

[19]中华人民共和国国家知识产权局

[51]Int. Cl⁷

G06F 11/00

G06F 13/00

[12]发明专利申请公开说明书

[21]申请号 97182186.0

[43]公开日 2000年10月4日

[11]公开号 CN 1269030A

[22]申请日 1997.11.21 [21]申请号 97182186.0

[30]优先权

[32]1996.11.21US [33]US [31]08/749,352

[86]国际申请 PCT/US97/21322 1997.11.21

[87]国际公布 WO98/22875 英 1998.5.28

[85]进入国家阶段日期 1999.6.21

[71]申请人 计算机联合国际公司

地址 美国纽约州

[72]发明人 丹尼尔·埃斯本森

[74]专利代理机构 中原信达知识产权代理有限责任公司

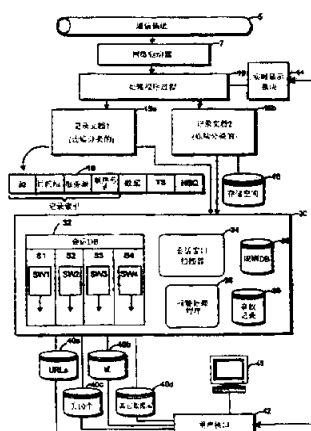
代理人 余 蓉 穆德骏

权利要求书3页 说明书12页 附图页数5页

[54]发明名称 自动化网络监视和安全违规干预的方法和装置

[57]摘要

一种网络监视系统,包括用于捕获网络信息包和过滤无效信息包的处理程序过程(10),第一和第二连续分类的记录文档(15a,15b),和用于扫描在网络上发生的所有会话和检查特定规则(38)存在的扫描器过程(30)。当符合规则而指示安全事故时,可以采取包括经过电子或其它邮件通知网络安全官员,或记录或终止网络会话等各种适当动作。监视系统完全地独立于任何其它网络通信和网络文档服务器操作,因此对网络性能没有影响。



I S S N 1 0 0 8 - 4 2 7 4

权 利 要 求 书

1. 一种不依赖于网络服务器在网络上进行监视的网络监视系统，包括：

- 5 用于捕获网络上数据的网络驱动器；
 用于接收来自所述网络驱动器的数据和实时存储所述数据的处理程序过程；
 多个用于接收网络数据和在进一步检查之前存储所述数据的记录文档；
10 用于指定所述多个记录文档中的一个为接收文档同时从所述多个记录文档中另一个文档读取数据，并且用于利用所述数据构造多个会话数据流的扫描器过程，所述会话数据流提供了由会话组织的网络数据通信的顺序再建；
 用于在所述多个会话数据流中的一个读取数据窗口的会话窗口扫描器；
15 一组定义了数据图形的监视规则，在符合所述规则时将触发报警；
 和
 用于响应激发的规则和采取定义的动作的报警处理程序。

20 2. 根据权利要求 1 所述的装置，还包括：

 使用户可以实时看到会话和访问多个包含所述会话窗口处理器维护的会话事件的数据库的用户接口。

25 3. 根据权利要求 1 所述的装置，其中所述处理程序过程过滤特定的网络数据并在从网络接收特定网络数据时加上时间指示。

 4. 根据权利要求 1 所述的装置，其中所述多个记录文档是根据记录索引连续分类的。

30 5. 根据权利要求 1 所述的装置，其中所述会话窗口包括以前检查

过的来自所述会话数据库的数据的一个重叠部分，以便测试应用到包含在一个以上的记录中的数据的规则。

5 6. 根据权利要求 5 所述的装置，其中所述会话窗口重叠是由可能触发规则的最长的文本串确定的。

10 7. 根据权利要求 1 所述的装置，其中所述报警处理程序可以通过向特定的多个目的地发送消息来响应报警。

15 8. 根据权利要求 1 所述的装置，其中所述报警处理程序可以通过强迫用户会话终止来响应报警。

20 9. 根据权利要求 1 所述的装置，其中所述报警处理程序可以通过记录会话来响应报警。

15 10. 一种包含计算机可执行程序编码的固定的计算机可读介质，当把该程序编码装载到一个适当构造的计算机系统中时将使计算机实现权利要求 1 的装置。

20 11. 一种用于在网络上进行监视的方法，包括：
 捕获网络上的数据；
 把所述数据实时存储在多个记录文档之一中；
 利用所述数据构造多个会话数据流，所述会话数据流提供了由会话组织的网络数据通信的顺序再建；

25 读取所述多个会话数据流之一中的数据窗口；
 相对于一组监视规则测试所述数据窗口； 和
 通过采取定义的干预动作响应激发的规则。

30 12. 根据权利要求 11 所述的方法，进一步包括把再建的会话视图实时提供给用户。

13. 根据权利要求 11 所述的方法，进一步包括在存储前过滤特定
网络数据信息包。

5 14. 根据权利要求 11 所述的方法，进一步包括连续地分类记录文
档。

10 15. 根据权利要求 11 所述的方法，进一步包括检查以前检查过的
数据的一个重叠部分以便测试应用到包含在一个以上的记录中的数据
的规则。

16. 根据权利要求 15 所述的方法，其中所述会话窗口重叠是由可
能触发规则的最长的文本串确定的。

15 17. 根据权利要求 11 所述的方法，进一步包括通过向特定的多个
目的地发送消息来响应报警。

18. 根据权利要求 11 所述的方法，进一步包括通过强迫终止用户
会话来响应报警。

20 19. 根据权利要求 11 所述的方法，进一步包括通过记录会话来响
应报警。

25 20. 一种包含计算机可执行程序编码的固定的计算机可读介质，当
把该程序编码装载到一个适当构造的计算机系统中时将使计算机实现
权利要求 11 的方法。

说 明 书

自动化网络监视和安全违规干预的方法和装置

5 本专利文件所公开的一部分内容包含属于版权保护范围的材料。只要它出现在专利和商标局的专利文档或记录中，版权所有人并不反对本专利文件或专利公开的任何复制，但保留所有的版权。

10 本发明涉及一个网络中多个数字设备之间的信息传输和一个互联网中多个网络之间的信息传输。更具体地讲，本发明涉及通过对网络上所有或几乎所有发送的数据进行监视和检查，网络会话的再建，和安全违规干预以保证安全网络通信的方法和装置。

网络设备标准

15 本说明书假定读者对当前 LAN 网应用和 WAN 互联网应用中使用的一般概念、协议和设备有一定了解。由于这些标准是广泛公开使用的，因此不再对它们进行全面的讨论。

一般 LAN 配置

20 图 3 示出了当今可以在中等规模办公单位或院校环境中使用的一种类型的局域网(LAN)80 的概况图，并且作为讨论其中可以有效地使用本发明的一种网络类型实例。LAN 是由各种硬件和软件元件装备而成的，它们共同操作以使多个数字设备可以在 LAN 内交换数据，并且 LAN 也可以包括对，例如 WAN82 和 84 这样的外部广域网(WAN)的互联网连接。像 80 这样的典型现代 LAN 包括一至多个可以对整个 LAN 上的数据传输作出响应的中间系统(IS)，例如 IS60-62，和代表终端用户设备的多个终端系统(ES)，例如 ES 50a-d，51a-c，和 52a-g。ES 可以是熟悉的终端用户数据处理设备，例如，个人计算机，工作站，用于拨号连接的调制解调器，和打印机，并且可以是额外的数字设备，例如数字电话或实时视频显示器。不同类型的 ES 可以在同一个 LAN 上共同操作。可

以有许多不同的 LAN 结构，而且本发明并不限于应用在图 3 所示的网络中。

网络通信中的安全问题

5 LAN 和 WAN 环境中一个日益突出的问题是，在大多数现有技术的网络中，线路上信息包通信基本上是不安全的。LAN 通常是设计为包括通过互联网或拨号连接连接的处理设备在内的任何连接到 LAN 的用户处理设备提供容易和灵活的网络资源访问。在一个企业 LAN 中，许多用户可以访问包含诸如帐目结算或金融交易信息之类的能够操纵以进行犯罪或掩盖罪行的数据的计算机文档。防火墙是一种防止从 LAN 外部非法访问 LAN 上文档的技术。但是，大量的计算机犯罪是由 LAN 合法的、内部使用人员以非法的方式访问或操纵数据进行的。防火墙不能防止未经授权的内部人员访问 LAN 资源。

15 其它的安全问题涉及电子欺诈和嗅探(spoofing and sniffing)。在 LAN 的一个部分，例如 72d，该 LAN 部分上每个 ES 都会听到发送给该部分上任何 ES 的每个信息包。网络中每个 ES 一般都有一个唯一的以太网(或 MAC)地址，一个 ES 将放弃它听到的任何不是以它的 MAC 地址定址的信息包。但是，网络并不强迫 ES 放弃非定址于它们的信息包，
20 并且能够以一种不加选择的模式(promiscuous mode)操作，在这种模式中 ES 读取它在网络上听到的每个信息包并把该信息包向上传送到该 ES 中运行的更高级的软件。既然适配器配置或调试过程中可以合法地使用不加选择的模式，一个 ES 也可以使用它不经授权地读取和检查网络上所有网络通信。在本领域中有时把这种行为称为嗅探。

25 有关嗅探的问题可能发生在从一个 LAN 发射的过程中，其中在 LAN 上运行的软件可以发送出网信息包地址，以模仿另一个 ES 的信息包。这种技术在本领域中称为电子欺诈。一个欺骗另一个 ES 的信息包的不道德的用户可以在从该 ES 发送的信息包流中引入不需要的数据，
30 例如病毒，或是可以劫持一个用户的网络会话和得以非法访问其它系统

资源。

已经提出或使用了许多技术来加强网络安全。所有这些技术一般都依赖于对 MAC 地址和 IP 地址或用户识别码的验证。但是，这些技术存在局限性，因为不能保证网上发送的信息包在它们的包标题中有一个有效的 MAC 或 IP 地址，并且也不能保证 LAN 的合法用户不会以非法方式访问或操纵 LAN 数据。
5

需要的是一种能够监视网上行为和扫描非法网络行为并且在检测到非法行为时自动采取动作的简单、廉价的系统。最好这种技术能够在
10 网络中使用而又不会降低网络的操作性能。

为了简明，本发明的讨论参考特定实施例的网络设备和概念。但是，本发明的方法和装置可以用各种类型的网络设备操作，包括与图 3 中所示的以及下面要说明的特定实例极不相同的网络。因此本发明除了
15 受附属的权利要求的限定外，不受上述实施例的限制。

在许多现有的 LAN 系统中，网络上的数据被分组成称为信息包的离散单元，每个信息包具有一个来源和目的地的指示。尽管本发明并不限于打包的数据，但为了易于理解，在这里是以信息包来说明数据的。
20

本发明是一种用于在 LAN 上发送数据的改进方法和装置。根据本发明，一种网络安全代理™(Network Security Agent™)监视系统能够读取在一网络部分上发送的所有信息包，再建所有的用户会话，和为值得注意的或可疑的行为扫描所有用户会话，所有这些都是实时进行的并且对网络性能没有任何显著影响。当检测到任何值得注意或可疑行为时，
25 产生警告并可以采取适当的干预动作。

本发明利用了信息包嗅探，会话再建，和会话扫描，以便扫描会话
30 检查非法行为，并且在检测到非法行为时，采取预定的自动干预动作。

本发明使用了自动实时会话再建和扫描，以完成对典型的 LAN 上每日产生的数千万信息包的网络监视。

根据本发明，优化地设计硬件和软件元件，以便能够实时地读取 LAN 上所有信息包，和再建会话。在本发明中结合了从以太网控制器直接读取低级信息包的定制例程，以便 100% 地捕获全部网络信息。

在一个实施例中，本发明包括以一种为数据操作和 I/O 而优化的语言写出的软件元件。本发明包括一组用户接口，以使网络管理人员能够检查本发明收集的数据和设定某些参数。

参考以下的附图和详细说明将会更好地了解本发明。

图 1 是根据本发明的网络监视系统的方框图；

图 2 是根据本发明的一个实施例的处理程序过程的方框图；

图 3 是一个其中可以使用本发明的一般化 LAN 的示意图；

图 4 示出了根据本发明的一个实施例的带有远程监视系统代理的多个远程网络；

图 5 示出了根据本发明的一个实施例的远程监视系统代理；

图 6 是根据本发明的一个可以用一个软件实施例配置的计算机系统的方框图。

综述

图 1 是根据本发明的一个实施例的网络监视系统的方框图。图 1 中示出了一个指示连接到 LAN 或其它数据通信媒介的通信信道 5。网络驱动器 7 从信道 5 接收打包的或其它形式的数据，网络驱动器 7 可以包括硬件和软件组成部分，以快速读取信道 5 上的信号，并把它们转换成计算机可读数据。网络驱动器 7 可以是预先存在的或客户网络接口，并设置为它在其中接收所有或几乎所有信道 5 上发送的数据的不加选择模式。把网络驱动器 7 上接收的数据送到处理程序过程 10，在如下面将要说明的那样把数据作为记录放在文档 15a 或 15b 之一中之前，处理程序

过程 10 可以进行像下面将要说明的某种数据过滤或处理。如已知的现有技术那样，对文档 15a 和 15b 进行连续的分类。扫描器过程 30 从文档 15a-b 读取记录，并把记录组织到会话数据库 32 中。会话数据库 32 包含在一特定会话中接收的所有信息包的顺序列表。根据本发明，扫描器过程 30 包括会话窗口(SW)扫描器 34。SW 扫描器 34 定义了用于读取会话数据库 32 中数据窗口和对那些数据窗口测试一组规则 38 的会话窗口。

根据本发明，适当构造会话窗口，以便提供叠加的和滑动的数据窗口，因而可以充分地测试规则，即使会激发规则的数据在接收信息包时被分割在记录文档 1 和记录文档 2 之中。维护数据库 40a-d，以提供诸如访问过的 URL，访问过的域，访问过的头十个 URL 之类的有关网络使用参数的信息。设计用户接口 42，以从一工作站，例如 45，接受用户指令，和像以下将说明的那样向工作站 45 显示请求的数据。一种可选的实时显示引擎 44 可以与处理程序过程 10 交互作用，显示实时会话数据。

根据本发明，通过组合两个记录文档 15a 和 15b，在前面捕获的信息包正在被扫描的同时，在信道 5 上捕获最新发送的信息包，两个文档的组合是这样操作的，在为监视事故而扫描和分析一个记录文档的同时，处理程序过程 10 用连续分类的信息包填写另一个记录文档。与记录文档相关联的也可以是一个用于存储更大数量的信息包数据的存储空间 16。

25 处理程序过程

图 2 示出了根据本发明的一个实施例的处理程序过程 10 的功能。处理程序 10 读取信道 5 上所有数据或数据的大子集，并且选择用于以后再建的会话信息包。处理程序 10 与扫描器 30 和实时显示引擎 44 通信。

处理程序 10 确定从信道 5 读取信息包的优先次序，在繁忙的 LAN 上一天可以有超过 50,000,000 个信息包。处理程序的一个实施例使用了小状态表，并且完全是事件驱动的。从网络 5 信息包读取数据得到最高优先次序，因而不会丢失希望的信息包。

5

处理程序过程 10 包括用于初始信息包过滤的过滤过程 22。根据本发明，可以把过滤过程 22 设定为根据多个标准滤除信息包，包括由于不正确的校验和或某些识别滤除无效信息包。

10

处理程序过程 10 也包括用于为每个接收的网络信息包加上时间标记的定时器 23，和为每个接收的信息包加上顺序号的定序器 25，以便唯一地标识每个信息包。处理程序译码器 26 为网络信息包部分译码，并且可以被编程以处理某种内部信息包压缩。

15

记录器 28 把每个处理过的数据信息包作为记录写入连续分类的记录文档 15a—15b。写入哪一个文档是由如下所述的扫描器过程 30 确定的。图 1 中示出了代表性的记录 18，具有包括指示源、目的地或目的地组、服务器、顺序号、数据、时标(T.S.)、和处理顺序号(HSQ)的多个字段。

20

扫描器过程

25

扫描器 30 的基本任务是会话再建和会话扫描。扫描器 30 以定时的间隔设置一个请求一组用于会话再建的信息包的标记。信息包一般是由处理程序 10 从文档 15a 或 15b 提供的，并且处理程序 10 开始在没有被扫描器 30 访问的文档中存储新接收的记录。在扫描器 30 接收信息包时，它立即进行处理以再建会话。

30

会话是根据诸如 IP 地址和端口(对于 TCP/IP)或本地传输协议(LAT)虚拟电路和槽之类的源和目的地指示的任何组合再建的。与一个会话标识符一起独立地再建每个识别的会话。保留以前再建的会话数据的某部

分，以使 SW 扫描器 34 能够检测可能跨越两个记录文档的图形。

规则和干预动作

使再建的会话通过一系列用户定义的规则 38。在一个实施例中，
5 每个规则仅由报警名和图形组成。当 SW 扫描器 34 检测到会话窗口包含图形时，触发报警。

与每个报警名相关联的是报警说明，在报警触发时要采取的动作的
10 列表，和报警的优先等级。当触发报警时，在记录 39 中记录一个事故。
事故记录 39 包含事故的识别数据，例如报警名，说明，用户注册名，
位置(TCP/IP 或 LAT 地址/端口)，和一个会话的快照，其有一箭头指向
引起报警触发的图形。

在记录了事故之后，报警处理程序 36 采取任何报警动作。可能的
15 报警动作包括向某个人或一组人发送电子邮件，包含例如触发报警的
名，位置(TCP/IP 或 LAT 地址/端口)，用户注册名，和具有对引起报警
触发的图形的指示的会话快照。

另一种可能的报警动作包括记录从报警瞬间向前的会话以便以后
20 重放。记录包括用户所做的涉及通过网络发送的每一次击键、每一件事。
报警还可能采取动作终止产生报警的用户连接。

扫描器 30 也可以进行会话数据库清除过程，例如清除非活动的注
册信息。

实时显示模块

实时显示模块 44 是本发明的一个可选组成部分，它负责实时显示会话。
当实时显示模块 44 从报警处理程序 36 或用户接口模块 42 接收到监视消息时，它产生终端仿真弹出式窗口。每个窗口一次击键接一次
30 击键地实时显示用户会话。在这种场合，扫描器 30 和实时显示模块 44

都从处理程序 10 接收某些信息包。然后，实时显示模块 44 向处理程序 10 发送消息，请求复制来自被监视会话的信息包并送到实时显示模块 44。当接收到监视信息包时，把它们格式化并送到适当的终端仿真弹出式窗口。

5

如果会话中断连接，在弹出式窗口上显示会话被关闭的消息，并且停止会话监视。如果用户手动关闭弹出式窗口，该会话的会话监视也被中断。

10

用户接口模块

用户接口模块 42 提供了至网络监视系统的用户接口。从模块 42 可以看到会话，产生报告，定义报警和规则，以及采取会话动作。

15

在请求会话监视时，模块 42 与实时显示模块 44 通信。模块 42 执行的所有其它显示和动作都是通过数据库操作执行的。扫描器 30 注意数据库变化(例如新的报警或规则)，并在需要时重建它的内部表。

20

模块 42 可以用鼠标，直接从键盘，或通过任何其它计算机工作站和用户之间的连接方法操作。在所有的决定点都提供有广泛的在线帮助。

实例

通过一个实例可以进一步理解本发明的操作。为了这个实例，假设 LAN80 是一个投资管理公司中的局域网。该网络可以包括一个特定雇员被授权在任何时间从包括拨号连接在内的任何地点使用的多种功能。雇员可以在任何时间访问的一个功能是办公室间电子邮件功能。此外，LAN 可以包括有关顾客帐目的敏感性数据，一般这种数据只有授权的雇员在工作时间在办公室处理顾客帐目时才能访问。标准现有安全措施，例如文档访问授权，可以指定某些雇员使用这种数据，但是这种措施通常不能限制基于该雇员是否正在通过拨号连接连通的访问，或基于该雇

30

员是否在有效工作时间中试图访问数据的访问。

根据本发明，可以设定一个规则，监视对顾客文档结构内任何文档的访问。这种规则可以是十分简单的规则，检查通过网络从客户机处理器发往服务器处理器的特定文本串，其中该文本串代表一个文档路径名。为进一步说明本发明的这些方面，假设完整的文档路径名被分割在一个以上的网络信息包中，并且正在扫描器 30 请求从记录文档 1 切换到记录文档 2 时，接收到两个网络信息包。

10 这一规则可以表达为：

```

IF      text_contains("\data\customer") AND
        (time()=off_hours OR connection()=dial_up)
THEN
    email(session_data, supervisor)
    terminate_session()
ENDIF

```

根据这个实例，在信道 5 上发送来自会话 S2 的以数据 “\data\cu” 结束的第一信息包，并由处理程序 10 放入记录文档 15a 中，在从 S2 接收 20 到下一个信息包之前，扫描器 30 向处理程序 10 发出切换记录文档的信号。然后，扫描器 30 读取记录文档 1 中的数据，并把来自 S2 的数据放入适当的会话数据库文档中。接下来，会话窗口扫描器 34 为上述规则扫描 SW2 中的文本，并且由于没有发现文本，不激发该规则。

25 此时，在信道 5 上发送来自会话 S2 的以数据 “stomer” 开始的第二信息包，并由处理程序 10 放入记录文档 15b 中。当扫描器 30 充分地分析了来自 15a 的数据之后，它切换到 15b，并把来自 S2 的附加数据放入适当的会话数据库文档中。接着，会话窗口扫描器 34 为上述规则扫描 SW2 中的文本，并且由于 SW2 包括至少 13 个字节的重叠，激发了 30 规则。事故记录在 39 中，并由处理程序 36 处理报警。

特定实施

本发明的主要挑战是要能够实时地读取 LAN 上所有数据信息包。在一种专用的装备中，选择了在 233Mhz 至 500Mhz 速度的 Digital Alpha/AXP CPU 上运行的 OpenVMS 操作系统在处理会话再建，实时扫描和实时显示任务的同时满足读取 100% 的繁忙的 LAN 信息包的沉重处理要求。

用于从网络控制器直接读取低级信息包的定制例程是利用 OpenVMS 的异步 QIO 服务以 C 语言写的。实时显示模块也是用 C 语言写的。

对于会话再建和实时会话扫描，一个实施例是用 INTOUCH 4GL(TM) 编程语言实现的，该语言是本发明的受让人开发的。INTOUCH 4GL 是一种专门设计用于数据操作和文本扫描的高性能语言。为了监视代理使用，包括有专门高速图形匹配功能来加强 INTOUCH 4GL。

INTOUCH 4GL 也可以用于用户接口和事故跟踪，报告，数据库维护，和记录的会话重放。

远程监视代理

图 4 和 5 示出了本发明的一个不同实施例，其中可以与互联网一同使用多个远程监视代理(RSA)，以便在一个地点捕获网络数据通信，并在另一个地点进行通信分析和会话再建。图 4 显示了连接于不同 WAN/LAN 网 105a 的 RSA100a-c。根据这个实施例，RSA100a-c 收集来自它们连接的 LAN 或 WAN 的所有网络数据通信，但 RSA100a-c 不是充分地扫描该通信，而是以可以发送到远程监视服务器(RSS)110 的形式存储收集的信息包。RSS110 接收用于 RAS100a-c 的信息，并把这个信息发送至根据本发明的执行如上所述的会话再建，规则检查和报警处理的监视系统 1。

根据一个特定的实时例，RSA100a-c 在它们连接的 WAN/LAN 上收集多个信息包，并把多个信息包压缩成可以跨越互联网通过 WAN/LAN 发送回 RSS110 的单个互联网信息包。根据这个实施例，以这种方式，
5 RSA100a-c 能够允许位于一个城市的监视系统 1 监视位于不同城市的几个 WAN/LAN，其仅需要把 RSA 插入到远程网中而无需对该网络进行任何其它的改变。

图 5 示出了根据本发明的一个 RSA 的实例。处理程序过程 10 实际上如上面所述的一样接收并处理 LAN/WAN 数据，并存储在多个记录文档 15a-b 之一中。然后，互联网打包器 130 读取记录文档数据，互联网打包器 130 把多个 LAN/WAN 信息包存储到一个互联网信息包中，然后把它送到驱动器 7，以便经互联网发送到 RSS110。在一个替代实施例中，由一个 RSA 接收 LAN/WAN 信息包并标时，并立即以 RSA 最少的
10 附加处理经互联网单独或多组发送。
15

本发明可以以记录在固定介质上的或电子发射的软件指令实现。在这种情况下，图 3 的监视系统 1 将是一个高性能的计算机系统，软件指令将使计算机 1 的存储器和其它存储介质构造成如图 1 所示的形式，并
20 使计算机 1 的处理器根据本发明操作。

图 6 示出了一个用于执行本发明软件的计算机系统的实例。图 7 示出了一个计算机系统 700，它包括监视器 705，机箱 707，键盘 709，
25 和鼠标 711。机箱 707 里安装着用于读取 CD-ROM 或其它类型盘 717 的盘驱动器 715，并安装着诸如处理器、存储器，磁盘驱动器等其它熟悉的计算机组件(未示出)，以及用于连接到通信信道 5 的适配器 1。

现在已经参考特定的实时例说明了本发明。对于熟悉本领域的技术人员其它实施例是显而易见的。具体地说，已经说明了特定的处理次
30 序，并且各种功能也是以特定的顺序说明的，但是可以以不同的顺序安

00·00·21

排许多这样的子功能而不改变本发明的基本操作。因此，除了附属权利要求所指示的之外，本发明并不受上述实施例的限制。

说 明 书 附 图

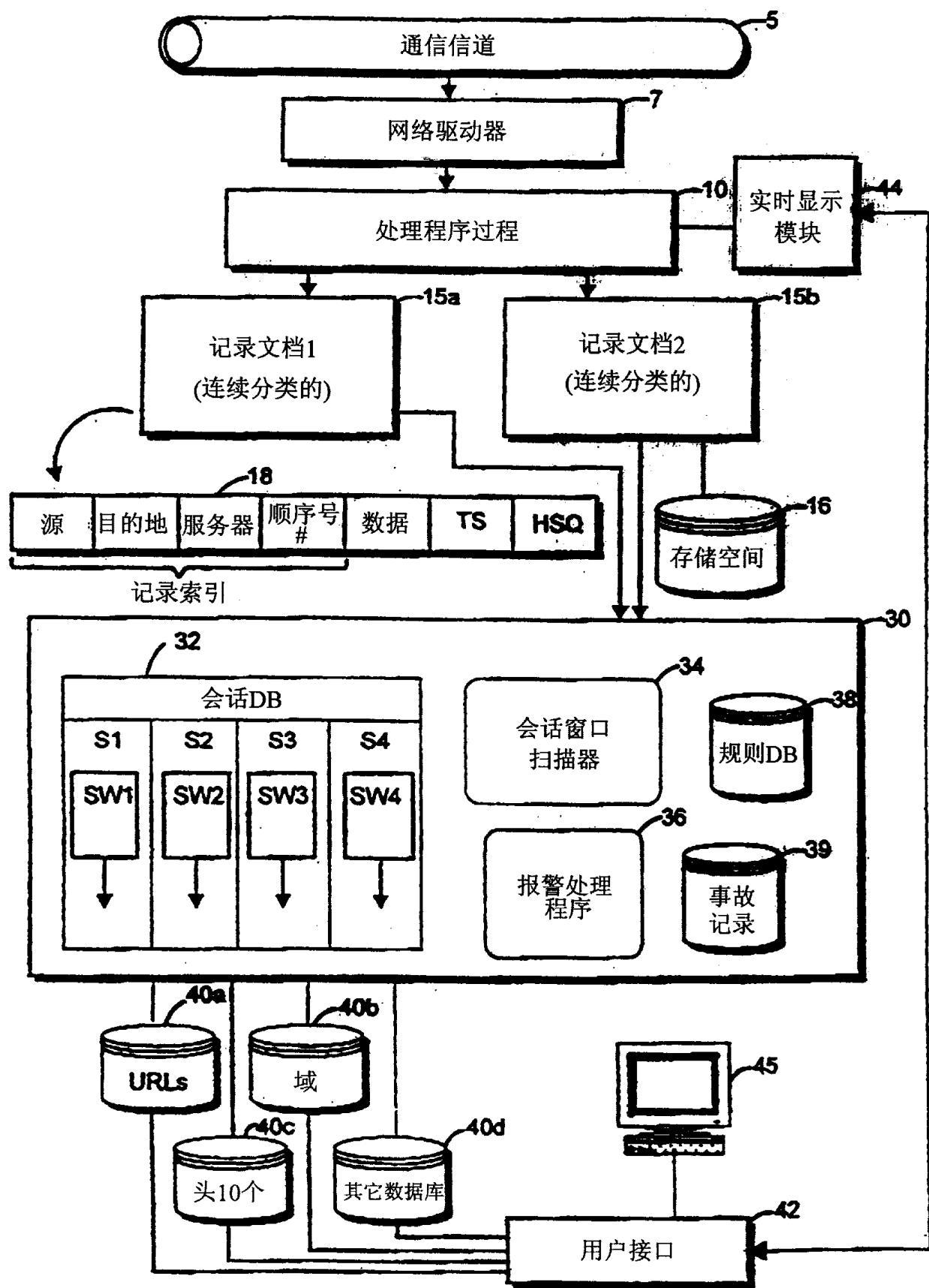


图 1

99·06·21

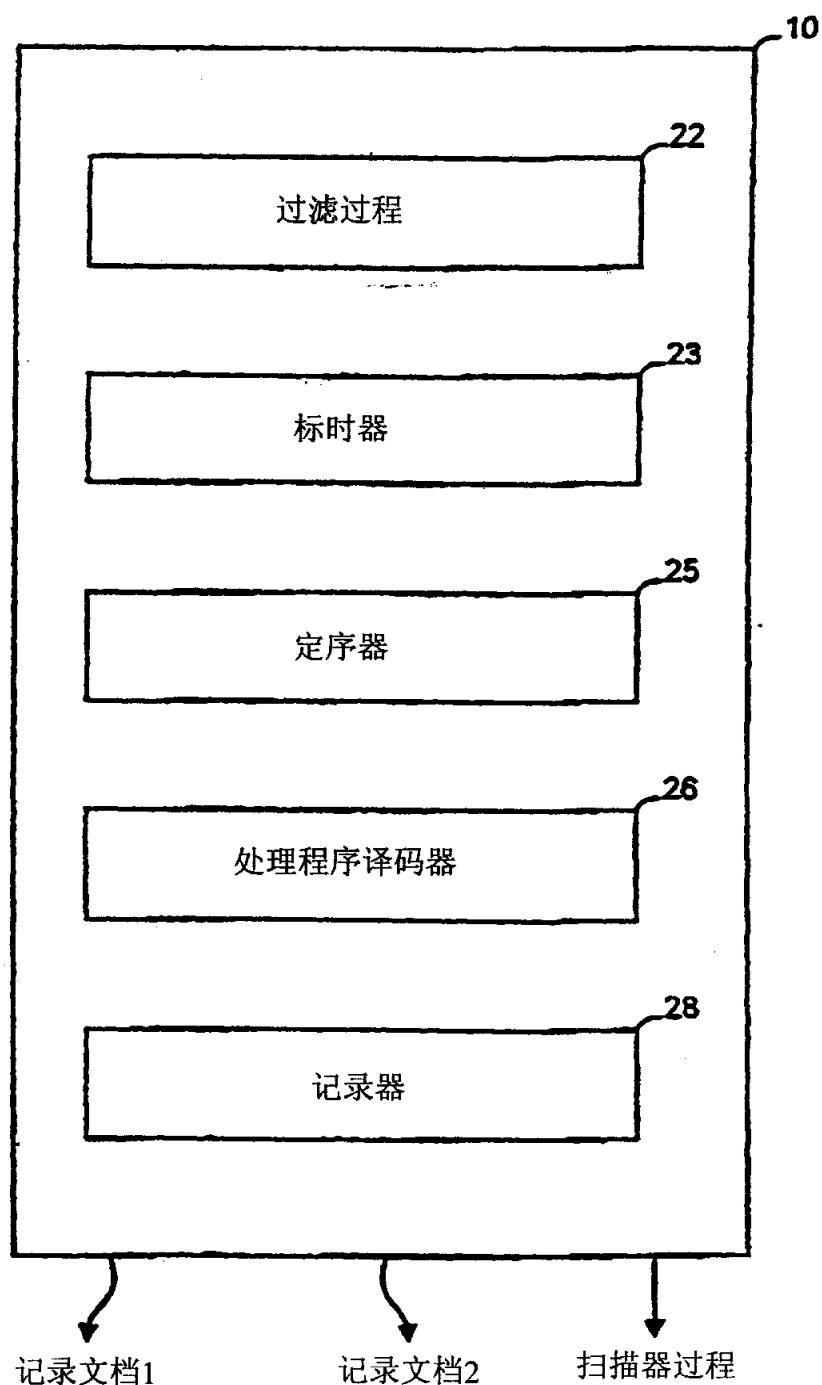


图2

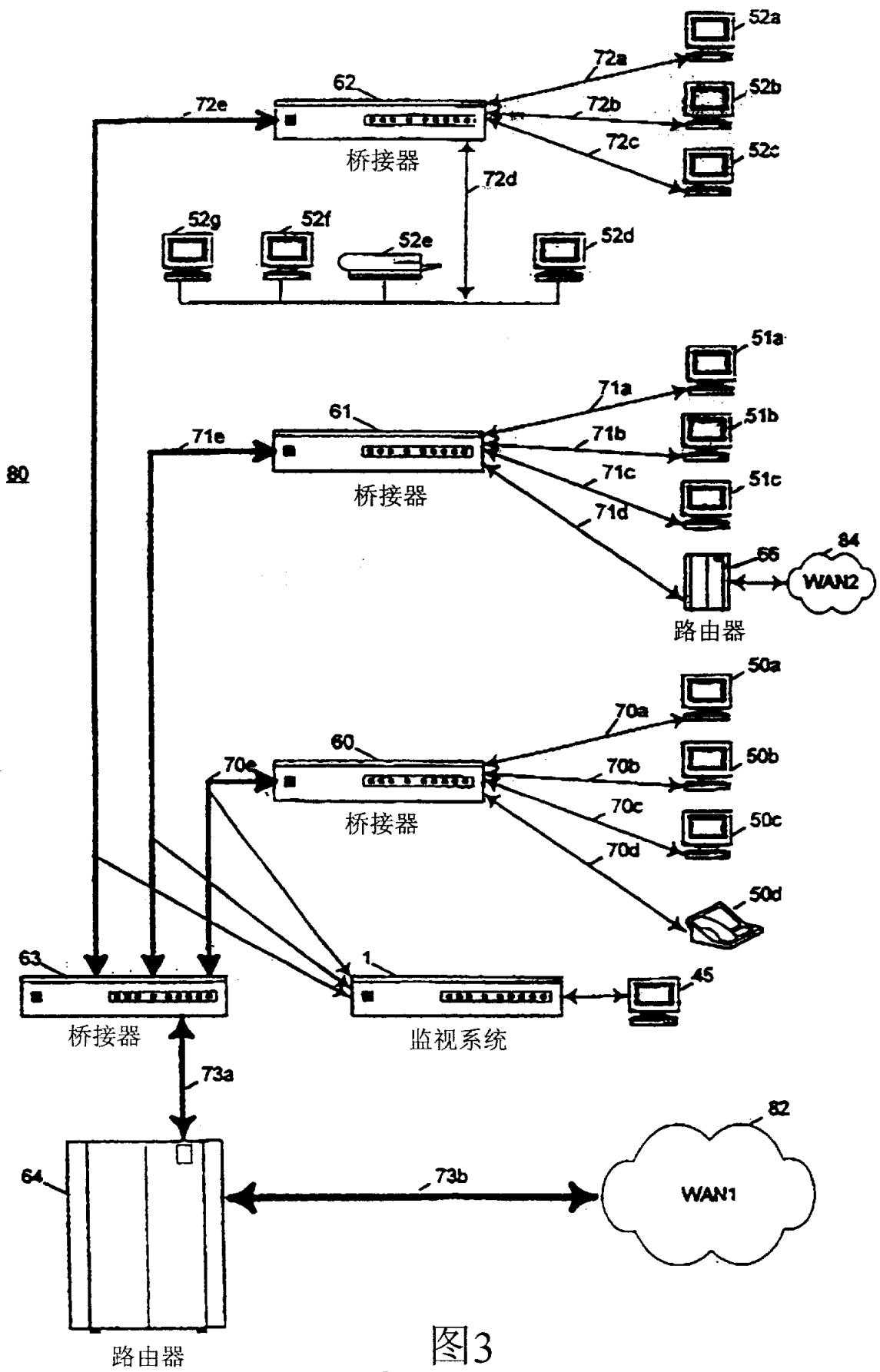


图3

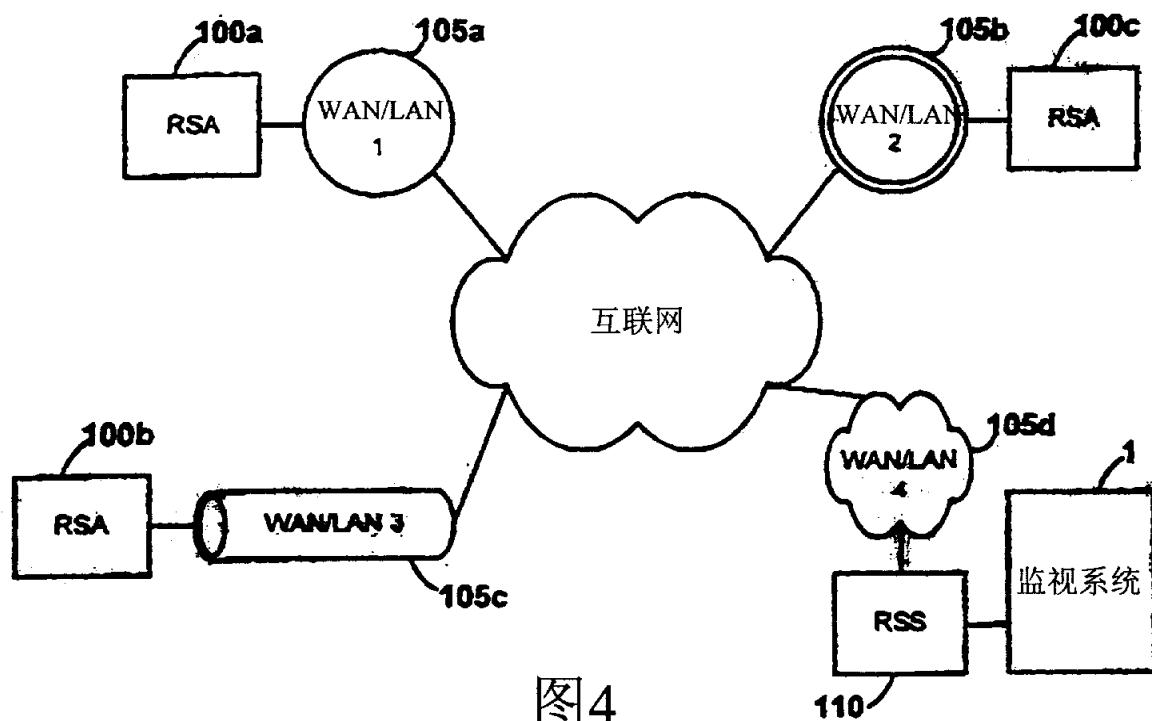


图4

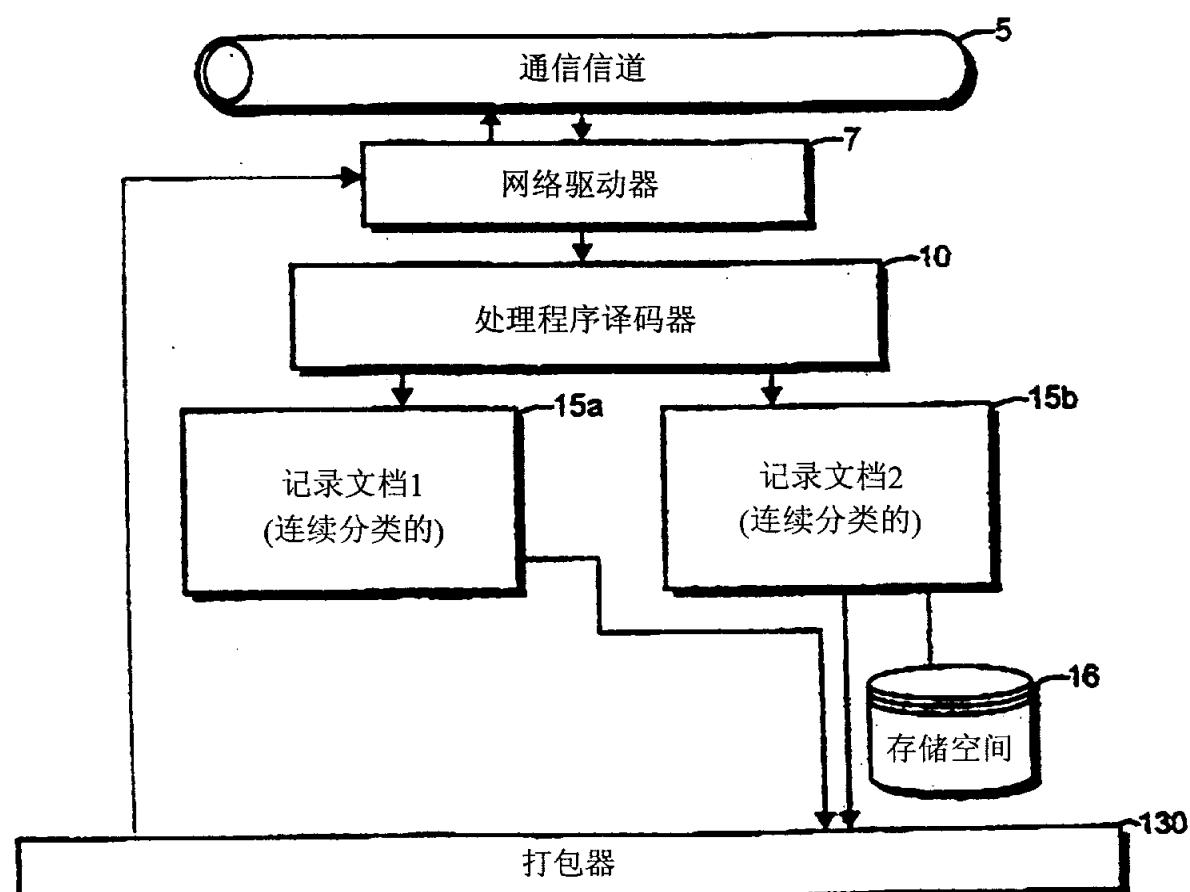


图5

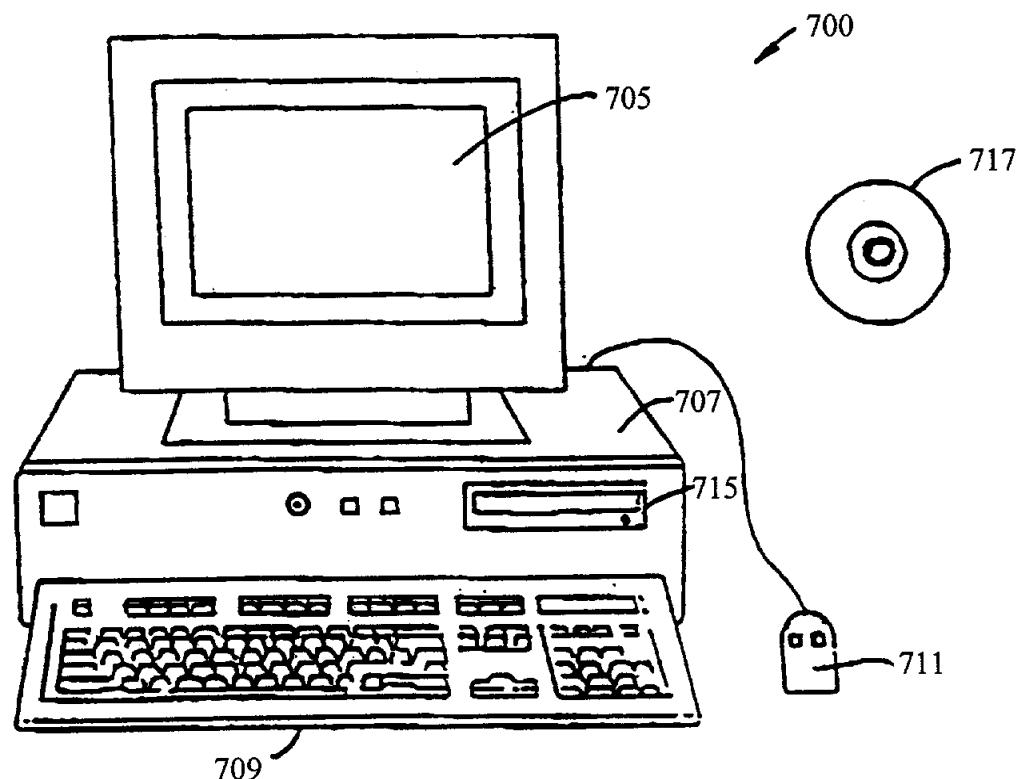


图6