

[12] 发明专利申请公开说明书

[21] 申请号 01132340.X

[43] 公开日 2002 年 6 月 5 日

[11] 公开号 CN 1352429A

[22] 申请日 2001.11.29 [21] 申请号 01132340.X

[71] 申请人 上海复旦光华信息科技股份有限公司
 地址 200437 上海市邯郸路 191 号
 [72] 发明人 张世永 廖志成 皮晓东

[74] 专利代理机构 上海市华诚律师事务所

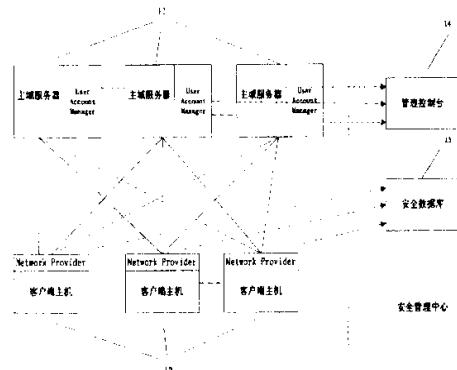
代理人 徐申民

权利要求书 2 页 说明书 5 页 附图页数 3 页

[54] 发明名称 域用户集中授权和管理系统

[57] 摘要

本发明提供一种域用户集中授权和管理系统，该系统包括一个安全管理中心，若干个主域服务器和若干个客户端主机构成，安全管理中心由一个管理控制台和一个安全数据库组成。所述的域用户集中授权和管理系统在主域服务器上安装相应的域管理代理软件后，通过安全管理中心的管理控制台可以对这些主域服务器的进行集中授权和管理。本发明在不改变网络物理结构，不加重网络负担，不加重邮件服务器负担的情况下实现了用户身份认证及授权的集中统一。



权利要求书

1、一种域用户集中授权和管理系统，其特征在于，所述授权管理系统包括一个安全管理中心，若干个主域服务器和若干个客户端主机构成，所述安全管理中心由一个管理控制台和一个安全数据库组成，所述系统在所述主域服务器上安装相应的域管理代理软件后，通过所述安全管理中心的管理控制台对这些主域服务器的进行集中授权和管理。

2、如权利要求 1 所述的系统，其特征在于，所述管理控制台实现对主域服务器的集中授权和管理，包括如下步骤：

- a. 在各个主域服务器上安装域管理代理软件；
- b. 在所述管理控制台上添加各个安装好了域管理代理软件的主域服务器；
- c. 在添加好的主域服务器上再添加各个用户组；
- d. 在所述管理控制台上添加用户基本信息；
- e. 所述用户基本信息被存放到所述安全数据库中；
- f. 所述管理控制台同步将用户基本信息传输到所述主域服务器，与主域服务器的域用户代理进行 socket 通讯；
- g. 所述主域服务器的域用户代理通过用户数据处理函数处理用户基本信息；
- h. 所述客户端主机上用户登录或执行某些被授权的应用。

3、如权利要求 1 所述的方法，在步骤 d 中，所述用户基本信息包括各个应用的用户名、用户口令以及应用所涉及的主域服务器，所添加的用户可以在不同的主域服务器及用户组上有帐号；

4、如权利要求 1 所述的方法，其特征在于，所述安全管理中心上具有一网络服务提供程序，该程序提供客户端用户身份认证的接口和客户端应用程序 SSO 的接口。

5、如权利要求 1 所述的方法，其特征在于，所述域管理代理软件包括两个独立模块，用户数据处理模块和 Socket 通讯模块，在步骤 g 中，所述域管理代理软件处理用户基本信息的流程如下：

- a. 系统启动后，由 Windows NT 服务控制程序启动用户管理服务；
- b. 用户管理服务启动一个用户数据处理部分的主线程，并调用 socket 初始化函数，登记主线程的入口函数地址，socket 初始化程序调用主线程的入口函数，获得一个对应于端口的消息处理函数入口，启动一个 socket 主线程，完成 Socket 的初始化，并绑定监听端口；

c. 当有连接到来时，socket 主线程调用用户数据处理主线程的消息处理函数，要求建立该连接的数据处理子线程；用户数据处理主线程的消息处理函数根据收到的消息建立数据处理子线程，并返回针对该连接的数据处理函数入口；

d. socket 创建一个对应于连接的子线程，接收数据，查询数据处理子线程的状态并调用数据处理函数发送数据，循环直至连接结束。

6、如权利要求 1 所述的方法，其特征在于，所述的管理控制台是一个在 Windows 系列上运行应用程序，实现了统一的管理界面，通过所述的管理界面对用户、用户组、域、应用及其它它们之间的关系进行管理；用户、用户组的全局同步；对用户进行授权。

7、如权利要求 2 所述的方法，其特征在于，所述客户端主机登录主域服务器之前需访问所述安全数据库，从所述安全数据库中得到授权用户的基本信息，所述客户端主机根据从所述安全数据库中得到的用户基本信息发出向所述主域服务器的登录。

说 明 书

域用户集中授权和管理系统

技术领域

本发明涉及身份认证、授权与网络安全的方法，尤其涉及对域用户集中授权和管理的系统。

背景技术

在一个网络集成系统中，对于用户的管理和授权的重要性往往是居于第一位的。如果用户的管理和授权有问题，整个网络将是不安全的，通常会被黑客们突破安全系统中的第一道关卡，发现其他更多的漏洞，导致无法挽回的损失。在比较大的网络集成系统中，通常存在多种类型的机器和操作系统，例如 Windows 95/98、Windows NT Server、Windows 2000 Server 等。同时也会存在多个主域服务器。这时，系统管理员需要管理两个以上的主域服务器以及两个以上的操作系统的用户和组，增加了系统维护费用。随着企业全球化加快，其分支机构地理跨度很大，如何管理这些主域服务器是系统管理员关心的问题。

对于域用户管理，绝大多数的操作人员使用的是 Windows 的域用户管理器，不少系统管理人员感到在使用的时候非常不方便。虽然微软公司正着力在 Windows 的较高版本中改进域用户管理器，至少目前，我们仍然没有一个很理想的管理工具。虽然 Windows 域用户管理器提供了非常友好的界面来帮助操作人员实施用户管理，但其实际效果并不尽人意。如果不能对网络中的用户实施有效的管理，将会给企业造成巨大的浪费。系统管理员迫切需要一种集中的管理模式。

传统域用户管理方法如图 1 所示，如果让其中一台计算机集中管理所有账号，其它计算机依靠它来保证账号安全，这种基于服务器的网络在 Windows NT 中称为域 (Domain)，集中管理账户的计算机称为主域控制器 (Primary Domain Controller, PDC)，域中还可以设置备份域控制器 (Backup Domain Controller, BDC)。只有安装了 Windows NT Server 的计算机才能担当。若是网络设计成域模型，则必须有且只能有一个主域控制器，而且 PDC 必须首先安装。BDC 则不是网络中必须的。

在传统的方案中，管理员很难同时管理多个主域服务器，无法统一对各个普通用户集中授权。各个主域服务器时间可能有所差异，无法同步。由于一个用户可能拥有多个用户帐号，用户可能采用相同的登录口令或强度较低的口令。

发明内容

本发明的主要目的是解决当前 Windows 主域服务器域用户管理中存在的问题，实现当前 Windows 域用户管理技术无法实现的功能，使系统中所有主域服务器中的域用户由域用户管理中心控制台统一控制，极大地增强了域用户管理的有效性和便利性。

本发明的目的是这样实现的，一种域用户集中授权和管理系统，包括一个安全管理中心，若干个主域服务器和若干个客户端主机构成，所述安全管理中心由一个管理控制台和一个安全数据库组成，所述系统在所述主域服务器上安装相应的域管理代理软件后，通过所述安全管理中心的管理控制台 对这些主域服务器进行集中授权和管理，所述的管理控制台是一个在 Windows 系列上运行应用程序，实现了统一的管理界面，通过所述的管理界面 对用户、用户组、域、应用及其它它们之间的关系进行管理；用户、用户组的全局同步； 对用户进行授权。

上述安全管理中心的管理控制台实现 主域服务器的集中授权和管理，包括如下步骤：

- a. 在各个主域服务器上安装域管理代理软件；
- b. 在所述管理控制台上添加各个安装好了域管理代理软件的主域服务器；
- c. 在添加好的主域服务器上再添加各个用户组；
- d. 在所述管理控制台上添加用户基本信息；
- e. 所述用户基本信息被存放到所述安全数据库中；用户基本信息包括各个应用的用户名、用户口令以及应用所涉及的主域服务器，所添加的用户可以在不同的主域服务器及用户组上有帐号；
- f. 所述管理控制台同步将用户基本信息传输到所述主域服务器，与主域服务器的域用户代理进行 socket 通讯；
- g. 所述主域服务器的域用户代理通过用户数据处理函数处理用户基本信息；
- h. 所述客户端主机上用户登录或执行某些被授权的应用，客户端主机登录主域服务器之前需访问所述安全数据库，从所述安全数据库中得到授权用户的基本信息，所述客户端主机根据从所述安全数据库中得到的用户基本信息发出向所述主域服务器的登录。

上述安全管理中心上具有一网络服务提供程序，该程序提供客户端用户身份认证的接口和客户端应用程序 SSO 的接口。

前述的域管理代理软件包括两个独立模块，用户数据处理模块和 Socket 通讯模块，在步骤 g 中，所述域管理代理软件处理用户基本信息的流程如下：

- a. 系统启动后，由 Windows NT 服务控制程序启动用户管理服务；
- b. 用户管理服务启动一个用户数据处理部分的主线程，并调用 socket 初始化函数，登记主线程的入口函数地址，socket 初始化程序调用主线程的入口函数，获得一个对应于端口的消息处理函数入口，启动一个 socket 主线程，完成 Socket 的初始化，并绑定监听端口；
- c. 当有连接到来时，socket 主线程调用用户数据处理主线程的消息处理函数，要求建立该连接的数据处理子线程；用户数据处理主线程的消息处理函数根据收到的消息建立数据处理子线程，并返回针对该连接的数据处理函数入口；
- d. socket 创建一个对应于连接的子线程，接收数据，查询数据处理子线程的状态并调用数据处理函数，发送数据，循环直至连接结束。

本发明在不改变网络物理结构，不加重网络负担，不加重邮件服务器负担的情况下实现了用户身份认证及授权。系统安全认证解决方案，保证了与用户应用程序的无关性，大大降低程序的移植成本。并且改变了以往只能对单个主域服务器管理并且只能在本机上进行管理的局面，可以对多个主域服务器进行管理，对一个比较大的网络集成系统中用户信息的集中控制。在这种方法之上，我们在一个管理控制台上对多个主域服务器中的用户组、用户集中管理，统一授权。对于一个稳定的系统，成功的实现了各个主域服务器时间上的同步。同时，为用户分配高强度的用户口令，不易被黑客通过字典攻击的方法进行口令攻击。如果系统中某个主域服务器出现问题，仍然可以实施有效的认证与授权。

附图说明

图 1：传统域用户授权和管理系统

图 2：本发明的域用户授权和管理系统

图 3：域管理代理软件的基本处理流程

具体实施方式

下面结合附图和实施例来进一步说明本发明。

如图 2 所示，我们设计了一个域用户用户管理中心，域管理同步技术应用在一个身

份认证系统中，网络环境是百兆以太网，硬件设备包括 HP 服务器或其它服务器、百兆以太网卡，运行平台是中文 Windows NT Server4.0+Service Pack6。

该系统包括一个安全管理中心的管理控制台 14、一个安全数据库 13、十几个主域服务器 11、几百台客户端主机 12。客户端主机 12 分别与各个主域服务器 11 连接，安全数据库 13 与管理控制台 14 连接。在安全管理中心的管理控制台上安装管理控制软件，在各个主域服务器上安装域用户代理软件，在各个客户端主机安装客户端软件。在本系统中用户基本信息将通过安全管理中心存放在 IC 卡中。

用户得到授权的过程为，在域用户管理中心控制台上添加各个安装好了域管理代理软件的主域服务器，这样域用户管理中心控制台就可以管理控制这些主域上的用户组和用户；在域用户管理中心控制台输入用户基本信息；将用户基本信息存放到安全数据库中；将用户基本信息传输到主域服务器，与主域服务器的域用户代理进行 Socket 通讯；主域服务器的域用户代理通过用户数据处理函数处理用户基本信息，将这些信息输入到主域服务器操作系统本身的域用户管理器中，这样用户就得到了操作系统的授权。

域用户代理软件具有两个模块，即用户数据处理模块和 Socket 通讯模块，其处理流程如图 3 所示，由于采用 Windows NT 服务程序模式，当系统启动后由 Windows NT 服务控制程序（Service controller）启动用户管理服务。用户管理服务启动一个用户数据处理部分的主线程，并调用 socket 初始化函数，登记主线程（MainProcThread）的入口函数（MainProcThread.ThreadMain）地址。socket 初始化程序调用主线程（MainProcThread）的入口函数（MainProcThread.ThreadMain），获得一个对应于端口的消息处理函数入口（MainProcThread.Dispatch），启动一个 socket 主线程（SocketMainThread），完成 Socket 的初始化，并绑定监听端口。

当有连接到来时，socket 主线程（SocketMainThread）调用用户数据处理主线程的消息处理函数（MainProcThread.Dispatch），要求建立该连接的数据处理子线程（NetDataProcess）；用户数据处理主线程的消息处理函数（MainProcThread.Dispatch）根据收到的消息建立数据处理子线程（NetDataProcess），并返回针对该连接的数据处理函数入口（NetDataProcess.DataProcess）。socket 创建一个对应于连接的子线程（SocketConnectThread），接收数据，查询数据处理子线程（NetDataProcess）的状态（通过 MainProcThread.Dispatch）并调用数据处理函数（NetDataProcess.DataProcess），发送数据，循环直至连接结束。

上述过程是由系统自动完成的，系统的组件功能如下：安全管理中心的控制台是一

个在 Windows 95/98、Windows NT、Windows2000 上运行的应用程序，其实现了集成的管理界面，管理员通过安全管理中心管理多个主域服务器，并通过这个管理界面，对用户、用户组、域、用户与用户组的关系及用户在各个主域服务器上的授权进行统一的管理。安全数据库存放用户数据、用户组数据、域数据及三者相互关系的数据。各个主域服务器上安装有域管理代理软件，域管理代理和各个主域服务器相结合，实现集中统一的用户、用户组管理。

说 明 书 附 图

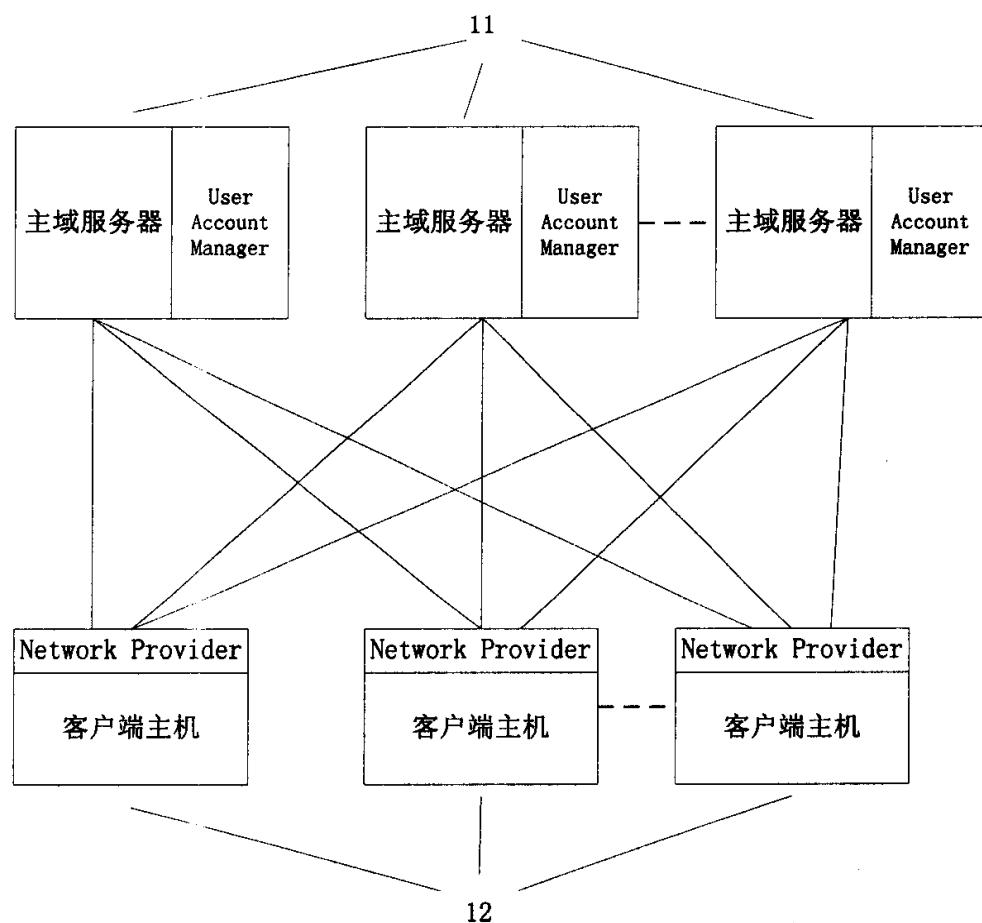


图 1

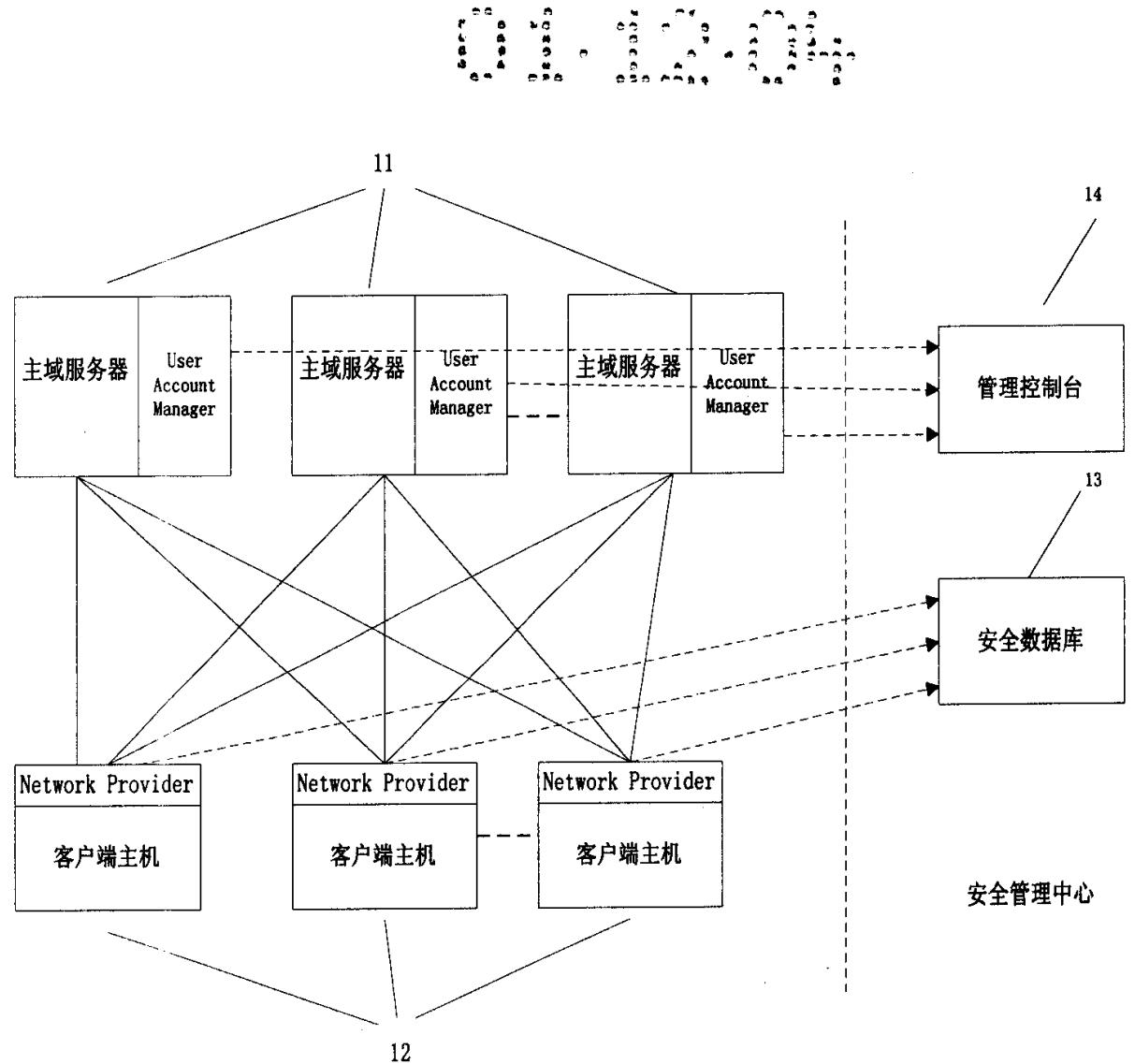


图 2

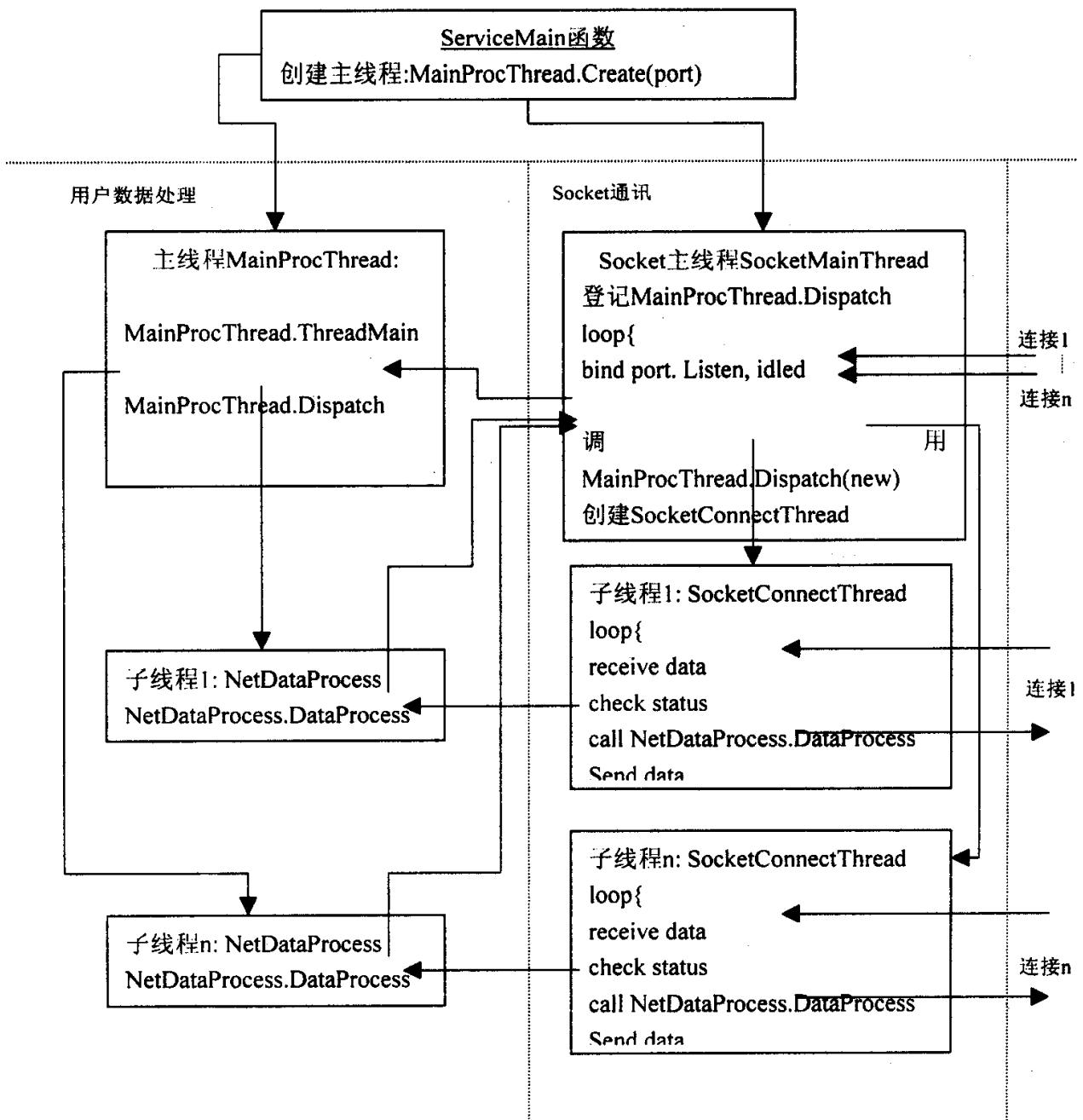


图 3