[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)
G06F 1/00 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200480010953.0

[43] 公开日 2006 年 5 月 24 日

[11] 公开号 CN 1778091A

[22] 申请日 2004.4.22
[21] 申请号 200480010953.0
[30] 优先权
[32] 2003. 4.24 [33] EP [31] 03101122.4
[86] 国际申请 PCT/IB2004/050488 2004.4.22
[87] 国际公布 WO2004/095797 英 2004.11.4
[85] 进入国家阶段日期 2005.10.24
[71] 申请人 皇家飞利浦电子股份有限公司
地址 荷兰艾恩德霍芬
[72] 发明人 E·J·B·科尔伯

[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 程天正 张志醒

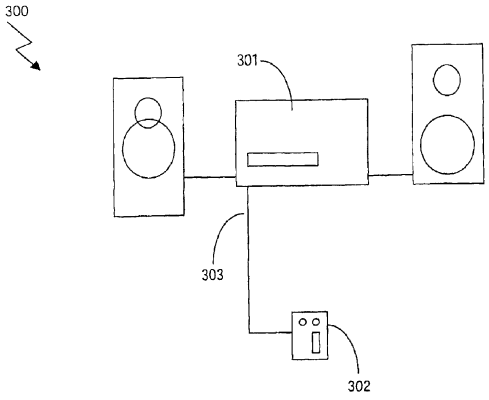
权利要求书 2 页 说明书 9 页 附图 3 页

[54] 发明名称

在设备之间进行基于分类的内容转送

[57] 摘要

本发明涉及一种用于把信息从分发设备分发到接收设备的方法和系统。 本发明的思想在于给每个设备分配类别号。 当要转送信息时，该分发设备验证该接收设备的类别号。 如果该接收设备比该分发设备具有更低的类别号，那么允许该分发设备向该接收设备转送所述内容。 优选地是，此类别号表示可以访问该设备的潜在用户的数目。 可以使用所签名的证书来分配所述类别号。 可以给要分发的信息提供加有水印的类别号，所述加有水印的类别号指定该接收设备可以具有并且还允许它接收该信息的最高类别号。



1. 一种用于把信息从分发设备（301）分发到接收设备（302）的方法，其中每个设备都已被分配有各自的信息分发授权等级，所述方法其特征在于:

使用类别号来表示信息分发授权等级；并且其中所述方法包括如下步骤:

当要从该分发设备（301）向该接收设备（302）分发信息时，验证（401）该接收设备（302）的类别号；并且

如果该接收设备（302）比该分发设备（301）具有更低的类别号，那么把信息从该分发设备（301）分发（404）到该接收设备（302）。

2. 如权利要求 1 所述的方法，其中分配给设备（301，302）的类别号对应于从所述设备向另一设备分发信息的能力，更低的类别号表明更低的分发（404）信息的能力。

3. 如权利要求 1 或 2 中任何一个所述的方法，其中要从该分发设备（301）分发（404）到该接收设备（302）的信息的至少一部分被加密，以致在该接收设备（302）比该分发设备（301）具有更低的类别号的情况下，所述接收设备（302）能够解密所加密的信息。

4. 如在前权利要求中任何一个所述的方法，其中设备（301，302）必须被分配一个数字签名的类别号以便使其自身具有作为信息分发器和接收器的资格。

5. 如在前权利要求中任何一个所述的方法，其中所述设备（301，302）布置在家庭网络（100）中。

6. 如权利要求 5 所述的方法，其中由所述家庭网络管理者给设备（301，302）分配类别号。

7. 如权利要求 1 到 5 中任何一个所述的方法，其中由设备制造商给设备（301，302）分配类别号。

8. 如在前权利要求中任何一个所述的方法，其中可以给包含在设备（301，302）中不同的子设备分配不同的类别号。

9. 如在前权利要求中任何一个所述的方法，其中要从该分发设备（301）分发到该接收设备（302）的信息被提供加有水印的类别号，所述加有水印的类别号指定该接收设备（302）可以具有并且还允许它接收该信息的最高类别号。

10. 一种用于把信息从分发设备（301）分发到接收设备（302）的系统（300），其中每个设备（301，302）都已被分配了各自的信息分发授权等级，所述系统（300）其特征在于：

每个设备（301，302）配置有类别号；

该分发设备（301）配置有用于当要实现从该分发设备（301）向该接收设备（302）分发信息时验证该接收设备（302）的类别号的装置（202，203）；和

该分发设备（301）配置有用于在该接收设备（302）比该分发设备（301）具有更低的类别号的情况下向该接收设备（302）分发信息的装置（202）。

11. 如权利要求 10 所述的系统（300），其中分配给设备（301，302）的类别号还对应于从所述设备向另一设备分发信息的能力，更低的类别号表明更低的分发信息的能力。

12. 如权利要求 10 或 11 中任何一个所述的系统（300），其中该分发设备（301）被配置成加密要从该分发设备（301）分发到该接收设备（302）的信息的至少一部分，以致在该接收设备（302）比该分发设备（301）具有更低的类别号的情况下，所述接收设备（302）能够解密所加密的信息。

13. 如权利要求 10 到 12 中任何一个所述的系统（300），其中一个设备（301，302）配置有数字签名的类别号以便使自身具有作为信息分发器和接收器的资格。

14. 如权利要求 10 到 13 中任何一个所述的系统（300），其中所述设备（301，302）布置在家庭网络（100）中。

15. 如权利要求 14 所述的系统，其中由所述家庭网络管理者给所述设备（301，302）分配类别号。

16. 如权利要求 10 到 14 中任何一个所述的系统，其中由设备制造商给所述设备（301，302）分配类别号。

17. 如权利要求 10 到 16 中任何一个所述的系统，其中可以给包含在设备（301，302）中不同的子设备分配不同的类别号。

18. 如权利要求 10 到 17 中任何一个所述的系统，其中要从该分发设备（301）分发到该接收设备（302）的信息被提供了加有水印的类别号，所述加有水印的类别号指定该接收设备（302）可以具有并且还允许它接收该信息的最高类别号。

在设备之间进行基于分类的内容转送

本发明涉及一种用于把信息从分发设备分发到接收设备的方法和系统，其中每个设备都已被分配了各自的信息分发授权等级。

近年来，内容保护系统的数目快速增加。这些系统中的某些只防止内容被非法拷贝，而其它系统还禁止用户访问该内容。第一类被称作拷贝保护（copy protection CP）系统。传统上 CP 系统是消费者电子设备（CE）设备的主要焦点，这是因为这类内容保护被认为是能够低廉地实现并且不必与内容供应商进行双向交互。某些例子是内容加扰系统（Content Scrambling System CSS），DVD ROM 盘片和 DTCP 的保护系统，用于 IEEE 1394 连接的保护系统。

已知的第二类系统有以下几个名称。在广播世界中，这类系统通常被称为条件访问（Conditional Access CA）系统，而在因特网世界中它们通常被称为数字权利管理（Digital Rights Management DRM）系统。

某些类型的 CP 系统还可以提供与 CA 或 DRM 系统相接口的服务。其例子是目前由 DVB - CPT 小组和 TV - Anytime RMP 组开发的系统。目标是这样的一种系统，其中一组设备可以通过双向连接来彼此身份认证。基于此身份认证，这些设备将彼此信任并且这将使/允许它们能够交换所保护的内容。附加许可描述了用户具有那些权利以及允许用户对内容执行什么操作。该许可使用某些通用网络秘密来保护，其只在某个家庭内的设备之间交换。这种设备的网络被称作授权域（Authorized Domain AD）。

授权域的原理在于试图找到一种能同时满足内容拥有者（想要保护他们的版权的人）和内容消费者（想要不受限制地使用内容的人）的利益的解决办法。基本原理是具有一种受控的网络环境，在该网络环境中只要内容不越过授权域的边界就可以相对自由地使用该内容。典型情况下，授权域以家庭环境为中心，其也被称为家庭网络。当然，其它方案也是可以的。用户例如可以在旅行时随身携带便携式电视机，并且在他的旅馆房间中使用它来访问在家里存储在个人录像机上的内容。即使便携式电视机在家庭网络以外，它也是用户授权域的一

部分。

家庭网络可以被定义为一组设备，这些设备使用某种网络技术（例如以太网、IEEE 1394、蓝牙、802.11b 等）相互连接。尽管网络技术允许不同的设备相互通信，但是这还不足以允许这些设备互相操作。为了能够实现这一点，设备需要能够挖掘出并访问存在于网络中的其它设备的功能。这种互操作性由家庭联网的中间件（HN－MW）来提供。家庭联网中间件的例子是 Jini、HAVi、UPnP、AVC。

多级安全保护（multilevel security MLS）的原理常常用于网络中以便在网络内有不同的安全等级。在网络内分发具有不同类别等级的信息，并且包含在该网络中的用户关于所分类的信息具有不同的安全许可及授权。借助于此原理，可以防止未被授权的用户访问信息。

现有技术中的问题（正是本发明所要解决的问题）在于：通常认为难于防止未被授权的消费者复制和／或分发有版权的数字内容。从而，这个问题导致很难保护有版权的数字内容的创建者的权利和分发该内容的内容供应商的权利。当然该问题可以通过使用拷贝保护来缓和，不过这出现了另一个问题，即如果用户在一个设备上具有内容，那么该用户就不能把该内容拷贝到他是唯一用户的另一设备上。

本发明的目的是提供一种方法和系统，能够直接、简单且有效地保护有版权的数字内容，以致该内容不能轻易地被复制和／或分发给没有被授权去访问该数字内容的用户和设备。还应该给授权的用户提供某些灵活性，这是因为把内容拷贝到由数目有限的用户使用的个人设备上也应该是可行的。

此目的由依照权利要求 1 的用于把信息从分发设备分发到接收设备的方法以及依照权利要求 10 的用于把信息从分发设备分发到接收设备的系统来实现的，在该方法和系统中，每个设备都已经被分配了各自的信息分发授权等级。由从属权利要求定义了优选的实施例。

依照本发明的第一方面，提供了一种方法，其中使用分配给设备的类别号来表示信息分发授权的等级。当要实现从分发设备向接收设备分发信息时，验证该接收设备的类别号。如果接收设备比分发设备具有更低的类别号，那么就从分发设备向接收设备分发信息。

依照本发明的第二方面，提供了一种系统，其中已经使用类别号给系统中的每个设备分配了各自的信息分发授权等级。包含在系统中

的分发设备配置有用于当从分发设备向系统中的接收设备分发信息时验证该接收设备的类别号的装置。该分发设备还配置有用于在接收设备比分发设备具有更低的类别号的情况下向该接收设备分发信息的装置。

本发明的思想在于以类别号的形式给设备分配信息分发授权等级。优选地是，此类别号表示可以访问设备的潜在用户数目。例如，个人MP3播放器比可由家庭网络所有成员访问的CD播放器具有更少的潜在用户。这意味着CD播放器比MP3播放器具有更高的类别号。更高的类别号是否表明更大的用户数目是个定义的问题，并且如果想要的话，那么可以选择高类别号来表明低的用户数目。然而，贯穿此说明书，类别号越高，潜在用户的数目越大。这将以任何方式都不会限制本发明，因为很显然的是：关于分类，上面给出的两个定义都是可以的。当要把采用有版权的数字内容形式的信息从分发设备转送到接收设备时，该分发设备验证该接收设备的类别号。如果该接收设备比该分发设备具有更低的类别号，那么允许该分发设备把该内容转送到该接收设备。

本发明是有益的，这是因为它一方面提供了对有版权的数字内容的保护而另一方面为授权的用户提供了一定的灵活性。内容可以被拷贝和分发，但是只能按照把拷贝分发给一个比分发设备具有更低的类别号的设备的方式来进行。更低的类别号表明该设备意在由数目更有限的用户来使用。唯一可能的是向比该分发设备具有更低的类别号的接收设备分发内容。例如，可以把类别号2给予CD播放器而把类别号1给予个人MP3播放器。这允许用户把内容拷贝到更小的设备上以供个人使用。这不会损害内容创建者和／或内容供应商的利益，并且它给予用户一定的灵活性。

依照本发明实施例，当向一个设备分配类别号时，考虑该设备向其它设备分发信息的能力。该设备越容易向另一设备转送信息，类别号越高。这是有益的，因为即使一个设备具有低的潜在用户数目，该设备或包含在该设备中的子设备也可能具有以容易的方式来传播信息的能力。例如，PC可能具有数目相当有限的潜在用户。然而，包含在PC中且连接到因特网的网卡可以被用来迅速地在世界范围内广播信息。因而，可以给予网卡高的类别号，而给予相同PC中的个人硬盘以

低的类别号。通过对包含在 PC 中的网卡和硬盘使用分类，用户就可以把内容拷贝到硬盘，但是不能把它从硬盘转送到连接到因特网的网卡上。

依照本发明另一实施例，对于一个使自身具有作为信息收件方或分发者的资格的设备而言，该设备必须被分配给一个数字签名的类别号。通过把所签名的类别号用作标识符，恶意的第三方就不可能引入未授权的设备，这是因为该设备是通过数字签名而被授权的。

依照本发明的又一实施例，把类别号分配给设备可以由设备制造商或由制造商所授权的分包商或家庭网络管理者来执行，在该家庭网络中要包括该设备。如果由制造商进行分配，那么就可以假定防止来自恶意第三方攻击的安全性更高，这是因为处理例如类别号和加密/解密密钥的权威机构没有被推广到若干当事方，由此降低了敏感信息泄露的风险。另一方面，如果允许网络管理者处理分配，那么该网络会变得灵活得多。

当学习所附的权利要求及以下描述时，本发明进一步的特征和优点将变得显而易见。本领域内技术人员认识到：可以组合本发明的不同特征来创建不同于以下所描述的那些实施例的实施例。对于那些本领域内技术人员来说各种不同的变化、修改和组合将变得显而易见。因此所描述的实施例并不意在限制本发明的范围，本发明的范围仅由附加权利要求来限定。

以下参考附图将要给出本发明实施例的详细说明，其中：

图 1 示意地示出了一个包括经由网络相互连接的设备的系统，在该系统中可以有益地应用本发明；

图 2 示意地示出了实现本发明实施例的 CE 设备；

图 3 示意地示出了当把内容从分发设备转送到接收设备时本发明的实施例；和

图 4 示出了依照本发明方法的实施例的流程图。

图 1 示意地示出了包括经由网络 110 相互连接的设备 101 - 105 的系统 100。在此实施例中，系统 100 是家庭内的网络。注意，该系统也可具体化为其它类型的网络，诸如大规模企业中的网络或大学网络，典型的数字家庭网络包括多个设备，例如收音机、调谐器／解码器、CD 播放器、一对扬声器、电视、VCR、磁带录放机等。这些设备通

常被相互连接起来以允许例如电视之类的一个设备控制例如 VCR 之类的另一个设备。一个诸如调谐器／解码器或机顶盒（set top box STB）之类的设备通常是中央设备，提供对其它设备的中央控制。

内容(典型情况下包括像音乐、歌曲、电影、TV 节目、图片、书等之类的东西，但是也包括交互式服务),经由住宅网关或机顶盒 101 来接收。内容还可以经由其它源或便携式设备进入家庭，其它源诸如作为盘片的存储介质。该源可以到宽带电缆网络、因特网连接、卫星下行链路等的连接。然后可以经由网络 110 向信宿转送该内容以便再现。一个信宿例如可以是电视显示器 102、便携式显示设备 103、移动电话 104 和／或音频播放设备 105。

再现内容项所采用的确切方式取决于设备的类型和内容的类型。例如,在收音机中,再现包括产生音频信号并且把它们馈送到扬声器。对于电视机，再现通常包括产生音频和视频信号并且把这些信号馈送到显示屏和扬声器。对于其它类型的内容，必须采取类似的适当动作。再现还可以包括诸如解密或解扰所接收的信号、使音频与视频信号同步等之类的操作。

在系统 100 中的机顶盒 101 或任何其它设备，可以包括诸如硬盘之类的存储介质 S1，这样就能够实现所接收的内容的记录以及稍后的播放。存储介质 S1 可以是该机顶盒 101 与其连接的某种类型的个人数字记录器（personal digital recorder PDR），例如 DVD+RW 记录器。内容还可以通过存储在诸如 CD 或 DVD 之类的载体 120 上来进入系统 100。

便携式显示设备 103 和移动电话 104 使用基站 111（例如使用蓝牙或 IEEE 802.11b）采用无线方式连接到网络 110。使用常规的硬接线连接来连接其它设备。为了使得设备 101 - 105 能够相交互，可用几种互操作性标准，这样就使得不同的设备能够交换消息和信息并且彼此控制。一种众所周知的标准是家庭音频/视频互操作性（Home Audio/Video Interoperability HAVi）标准，版本 1.0。其它众所周知的标准是家用数字总线（domestic digital bus D2B）标准、在 IEC 1030 中描述的通信协议以及通用的即插即用。

重要的是确保家庭网络中的设备 101 - 105 不会对内容进行未被授权的拷贝。为此，一种安全框架结构（典型情况下称为 DRM 系统）

是必须的。依照一种这样的框架结构，遵照本发明的特征，该网络中的每个设备都被分配一个用于表示可以访问该设备的潜在用户数目的类别号。例如，个人便携式显示设备 103 比可由该家庭网络中所有成员访问的机顶盒 101 具有更少的潜在用户。这意味着机顶盒 101 比显示设备 103 具有更高的类别号。当要把以有版权的数字内容形式的信息从分发设备（例如机顶盒 101）转送到接收设备（例如个人便携式显示设备 103）时，该分发设备就验证该接收设备的类别号。在这种情况下，该接收设备比该分发设备具有更低的类别号，这样允许机顶盒 101 向个人便携式显示设备 103 转送内容。如果该设备 103 曾经试过向机顶盒 101 转送内容，那么该设备 103 就有可能不被允许这样做，这是因为机顶盒 101 比该设备 103 具有更高的类别号。

使用这个框架结构，如下面将要描述的，关于内容分发，将使用密码操作。这些设备可以彼此身份认证并且通过加密内容来安全地分发该内容。这防止不受保护的内容被“不受阻碍地”泄露到未被授权的设备，并且防止来源于不受信任的设备的数据进入该系统。

重要的是设备只向它们预先已经成功身份认证的其它设备分发内容。这确保对手不能使用恶意的设备来进行未被授权的拷贝。设备如果是由授权的制造商或授权的分包商所构建的，那么它将只能够成功地身份认证自身，例如这是因为只有授权的制造商知道成功地身份认证所需要的特定秘密，或者是因为他们的设备是由受信任的网络管理者所装配的。

图 2 示意地示出了实现本发明实施例的、音频播放设备 201 形式的 CE 设备。播放设备 201 包含 CPU 202 或具有处理能力的等效设备，诸如可编程序逻辑器件（PLD）、专用集成电路（ASIC）等。设备 201 还包含存储器形式的存储设备 202，用于存储执行密码操作所要求的软件并且用于存储诸如类别号和密码密钥之类的数据。应当能够认识到的是：要求所有设备包括处理能力和存储设备以便实现本发明。

在生产中，给设备 201 分配一个表示可以访问该设备的潜在用户数目的类别号。依照本发明的实施例，当给该设备分配类别号时，还考虑该设备分发信息的能力。优选地是，利用设备 201 的私有的、非对称密钥来加密类别号，这样就把数字签名附加到该类别号上。然后满足被称为不可抵赖的准则，即信息的发送方在以后的阶段不能否认

信息传输。作为选择，使用对称密钥来加密类别号，在这种情况下提供身份认证。注意，非对称加密过程比对称加密过程多走一步，这是因为除提供身份认证之外它还提供不可抵赖。可以使用强大的标准算法来提供身份认证和／或不可抵赖，该标准算法诸如用于对称加密的三重数据加密标准（3 - DES）算法、高级加密标准（AES）算法或国际数据加密算法（IDEA），以及例如用于非对称加密的 Diffie - Hellman（DH）算法或 Rivest - Shamir - Adleman（RSA）算法。这样就对与设备 201 通信的另一设备确保了它的类别号已经由受信任的制造商所发出。

如前所述，可以由授权的分包商或受信任的网络管理者来执行把类别号实际分配给一个设备。当考虑谁来进行实际分配时，必须在一方面为系统安全而另一方面为灵活性之间进行权衡。如果由制造商进行分配，那么可以认为防止恶意第三方攻击的安全性较高，这是因为处理例如类别号和加密/解密密钥的任务由一方来执行。另一方面，如果允许网络管理者来处理所述分配，那么该网络变得更为灵活，这是因为管理者最有可能知道该网络以及包括在其中的设备。谁实际上来执行分配类别号是一项必须由设备制造商、网络拥有者以及可能是有版权内容的供应商所议定的协议。

图 3 示意地示出了依照本发明的系统 300 的实施例。在图 3 中，内容要被从分发设备 301 转送到接收设备 302。在分发设备（在这种情况下为音频播放设备 301）和接收设备（在图 3 中为便携式 MP3 播放器 302）之间建立连接 303。在此具体实施例中连接 303 由意在用于传送 MP3 文件的电缆组成。在其它所设计的实施例中，分发设备和接收设备可以是包括收音机的设备，在这种情况下可以使用 RF 来建立连接 303。

图 4 示出了依照本发明方法的实施例的流程图。在步骤 401，当已经在分发设备（DD）和接收设备（RD）之间建立连接时，DD 的 CPU（未示出）执行适当的软件来验证 RD 的类别号。这是通过解密所加密的类别号来执行的。利用由 DD 和 RD 共享的对称密钥或对应于 RD 私钥的公钥来执行所述加密，这取决于所使用的加密的类型。密钥的分发可以由设备制造商来处理，但是和分配类别号的情况一样，这可以由授权的分包商或受信任的网络管理者或受信任的第三方来完成。在步骤

402，DD 决定 RD 的类别号是否低于它自己的类别号。如果 RD 的类别号等于或高于 DD 的类别号，那么方法在步骤 403 终止并且不实现从 DD 向 RD 传输内容。

如果在步骤 402 DD 决定 RD 的类别号低于它自己的类别号，该方法继续至步骤 404，其中 DD 向 RD 分发有版权的内容。取决于系统中被认为有必要的安全等级，在 DD 可以结合分发来加密内容，由此向内容提供保密性。作为选择，可以预先加密内容。所述加密利用由 DD 和 RD 共享的对称密钥或对应于 RD 私钥的公钥来执行。如果该内容被加密，那么在步骤 405 RD 将解密该内容。与加密类似，该内容利用由 DD 和 RD 共享的对称密钥或 RD 的私钥来解密，所述私钥对应于在加密中所使用的公钥。在步骤 405，在解密之后，该内容为明文，并且 RD 可以自由地访问该内容。

作为选择，一个独立的验证设备（未示出）可以被配置成执行对类别号的验证，借此大量的处理负荷被从接收设备转移到验证设备。该验证设备还可以存储并分发关于密码操作所使用的密钥。如果一个网络包括许多接收和分发设备，那么这就很有益，这是因为分发设备可以不那么复杂。在大规模网络中，可以布置许多验证设备。

依照本发明的又一实施例，从分发设备分发到接收设备的内容要经受加水印的处理。优选地是，这在内容分发商或设备制造商或由此二者合作执行。通过对类别号执行加水印操作并且把加有水印的类别号插入内容中，就可以指定一个设备可以具有并且还允许它接收加有水印的内容的最高类别号。如果恶意的第三方取得一个高类别号的设备，那么此第三方可以向数目更大的其它设备分发内容。通过使用水印，内容本身决定它是否可以被分发给接收设备。假定向某个内容分配加水印的类别号 3，并且接收设备具有类别号 4，那么不可以向该设备分发该内容。实际上，把内容分发到一个其类别号高于该内容中包含的加水印的类别号的设备是不可能的。由设备 CPU 执行适当的软件来确认该加水印的类别号。

加水印是有益的，这是由于非法拥有具有高分类的设备以便广播有版权的内容变得无用，这是因为内容本身使用水印操作确定了其可以被引入所分类设备网络的等级。

应当注意到，上述实施例举例说明了本发明，而本领域内的技术

人员在不脱离所附权利要求的范围内的情况下将能够设计很多候选的实施例。例如，可以根据设备的昂贵情况来分配类别号，或者可以根据分类中设备的某些属性来分配分类号。这种选项的一个实施例可以是对于服务器使用分类‘2’，对于固定设备使用分类‘1’，而对于移动设备使用分类‘0’。

词“包括”并不排除那些没有记载在权利要求中的元件或步骤的存在。位于元件之前的词“一个”或“一种”并不排除存在多个这样元件。在列举多个设备的系统权利要求中，这些设备中的某几个可以被具体化为同一个硬件项。

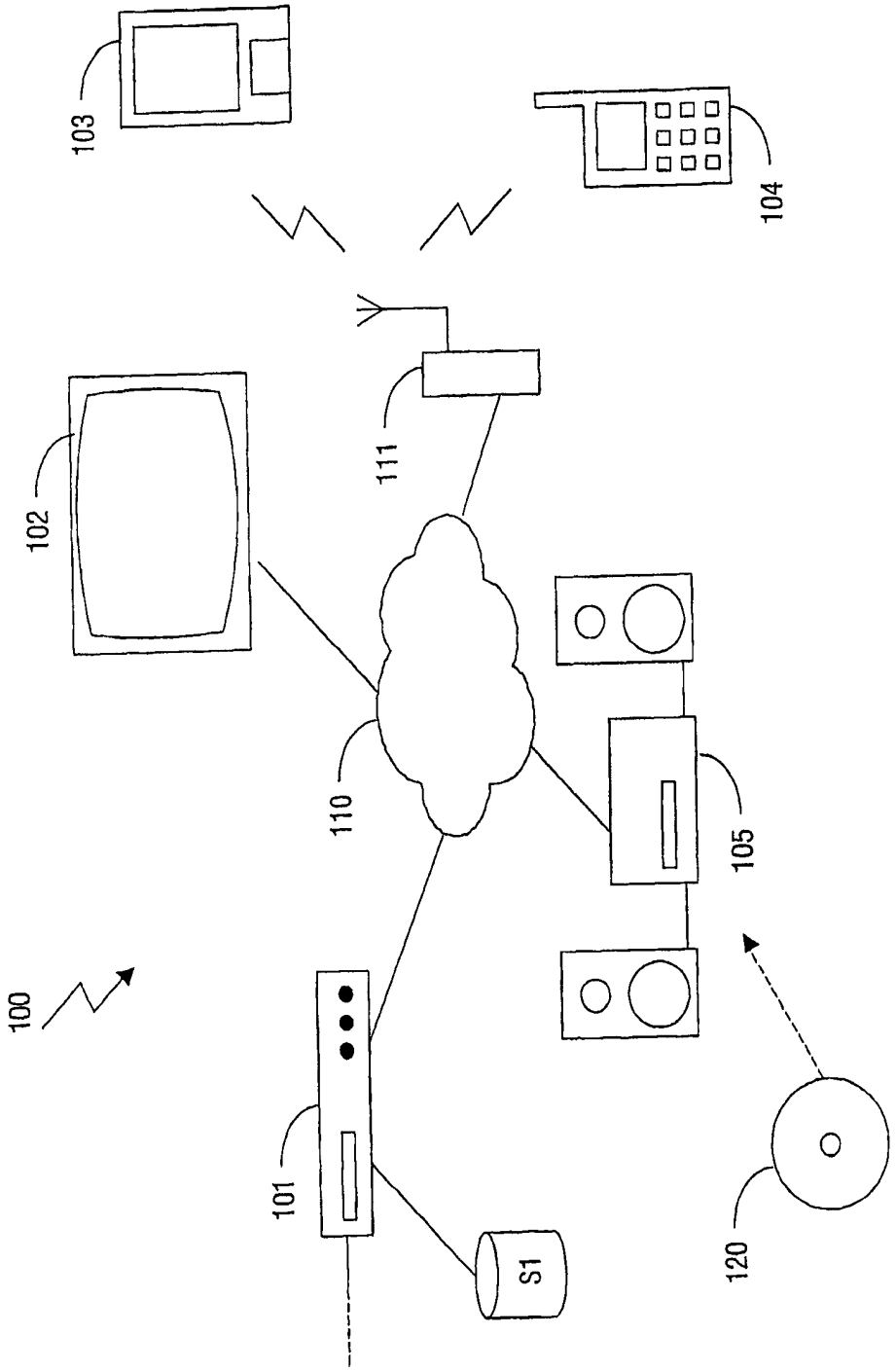


图 1

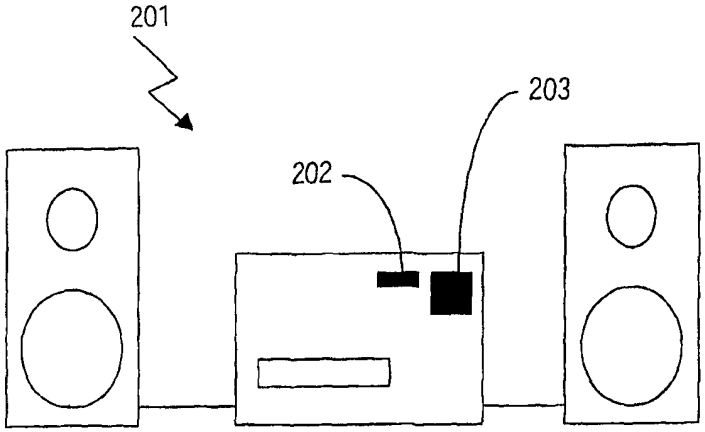


图 2

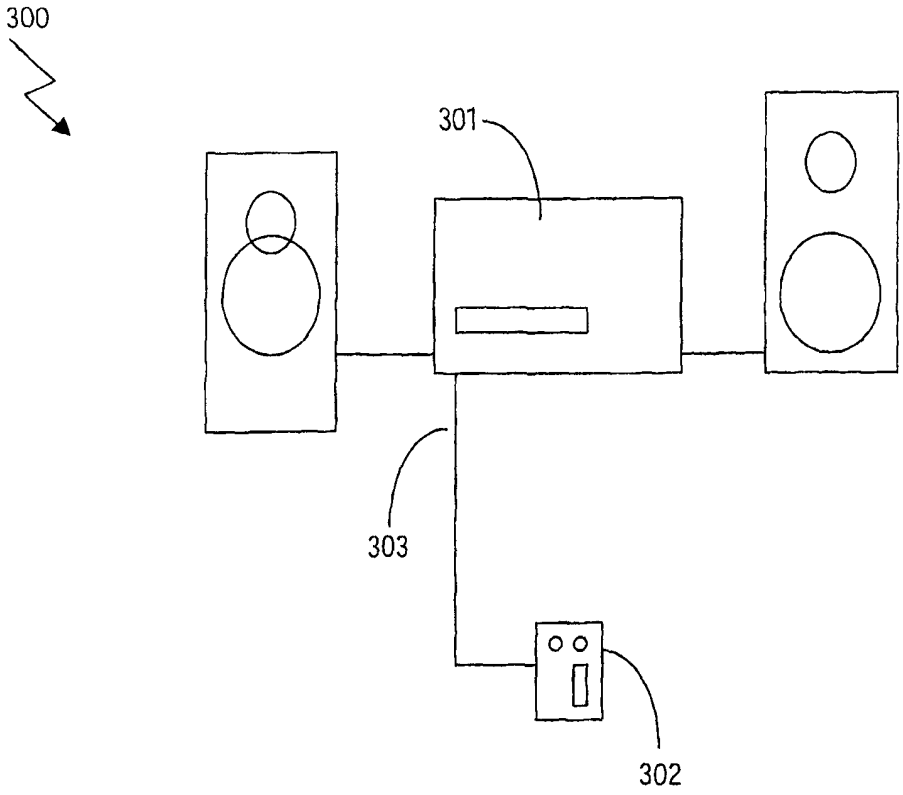


图 3

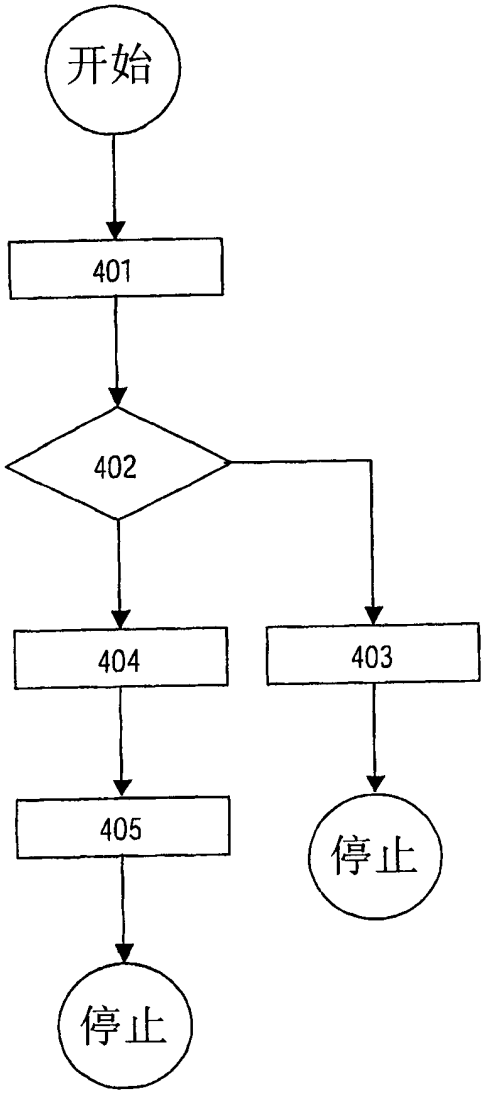


图4