[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200510093608.4

[43] 公开日 2007 年 3 月 7 日

[11] 公开号 CN 1925391A

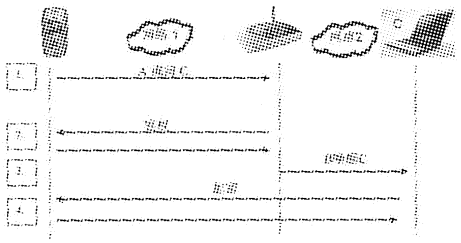
[22] 申请日 2005.8.31
[21] 申请号 200510093608.4
[71] 申请人 西门子（中国）有限公司
地址 100102 北京市朝阳区望京中环南路 7 号
[72] 发明人 汉顿·克里斯蒂安
权利要求书 2 页 说明书 6 页 附图 2 页

[54] 发明名称

一种使用中介设备的通信方法及其通信系统

[57] 摘要

本发明提出一种在通信网络中使用中介设备的通信方法，该通信网络中包括至少两个终端设备、至少一个中介设备，中介设备和其中一个终端设备组成一个网络。 该通信方法是，另一个终端设备向中介设备发出通信请求；中介设备对发出请求的终端设备进行鉴权；中介设备唤醒上述网络内的终端设备；上述两个终端设备进行通信。 本发明还提出了应用上述通信方法的通信系统。 采用本发明方法，局域网中的网络设备无需时时连接在局域网络上，因此节约了能量，进一步保证了数据的安全，减少了局域网内的终端用户受到网络攻击的可能性。



1. 一种在通信网络中使用中介设备的通信方法，上述通信网络中包括至少两个终端设备、至少一个中介设备，上述中介设备和上述一个终端设备组成一个网络，其特征在于该方法包含以下步骤：

（1） 上述另一个终端设备向上述中介设备发出通信请求；

（2） 上述中介设备对上述发出请求的终端设备进行鉴权；

（3） 上述中介设备唤醒上述网络内的终端设备；

（4） 上述两个终端设备进行通信。

2. 如权利要求 1 所述的在通信网络中使用中介设备的通信方法，其特征在于：上述步骤（3）中，上述中介设备通过有线方式唤醒上述网络内的终端设备。

3. 如权利要求 1 所述的在通信网络中使用中介设备的通信方法，其特征在于：上述步骤（3）中，上述中介设备通过无线方式唤醒上述网络内的终端设备。

4. 如权利要求 2 所述的在通信网络中使用中介设备的通信方法，其特征在于：上述有线方式为网络唤醒方式。

5. 如权利要求 3 所述的在通信网络中使用中介设备的通信方法，其特征在于：上述无线方式为蓝牙方式。

6. 如权利要求 1 所述的在通信网络中使用中介设备的通信方法，其特征在于：上述步骤（4）中，上述两个终端设备用加密方式进行通信。

7. 如权利要求 6 所述的在通信网络中使用中介设备的通信方法，其特征在于：上述加密通信采用安全套接层协议或者传输层安全协议。

8. 应用上述通信方法的通信系统，该系统包括至少两个终端设备，其特征在于：上述通信系统还包括一个中介设备，该中介设备与上述一个终端设备组成一个网络。

9. 如权利要求 8 所述的通信系统，其特征在于：上述中介设备具有一个接收装置，该接收装置接收上述另外一个终端设备的信号；上述中介设备具有一个鉴权装置，该鉴权装置在接收上述终端设备的信号后对该终端设备进行鉴权；上述中介设备具有一个发射装置，在对上述终端设备鉴权成功后，该发射装置发射信号给上述网络中的终端设备。

10. 如权利要求 9 所述的通信系统，其特征在于：上述中介设备的发射装置发射的信号包括唤醒帧。

一种使用中介设备的通信方法及其通信系统

（一）技术领域

本发明涉及一种通信方法，尤其是一种使用中介设备的通信方法以及采用该通信方法的通信系统。

（二）背景技术

随着计算机网络（Computer Network；Net）和移动电话技术的迅猛发展，计算机网络和终端用户之间的业务数据交换也越来越频繁。为了保证计算机网络和终端用户之间的通信安全，避免非法用户入侵和数据窃听，进行上述数据交换必须考虑身份验证、访问控制以及信息保密的问题，这些问题常常需要通过鉴权与加密过程来解决。

鉴权通常采用查询-应答（Challenge-response）方式，在连接过程中，可能需要一次鉴权或两次鉴权。通过鉴权可防止盗用和误用。加密技术则增加了系统安全性，密钥长度可以是 0、40 或 64 位，密钥一般由高层软件管理。如果用户需要更高级别的保密要求，可在传输层和应用层使用特别的安全机制。

图 1 举例说明了一个终端用户 A 和一个计算机 C 进行通信时的上述情形。图 1 中 A 为一个移动终端（Mobile Terminal；MT），C 为一个个人计算机（Personal Computer；PC）。如果 A 想要和 C 相连接从而和 C 进行通信，则首先 C 要对 A 进行鉴权，即识别 A 的身份，并且 C 还要对传送给 A 的数据进行加密，对 A 传送来的数据进行解密。同样，A 也需要对 C 进行鉴权，对传送给 C 的数据进行加密，并且对 C 传送来的数据进行解密。

使用如上所述的通信系统虽然能够正常通信，但却存在以下几方面问题：

第一，如果终端用户想要随时和个人计算机进行通信，那么个人计算机就要时时连接在网络中。如果有某个瞬间该个人计算机没有连接到网络中，那么这一时刻就无法和上述终端用户进行通信。

第二，由于终端用户和个人计算机之间的网络并不总是安全的，个人计算机既要对终端用户进行鉴权，又要对终端用户进行数据传输，这增大了未经鉴权的用户得到个人计算机中的数据的危险性。

第三，如果一个终端用户对该个人计算机进行了一次误访问，例如拨错了连接号码或者访问地址，则个人计算机首先要对该终端用户进行鉴权，上述鉴权过程需要持续一段时间。对该误访问的终端用户来说，需要等待一段时间以后才被告知鉴权失败；对个人计算机来说，则因为终端用户的误访问而进行一次鉴权，浪费其能量。

（三）发明内容

因此，本发明的主要目的在于提供一种通信方法，使得一个终端用户无需时时连接在网络上就能够和其它终端用户通信，并且能够减少该终端用户受到网络攻击的可能性，增加通信网络的安全。

为达到上述目的，本发明提出一种在通信网络中使用中介设备的通信方法，该通信网络中包括至少两个终端设备、至少一个中介设备，中介设备和上述一个终端设备组成一个网络，该方法包含以下步骤：

（1） 上述另一个终端设备向上述中介设备发出通信请求；

（2） 上述中介设备对上述发出请求的终端设备进行鉴权；

（3） 上述中介设备唤醒上述网络内的终端设备；

（4） 上述两个终端设备进行通信。

其中，在步骤（3）中，在中介设备对请求通信的终端设备鉴权通过后，该中介设备能够唤醒上述网络内的终端设备。唤醒方式既可以采用有线方式，例如采用网络唤醒技术（Wake on Lan；WoL）；唤醒方式也可以采用无线方式，例如采用蓝牙技术（Blue Tooth）。

另外，在步骤（4）中，上述两个终端设备一般采用加密方式进行通信，例如可以采用安全套接层（Secure Sockets Layer；SSL）协议进行加密，或者采用 SSL 协议的后继协议，即传输层安全协议（Transport Layer Security；TLS）进行加密。

本发明还提出了一种应用上述通信方法的通信系统，该系统包括至少两个终端设备，上述通信系统还包括一个中介设备，该中介设备与上述一个终端设备组成一个网络。

其中，上述中介设备具有一个接收装置，该接收装置接收上述另外一个终端设备的信号；上述中介设备具有一个鉴权装置，该鉴权装置在接收上述终端设备的信号后对该终端设备进行鉴权；上述中介设备具有一个发射装置，在对上述终端设备鉴权成功后，该发射装置发射信号给上述网络中的终端设备。通常该发射信号中包括唤醒帧，以便上述网络内的终端设备接收到该唤醒帧后能够启动。

可见，本发明所提供的在通信网络中使用中介设备的通信方法，具有以下的优点和特点：

(1) 采用本发明的方法进行通信，将中介设备同时连接在两个网络上，这使得用中介设备唤醒的网络设备无需时时连接在网络上，因此节约了能量。

(2) 将原来由终端设备进行的鉴权业务改由中介设备来进行，鉴权业务和业务数据分别由不同的设备来完成，这样进一步保证了数据的安全，减少了该终端用户受到网络攻击的可能性。

(3) 在一个终端用户误访问的情况下，中介设备立刻能够进行鉴权，通知该用户鉴权失败，该用户无需等待太长时间；对于网络内的终端用户而言，则无需因为一次误访问而启动依次而浪费其能量。

（四）附图说明

图 1 是现有技术中通信方法步骤示意图。

图 2 是本发明的通信方法及其通信系统示意图。

图 3 是本发明的实施例示意图。

（五）具体实施方式

下面结合附图、通过具体实施例对本发明进行详细说明，这些实施例是说明性的，不具有限制性。

图 2 是本发明的通信方法及其通信系统示意图。在图 2 中的通信设备包含一个终端用户 A，中介设备 B，一个终端用户 C。A 和 B 同时位于一个通信网络 1 中，B 和 C 同时位于一个通信网络 2 中。中介设备 B 具有对来自 A 的信号进行鉴权的功能。

如果 A 想跟 C 进行通信，则经过的通信步骤如下：首先，A 向上述中介设备 B 查询是否能和 C 通信；然后，中介设备 B 对 A 进行鉴权，即对 A 的合法身份进行认证；再后，如果 B 对 A

的鉴权通过，则 B 将 C 唤醒，使得 C 做好与 A 进行通信的准备；最后，A 和 C 通过加密方法进行通信。

图 3 是本发明的一个实施例。图 3 所示的通信网络中存在两个终端用户和一个中介设备，其中一个终端用户为一个手机设备（Mobile Terminal；MT），另一个终端用户为一个个人计算机（Personal Computer；PC），中介设备则可以是一个家用设备服务器（EasyHome Server）。在该家用服务器上具有一个接收装置，能够接收上述手机设备的信号；该家用服务器上还具有一个鉴权装置，能够在接收手机设备的信号后对该手机设备进行鉴权；另外该家用服务器上还具有一个发射装置，在对手机设备鉴权成功后，该发射装置发射唤醒帧信号给上述个人计算机。

一方面，该家用设备服务器支持 Internet 协议，它与手机设备之间的通信是基于 Internet 协议进行的，如图 3 中的椭圆框所示；另一方面，该家用设备服务器支持基于 IEEE 标准 802.11b（又名 Wi-Fi）的无线局域网（Wireless Local Area Network；WLAN）协议，它和个人计算机组成一个局域网（Local Area Network；LAN）并通过 WLAN 协议进行通信，如图 2 中的方框所示。

上述家用设备服务器随时能够和手机设备进行通信，而个人计算机则无需时时连接在上述局域网上。如果该手机设备想要访问位于家庭中的个人计算机中的数据，则手机设备先要向家用设备服务器提出通信请求，家用设备服务器上的接收装置接收到上述信号以后，家用设备服务器会发出查询指令给手机设备，手机设备接收到查询指令后，向家用设备服务器发送一系列信息，用来证明其身份。家用设备服务器收到该信息后，就可以通过鉴权装置验证上述手机设备的身份。

如果上述鉴权通过，则家用设备服务器发送唤醒帧，通过网络唤醒（Wake on LAN；WoL）方式唤醒个人计算机。家用服务器上装有远程网络管理软件，而在个人计算机上装有支持网络唤醒的网卡、支持网络唤醒的主板。支持网络唤醒的网卡不断的监视着整个网络，看网络

中是否存在唤醒帧，判断的方式有多种，例如可以设定在唤醒帧中媒体接入控制（Media Access Control；MAC）地址不间断的重复 16 次；网卡有持续不断的电源以能够启动计算机。一般情况下，个人计算机的主板还包含一个为使用网络唤醒技术专门设计的 CMOS。

当个人计算机上的网卡收到唤醒帧时，计算机就会开启，手机设备和个人计算机之间可以开始通信。

手机设备和个人计算机之间一般采用加密通信，例如可以采用安全套接层协议 SSL 进行加密，或者采用 SSL 协议的后继协议，即传输层安全协议 TLS 进行加密。SSL/TLS 是一种行业标准安全协议，使用 SSL/TLS 时会生成一个发送发和接收方共享的数字密钥，只有信息传输的发送方和接收方可以通过该密钥对信息进行编译或解码。任何其它一方，即使是传递这些信息的服务器均无法对 SSL/TLS 传输进行破译。

当手机设备和个人计算机之间的通信完成时，个人计算机发出信息通知家用设备服务器，家用设备服务器上的远程网络管理软件通知计算机关机或者进入休眠状态。

由上述实施例可以看出，采用本发明的方法，等待唤醒的网络设备无需时时连接在网络上，因此节约了能量。并且由于用单独的中介设备实现鉴权功能，进一步保证了数据的安全，减少了网络内的终端用户受到网络攻击的可能性。

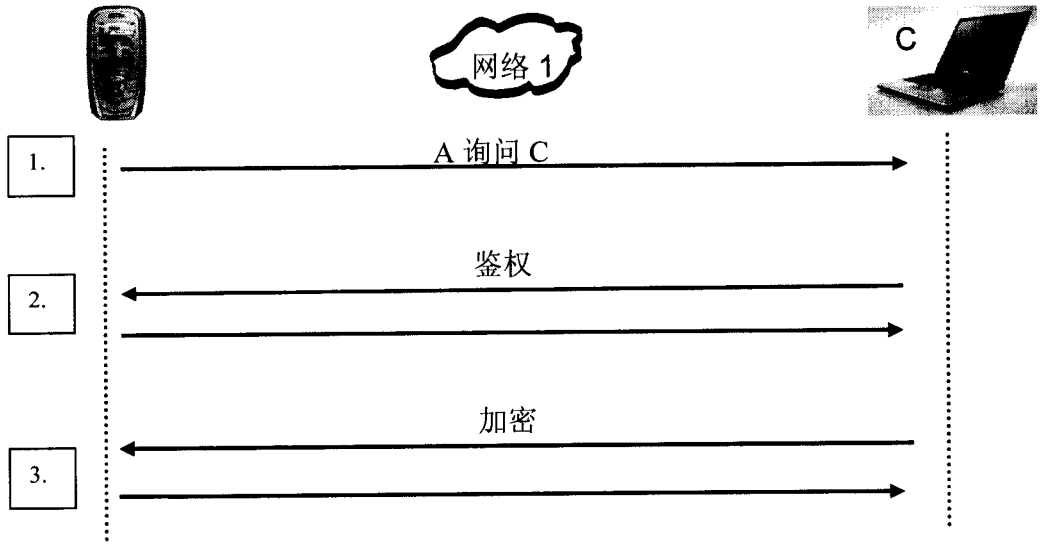


图 1

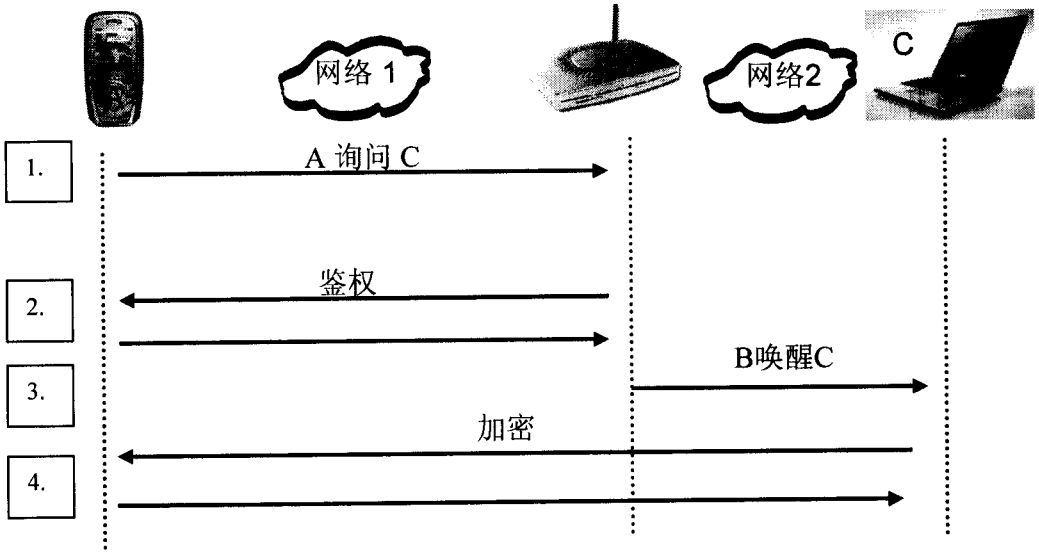


图 2

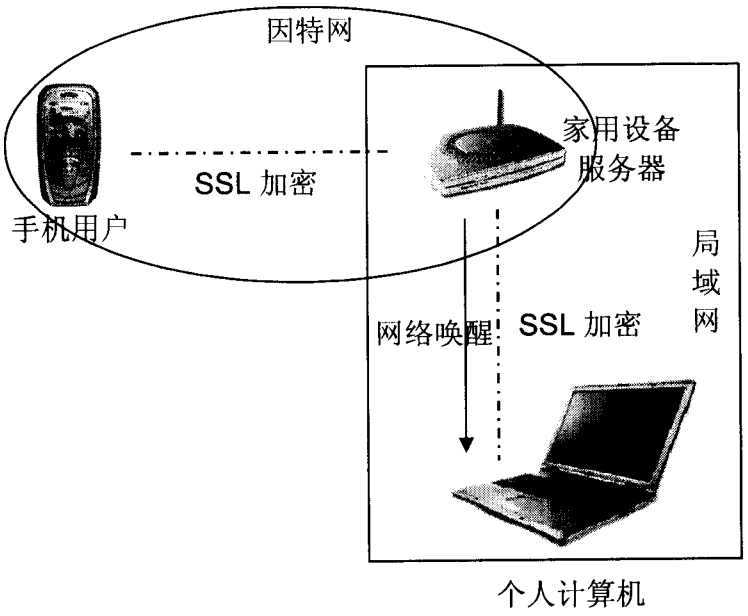


图 3