[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/24 (2006.01)

[12] 发明专利说明书

专利号 ZL 200410098117.4

[45] 授权公告日 2007 年 7 月 11 日

[11] 授权公告号 CN 1326365C

[22] 申请日 2004.9.3
[21] 申请号 200410098117.4
[30] 优先权
[32] 2003.9.3 [33] KR [31] 10-2003-0061541
[73] 专利权人 LG N-SYS 株式会社
地址 韩国首尔
[72] 发明人 李尙雨 柳渊植 表胜钟
[56] 参考文献
CN2485724Y 2002.4.10
DE10028054A1 2001.12.6
TW451127 2001.8.21
审查员 李晓莉

[74] 专利代理机构 上海专利商标事务所有限公司
代理人 陆 嘉

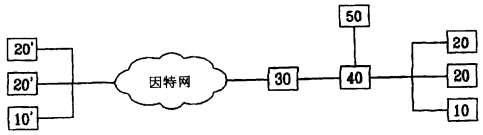
权利要求书 3 页 说明书 6 页 附图 6 页

[54] 发明名称

使用基于硬件的模式匹配的蠕虫阻击系统和方法

[57] 摘要

本发明通常涉及包括用于在不改变现有网络环境的情况下实施模式匹配的专用基于硬件的主板的蠕虫阻击系统，该系统安装在将要保护的网络前端，检测蠕虫相关模式是否没有损耗或延迟地存在于通信链路上的所有包中，根据相应安全性规则传递包通过系统或阻击包，并实时通知管理者其结果，以及蠕虫阻击方法。 尤其是，本发明涉及用于检测和阻击蠕虫相关包的基于硬件的系统和方法，该方法和系统适合于吉比特环境。



1．利用蠕虫阻击系统进行蠕虫包检测和阻击的方法，所述系统由主机系统和安装在所述主机系统中的外围部件互连主板构成，包括步骤：

所述主机系统初始化所述外围部件互连主板；

当所述主机系统将蠕虫模式和安全性规则传输到外围部件互连主板时，所述外围部件互连主板存储蠕虫模式和相应安全性规则；

所述外围部件互连主板通过将输入数据的模式和所述存储的蠕虫模式进行比较以搜索蠕虫；

当已检测到一蠕虫模式时，所述外围部件互连主板传输一警告信号到所述主机系统；以及

所述外围部件互连主板为对应于所述检测的蠕虫模式的安全性规则搜索存储的安全性规则并根据所述搜索出的规则处理所述蠕虫。

2．如权利要求1所述的利用蠕虫阻击系统进行蠕虫包检测和阻击的方法，还包括步骤：

当所述安全性规则从通过网络连接到所述蠕虫阻击系统的管理控制台传输到所述主机系统时，所述主机系统将安全性规则传输到所述外围部件互连主板；以及

所述外围部件互连主板存储所述安全性规则。

3．如权利要求2所述的利用蠕虫阻击系统进行蠕虫包检测和阻击的方法，其中：

从管理控制台传输到所述主机系统的安全性规则已经加密；以及

所述主机系统在将所述安全性规则传输到所述外围部件互连主板前对接收的安全性规则进行解码。

4．如权利要求1所述的利用蠕虫阻击系统进行蠕虫包检测和阻击的方法，其中，当从外围部件互连主板接收警告信号时，所述主机系统将所述警告信号传输到管理控制台。

5．如权利要求4所述的利用蠕虫阻击系统进行蠕虫包检测和阻击的方法，其中，每条安全性规则包括警告信号格式，当检测到蠕虫时，所述警告信号由外围部件互连主板传输。

6．如权利要求5所述的利用蠕虫阻击系统进行蠕虫包检测和阻击的方法，其中，所述警告信号的格式包括一当攻击名称和包标题传输时使用的格式，和当攻击名称和全部包数据传输时使用的格式。

7．如权利要求4所述的利用蠕虫阻击系统进行蠕虫包检测和阻击的方法，其中，主机系统在将警告信号传输到管理控制台前将所述警告信号加密。

8．如权利要求1所述的利用蠕虫阻击系统进行蠕虫包检测和阻击的方法，其中：

每条安全性规则具有一包括NUM、日志类型、动作和蠕虫模式域的消息格式，其中NUM表示有序位置；以及

所述警告信号包括源网际协议地址、源端口、目的网际协议地址、目的端口、时间、网际协议上层协议、蠕虫攻击名称和包数据。

9．使用基于硬件的模式匹配的蠕虫包检测和阻击系统，包括：

以透明方式连到网关后并安装在抵御蠕虫攻击的网络客户或服务器前面以阻击蠕虫攻击的主机系统；以及

安装在主机系统中的外围部件互连主板，适于根据从主机系统接收的安全性规则在已接收的包上执行模式匹配，以及适于根据相应安全性规则阻击匹配包。

10．如权利要求9所述的使用基于硬件的模式匹配的蠕虫包检测和阻击系统，其中，所述主机系统是配备网卡的通用计算机。

11. 如权利要求9所述的使用基于硬件的模式匹配的蠕虫包检测和阻击系统，还包括管理控制台，用于将安全性规则传输到主机系统、从主机系统接收蠕虫警告信号并显示所述蠕虫警告信号。

12. 如权利要求9所述的使用基于硬件的模式匹配的蠕虫包检测和阻击系统，其中，所述外围部件互连主板包括：

标题搜索引擎，用于检测包标题；

内容搜索引擎，用于执行模式匹配；

在线控制，负责包处理；以及

安全性规则数据库，用于存储安全性规则。

13. 如权利要求12所述的使用基于硬件的模式匹配的蠕虫包检测和阻击系统，其中，所述在线控制将输入数据包传输到标题搜索引擎和内容搜索引擎用于标题和内容的模式匹配、当蠕虫模式做为标题和内容搜索引擎中的模式匹配的结果被检测时传输一警告信号给所述主机系统、从安全性规则数据库中读取对应于检测的蠕虫模式的安全性规则、以及根据该对应于检测的蠕虫模式安全性规则传递或阻击该包。

使用基于硬件的模式匹配的蠕虫阻击系统和方法

发明背景

发明领域

本发明通常涉及一种蠕虫阻击系统，该系统包括用于在不改变现有网络环境的情况下实施模式匹配的专用基于硬件的主板，该系统安装在将要保护的网络前端，检测蠕虫相关模式是否没有损耗或延迟地存在于通信链路上的所有包中，根据相应安全性规则传递包通过系统或阻击包，并实时通知管理者其结果，以及蠕虫阻击方法。具体地，本发明涉及用于检测和阻击蠕虫相关包的基于硬件的系统和方法，该方法和系统适合于吉比特环境。

相关技术描述

蠕虫是单个计算机系统中程序间移动或通过网络自动传播到其他计算机的程序碎片。不同于病毒，蠕虫不具有特定传染目标，同时也不包括直接破坏计算机系统或引起计算机系统非法操作的代码。然而，由于蠕虫传播时在计算机系统和网络上强加额外的负载，因此蠕虫导致计算机系统或网络故障。特别地，因为蠕虫不具有特定传染目标，蠕虫基于从传染目标获取的任意信息传播，所以其特征在于：当蠕虫从源处发布到网络后，几乎不可能使用一些常规方法以控制或处理该蠕虫。

计算机病毒是恶意性程序，它渗透到计算机中并破坏数据或导致其他程序变得不可操作。该计算机病毒具有这种特征：他们具有传染目标、传染当前传染目标并自我复制以传染其他传染目标。

蠕虫病毒是上述蠕虫和计算机病毒组合成的病毒，其特征在于：该计算机病毒使用该蠕虫迅速传播。实际上，蠕虫病毒的传播速度如此快且具有破坏性，所以，最初在外国报告的蠕虫病毒仅在几小时内传入韩国并在蠕虫病毒开始传入韩国后不到一天时间传染好几万台计算机。近来，除蠕虫和计算机病毒的基本功能以外，诸如后门的黑客工具和诸如特洛伊的间谍软件功能增加到蠕虫病毒中。蠕虫病毒的功能和破坏力正在增强，该蠕虫病毒的传播速度正在渐增，

以及他们导致的破坏的货币值急剧上升。

因此，阻击蠕虫或蠕虫病毒的各种方法已经使用。

通常，为了阻击蠕虫，防病毒程序安装在单个主机上，或预先安装基于软件病毒阻击系统以抵御蠕虫预先渗透到计算机网络中。此外，在L7应用交换中，可以使用内容过滤以阻击蠕虫攻击。

过去，在主机安装防病毒程序的时候，检测即将传输到主机的数据和文件是否被蠕虫传染以及杀毒方法的功能执行。在网关级病毒阻击系统中，检测数据和文件是否已经传染以及杀毒方法的功能在所有流量上执行，以便从根本上抵御病毒或恶意信息进入或退出网络起点的网关。在L7应用交换中，当传递包的数据部分在应用级时，蠕虫攻击相关的模式匹配执行，同时，如果确定该包是攻击的包，该L7应用交换通过阻击攻击包以抵御蠕虫攻击。通过安装基于主机的防病毒程序阻击蠕虫攻击的时候，引发当网络范围增加而导致管理者面临管理困难的问题。通过安装网关级病毒阻击系统以阻击蠕虫攻击时，因为该阻击系统基于软件实施的，所以当流量增长时，强加于该病毒阻击系统的负载也增长，这样导致速度等等降低。同样，通过使用L7应用交换阻击蠕虫攻击时，引发性能降低以及在执行内容过滤时系统停止的问题。

发明概述

因此，本发明已经牢记出现在现有技术中的上述问题，并且本发明的目的是提供蠕虫阻击系统和蠕虫阻击方法，该系统包括用于在不改变现有网络环境的情况下实施模式匹配的专用基于硬件的主板，该系统安装在将要保护的网络前端，检测蠕虫相关模式是否没有损耗或延迟地存在于通信链路上的所有包中，根据相应安全性规则传递包通过系统或阻击包，并实时通知管理者其结果。具体地，本发明涉及用于检测和阻击蠕虫相关包的基于硬件的系统和方法，该方法和系统适合于吉比特环境。

为了实现上述目的，本发明提供通过使用基于硬件的模式匹配的蠕虫包检测和阻击系统，该系统包括一为了阻击蠕虫攻击以透明方式连接到网关后面并安装在网络客户端和服务端前以抵御蠕虫攻击的主机系统，和安装在该主机系统中的外围部件互连（PCI）主板，该主板适于根据从主机系统接收的安全性规则在接收的包上执行模式匹配，以及适于根据相应安全性规则阻击匹配包。

该蠕虫包检测和阻击系统还包括管理控制台，用于传输该安全性规则给主

机系统、从主机系统接收蠕虫警告信号并显示该蠕虫警告信号。

该主机系统是配备网卡的通用计算机。该**PCI**主板包括一个用于检测包标题的标题搜索引擎、用于执行模式匹配的内容搜索引擎、负责包处理的在线控制（**in line-control**）（**ILC**）以及用于存储安全性规则的安全性规则数据库。**ILC**传输输入数据包到标题搜索引擎和内容搜索引擎用于标题和内容模式匹配、当蠕虫模式做为标题和内容搜索引擎中模式匹配的结果被检测时传输一警告信号给主机系统、从安全性规则数据库中读取检测的蠕虫模式对应的安全性规则、并根据该安全性规则传递或阻击该包。

为了实现上述目的，本发明提供一蠕虫包检测和阻击方法，该方法使用主机系统和安装在该主机系统的**PCI**主板构成的蠕虫阻击系统，包括步骤：主机系统初始化**PCI**主板；当主机系统传输蠕虫模式和安全性规则到**PCI**主板时该**PCI**主板存储蠕虫模式和相应安全性规则；**PCI**模式通过将输入数据模式和存储的蠕虫模式进行比较以搜索蠕虫；当蠕虫病毒已被检测到时**PCI**主板传输警告信号到主机系统；以及**PCI**主板为检测的蠕虫模式的相应安全性规则搜索存储的安全性规则并根据该安全性规则处理蠕虫。

安全性规则通过网络从连接到蠕虫阻击系统的管理控制台传输到主机系统。优选的是从管理控制台传输到主机系统中的安全性规则已经加密，以及在安全性规则传输到**PCI**主板前主机系统对接收的安全性规则解码。

附图简述

结合附图，从下面详细描述中，本发明的上述以及其他目的、特征和优点将更容易理解，其中：

图**1**是根据本发明的系统的结构图；

图**2**是管理控制台日志信息接收和安全性规则传输功能的流程图；

图**3**是主机系统功能的流程图；

图**4a**是**PCI**主板的内部结构的框图；

图**4b**是**PCI**主板功能的流程图；

图**5**是安全性规则消息的格式；以及

图**6**是从蠕虫阻击系统传输到管理控制台的日志消息的格式。

优选实施方案详述

现在参照附图，其中，不同附图中的相同附图标记表示相同或相似组件。

本发明的优选实施例参照附图在下面进行详细描述。

图1是使用基于硬件模式匹配来阻击蠕虫的系统构造的结构图。

在图1，客户10’和服务器20’连到因特网上，以及用于阻击蠕虫攻击的蠕虫阻击系统40在现有网络环境中没有变化以透明方式定位于要保护的网络的网关30后面。在这位置，该蠕虫阻击系统40在要保护的网络的主机10和连到因特网的主机10’之间的所有通信量上执行实时蠕虫检测和阻击，并传输检测和阻击结果到管理控制台50。然后管理控制台50通过将结果显示到屏幕上以提醒管理者已经检测到蠕虫。此外，管理控制台50产生要应用到蠕虫阻击系统40的安全性规则，并将该安全性规则应用到联机的蠕虫阻击系统40。

蠕虫阻击系统40包括主机系统和安装在该主机系统的PCI格式主板。该主机系统具有通用计算机形式，但实际上具有通过PCI总线接收PCI格式主板提供的日志信息并将该日子信息传输到管理控制台50的功能。提供用于执行模式匹配的具有吉比特接口的PCI主板，以便在不改变网络环境的情况下以内嵌模式安装PCI主板。PCI主板使用主机的网路接口与管理控制台50通信。主机系统使用传输控制协议/网际协议（TCP/IP）经由因特网连接到管理控制台50，同时单个管理控制台能远程管理多个蠕虫阻击系统。

图2是管理控制台50执行的日志信息接收和安全性规则传输的流程图。管理控制台50检测从蠕虫阻击系统40接收的日志是否存在（步骤A1）。如果该接收的数据存在，使用SEED算法解码该数据（步骤A1），并输出到屏幕和存储在数据库中（步骤A3）

如果在步骤A1不存在从蠕虫阻击系统40接收的日志，和管理者意图传输包括蠕虫相关模式和策略的安全性规则（步骤A4），则管理控制台50将要传输的安全性规则进行加密（步骤A5），并将该加密的安全性规则传输到相应蠕虫阻击系统40（步骤A6）。如果该处理没有结束（步骤A7），则重复步骤A1到A6的操作。

图3是主机系统的功能性流程图。该主机系统执行PCI格式主板初始化，该主板安装在主机系统上负责模式匹配（步骤B1），同时从管理控制台50接收的文件中读取安全性规则并将该安全性规则应用到该主板上以检测蠕虫攻击(步骤B2)。此外，该主机系统监控是否接收到该安全性规则（步骤B3）。如果已接收到该安全性规则，则该主机系统使用SEED算法解码该安全性规则并将该

解码的安全性规则存储在文件中（步骤B4），并将该文件存储到PCI主板（步骤B5）。

如果从管理控制台50接收到的安全性规则不存在，则检测信息（具有蠕虫攻击包已检测的事实的）是否从负责基于硬件模式匹配的PCI主板传输（步骤B6）。如果从PCI主板接收该蠕虫攻击包上的信息，主机系统将该信号转换成用于管理控制台50的日志类型（步骤B7），使用SEED算法对该信息加密（步骤B8），并将加密的信息传输到管理控制台50（步骤B9）。该步骤一直重复直到主机系统的操作结束（步骤B10）。

图4a显示专用于模式匹配的PCI主板的内部构造的框图。该PCI主板包括用于检测包标题的标题搜索引擎430、用于执行模式匹配的内容搜索引擎450、负责包处理的ILC410以及安全性规则数据库470。

图4b是PCI主板的功能性流程图。当PCI主板根据主机系统指令在图3的步骤B1初始化时（步骤C1），PCI主板的ILC410将输入数据包发送到标题搜索引擎430和内容搜索引擎450，并在标题和内容上执行模式匹配（步骤C2）。当蠕虫模式做为标题和内容搜索引擎中模式匹配的结果被检测时（步骤C3），ILC410将日志消息传输到主机系统（步骤C4）、从安全性规则数据库470中读取相应于已检测的蠕虫模式的安全性规则，并根据安全性规则传递或阻击包（步骤C5）。这些步骤一直重复直到PCI主板操作结束（步骤C6）。

同时，即使没有显示在图4b，当从主机系统接收到加载安全性规则的加载指令时，ILC410使用已接收的安全性规则更新安全性规则数据库470。

图5显示从管理控制台50传输到蠕虫阻击系统40的安全性规则的消息格式的视图。在这种情况中，NUM表示有序位置（sequential position），以及当有序位置（sequential position）较低时检测优先权变得相对高。日志类型是定义日志（其中蠕虫攻击包的警告信息通过PCI总线从主板传输到包括主板的主机）类型的域。根据日志类型，消息格式（其中攻击名称和包标题信息传输），和完整格式（其中攻击名称和包数据传输）是可能的。动作是定义当相应蠕虫攻击包被检测时主板呈现的动作的域，以及动作可以设置为包容差或包阻碍。蠕虫模式是相应蠕虫攻击的特定模式。

图6显示从蠕虫阻击系统40传输到管理控制台50的日志消息格式的视图。在这种情况中，src ip、src port、dst ip和dst port分别表示蠕虫攻击包的源IP地

址、源端口、目的IP以及目的端口，同时时间表示当蠕虫攻击检测到的时间。协议表示蠕虫攻击包属于的IP上端协议（TCP、用户数据报协议（UDP）或网络控制报文协议（ICMP）），蠕虫名称表示蠕虫攻击名称，以及包数据表示包的全部数据，其中安全性规则的日志类型是完整格式。

如上所描述，本发明能在没有损耗或延迟包的情况下使用基于硬件PCI卡实时检测并阻击包括蠕虫攻击模式的包，从而有效防御蠕虫攻击。此外，本发明在现有网络中没有变化的情况下能安装，使得它易于管理。此外，管理控制台和蠕虫阻击系统使用SEED算法执行加密和解码，使得管理控制台和蠕虫阻击系统能相互安全通信。

尽管本发明优选实施例以示例目的公开，本领域的普通技术人员能理解不脱离公开在随后的权利要求中的本发明范围和实质的各种修改、附加和置换都有可能。

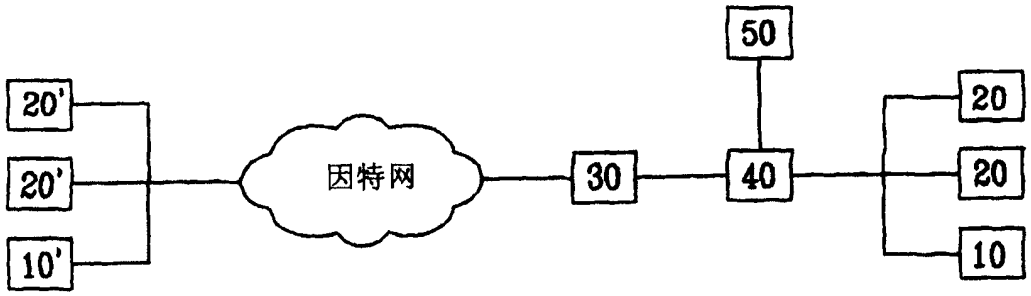


图 1

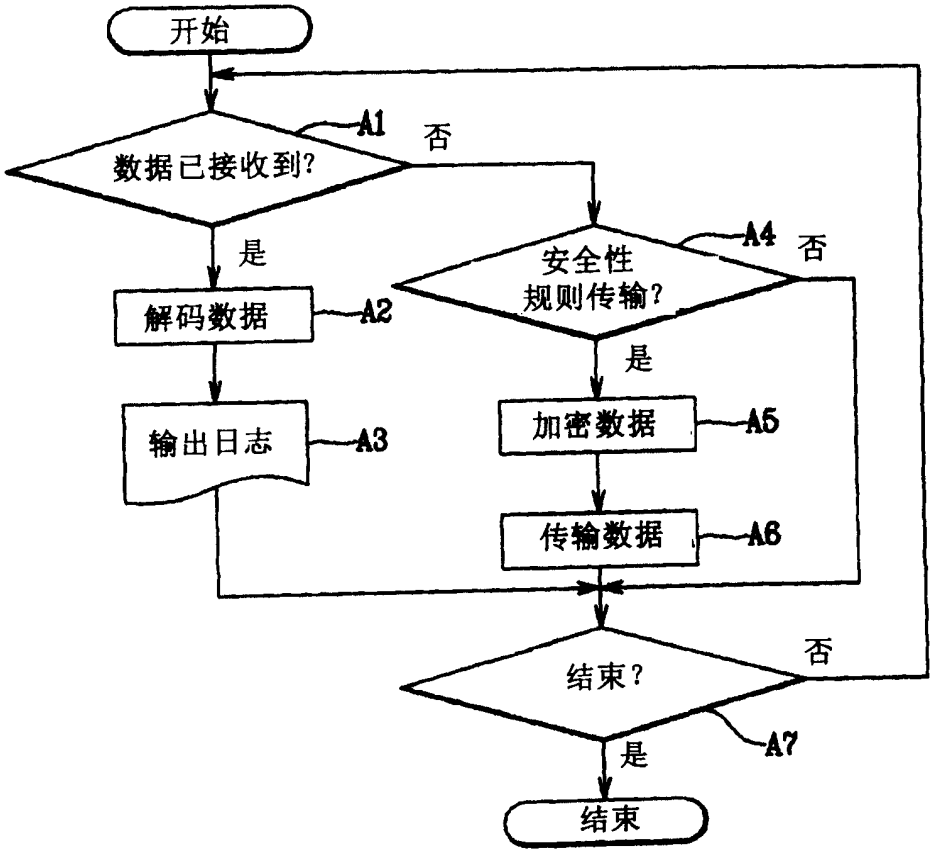

开始
A1
数据已接收到?
否
是
解码数据
A2
输出日志
A3
A4
安全性
规则传输?
否
是
加密数据
A5
传输数据
A6
结束?
否
A7
是
结束

图 2

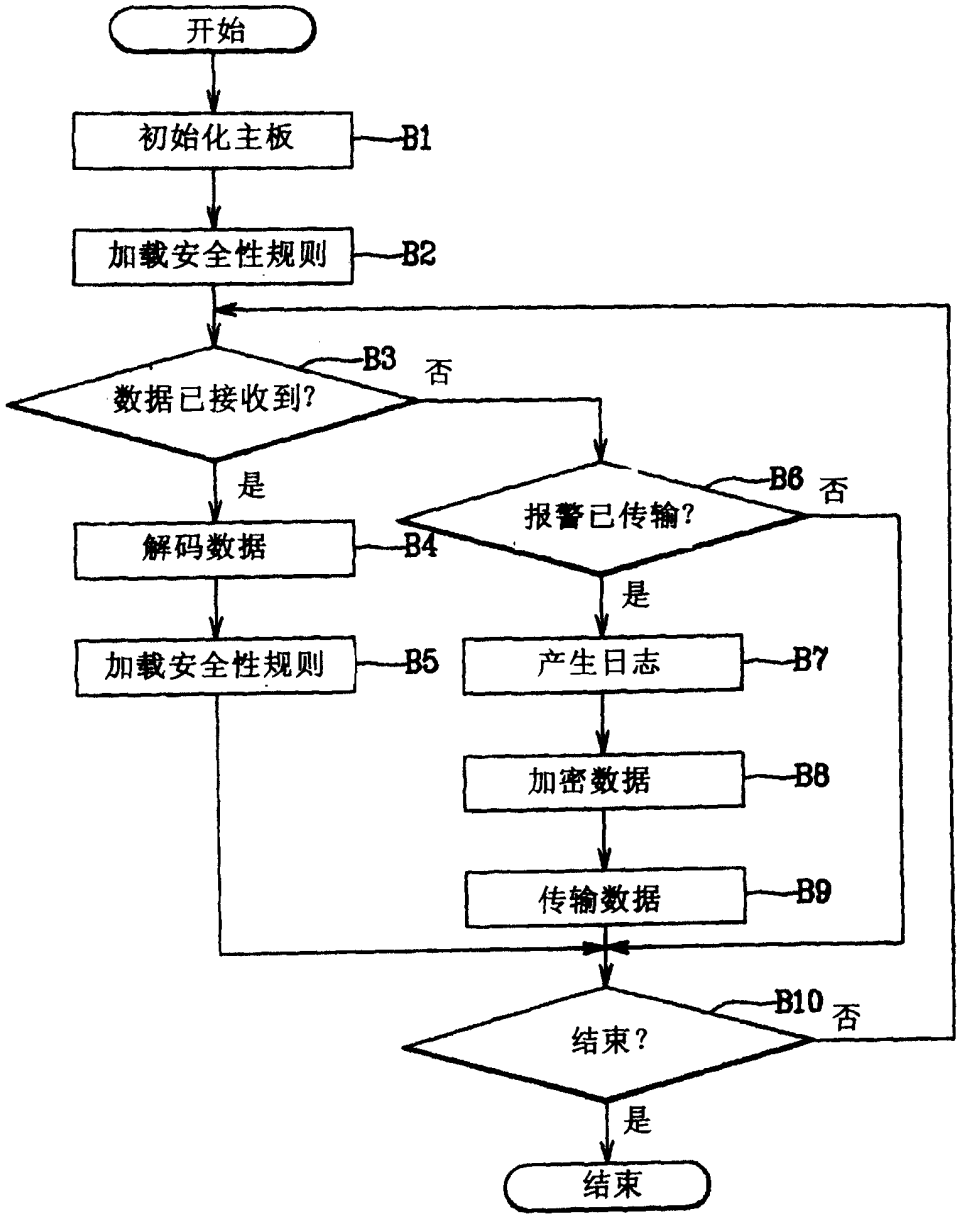

开始
初始化主板
B1
加载安全性规则
B2
数据已接收到?
B3
否
是
解码数据
B4
加载安全性规则
B5
报警已传输?
B6
否
是
产生日志
B7
加密数据
B8
传输数据
B9
结束?
B10
否
是
结束

图 3

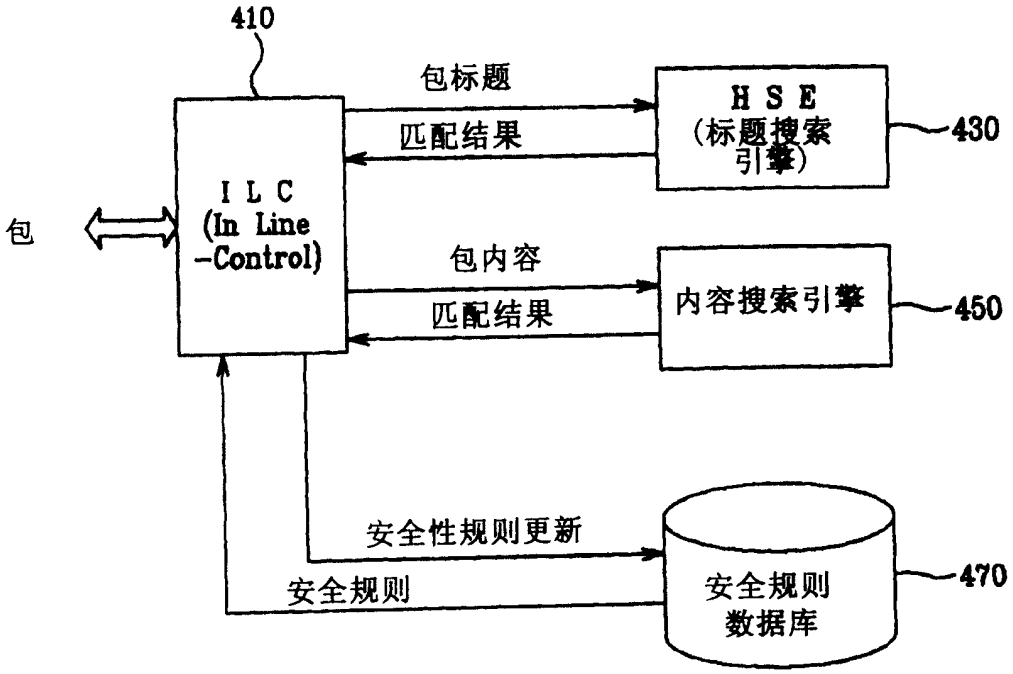

410
包标题
匹配结果
H S E
(标题搜索
引擎)
430
包
I L C
(In Line
-Control)
包内容
匹配结果
内容搜索引擎
450
安全性规则更新
安全规则
安全规则
数据库
470

图 4A

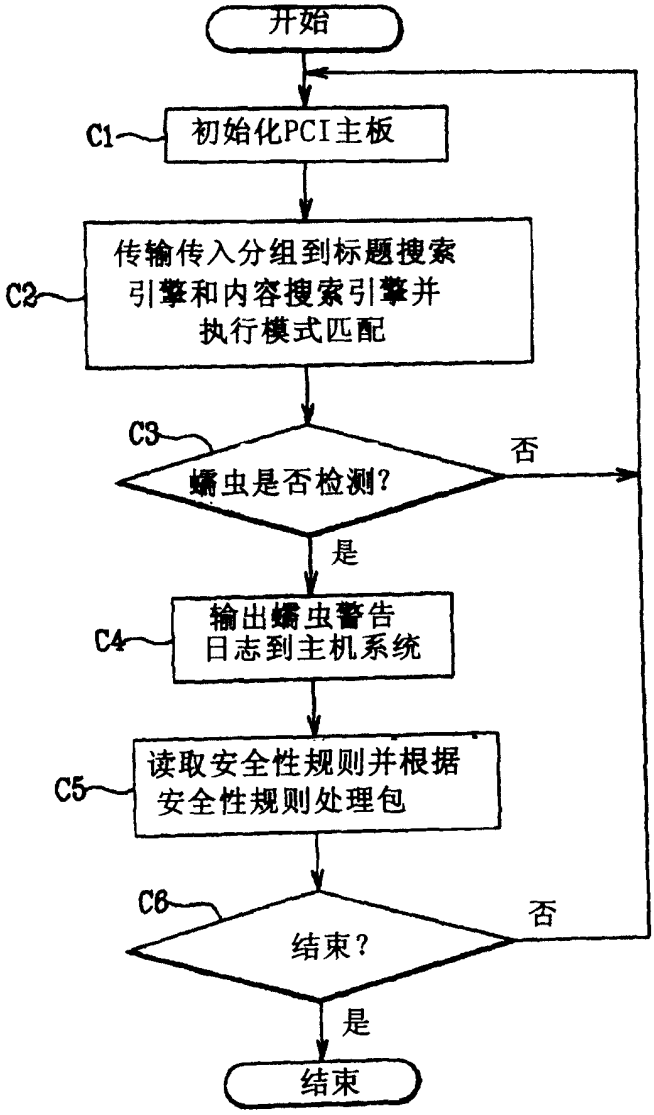

开始
C1
初始化PCI主板
C2
传输传入分组到标题搜索引擎和内容搜索引擎并执行模式匹配
C3
蠕虫是否检测?
否
是
C4
输出蠕虫警告日志到主机系统
C5
读取安全性规则并根据安全性规则处理包
C6
结束?
否
是
结束

图 4B

图 5

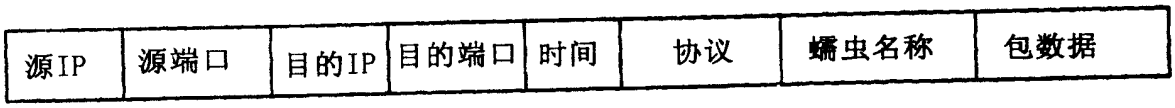


图 6