客户端也可以是安装了远程控制软件的终端,包括电脑、平板、甚至手机等电子设备。可以预见,为了控制客户端和被控服务器之间的远程控制能实现,被控服务器上也需要安装有与监控客户端对应的实现远程控制的软件。

[0081] 控制客户端可以通过windows自带的远程桌面(mstsc.exe)或RemoteApp模式远程连接到被控服务器上,当然,在本实施例中,也可以采用其他的可行的远程控制的软件实现控制客户端与被控服务器的远程连接,不局限于远程桌面(mstsc.exe)或RemoteApp模式。

[0082] 为了实现网关服务器对控制客户端和被控服务器的数据的接收和发送,需要先建立网关服务器与控制客户端和被控服务器的连接,一般是由控制客户端先向网关服务器发送第一连接请求,第一连接请求中携带了被控服务器的信息。

[0083] 网关服务器的接收模块可以接收第一连接请求,分析模块可以对第一连接请求进行解压,从中去除被控服务器的信息,根据此信息确定控制客户端需要控制的被控服务器具体是哪一个,本实施例的网关服务器还包括连接模块,用于根据被控服务器的相关信息与控制客户端进行相关协议(例如RDP协议)需要的协商,完成控制客户端到网关服务器之间的连接。其中,如果被控服务器设置有登录用户名和登录密码,第一连接请求中可以携带被控服务器的登录用户名和登录密码,便于与被控服务器的连接时,连接模块完成被控服务器的解锁。本实施例中,在与控制客户端完成协议协商后,连接模块可以使用控制客户端发送的第一连接请求携带的信息发起与被控服务器的连接,并进行相关协议(例如RDP协议)需要的协商,如登录用户名和登录密码的认证等等。其中,连接模块发起与被控服务器的连接可以和控制客户端的连接同时进行。

[0084] 网关服务器与控制客户端和被控服务器的协议协商过程均完成后,被控服务器就可以输出包含自身当前操作界面的图像数据和其他的协议规定的通道数据如语音数据等给网关服务器,网关服务器的接收模块31接收到这些输出的协议数据后,分析模块32可以解压这些协议数据,然后按照RDP协议在对这些数据进行压缩,发送模块33后将压缩的数据转发到控制客户端上。

[0085] 可以预见在被控服务器上可能有多个客户端在使用,也就会造成被控服务器上同时存在多个会话,一般为了对多个会话进行区分,被控服务器上的多个会话均有各自对应的会话ID(SESSION ID),在被控服务器发送给网关服务器的协议数据中也包括会话ID,网关服务器的分析模块32在将被控服务器输出的协议数据解压后,可以将其中的会话ID识别出来并保存,在监控客户端需要接入网关服务器对某一对控制客户端和被控服务器进行监控时,连接模块将会话ID作为区别监控对象(区别监控客户端具体连接哪一个会话)的标识。

[0086] 本实施例上述的监控客户端用于向网关服务器发送第二连接请求;第二连接请求包括用户名,用户名包括需要被监控的控制客户端和被控服务器的会话的会话ID;接收网关服务器发送的监控数据;监控数据由网关服务器从被控服务器根发送的输出数据中分析得到,用于反映控制客户端对被控服务器的操作。

[0087] 网关服务器的接收模块31还用于在发送模块31将监控数据发送给至少一个客户端前,接收至少一个监控客户端的第二连接请求。这里的至少一个监控客户端是与网关服务器完成连接的客户端。连接模块还用于根据第二连接请求建立与监控客户端的连接。其中,连接模块可以根据第二连接请求中的会话ID确定监控客户端需要监控的会话具体是哪

一个。

[0088] 进一步地,为了避免其他客户端非法连接网关服务器,造成用户的隐私泄露,本实施例中,网关服务器可以对监控客户端的进行身份认证,认证通过,才完成协议协商。其中,监控客户端可以在第二连接请求中写入自身与网关服务器的认证信息,例如采用令牌作为监控客户端与网关服务器的认证信息。优选地,本实施例的网关服务器还包括认证模块,用于根据第二连接请求携带的认证信息进行认证,认证通过,则认为监控客户端是合法的监控客户端。

[0089] 接收模块31接收的输出数据中一般包含了图像数据,这些图像数据是由被控服务器根据自身的界面获取到的图像数据,可以准确反映被控服务器在控制客户端的控制下的操作。其中,被控服务器获取图像数据的方式包括但不限于截屏。优选的,本实施例的分析模块32用于对输出数据进行分析,将输出数据中的图像数据作为监控数据。当然,除了图像数据之外,也可以将其他可以反映控制客户端对被控服务器的操作的数据作为监控数据发送给监控客户端。

[0090] 此外,在本实施例中,监控客户端只是监控控制客户端的操作,因此通常不会有任何输入的要求。但是监控客户端一般也是具有如键盘、鼠标等输入工具的,为了防止监控客户端输入对被控服务器造成影响,以及用户在监控客户端的误操作。在网关服务器上需要对监控客户端的输入进行过滤。优选的,本实施例的接收模块31还用于接收监控客户端的输入数据;分析模块32还用于对接收模块接收的输入数据进行分析,识别出监控客户端的输入数据,并将其丢弃。

[0091] 在另一实施例中,还提供一种视窗窗口的共享系统,包括控制客户端、被控服务器、监控客户端以及实施例三中的网关服务器;控制客户端、被控服务器、监控客户端分别与网关服务器连接;控制客户端用于向网关服务器发送输入数据,接收网关服务器发送的输出数据;输入数据用于控制被控服务器的操作;被控服务器用于接收网关服务器转发的输入数据;向网关服务器发送对应于输入数据的输出数据;监控客户端用于接收网关服务器的监控数据。

[0092] 采用本实施例,网关服务器在接收到控制客户端的输入数据后,通过发送模块发送给被控服务器,控制被控服务器的操作,被控服务操作完成,反馈输出数据给网关服务器,网关服务器将输出数据发送给控制客户端,将输出数据中的能反映控制客户端对所述被控服务器的操作的监控数据发送给监控客户端,使得监控客户端可以实时看到在控制客户端上显示的被控服务器的界面,实现监控控制客户端对被控服务器的操作的目的,相对于现有技术中使用远程桌面的共享功能实现监控只能在桌面模式下实现的限制,采用本实施例的网关服务器实现监控目的,对于远程桌面服务的应用模式没有要求,在被控服务器上也无需安装其他的共享软件,适用范围更广,实用性更强。

[0093] 显然,本领域的技术人员应该明白,上述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介质(ROM/RAM、磁碟、光盘)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。所以,本发明不限制于任何特定

的硬件和软件结合。

[0094] 以上内容是结合具体的实施方式对本发明所作的进一步详细说明,不能认定本发明的具体实施只局限于这些说明。对于本发明所属技术领域的普通技术人员来说,在不脱离本发明构思的前提下,还可以做出若干简单推演或替换,都应当视为属于本发明的保护范围。

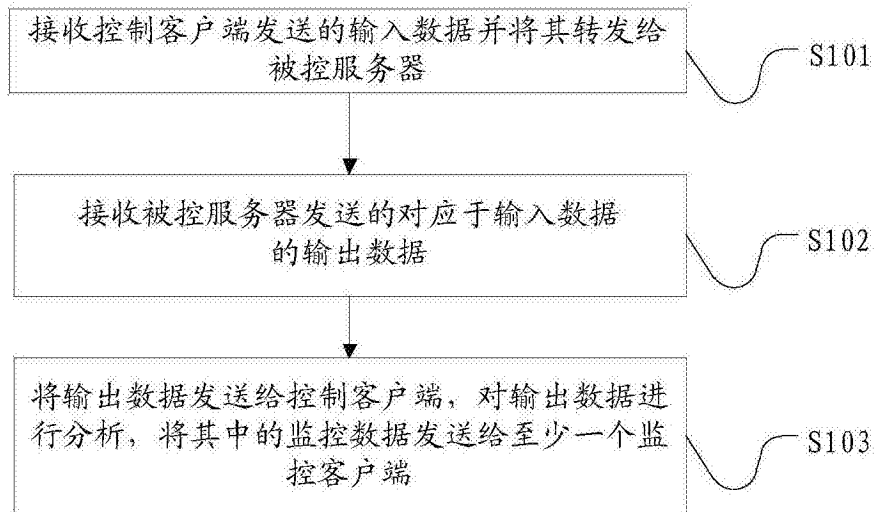


图1

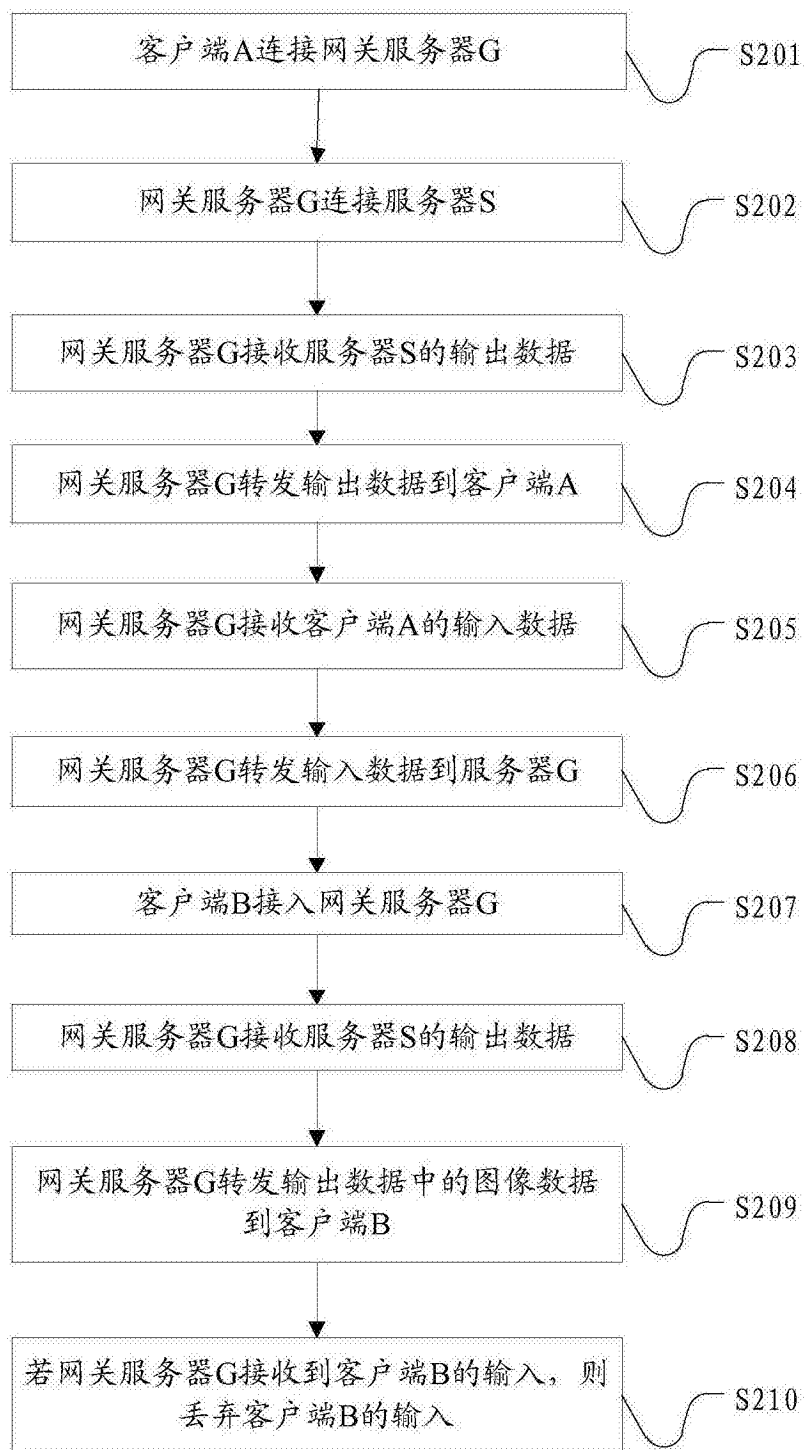


图2



图3