[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)
G06F 21/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200810065370.8

[43] 公开日 2009 年 8 月 26 日

[11] 公开号 CN 101515923A

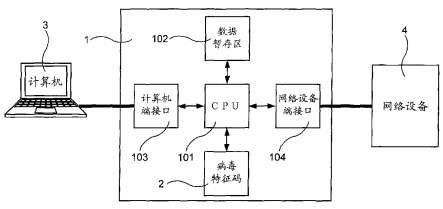
[22] 申请日 2008.2.19
[21] 申请号 200810065370.8
[71] 申请人 黄金富
地址 100032 北京市西城区金融街 27 号投资广场 B 座 19 层
[72] 发明人 黄金富
权利要求书 3 页 说明书 7 页 附图 2 页

[54] 发明名称

设于计算机与网络设备之间的防病毒装置和方法

[57] 摘要

一种设于计算机与网络设备之间的防病毒装置和方法，由防病毒装置(1)将计算机与网络设备之间传送的数据暂存于数据暂存区(102)，并对数据暂存区(102)内的暂存数据进行病毒过滤操作，以查找出暂存数据是否带有与其中任何一病毒特征码(2)相符合的数据，当发现暂存数据带有其中任何一病毒特征码(2)相符合的特征时，对该暂存数据进行拦截，使该带有病毒特征的暂存数据不能通过防病毒装置(1)传送到目的地。 本发明的防病毒装置(1)与计算机的操作系统无关，由于防病毒装置(1)是一个独立的硬体设备，即使操作系统出现漏洞被病毒攻击，防病毒装置(1)仍然能不受干扰继续对计算机与网络设备之间传送的数据进行病毒过滤。



1. 一种计算机防病毒装置，设置于计算机与网络设备之间，主要用于检测计算机与网络设备之间传送的数据是否含有病毒特征，其特征在于，所述的防病毒装置（1）内设有包括CPU（101）、数据暂存区（102）、计算机端接口（103）和网络设备端接口（104），所述的防病毒装置（1）并储存有各病毒特征码（2），其中，所述的 CPU（101）通过计算机端接口（103）与计算机（3）相连接，及通过网络设备端接口（104）与网络设备（4）相连接，以及，所述的防病毒装置（1）按预定程序运作，将计算机（3）与网络设备（4）之间传送的数据暂存于数据暂存区（102），并对数据暂存区（102）内的暂存数据进行病毒过滤操作，以查找出暂存数据是否带有与其中任何一病毒特征码（2）相符合的数据，当发现暂存数据带有其中任何一病毒特征码（2）相符合的特征时，对该暂存数据进行拦截，使该带有病毒特征的暂存数据不能通过防病毒装置（1）传送到目的地，而没带病毒特征的暂存数据则于病毒过滤操作后由防病毒装置（1）转送到目的地。

2. 如权利要求 1 所述的计算机防病毒装置，其特征在于，所述的计算机端接口（103）可以是以太网（Ethernet）网络接口、或 USB 接口、或 WIFI 无线网络接口、或蓝芽（Bluetooth）无线网络接口。

3. 如权利要求 1 所述的计算机防病毒装置，其特征在于，所述的网络设备端接口（104）可以是以太网（Ethernet）网络接口、或 USB 接口、或 WIFI 无线网络接口、或蓝芽（Bluetooth）无线网络接口。

4. 如权利要求 1 所述的计算机防病毒装置，其特征在于，所述的防病毒装置（1）上设有记忆卡接口（105）和与该记忆卡接口（105）相连接的记忆卡（5），以及，所述的记忆卡（5）内储存有各病毒特征码（2）。

5. 一种计算机防病毒方法，采用如权利要求 1 至 4 任一项所述的计算机防病毒装置，其特征在于，所述的方法包括如下步骤:

   1. 在计算机（3）与网络设备（4）之间加设防病毒装置（1）；
   2. 在防病毒装置（1）内预先储存有各病毒特征码（2）；
   3. 防病毒装置（1）将计算机（3）与网络设备（4）之间传送的数据暂存于数据暂存区（102）；
   4. 防病毒装置（1）对数据暂存区（102）内的暂存数据进行病毒过滤操作，以查找出暂存数据是否带有与其中任何一病毒特征码（2）相符合的数据;
   5. 当防病毒装置（1）发现暂存数据带有其中任何一病毒特征码（2）相符合的特征时，对该暂存数据进行拦截，使该带有病毒特征的暂存数据不能通过防病毒装置（1）传送到目的地，而没带病毒特征的暂存数据则于病毒过滤操作后由防病毒装置（1）转送到目的地。

6. 如权利要求 5 所述的计算机防病毒方法，其特征在于，当所述的防病毒装置（1）发现暂存数据中带有其中任何一病毒特征码（2）相符合的特征时，向用户发出提示信号。

7. 如权利要求 5 所述的计算机防病毒方法，其特征在于，所述的方法还包括如下步骤，是防病毒装置（1）发现暂存数据中带有其中任何一病毒特征码（2）相符合的特征时，向用户发出提示信号后，用户在防病毒装置（1）上作出如下的操作步骤:

用户按一次拦截键后，防病毒装置（1）拦截该数据，使该数据不能通过防病毒装置（1）传送到目的地;

或

.用户按一次通行键后，防病毒装置（1）允许该数据转送到目的地。

设于计算机与网络设备之间的防病毒装置和方法

【技术领域】

本发明涉及计算机数据安全技术领域，特别是涉及一种设于计算机与网络设备之间的防病毒装置和方法。

【背景技术】

计算机技术发展突飞猛进，计算机已经成为人们日常工作必需的工具之一，但是计算机病毒的出现，干扰了人们使用计算机的工作，现时绝大部分的计算机病毒具有传染性，尤其是通过网络传播的病毒,可以在很短时间内通过网络感染网络上其他的计算机。这些感染了病毒的计算机，可以给计算机用户带来严重的影响，用户储存在计算机内的数据随时会被病毒破坏，给用户造成无法估量的损失，是一个极待解决的问题。

【发明内容】

本发明的目的，在于提供一种计算机防毒装置和方法，设置于计算机与网络设备之间，对计算机与网络设备之间传送的数据进行病毒过滤，使计算机病毒不能通过网络设备传播。

本发明的目的是这样实现的，采用这样一种计算机防病毒装置，设置于计算机与网络设备之间，主要用于检测计算机与网络设备之间传送的数据是否含有病毒特征，其特征在于，所述的防病毒装置（1）内设有包括 CPU（101）、数据暂存区（102）、计算机端接口（103）和网络设备端接口（104），所述的防病毒装置（1）并储存有各病毒特征码（2），其中，所述的 CPU（101）通过计算机端接口（103）与计算机（3）相连接，及通过网络设备

端接口（104）与网络设备（4）相连接，以及，所述的防病毒装置（1）按预定程序运作，将计算机（3）与网络设备（4）之间传送的数据暂存于数据暂存区（102），并对数据暂存区（102）内的暂存数据进行病毒过滤操作，以查找出暂存数据是否带有与其中任何一病毒特征码（2）相符合的数据，当发现暂存数据带有其中任何一病毒特征码（2）相符合的特征时，对该暂存数据进行拦截，使该带有病毒特征的暂存数据不能通过防病毒装置（1）传送到目的地，而没带病毒特征的暂存数据则于病毒过滤操作后由防病毒装置（1）转送到目的地。

以及，采用这样一种计算机防病毒方法，采用如前面所述的计算机防病毒装置，其特征在于，所述的方法包括如下步骤:

1. 在计算机（3）与网络设备（4）之间加设防病毒装置（1）；
2. 在防病毒装置（1）内预先储存有各病毒特征码（2）；
3. 防病毒装置（1）将计算机（3）与网络设备（4）之间传送的数据暂存于数据暂存区（102）；
4. 防病毒装置（1）对数据暂存区（102）内的暂存数据进行病毒过滤操作，以查找出暂存数据是否带有与其中任何一病毒特征码（2）相符合的数据；
5. 当防病毒装置（1）发现暂存数据带有其中任何一病毒特征码（2）相符合的特征时，对该暂存数据进行拦截，使该带有病毒特征的暂存数据不能通过防病毒装置（1）传送到目的地，而没带病毒特征的暂存数据则于病毒过滤操作后由防病毒装置（1）转送到目的地。

这样就实现了本发明的目的。

只要在计算机（3）与网络设备（4）之间设置了本发明的防病毒装置（1），就可以切断传播病毒的其中一条最主要的途径，令病毒无法通过网络设备（4）传播给计算机（3）。这种采用独立的硬体设备对病毒的传播途径进行过滤拦截的防病毒方法，比一般采用软件扫描内存的防病毒方法更有效，由于防病毒装置（1）是一个独立的硬体设备，所以不会出现扫毒软件被病毒骑劫的类似情况。

【附图说明】

图 1 是本发明的防病毒装置（1）第一实施例的结构示意说明图；

图 2 是本发明的防病毒装置（1）第二实施例的结构示意说明图；

图 3 是本发明的防病毒装置（1）第三实施例的结构示意说明图；

图 4 是本发明的防病毒装置（1）第四实施例的结构示意说明图。

图中，相同的数字代表相同的装置、部件器件，附图是示意性的，用以说明本发明的构成和主要特征。

【具体实施方式】

下面结合附图，对本发明的计算机防病毒装置和方法作进一步详细说明。

参阅图 1，图 1 是本发明的防病毒装置（1）第一实施例的结构示意说明图，图中示出的防病毒装置（1）内设有包括 CPU（101）、数据暂存区（102）、计算机端接口（103）和网络设备端接口（104），所述的防病毒装置（1）并储存有各病毒特征码（2），其中，所述的 CPU（101）通过计算机端接口（103）与计算机（3）相连接，及通过网络设备端接口（104）与网络设备（4）相连接，以及，所述的防病毒装置（1）按预定程序运作，将计算机

（3）与网络设备（4）之间传送的数据暂存于数据暂存区（102），并对数据暂存区（102）内的暂存数据进行病毒过滤操作，以查找出暂存数据是否带有与其中任何一病毒特征码（2）相符合的数据，当发现暂存数据带有其中任何一病毒特征码（2）相符合的特征时，对该暂存数据进行拦截，使该带有病毒特征的暂存数据不能通过防病毒装置（1）传送到目的地，而没带病毒特征的暂存数据则于病毒过滤操作后由防病毒装置（1）转送到目的地。

在设置方面，病毒特征码（2）是预先储存到防病毒装置（1）内，防病毒装置（1）可以通过不同的途径更新所储存的病毒特征码（2），例如防病毒装置（1）可通过网络连线到指定的防病毒网站，从防病毒网站下载包含病毒特征码（2）的文件。在防病毒网站方面，防病毒网站可以采用数字证书等的加密方法，以确保包含病毒特征码（2）的文件的完整性和不被窜改，例如防病毒网站预先将包含病毒特征码（2）的文件以指定的密钥加密，然后由防病毒装置（1）下载该文件，并将该文件以对应的密钥进行解密，这样可保证该文件不会被病毒或其他程式窜改。

在本说明书中，网络设备（4）是指供计算机连接到网络的设备，包括各类网络集线器（HUB）、路由器（Router）、网关（Gateway）等等之类网络上的设备。

参阅图 2，图 2 是本发明的防病毒装置（1）第二实施例的结构示意说明图，与第一实施例相比，不同之处在于图 2 的实施例增设了记忆卡（5），图 2 的实施例是本发明的更进一步改进，图中示出的防病毒装置（1）上设有记忆卡接口（105）和与该记忆卡接口（105）相连接的记忆卡（5），以及，所述的记忆卡（5）内储存有各病毒特征码（2）。与图 1 的实施例相比，不同之处在于图 2 的实施例中，将病毒特征码（2）储存到记忆卡（5）上，然后通过记忆卡接口（105）与 CPU（101）相连接，这样就可以随时为

防病毒装置（1）更换储存有最新的病毒特征码（2）的记忆卡（5），方便随时更新病毒特征码（2）。例如使用计算机连线到指定的防病毒网站下载包含最新的病毒特征码（2）的文件到记忆卡（5）上，然后将该记忆卡（5）插到防病毒装置（1）的记忆卡接口（105），而该包含最新的病毒特征码（2）的文件可以由防病毒网站预先采用数字证书等的加密方法，将该包含最新的病毒特征码（2）的文件以指定的密钥加密，然后由计算机下载该文件并储存到记忆卡（5）上，再由防病毒装置（1）将该记忆卡（5）上的该文件以对应的密钥进行解密。

继续参阅图 1 和图 2，图 1 和图 2 所示的防病毒装置（1）所采用的防病毒方法，可以概括为如下步骤:

1. 在计算机（3）与网络设备（4）之间加设防病毒装置（1）；
2. 在防病毒装置（1）内预先储存有各病毒特征码（2）；
3. 防病毒装置（1）将计算机（3）与网络设备（4）之间传送的数据暂存于数据暂存区（102）；
4. 防病毒装置（1）对数据暂存区（102）内的暂存数据进行病毒过滤操作，以查找出暂存数据是否带有与其中任何一病毒特征码（2）相符合的数据；
5. 当防病毒装置（1）发现暂存数据带有其中任何一病毒特征码（2）相符合的特征时，对该暂存数据进行拦截，使该带有病毒特征的暂存数据不能通过防病毒装置（1）传送到目的地，而没带病毒特征的暂存数据则于病毒过滤操作后由防病毒装置（1）转送到目的地。

参阅图 3，图 3 是本发明的防病毒装置（1）第三实施例的结构示意说明图，图中示出的防病毒装置（1）是设置于计算机（3）与网络设备（4）

之间，防病毒装置（1）是通过无线方式与计算机（3）和网络设备（4）连线。在本发明的防病毒装置（1）中，所述的计算机端接口（103）可以是以太网（Ethernet）网络接口、或 USB 接口、或 WIFI 无线网络接口、或蓝芽（Bluetooth）无线网络接口等等之类的接口。以及，所述的网络设备端接口（104）可以是以太网（Ethernet）网络接口、或 USB 接口、或 WIFI 无线网络接口、或蓝芽（Bluetooth）无线网络接口等等之类的接口。继续参阅图 3，在图 3 的实施例中，其中带箭头的虚线所示出的是未设置本发明的防病毒装置（1）时，计算机（3）与网络设备（4）之间原来的数据传送通道，是采用 WiFi 或蓝芽等无线通讯方式传送数据，而带箭头的实线所示出的是设置了本发明的防病毒装置（1）后，计算机（3）与网络设备（4）之间的数据传送通道，同样是采用 WiFi 或蓝芽等无线通讯方式传送数据，但计算机（3）与网络设备（4）之间传送的数据是要通过防病毒装置（1）转发的，由防病毒装置（1）对这些传送的数据进行病毒过滤。

参阅图 4，图 4 是本发明的防病毒装置（1）第四实施例的结构示意说明图，与第三实施例相比，不同之处在于图 4 的实施例的防病毒装置（1）是通过有线方式与计算机（3）连线。在本实施例中，防病毒装置（1）可以整合到计算机（3）中，将防病毒装置（1）内藏于计算机（3）的外壳里，都可很好地实现本发明的目的。此外，本发明的可以作多种改变和变化，在不脱离本发明的精神的情况下的各种变通，都可很好地实现本发明的目的，都是属于本发明的保护范围。

本发明的更进一步改进是在防病毒装置（1）上增设提示装置，当防病毒装置（1）发现暂存数据中带有其中任何一病毒特征码（2）相符合的特征时，通过提示装置向用户发出提示信号，用户从提示信号就可知道有病毒出现，就可立即提高警觉，找出病毒来源，避免计算机感染病毒。此外，

更可在防病毒装置（1）上增设按键，包括：通行键和拦截键，当防病毒装置（1）发现暂存数据中带有其中任何一病毒特征码（2）相符合的特征时，通过提示装置向用户发出提示信号后，用户可在防病毒装置（1）上作出如下的操作步骤：

用户按一次拦截键后，防病毒装置（1）拦截该数据，使该数据不能通过防病毒装置（1）传送到目的地；

或

用户按一次通行键后，防病毒装置（1）允许该数据转送到目的地。

以上已经详细说明了本发明的计算机防病毒装置和方法，本发明的防病毒装置（1）与计算机的操作系统无关，由于防病毒装置（1）是一个独立的硬体设备，即使操作系统出现漏洞被病毒攻击或骑劫，防病毒装置（1）仍然能不受干扰继续运作，继续对计算机与网络设备之间传送的数据进行病毒过滤。即使计算机更新或更换操作系统软件，防病毒装置（1）也无需作任何改变，仍然能继续有效运作。

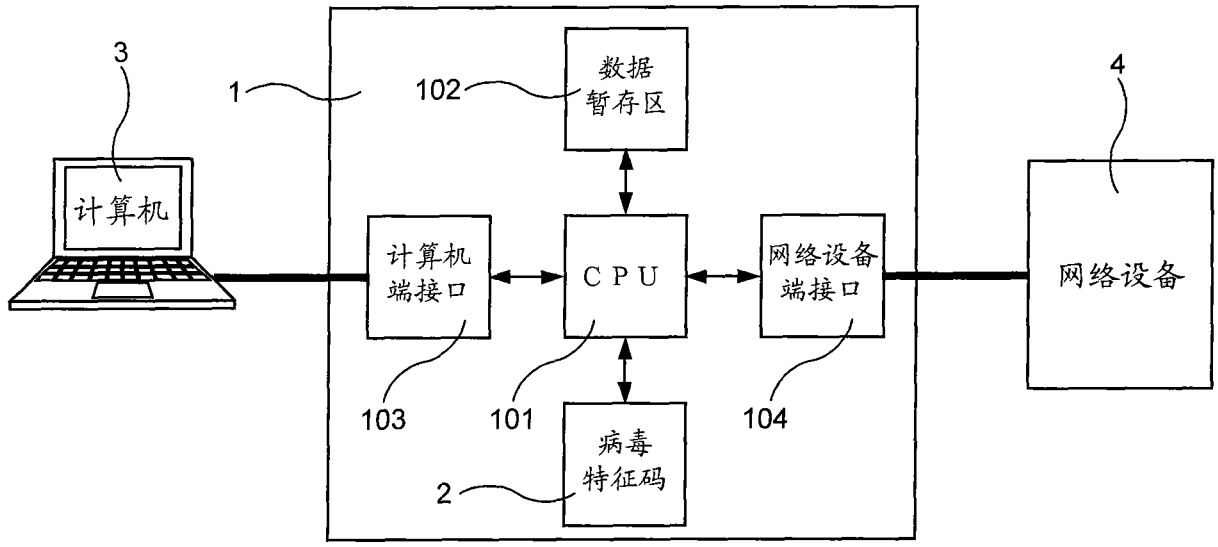

3
计算机
1
102
数据
暂存区
4
网络设备
计算机
端接口
CPU
网络设备
端接口
103
101
104
病毒
特征码
2

图 1

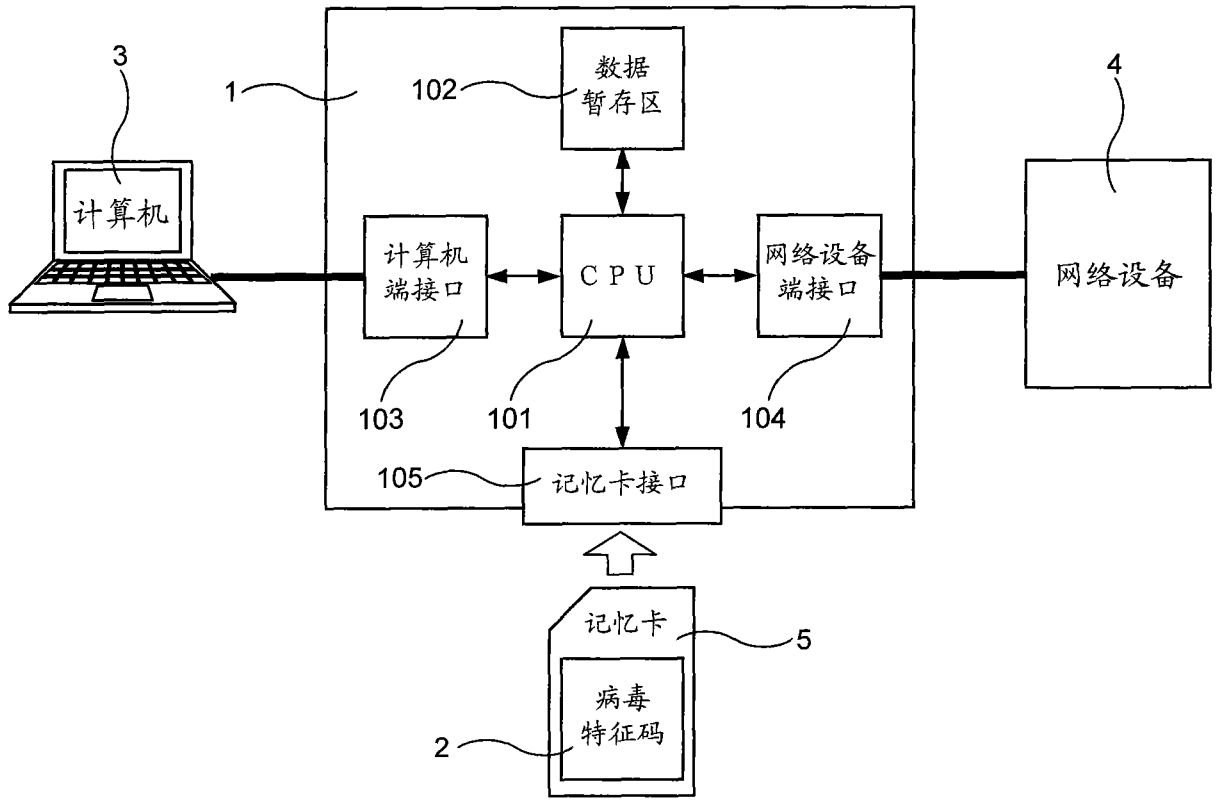

3
计算机
1
102
数据
暂存区
4
网络设备
计算机
端接口
CPU
网络设备
端接口
103
101
104
105
记忆卡接口
记忆卡
5
病毒
特征码
2

图 2

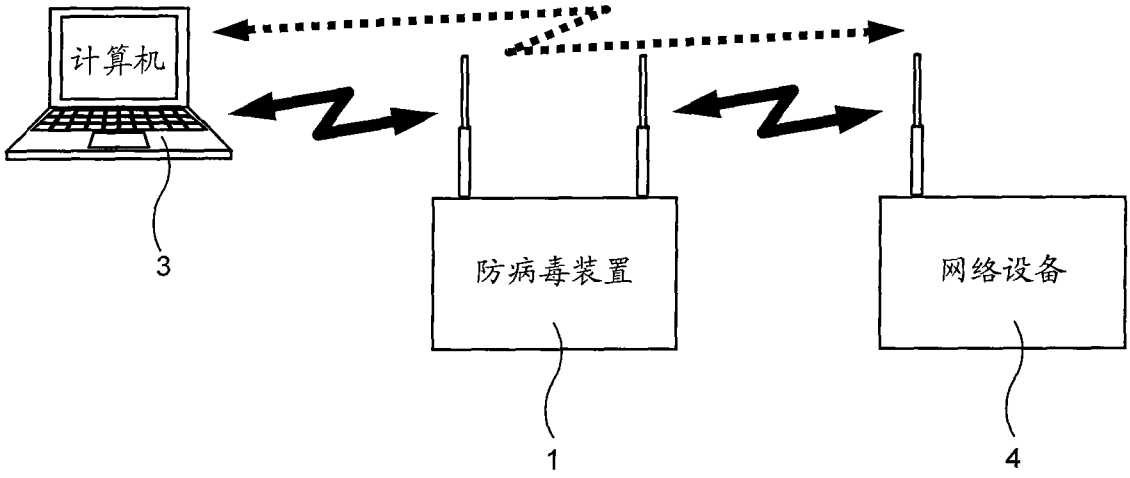


图 3

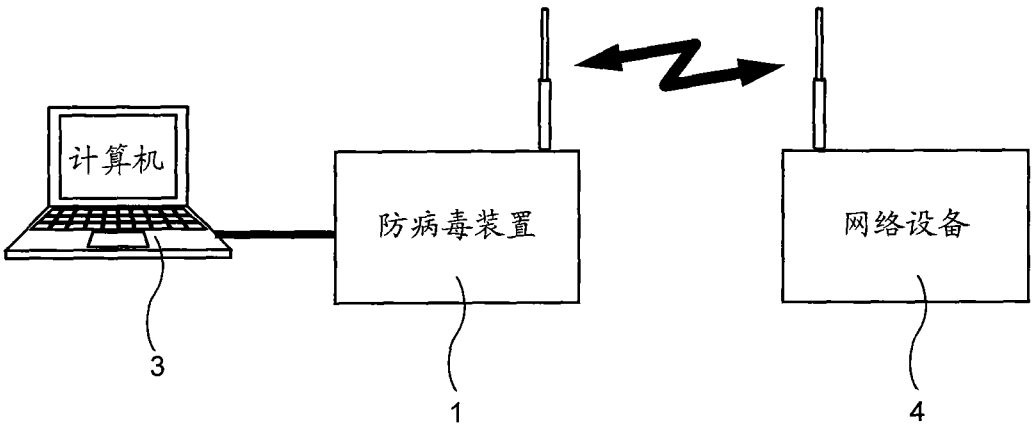


图 4