(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107332741 B
(45)授权公告日 2019.03.29

(21)申请号 201710740270.X

(22)申请日 2017.08.25

(65)同一申请的已公布的文献号
申请公布号 CN 107332741 A

(43)申请公布日 2017.11.07

(73)专利权人 OPPO广东移动通信有限公司
地址 523860 广东省东莞市长安镇乌沙海滨路18号

(72)发明人 胡亚东 刘铭 宋永耀 候祥

(74)专利代理机构 深圳中一联合知识产权代理有限公司 44414
代理人 张全文

(51)Int.Cl.
H04L 12/26(2006.01)
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04W 84/12(2009.01)

(56)对比文件
CN 106714206 A,2017.05.24,说明书第[0025]、[0079]-[0083]段.
CN 105940640 A,2016.09.14,说明书第[0001]-[0161]段、附图1-13.
US 2002176377 A1,2002.11.28,全文.

审查员 程佳丽

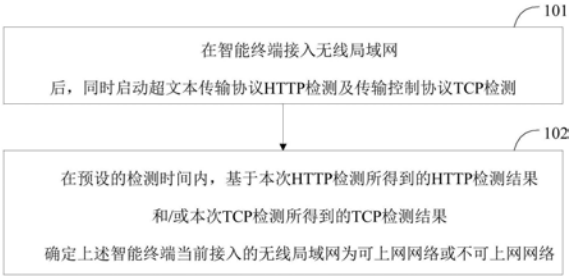
权利要求书5页 说明书14页 附图4页

(54)发明名称

一种网络检测方法、网络检测装置及智能终端

(57)摘要

本发明公开了一种网络检测方法、网络检测装置、智能终端及计算机可读存储介质，其中，该网络检测方法包括：在智能终端接入无线局域网后，同时启动超文本传输协议HTTP检测及传输控制协议TCP检测；所述HTTP检测为：通过所述无线局域网向预设的第一服务器发送HTTP连接请求，根据所述智能终端与所述第一服务器的连接状况得到HTTP检测结果；所述TCP检测为：周期性检测所述智能终端当前网络连接的TCP状态，根据所述TCP状态得到TCP检测结果；在预设的检测时间内，基于本次HTTP检测所得到的HTTP检测结果和/或本次TCP检测所得到的TCP检测结果确定所述智能终端当前接入的无线局域网为可上网网络或不可上网网络。本发明方案提高了检测无线局域网的网络状态的效率。



CN 107332741 B

1.一种网络检测方法,其特征在于,所述网络检测方法包括:

在智能终端接入无线局域网后,同时启动超文本传输协议HTTP检测及传输控制协议TCP检测;

所述HTTP检测为:通过所述无线局域网向预设的第一服务器发送HTTP连接请求,根据所述智能终端与所述第一服务器的连接状况得到HTTP检测结果;

所述TCP检测为:周期性检测所述智能终端当前网络连接的TCP状态,根据所述TCP状态得到TCP检测结果;

在预设的检测时间内,基于本次HTTP检测所得到的HTTP检测结果和/或本次TCP检测所得到的TCP检测结果确定所述智能终端当前接入的无线局域网为可上网网络或不可上网网络;

其中,所述周期性检测所述智能终端当前网络连接的TCP状态,根据所述TCP状态得到TCP检测结果,包括:

周期性获取当前所述智能终端的内核中所有的套接字Socket的参数信息;

基于各Socket的参数信息,分别判断与各Socket对应的链路的类型;

根据不同类型的链路之间的数量关系,确定当前网络连接的TCP状态;

若连续N1次确定所述TCP状态为连接成功,则确定本次TCP检测结果为连接成功;

若连续N2次确定所述TCP状态为连接失败,则确定本次TCP检测结果为连接失败;

若连续N3次确定所述TCP状态为连接受限,则确定本次TCP检测结果为连接受限;

其中,上述链路的类型包括网络差链路,网络受限链路,不再使用链路,未关闭链路;所述根据不同类型的链路之间的数量关系,确定当前网络连接的TCP状态,包括:

统计网络不佳链路的数量,其中,上述网络不佳链路的数量为网络受限链路的数量及网络差链路的数量之和;

确定当前网络连接的TCP状态是否为连接成功;

若当前网络连接的TCP状态不为连接成功,则继续检测当前网络连接的TCP状态是否为连接失败;

若当前网络连接的TCP状态不为连接失败,则继续检测当前网络连接的TCP状态是否为连接受限;

其中,所述确定当前网络连接的TCP状态是否为连接成功,包括:

若第一比值不大于预设的比值阈值C1,且第二比值不大于预设的比值阈值D1,则确定当前网络连接的TCP状态为连接成功,其中,上述第一比值为网络不佳链路的数量与未关闭链路的数量的比值,上述第二比值为不再使用链路的数量与未关闭链路的数量的比值;

所述检测当前网络连接的TCP状态是否为连接失败,包括:

若上述第一比值不小于预设的比值阈值C2,且上述第二比值不小于预设的比值阈值D2,且第三比值不小于预设的比值阈值E2,则确定当前网络连接的TCP状态为连接失败,其中,上述第三比值为网络受限链路的数量与未关闭链路的数量的比值;

所述检测当前网络连接的TCP状态是否为连接受限,包括:

若上述第一比值不小于预设的比值阈值C3,且上述第二比值不小于预设的比值阈值D3,且第三比值不小于预设的比值阈值E3,则确定当前网络连接的TCP 状态为连接失败,其中,上述比值阈值C3不同于上述比值阈值C2,上述比值阈值D3不同于上述比值阈值D2,上述

比值阈值E3不同于上述比值阈值E2。

2.如权利要求1所述的网络检测方法，其特征在于，所述基于本次HTTP检测所得到的HTTP检测结果和/或本次TCP检测所得到的TCP检测结果确定所述智能终端当前接入的无线局域网为可上网网络或不可上网网络之后，或者，在所述检测时间到达之后，所述网络检测方法还包括：

若本次TCP检测和/或本次HTTP检测仍在运行中，则停止本次TCP检测和/或本次HTTP检测。

3.如权利要求1所述的网络检测方法，其特征在于，若确定所述智能终端当前接入的无线局域网为不可上网网络，则所述网络检测方法还包括：

断开所述智能终端与所述无线局域网的连接。

4.如权利要求1所述的网络检测方法，其特征在于，若确定所述智能终端当前接入的无线局域网为不可上网网络，则所述网络检测方法还包括：

在预设的禁用时间内，禁用所述无线局域网。

5.如权利要求4所述的网络检测方法，其特征在于，所述在预设的禁用时间内，禁用所述无线局域网，包括：

获取当前记录的所述无线局域网被禁用的次数；

根据当前记录的所述无线局域网被禁用的次数设定所述无线局域网的禁用时间；

在所述无线局域网的禁用时间内，禁用所述无线局域网；

更新当前记录的所述无线局域网被禁用的次数。

6.如权利要求5所述的网络检测方法，其特征在于，所述网络检测方法还包括：

在无线局域网备选列表中，显示各个可连接的无线局域网曾被所述智能终端接入的次数及曾被所述智能终端禁用的次数，所述可连接的无线局域网为当前智能终端未接入的无线局域网。

7.如权利要求1至6任一项所述的网络检测方法，其特征在于，所述基于本次HTTP检测所得到的HTTP检测结果和/或本次TCP检测所得到的TCP检测结果确定所述智能终端当前接入的无线局域网为可上网网络或不可上网网络，包括：

若本次HTTP检测所得到的HTTP检测结果为连接成功，则确定所述智能终端当前接入的无线局域网为可上网网络。

8.如权利要求1至6任一项所述的网络检测方法，其特征在于，所述基于本次HTTP检测所得到的HTTP检测结果和/或本次TCP检测所得到的TCP检测结果确定所述智能终端当前接入的无线局域网为可上网网络或不可上网网络，包括：

若本次TCP检测所得到的TCP检测结果为连接失败，或者，若本次HTTP检测所得到的HTTP检测结果及本次TCP检测所得到的TCP检测结果均为连接受限，则确定所述智能终端当前接入的无线局域网为不可上网网络。

9.如权利要求1至6任一项所述的网络检测方法，其特征在于，所述通过所述无线局域网向预设的第一服务器发送HTTP连接请求，根据所述智能终端与所述第一服务器的连接状况得到HTTP检测结果，包括：

通过所述无线局域网向预设的第一服务器发送HTTP连接请求；

若与所述第一服务器连接成功，则确定本次HTTP检测结果为连接成功；

若与所述第一服务器连接失败，则根据接收到的HTTP状态值确定所述无线局域网是否为认证网络；

若确定所述无线局域网为认证网络，则确定本次HTTP检测结果为连接受限；

若确定所述无线局域网不为认证网络，则确定本次HTTP检测结果为连接失败。

10.如权利要求1所述的网络检测方法，其特征在于，所述周期性获取当前所述智能终端的内核中所有的套接字Socket的参数信息，包括：

检测当前所述智能终端的内核中是否存在Socket；

若当前所述智能终端的内核中存在Socket，则周期性获取当前所述智能终端的内核中所有的Socket的参数信息。

11.如权利要求10所述的网络检测方法，其特征在于，所述网络检测方法还包括：

若当前所述智能终端的内核中不存在Socket，则确定当前网络连接的TCP状态为连接失败。

12.一种网络检测装置，其特征在于，所述网络检测装置包括：

检测单元，用于在智能终端接入无线局域网后，同时启动超文本传输协议HTTP检测及传输控制协议TCP检测；

确定单元，用于在预设的检测时间内，基于本次HTTP检测所得到的HTTP检测结果和/或本次TCP检测所得到的TCP检测结果确定所述智能终端当前接入的无线局域网为可上网网络或不可上网网络；

其中，所述检测单元包括：

HTTP检测单元，用于通过所述无线局域网向预设的第一服务器发送HTTP连接请求，根据所述智能终端与所述第一服务器的连接状况得到HTTP检测结果；

TCP检测单元，用于周期性检测所述智能终端当前网络连接的TCP状态，根据所述TCP状态得到TCP检测结果；

其中，所述TCP检测单元包括：

信息获取子单元，用于周期性获取当前所述智能终端的内核中所有的套接字Socket的参数信息；

链路判断子单元，用于基于各Socket的参数信息，分别判断与各Socket对应的链路的类型；

TCP状态确定子单元，用于根据不同类型的链路之间的数量关系，确定当前网络连接的TCP状态；

TCP确定子单元，用于若所述TCP状态确定子单元连续N1次确定所述TCP状态为连接成功，则确定本次TCP检测结果为连接成功，若所述TCP状态确定子单元连续N2次确定所述TCP状态为连接失败，则确定本次TCP检测结果为连接失败，若所述TCP状态确定子单元连续N3次确定所述TCP状态为连接受限，则确定本次TCP检测结果为连接受限；

其中，上述链路的类型包括网络差链路，网络受限链路，不再使用链路，未关闭链路；所述TCP状态确定子单元，具体用于统计网络不佳链路的数量，其中，上述网络不佳链路的数量为网络受限链路的数量及网络差链路的数量之和；确定当前网络连接的TCP状态是否为连接成功；若当前网络连接的TCP状态不为连接成功，则继续检测当前网络连接的TCP状态是否为连接失败；若当前网络连接的TCP状态不为连接失败，则继续检测当前网络连接的

TCP状态是否为连接受限；

其中，所述确定当前网络连接的TCP状态是否为连接成功，包括：

若第一比值不大于预设的比值阈值C1，且第二比值不大于预设的比值阈值D1，则确定当前网络连接的TCP状态为连接成功，其中，上述第一比值为网络不佳链路的数量与未关闭链路的数量的比值，上述第二比值为不再使用链路的数量与未关闭链路的数量的比值；

所述检测当前网络连接的TCP状态是否为连接失败，包括：

若上述第一比值不小于预设的比值阈值C2，且上述第二比值不小于预设的比值阈值D2，且第三比值不小于预设的比值阈值E2，则确定当前网络连接的TCP状态为连接失败，其中，上述第三比值为网络受限链路的数量与未关闭链路的数量的比值；

所述检测当前网络连接的TCP状态是否为连接受限，包括：

若上述第一比值不小于预设的比值阈值C3，且上述第二比值不小于预设的比值阈值D3，且第三比值不小于预设的比值阈值E3，则确定当前网络连接的TCP状态为连接失败，其中，上述比值阈值C3不同于上述比值阈值C2，上述比值阈值D3不同于上述比值阈值D2，上述比值阈值E3不同于上述比值阈值E2。

13.如权利要求12所述的网络检测装置，其特征在于，所述网络检测装置还包括：

停止单元，用于在基于本次HTTP检测所得到的HTTP检测结果和/或本次TCP检测所得到的TCP检测结果确定所述智能终端当前接入的无线局域网为可上网网络或不可上网网络之后，或者，在所述检测时间到达之后，若本次TCP检测和/或本次HTTP检测仍在运行中，则停止本次TCP检测和/或本次HTTP检测。

14.如权利要求12所述的网络检测装置，其特征在于，所述网络检测装置还包括：

连接断开单元，用于当确定所述智能终端当前接入的无线局域网为不可上网网络时，断开所述智能终端与所述无线局域网的连接。

15.如权利要求12所述的网络检测装置，其特征在于，所述网络检测装置还包括：

无线局域网禁用单元，用于当确定所述智能终端当前接入的无线局域网为不可上网网络时，在预设的禁用时间内，禁用所述无线局域网。

16.如权利要求15所述的网络检测装置，其特征在于，所述无线局域网禁用单元包括：

禁用次数获取子单元，用于获取当前记录的所述无线局域网被禁用的次数；

禁用时间设定子单元，用于根据当前记录的所述无线局域网被禁用的次数设定所述无线局域网的禁用时间；

网络禁用子单元，用于在所述无线局域网的禁用时间内，禁用所述无线局域网；

禁用次数更新子单元，用于更新当前记录的所述无线局域网被禁用的次数。

17.如权利要求16所述的网络检测装置，其特征在于，所述网络检测装置还包括：

备选列表显示单元，用于在无线局域网备选列表中，显示各个可连接的无线局域网曾被所述智能终端接入的次数及曾被所述智能终端禁用的次数，所述可连接的无线局域网为当前智能终端未接入的无线局域网。

18.如权利要求12至17任一项所述的网络检测装置，其特征在于，所述确定单元，具体用于若所述HTTP检测单元本次所得到的HTTP检测结果为连接成功，则确定所述智能终端当前接入的无线局域网为可上网网络。

19.如权利要求12至17任一项所述的网络检测装置，其特征在于，所述述确定单元，具

体用于若所述HTTP检测单元本次所得到的TCP检测结果为连接失败，或者，若所述HTTP检测单元本次所得到的HTTP检测结果及所述TCP检测单元本次所得到的TCP检测结果均为连接受限，则确定所述智能终端当前接入的无线局域网为不可上网网络。

20.如权利要求12至17任一项所述的网络检测装置，其特征在于，所述HTTP检测单元包括：

HTTP请求子单元，用于通过所述无线局域网向预设的第一服务器发送HTTP连接请求；

HTTP确定子单元，用于若与所述第一服务器连接成功，则确定本次HTTP检测结果为连接成功；

HTTP检测子单元，用于若与所述第一服务器连接失败，则根据接收到的HTTP状态值确定所述无线局域网是否为认证网络；

所述HTTP确定子单元，还用于若所述HTTP检测子单元确定所述无线局域网为认证网络，则确定本次HTTP检测结果为连接受限，若所述HTTP检测子单元确定所述无线局域网不为认证网络，则确定本次HTTP检测结果为连接失败。

21.如权利要求12所述的网络检测装置，其特征在于，所述信息获取子单元，包括：

数量检测子单元，用于检测当前智能终端的内核中是否存在Socket；

获取子单元，用于若当前智能终端的内核中存在有Socket，则周期性获取当前智能终端的内核中的所有Socket的参数信息。

22.如权利要求21所述的网络检测装置，其特征在于，所述TCP状态确定子单元，具体用于当所述数量检测子单元检测到当前智能终端的内核中不存在Socket时，确定当前网络连接的TCP状态为连接失败。

23.一种智能终端，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现如权利要求1至11任一项所述方法的步骤。

24.一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求1至11任一项所述方法的步骤。

一种网络检测方法、网络检测装置及智能终端

技术领域

[0001] 本发明属于网络应用技术领域，尤其涉及一种网络检测方法、网络检测装置、智能终端及计算机可读存储介质。

背景技术

[0002] 随着通讯技术的快速发展，无线网络，特别是无线局域网(Wireless Local Area Net，WLAN)在生活中各个方面都得到了广泛应用。由于无线局域网不需要布线，且传输速度较快，因而能够很好的弥补有限局域网的不足。而当前几乎所有的智能终端都支持通过无线保真(Wireless Fidelity，Wi-Fi)接入无线局域网的热点(Hotspot)以实现上网功能。

[0003] 然而，很多公共场所提供的热点为Web认证热点，用户在接入Web认证热点后需要输入认证信息，才能访问互联网；还有些公共场所提供的热点由于访问人数过多，使得用户访问互联网的速度过慢，甚至无法访问互联网。这导致了在很多情况下，由于用户无法获知热点的状态，并不知晓智能终端在接入热点后仍然不能上网，浪费了用户的时间。

发明内容

[0004] 有鉴于此，本发明提供了一种网络检测方法、网络检测装置、智能终端及计算机可读存储介质，旨在及时获知当前接入的无线局域网的网络状态，提高对当前接入的无线局域网的网络检测的速度及效率。

[0005] 本发明第一方面提供了一种网络检测方法，上述网络检测方法包括：

[0006] 在智能终端接入无线局域网后，同时启动超文本传输协议HTTP检测及传输控制协议TCP检测；

[0007] 上述HTTP检测为：通过上述无线局域网向预设的第一服务器发送HTTP连接请求，根据上述智能终端与上述第一服务器的连接状况得到HTTP检测结果；

[0008] 上述TCP检测为：周期性检测上述智能终端当前网络连接的TCP状态，根据上述TCP状态得到TCP检测结果；

[0009] 在预设的检测时间内，基于本次HTTP检测所得到的HTTP检测结果和/或本次TCP检测所得到的TCP检测结果确定上述智能终端当前接入的无线局域网为可上网网络或不可上网网络。

[0010] 本发明第二方面提供了一种网络检测装置，上述网络检测装置包括：

[0011] 检测单元，用于在智能终端接入无线局域网后，同时启动超文本传输协议HTTP检测及传输控制协议TCP检测；

[0012] 确定单元，用于在预设的检测时间内，基于本次HTTP检测所得到的HTTP检测结果和/或本次TCP检测所得到的TCP检测结果确定上述智能终端当前接入的无线局域网为可上网网络或不可上网网络；

[0013] 其中，上述检测单元包括：

[0014] HTTP检测单元，用于通过上述无线局域网向预设的第一服务器发送HTTP连接请

求，根据上述智能终端与上述第一服务器的连接状况得到HTTP检测结果；

[0015] TCP检测单元，用于周期性检测上述智能终端当前网络连接的TCP状态，根据上述TCP状态得到TCP检测结果。

[0016] 本发明第三方面提供了一种智能终端，包括存储器，处理器及存储在存储器上并可在处理器上运行的计算机程序，上述处理器执行上述计算机程序时实现上述第一方面中提及的网络检测方法。

[0017] 本发明第四方面提供一种计算机可读存储介质，该计算机可读存储介质上存储有计算机程序，上述计算机程序被处理器执行时实现上述第一方面中提及的网络检测方法。

[0018] 由上可见，在本发明方案中，在智能终端接入无线局域网后，同时启动超文本传输协议HTTP检测及传输控制协议TCP检测，其中，上述HTTP检测为：通过上述无线局域网向预设的第一服务器发送HTTP连接请求，根据上述智能终端与上述第一服务器的连接状况得到HTTP检测结果，上述TCP检测为：周期性检测上述智能终端当前网络连接的TCP状态，根据上述TCP状态得到TCP检测结果，然后在预设的检测时间内，基于本次HTTP检测所得到的HTTP检测结果和/或本次TCP检测所得到的TCP检测结果确定上述智能终端当前接入的无线局域网为可上网网络或不可上网网络。在智能终端接入无线局域网后，由于在无线局域网处于不同网络状态下时，获取HTTP检测及TCP检测的结果所用时间不同，因而本发明方案通过同时进行HTTP检测及TCP检测，能够最快速度的获知智能终端接入的无线局域网的网络状态，减少用户的等待时间，避免出现智能终端接入的无线局域网无法上网，而用户却不知情的情况。

附图说明

[0019] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0020] 图1是本发明提供的网络检测方法一个实施例实现流程示意图；

[0021] 图2是本发明提供的网络检测方法步骤101中HTTP检测的具体实现流程示意图；

[0022] 图3是本发明提供的网络检测方法步骤101中TCP检测的具体实现流程示意图；

[0023] 图4是本发明提供的网络检测方法另一个实施例实现流程示意图；

[0024] 图5是本发明提供的网络检测装置一个实施例结构示意图；

[0025] 图6是本发明提供的智能终端一个实施例结构示意图。

具体实施方式

[0026] 以下描述中，为了说明而不是为了限定，提出了诸如特定系统结构、技术之类的具体细节，以便透彻理解本发明实施例。然而，本领域的技术人员应当清楚，在没有这些具体细节的其它实施例中也可以实现本发明。在其它情况中，省略对众所周知的系统、装置、电路以及方法的详细说明，以免不必要的细节妨碍本发明的描述。

[0027] 为了说明本发明上述的技术方案，下面通过具体实施例来进行说明。

[0028] 实施例一

[0029] 下面对本发明实施例提供的一种网络检测方法进行描述，请参阅图1，本发明实施例中的网络检测方法包括：

[0030] 在步骤101中，在智能终端接入无线局域网后，同时启动超文本传输协议HTTP检测及传输控制协议TCP检测；

[0031] 在本发明实施例中，上述智能终端接入无线局域网，可以是智能终端接收了用户输入的连接指令，并基于上述连接指令接入上述连接指令所确定的无线局域网，或者，也可以是在智能终端的Wi-Fi模式下，由智能终端主动扫描当前环境下可以接入的无线局域网，并由智能终端主动接入当前环境下智能终端可以接入的任一无线局域网，其中，上述由智能终端主动接入当前环境下智能终端可以接入的任一无线局域网可以是接入当前环境下信号最强的一个无线局域网，也可以是接入当前环境下随机指定的一个无线局域网，还可以是接入当前环境下上述智能终端曾接入次数最多的一个无线局域网，此处不作限定。在智能终端接入无线局域网后，可以立即或者等待一定时间触发智能终端同时启动HTTP检测及TCP检测；其中，上述HTTP检测为：通过上述无线局域网向预设的第一服务器发送HTTP连接请求，根据上述智能终端与上述第一服务器的连接状况得到HTTP检测结果；上述TCP检测为：周期性检测上述智能终端当前网络连接的TCP状态，根据上述TCP状态得到TCP检测结果。

[0032] 进一步地，图2示出了步骤101中HTTP检测的具体实现流程，详述如下：

[0033] 在步骤201中，通过上述无线局域网向预设的第一服务器发送超文本传输协议HTTP连接请求；

[0034] 在步骤202中，若与上述第一服务器连接成功，则确定本次HTTP检测结果为连接成功；

[0035] 在步骤203中，若与上述第一服务器连接失败，则根据接收到的HTTP状态值确定上述无线局域网是否为认证网络；

[0036] 可选地，上述根据接收到的HTTP状态值确定上述无线局域网是否为认证网络，具体包括：在向上述第一服务器发送了HTTP连接请求后，对接收到的HTTP状态值进行查阅；若上述HTTP状态值指示了在连接上述第一服务器的过程中，所请求访问的与上述第一服务器关联的统一资源定位符(Uniform Resource Locator，URL)被重定向，则进一步检测重定向后的URL所关联的页面是否包含预设的关键词，例如“用户名”、“登录名”、“密码”等关键词；若重定向后的URL所关联的页面包含预设的关键词，则确定上述无线局域网为认证网络。当然，也可以通过其它方式，检测上述无线局域网是否为认证网络，此处不作限定。需要注意的是，上述预设的关键词仅仅是示例性的。

[0037] 在步骤204中，若确定上述无线局域网为认证网络，则确定本次HTTP检测结果为连接受限；

[0038] 在步骤205中，若确定上述无线局域网不为认证网络，则确定本次HTTP检测结果为连接失败。

[0039] 可选地，考虑到与上述第一服务器连接失败可能不是上述无线局域网的原因，而是上述第一服务器自身的原因，在步骤201中，除了向第一服务器发送HTTP连接请求之外，还可以通过多线程并发的方式向预设的第二服务器发送HTTP连接请求；若与上述第一服务器和/或上述第二服务器连接成功，则确定本次HTTP检测结果为连接成功；若与上述第一服

务器及第二服务器均连接失败，则再执行根据接收到的HTTP状态值确定上述无线局域网是否为认证网络这一步骤及后续步骤。

[0040] 进一步地，图3示出了步骤101中TCP检测的具体实现流程，详述如下：

[0041] 在步骤301中，周期性获取当前上述智能终端的内核中所有的套接字Socket的参数信息；

[0042] 在本发明实施例中，在周期性检测当前网络连接的TCP状态时，首先从智能终端的内核中，周期性获取当前存在的所有的Socket的参数信息。具体地，对于任一Socket来说，步骤201中获取的Socket的参数信息包括但不限于状态(state)信息、重传超时(Retransmission Time-Out，rto)信息、往返时延(Round-Trip Time，rtt)信息、响应超时(ACKnowledge Time-Out，ato)信息。

[0043] 可选地，上述步骤301具体为：

[0044] 检测当前上述智能终端的内核中是否存在Socket；

[0045] 若当前上述智能终端的内核中不存在Socket，则确定当前网络连接的TCP状态为连接失败；

[0046] 若当前上述智能终端的内核中存在Socket，则周期性获取当前上述智能终端的内核中所有的Socket的参数信息。

[0047] 其中，一旦智能终端接入了无线局域网，则可以检测当前智能终端的内核中是否存在Socket。由于在智能终端处于可以上网的状态时，多数智能终端的系统后台会主动创建Socket进行TCP连接，因而，可以通过内核中的Socket的数量，初步确定当前是否存在TCP连接。若上述智能终端的内核中不存在Socket，则意味着当前也不存在与Socket对应的链路，即，当前不存在TCP连接，因而，可以确定当前网络连接的TCP状态为连接失败；而在当前内核中存在Socket时，则可以周期性获取当前各Socket的参数信息。

[0048] 在步骤302中，基于各Socket的参数信息，分别判断与各Socket对应的链路的类型；

[0049] 在本发明实施例中，基于内核中的各Socket的参数信息，分别判断与各Socket对应的链路类型。具体地，上述链路类型包括网络差链路，网络受限链路，不再使用链路，未关闭链路。其中，若Socket的state参数不为TCP_SYN_SENT，且rtt参数大于预设的rtt阈值(比如10000000)，且与该Socket对应的链路存在重传的数据包或者未响应的数据包时，则确定与该Socket对应的链路为网络差链路；若Socket的state参数为TCP_SYN_SENT，且与该Socket对应的链路最后一次发送数据包时间与最后一次接收数据包时间相等时，则确定与该Socket对应的链路为网络受限链路；若Socket对应的链路最后一次发送数据包时间、最后一次接收数据包时间及最后一次接收响应(Acknowledge，ACK)时间均大于预设的周期阈值时，则确定与该Socket对应的链路为不再使用链路；若Socket的state参数不为TCP_CLOSE_WAIT，则确定与该Socket对应的链路为未关闭链路。需要注意的是，允许一Socket所对应的链路同时属于上述两种以上的链路的类型，此处不作限定，例如，网络受限链路必然为未关闭链路，则一链路可以同时为网络受限链路及未关闭链路。

[0050] 在步骤303中，根据不同类型的链路之间的数量关系，确定当前网络连接的TCP状态；

[0051] 在本发明实施例中，根据步骤202中获得的各个类型的链路之间的数量关系，确定

当前网络连接的TCP状态。可选地，可以首先确定当前网络连接的TCP状态是否为连接成功；若当前网络连接的TCP状态不为连接成功，则继续检测当前网络连接的TCP状态是否为连接失败；若当前网络连接的TCP状态不为连接失败，则再继续检测当前网络连接的TCP状态是否为连接受限。具体地，在确定当前网络连接的TCP状态是否为连接成功之前，可以先统计网络不佳链路的数量，其中，上述网络不佳链路的数量为网络受限链路的数量及网络差链路的数量之和。

[0052] 其中，上述确定当前网络连接的TCP状态是否为连接成功，具体为：

[0053] 若第一比值不大于预设的比值阈值C1，且第二比值不大于预设的比值阈值D1，则确定当前网络连接的TCP状态为连接成功，其中，上述第一比值为网络不佳链路的数量与未关闭链路的数量的比值，上述第二比值为不再使用链路的数量与未关闭链路的数量的比值，上述C1、D1的取值可由开发人员或用户自行设置，此处不作限定。

[0054] 其中，在确定了上述TCP状态不为连接成功后，上述确定当前网络连接的TCP状态是否为连接失败，具体为：

[0055] 若上述第一比值不小于预设的比值阈值C2，且上述第二比值不小于预设的比值阈值D2，且第三比值不小于预设的比值阈值E2，则确定当前网络连接的TCP状态为连接失败，其中，上述第三比值为网络受限链路的数量与未关闭链路的数量的比值，上述C2、D2、E2的取值可由开发人员或用户自行设置，此处不作限定。

[0056] 其中，在确定了上述TCP状态不为连接失败后，上述确定当前网络连接的TCP状态是否为连受限，具体为：

[0057] 若上述第一比值不小于预设的比值阈值C3，且上述第二比值不小于预设的比值阈值D3，且第三比值不小于预设的比值阈值E3，则确定当前网络连接的TCP状态为连接失败，其中，上述比值阈值C3不同于上述比值阈值C2，上述比值阈值D3不同于上述比值阈值D2，上述比值阈值E3不同于上述比值阈值E2，上述C3、D3、E3的取值可由开发人员或用户自行设置，此处不作限定。

[0058] 在步骤304中，若连续N1次确定上述TCP状态为连接成功，则确定本次TCP检测结果为连接成功；

[0059] 在本发明实施例中，一旦步骤303中连续N1次确定上述TCP状态为连接成功，则确定本次TCP检测结果为连接成功，并停止执行上述周期性获取当前所有的套接字Socket的参数信息的步骤，避免浪费智能终端的运行资源。

[0060] 在步骤305中，若连续N2次确定上述TCP状态为连接失败，则确定本次TCP检测结果为连接失败；

[0061] 在步骤306中，若连续N3次确定上述TCP状态为连接受限，则确定本次TCP检测结果为连接受限；

[0062] 在本发明实施例中，当上述TCP状态为网络受限时，意味着此时智能终端所处的网络为受限制的网络，即，此时智能终端所连接的无线局域网很可能是认证网络。因此，一旦检测到上述TCP状态为连接受限的状态，则即刻输出提醒消息，以提示用户进行身份认证。上述提醒消息可以以音频的方式输出，也可以文字的方式输出，此处不作限定。

[0063] 可选地，上述N1少于上述N2，上述N2少于上述N3。由于每次获取TCP状态的时间相同，能够使得在上述无线局域网的网络连接状态良好时，在短时间内即可通过检测当前网

络连接的TCP状态快速确定上述无线局域网为可上网网络;在上述无线局域网的网络连接状态不佳时,通过稍长时间对当前网络连接的TCP状态的检测,避免对上述无线局域网的网络连接状态作出错误判断;而在上述无线局域网为受限制的网络时,由于进行认证操作需要耗费一定的时间,为了给用户留出时间,可以对上述N3取较大值,因此此处可以令N3大于N2。

[0064] 在步骤102中,在预设的检测时间内,基于本次HTTP检测所得到的HTTP检测结果和/或本次TCP检测所得到的TCP检测结果确定上述智能终端当前接入的无线局域网为可上网网络或不可上网网络。

[0065] 在本发明实施例中,上述步骤102表现为:若本次HTTP检测所得到的HTTP检测结果为连接成功,则确定上述智能终端当前接入的无线局域网为可上网网络;若本次TCP检测所得到的TCP检测结果为连接失败,或者,若本次HTTP检测所得到的HTTP检测结果及本次TCP检测所得到的TCP检测结果均为连接受限,则确定上述智能终端当前接入的无线局域网为不可上网网络。实际上,若智能终端能够通过上述无线局域网上网,则HTTP检测的速度通常快于TCP检测的速度,即在得到TCP检测结果之前,通过得到的HTTP检测结果就已经能够确定上述智能终端当前接入的无线局域网为可上网网络了,并且,当无线局域网为可上网网络时,HTTP检测结果通常可以在预设的第一时间内获得;与之对应的,在上述无线局域网不为认证网络的情况下,若智能终端不能够通过上述无线局域网上网,则TCP检测的速度通常快于HTTP检测的速度,即在得到HTTP检测结果之前,通过得到的TCP检测结果就已经能够确定上述智能终端当前接入的无线局域网为不可上网网络了,并且,当无线局域网为不可上网网络时,TCP检测结果通常可以在预设的第二时间内获得;因此在本步骤中,由于HTTP检测连接成功的速度较快,TCP检测连接失败的速度较快,通过结合HTTP检测及TCP检测,能够快速确定智能终端当前接入的无线局域网为不可上网网络或不可上网网络。进一步地,由于连接受限的状态相对于连接失败的状态及连接成功的状态较为复杂,为了提高网络检测的准确率,仅在HTTP检测结果及TCP检测结果均为连接受限时,才确定上述智能终端当前接入的无线局域网为不可上网网络。

[0066] 可选地,上述基于本次HTTP检测所得到的HTTP检测结果和/或本次TCP检测所得到的TCP检测结果确定上述智能终端当前接入的无线局域网为可上网网络或不可上网网络之后,或者,在上述检测时间到达之后,上述网络检测方法还包括:

[0067] 若本次TCP检测和/或本次HTTP检测仍在运行中,则停止本次TCP检测和/或本次HTTP检测。

[0068] 其中,上述预设的检测时间略大于一次HTTP检测或一次TCP检测所正常耗费的最长时间。一旦已经确定了上述无线局域网是否可上网,为了节约智能终端的运行资源,避免智能终端执行不必要的网络检测操作,当本次TCP检测和/或本次HTTP检测仍在运行中时,停止本次TCP检测和/或本次HTTP检测。进一步地,若在上述检测时间到达后,仍未确定上述智能终端当前接入的无线局域网是否可上网,则可能是在HTTP检测和/或TCP检测的过程中出现了问题而导致的本次网络检测超时,此时,若本次TCP检测和/或本次HTTP检测仍在运行中,也同样停止本次TCP检测和/或本次HTTP检测,并等待一定时间触发智能终端启动下次HTTP检测及TCP检测。

[0069] 由上可见,通过本发明实施例,在智能终端接入无线局域网后,由于在无线局域网

处于不同网络状态下时，获取HTTP检测及TCP检测的结果所用时间不同，因而通过同时进行HTTP检测及TCP检测，能够最快速度的获知无线局域网的网络状态，减少用户的等待时间，避免出现智能终端接入的无线局域网无法上网，而用户却不知情的情况。

[0070] 应理解，上述实施例中各步骤的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。

[0071] 实施例二

[0072] 在实施例一的基础上，下面对本发明实施例提供的另一种网络检测方法进行描述，请参阅图4，本发明实施例中的网络检测方法包括：

[0073] 在步骤401中，在智能终端接入无线局域网后，同时启动超文本传输协议HTTP检测及传输控制协议TCP检测；

[0074] 在本发明实施例中，上述步骤401与上述步骤101相同，具体可参见步骤101的相关描述，在此不再赘述。

[0075] 在步骤402中，在预设的检测时间内，基于本次HTTP检测所得到的HTTP检测结果和/或本次TCP检测所得到的TCP检测结果确定上述智能终端当前接入的无线局域网为可上网网络或不可上网网络；

[0076] 在本发明实施例中，上述步骤402与上述步骤102相同，具体可参见步骤102的相关描述，在此不再赘述。

[0077] 在步骤403中，若上述无线局域网被确定为不可上网网络，则断开上述智能终端与上述无线局域网的连接；

[0078] 在本发明实施例中，由于上述无线局域网已被确定为不可上网网络，若智能终端仍保持接入上述无线局域网，则会默认使用接入的无线局域网来进行网络访问，而当前接入的无线局域网实际上又是无法与外网进行连接的，这会给用户带来使用上的不便，影响智能终端的可操作性。为了避免上述情况的发生，在上述无线局域网被确定为不可上网网络后，断开上述智能终端与上述无线局域网的连接，避免给用户带来已经接入了无线局域网却仍然无法访问外网的疑惑。在断开与上述无线局域网的连接后，可以以文字的方式或者音频的方式主动提醒用户由于当前无线局域网的网络状态不佳，智能终端已经断开与上述无线局域网的连接。

[0079] 可选地，若上述无线局域网被确定为不可上网网络，则上述网络检测方法还包括：

[0080] 在预设的禁用时间内，禁用上述无线局域网。

[0081] 其中，由于上述无线局域网已经被确定不可上网网络，为了避免智能终端在手动断开或自动断开与上述无线局域网的连接后再次自动接入上述无线局域网，可以在预设的禁用时间内，禁用上述无线局域网，并记录上述无线局域网被禁用的次数。可选地，上述预设的禁用时间可以是智能终端设置的一个定值，例如五分钟，此处不作限定。

[0082] 可选地，上述在预设的禁用时间内，禁用上述无线局域网包括：

[0083] 获取当前记录的上述无线局域网被禁用的次数；

[0084] 根据当前记录的上述无线局域网被禁用的次数设定上述无线局域网的禁用时间；

[0085] 在上述无线局域网的禁用时间内，禁用上述无线局域网；

[0086] 更新当前记录的上述无线局域网被禁用的次数。

[0087] 其中，上述禁用时间可以与上述无线局域网被禁用的次数成正比例关系。例如，对于某一无线局域网A，在第一次禁用该无线局域网A时，禁用时间为5分钟；在第二次禁用该无线局域网A时，禁用时间为10分钟；在第三次禁用该无线局域网A时，禁用时间为15分钟，即，对该无线局域网的禁用时间随着该无线局域网的禁用次数的递增而递增。需要注意的是，上述禁用时间仅仅是示例性的，在实际应用中，上述禁用时间可以根据用户的需求而进行更改，此处不作限定。并且，每当无线局域网被禁用时，其对应的被禁用的次数也会得到更新。

[0088] 可选地，为了提高用户手动选择无线局域网的效率，上述网络检测方法还包括：

[0089] 在无线局域网备选列表中，显示各个可连接的无线局域网曾被上述智能终端接入的次数及曾被上述智能终端禁用的次数。

[0090] 其中，在用户手动连接无线局域网时，由于无线局域网备选列表中通常只显示各无线局域网的信号强度，使得用户在选择无线局域网时也只考虑到了无线局域网的信号强度，而忽略了选择的无线局域网是否能够进行网络访问。实际上，许多公共场所中开放的无线局域网的热点，虽然热点的信号强度较强，但由于访问的人数过多或者由于该热点的无线局域网为认证网络，而导致智能终端接入该无线局域网后根本无法实现上网功能。为了使得各无线局域网的真实网络连接状态能够在用户手动选择网络之前为用户所知，可以在无线局域网备选列表中，显示各个可连接的无线局域网曾被上述智能终端接入的次数及曾被上述智能终端禁用的次数，其中，上述可连接的无线局域网为当前智能终端还未接入的无线局域网。例如，若在无线局域网列表中存在A、B、C三个可连接的无线局域网，A的总连接次数为10次，被禁用次数为8次，信号强度为强；B的总连接次数为5次，被禁用次数为0次，信号强度为较强；C的总连接次数为8次，被禁用次数为3次，信号强度为强，上述总连接次数为无线局域网曾被上述智能终端接入的次数，上述被禁用次数为无线局域网曾被上述智能终端禁用的次数。由于用户可以直接通过无线局域网备选列表获知各无线局域网的历史连接情况，结合各无线局域网的信号强度，选择合适的无线局域网进行连接，因而在上述例子中，考虑到各热点曾被禁用的情况，用户很大可能会选择信号强度仅仅是较强的无线局域网B，而不是信号强的无线局域网A或C。

[0091] 由上可见，通过本发明实施例，在通过HTTP检测及TCP检测的检测结果确定智能终端当前接入的无线局域网为不可上网网络后，将主动断开与当前接入的无线局域网的连接避免给用户带来已经接入了无线局域网却仍然无法访问外网的疑惑；同时还将禁用上述无线局域网一段时间，以避免智能终端错误地主动接入该不可上网的无线局域网。

[0092] 实施例三

[0093] 本发明实施例还提供一种网络检测装置，如图5所示，本发明实施例中的网络检测装置500包括：

[0094] 检测单元501，用于在智能终端接入无线局域网后，同时启动超文本传输协议HTTP检测及传输控制协议TCP检测；

[0095] 确定单元502，用于在预设的检测时间内，基于本次HTTP检测所得到的HTTP检测结果和/或本次TCP检测所得到的TCP检测结果确定上述智能终端当前接入的无线局域网为可上网网络或不可上网网络；

[0096] 其中，上述检测单元501包括：

[0097] HTTP检测单元5011，用于通过上述无线局域网向预设的第一服务器发送HTTP连接请求，根据上述智能终端与上述第一服务器的连接状况得到HTTP检测结果；

[0098] TCP检测单元5012，用于周期性检测上述智能终端当前网络连接的TCP状态，根据上述TCP状态得到TCP检测结果。

[0099] 可选地，上述网络检测装置500还包括：

[0100] 停止单元，用于在基于本次HTTP检测所得到的HTTP检测结果和/或本次TCP检测所得到的TCP检测结果确定上述智能终端当前接入的无线局域网为可上网网络或不可上网网络之后，或者，在上述检测时间到达之后，若本次TCP检测和/或本次HTTP检测仍在运行中，则停止本次TCP检测和/或本次HTTP检测。

[0101] 可选地，上述网络检测装置500还包括：

[0102] 连接断开单元，用于当确定上述智能终端当前接入的无线局域网为不可上网网络时，断开上述智能终端与上述无线局域网的连接。

[0103] 可选地，上述网络检测装置500还包括：

[0104] 无线局域网禁用单元，用于当确定上述智能终端当前接入的无线局域网为不可上网网络时，在预设的禁用时间内，禁用上述无线局域网。

[0105] 可选地，上述无线局域网禁用单元包括：

[0106] 禁用次数获取子单元，用于获取当前记录的上述无线局域网被禁用的次数；

[0107] 禁用时间设定子单元，用于根据当前记录的上述无线局域网被禁用的次数设定上述无线局域网的禁用时间；

[0108] 网络禁用子单元，用于在上述无线局域网的禁用时间内，禁用上述无线局域网；

[0109] 禁用次数更新子单元，用于更新当前记录的上述无线局域网被禁用的次数。

[0110] 可选地，上述网络检测装置500还包括：

[0111] 备选列表显示单元，用于在无线局域网备选列表中，显示各个可连接的无线局域网曾被上述智能终端接入的次数及曾被上述智能终端禁用的次数，上述可连接的无线局域网为当前智能终端未接入的无线局域网。

[0112] 可选地，上述确定单元502，具体用于，若上述HTTP检测单元本次所得到的HTTP检测结果为连接成功，则确定上述智能终端当前接入的无线局域网为可上网网络；

[0113] 可选地，上述确定单元502，具体用于，若上述HTTP检测单元本次所得到的TCP检测结果为连接失败，或者，若上述HTTP检测单元本次所得到的HTTP检测结果及上述TCP检测单元本次所得到的TCP检测结果均为连接受限，则确定上述智能终端当前接入的无线局域网为不可上网网络。

[0114] 可选地，上述HTTP检测单元5011包括：

[0115] HTTP请求子单元，用于通过上述无线局域网向预设的第一服务器发送HTTP连接请求；

[0116] HTTP确定子单元，用于若与上述第一服务器连接成功，则确定本次HTTP检测结果为连接成功；

[0117] HTTP检测子单元，用于若与上述第一服务器连接失败，则根据接收到的HTTP状态值确定上述无线局域网是否为认证网络；

[0118] 上述HTTP确定子单元，还用于若上述HTTP检测子单元确定上述无线局域网为认证

网络，则确定本次HTTP检测结果为连接受限，若上述HTTP检测子单元确定上述无线局域网不为认证网络，则确定本次HTTP检测结果为连接失败。

[0119] 可选地，上述TCP检测单元5012包括：

[0120] 信息获取子单元，用于周期性获取当前上述智能终端的内核中所有的套接字Socket的参数信息；

[0121] 链路判断子单元，用于基于各Socket的参数信息，分别判断与各Socket对应的链路的类型；

[0122] TCP状态确定子单元，用于根据不同类型的链路之间的数量关系，确定当前网络连接的TCP状态；

[0123] TCP确定子单元，用于若上述TCP状态确定子单元连续N1次确定上述TCP状态为连接成功，则确定本次TCP检测结果为连接成功，若上述TCP状态确定子单元连续N2次确定上述TCP状态为连接失败，则确定本次TCP检测结果为连接失败，若上述TCP状态确定子单元连续N3次确定上述TCP状态为连接受限，则确定本次TCP检测结果为连接受限。

[0124] 可选地，上述信息获取子单元包括：

[0125] 数量检测子单元，用于检测当前智能终端的内核中是否存在Socket；

[0126] 获取子单元，用于若当前智能终端的内核中存在有Socket，则周期性获取当前智能终端的内核中的所有Socket的参数信息。

[0127] 可选地，上述TCP状态确定子单元，具体用于当上述数量检测子单元检测到当前智能终端的内核中不存在Socket时，确定当前网络连接的TCP状态为连接失败。

[0128] 由上可见，通过本发明实施例，在智能终端接入无线局域网后，由于在无线局域网处于不同网络状态下时，获取HTTP检测及TCP检测的结果所用时间不同，因而网络检测装置通过同时进行HTTP检测及TCP检测，能够最快速度的获知无线局域网的网络状态，减少用户的等待时间，避免出现智能终端接入的无线局域网无法上网，而用户却不知情的情况。

[0129] 实施例四

[0130] 本发明实施例提供一种智能终端，请参阅图6，本发明实施例中的智能终端包括：存储器601，一个或多个处理器602(图6中仅示出一个)及存储在存储器601上并可在处理器上运行的计算机程序。其中：存储器601用于存储软件程序以及模块，处理器602通过运行存储在存储器601的软件程序以及单元，从而执行各种功能应用以及数据处理，以获取上述预设事件对应的资源。具体地，处理器602通过运行存储在存储器601的上述计算机程序时实现以下步骤：

[0131] 在智能终端接入无线局域网后，同时启动超文本传输协议HTTP检测及传输控制协议TCP检测；

[0132] 上述HTTP检测为：通过上述无线局域网向预设的第一服务器发送HTTP连接请求，根据上述智能终端与上述第一服务器的连接状况得到HTTP检测结果；

[0133] 上述TCP检测为：周期性检测上述智能终端当前网络连接的TCP状态，根据上述TCP状态得到TCP检测结果；

[0134] 在预设的检测时间内，基于本次HTTP检测所得到的HTTP检测结果和/或本次TCP检测所得到的TCP检测结果确定上述智能终端当前接入的无线局域网为可上网网络或不可上网网络。

[0135] 假设上述为第一种可能的实施方式，则在上述第一种可能的实施方式作为基础而提供的第二种可能的实施方式中，在上述基于本次HTTP检测所得到的HTTP检测结果和/或本次TCP检测所得到的TCP检测结果确定上述智能终端当前接入的无线局域网为可上网网络或不可上网网络之后，或者，在上述检测时间到达之后，处理器602通过运行存储在存储器601的上述计算机程序时还实现以下步骤：

[0136] 若本次TCP检测和/或本次HTTP检测仍在运行中，则停止本次TCP检测和/或本次HTTP检测。

[0137] 在上述第一种可能的实施方式作为基础而提供的第三种可能的实施方式中，若确定上述智能终端当前接入的无线局域网为不可上网网络，则处理器602通过运行存储在存储器601的上述计算机程序时还实现以下步骤：

[0138] 断开上述智能终端与上述无线局域网的连接。

[0139] 在上述第一种可能的实施方式作为基础而提供的第四种可能的实施方式中，若确定上述智能终端当前接入的无线局域网为不可上网网络，则处理器602通过运行存储在存储器601的上述计算机程序时还实现以下步骤：

[0140] 在预设的禁用时间内，禁用上述无线局域网。

[0141] 在上述第四种可能的实施方式作为基础而提供的第五种可能的实施方式中，上述在预设的禁用时间内，禁用上述无线局域网，包括：

[0142] 获取当前记录的上述无线局域网被禁用的次数；

[0143] 根据当前记录的上述无线局域网被禁用的次数设定上述无线局域网的禁用时间；

[0144] 在上述无线局域网的禁用时间内，禁用上述无线局域网；

[0145] 更新当前记录的上述无线局域网被禁用的次数。

[0146] 在上述第五种可能的实施方式作为基础而提供的第六种可能的实施方式中，处理器602通过运行存储在存储器601的上述计算机程序时还实现以下步骤：

[0147] 在无线局域网备选列表中，显示各个可连接的无线局域网曾被上述智能终端接入的次数及曾被上述智能终端禁用的次数，上述可连接的无线局域网为当前智能终端未接入的无线局域网。

[0148] 在上述第一种可能的实施方式作为基础，或者上述第二种可能的实施方式作为基础，或者上述第三种可能的实施方式作为基础，或者上述第四种可能的实施方式作为基础，或者上述第五种可能的实施方式作为基础，或者上述第六种可能的实施方式作为基础而提供的第七种可能的实施方式中，上述基于本次HTTP检测所得到的HTTP检测结果和/或本次TCP检测所得到的TCP检测结果确定上述智能终端当前接入的无线局域网为可上网网络或不可上网网络，包括：

[0149] 若本次HTTP检测所得到的HTTP检测结果为连接成功，则确定上述智能终端当前接入的无线局域网为可上网网络；

[0150] 在上述第一种可能的实施方式作为基础，或者上述第二种可能的实施方式作为基础，或者上述第三种可能的实施方式作为基础，或者上述第四种可能的实施方式作为基础，或者上述第五种可能的实施方式作为基础，或者上述第六种可能的实施方式作为基础而提供的第八种可能的实施方式中，上述基于本次HTTP检测所得到的HTTP检测结果和/或本次TCP检测所得到的TCP检测结果确定上述智能终端当前接入的无线局域网为可上网网络或

不可上网网络，包括：

[0151] 若本次TCP检测所得到的TCP检测结果为连接失败，或者，若本次HTTP检测所得到的HTTP检测结果及本次TCP检测所得到的TCP检测结果均为连接受限，则确定上述智能终端当前接入的无线局域网为不可上网网络。

[0152] 在上述第一种可能的实施方式作为基础，或者上述第二种可能的实施方式作为基础，或者上述第三种可能的实施方式作为基础，或者上述第四种可能的实施方式作为基础，或者上述第五种可能的实施方式作为基础，或者上述第六种可能的实施方式作为基础而提供的第九种可能的实施方式中，上述通过上述无线局域网向预设的第一服务器发送HTTP连接请求，根据上述智能终端与上述第一服务器的连接状况得到HTTP检测结果，包括：

[0153] 通过上述无线局域网向预设的第一服务器发送HTTP连接请求；

[0154] 若与上述第一服务器连接成功，则确定本次HTTP检测结果为连接成功；

[0155] 若与上述第一服务器连接失败，则根据接收到的HTTP状态值确定上述无线局域网是否为认证网络；

[0156] 若确定上述无线局域网为认证网络，则确定本次HTTP检测结果为连接受限；

[0157] 若确定上述无线局域网不为认证网络，则确定本次HTTP检测结果为连接失败。

[0158] 在上述第一种可能的实施方式作为基础，或者上述第二种可能的实施方式作为基础，或者上述第三种可能的实施方式作为基础，或者上述第四种可能的实施方式作为基础，或者上述第五种可能的实施方式作为基础，或者上述第六种可能的实施方式作为基础而提供的第十种可能的实施方式中，上述周期性检测上述智能终端当前网络连接的TCP状态，根据上述TCP状态得到TCP检测结果，包括：

[0159] 周期性获取当前上述智能终端的内核中所有的套接字Socket的参数信息；

[0160] 基于各Socket的参数信息，分别判断与各Socket对应的链路的类型；

[0161] 根据不同类型的链路之间的数量关系，确定当前网络连接的TCP状态；

[0162] 若连续N1次确定上述TCP状态为连接成功，则确定本次TCP检测结果为连接成功；

[0163] 若连续N2次确定上述TCP状态为连接失败，则确定本次TCP检测结果为连接失败；

[0164] 若连续N3次确定上述TCP状态为连接受限，则确定本次TCP检测结果为连接受限。

[0165] 在上述第十种可能的实施方式作为基础而提供的第十一种可能的实施方式中，上述周期性获取当前上述智能终端的内核中所有的套接字Socket的参数信息，包括：

[0166] 检测当前上述智能终端的内核中是否存在Socket；

[0167] 若当前上述智能终端的内核中存在Socket，则周期性获取当前上述智能终端的内核中所有的Socket的参数信息。

[0168] 在上述第十种可能的实施方式作为基础而提供的第十二种可能的实施方式中，上述网络检测方法还包括：

[0169] 若当前上述智能终端的内核中不存在Socket，则确定当前网络连接的TCP状态为连接失败。

[0170] 进一步，如图6所示，上述智能终端还可包括：一个或多个输入设备603(图6中仅示出一个)和一个或多个输出设备604(图6中仅示出一个)。存储器601、处理器602、输入设备603和输出设备604通过总线605连接。

[0171] 应当理解，在本发明实施例中，所称处理器602可以是中央处理单元(Central

Processing Unit,CPU),该处理器还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现成可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0172] 输入设备603可以包括键盘、触控板、指纹采传感器(用于采集用户的指纹信息和指纹的方向信息)、麦克风等,输出设备604可以包括显示器、扬声器等。

[0173] 存储器601可以包括只读存储器和随机存取存储器,并向处理器602提供指令和数据。存储器601的一部分或全部还可以包括非易失性随机存取存储器。例如,存储器601还可以存储设备类型的信息。

[0174] 由上可见,通过本发明实施例,在接入无线局域网后,由于在无线局域网处于不同网络状态下时,智能终端获取HTTP检测及TCP检测的结果所用时间不同,因而智能终端通过同时进行HTTP检测及TCP检测,能够最快速度的获知无线局域网的网络状态,减少用户的等待时间,避免出现智能终端接入的无线局域网无法上网,而用户却不知情的情况。

[0175] 所属领域的技术人员可以清楚地了解到,为了描述的方便和简洁,仅以上述各功能单元、模块的划分进行举例说明,实际应用中,可以根据需要而将上述功能分配由不同的功能单元、模块完成,即将上述装置的内部结构划分成不同的功能单元或模块,以完成以上描述的全部或者部分功能。实施例中的各功能单元、模块可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中,上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。另外,各功能单元、模块的具体名称也只是为了便于相互区分,并不用于限制本申请的保护范围。上述系统中单元、模块的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。

[0176] 在上述实施例中,对各个实施例的描述都各有侧重,某个实施例中没有详述或记载的部分,可以参见其它实施例的相关描述。

[0177] 本领域普通技术人员可以意识到,结合本文中所公开的实施例描述的各示例的单元及算法步骤,能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能,但是这种实现不应认为超出本发明的范围。

[0178] 在本发明所提供的实施例中,应该理解到,所揭露的装置和方法,可以通过其它的方式实现。例如,以上所描述的系统实施例仅仅是示意性的,例如,上述模块或单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通讯连接可以是通过一些接口,装置或单元的间接耦合或通讯连接,可以是电性,机械或其它的形式。

[0179] 上述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0180] 上述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明实现上述实施例方法中的全部或部分流程，也可以通过计算机程序来指令相关的硬件来完成，上述的计算机程序可存储于一计算机可读存储介质中，该计算机程序在被处理器执行时，可实现上述各个方法实施例的步骤。其中，上述计算机程序包括计算机程序代码，上述计算机程序代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。上述计算机可读介质可以包括：能够携带上述计算机程序代码的任何实体或装置、记录介质、U盘、移动硬盘、磁碟、光盘、计算机存储器、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、电载波信号、电信信号以及软件分发介质等。需要说明的是，上述计算机可读介质包含的内容可以根据司法管辖区内立法和专利实践的要求进行适当的增减，例如在某些司法管辖区，根据立法和专利实践，计算机可读介质不包括是电载波信号和电信信号。

[0181] 以上上述实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围，均应包含在本发明的保护范围之内。

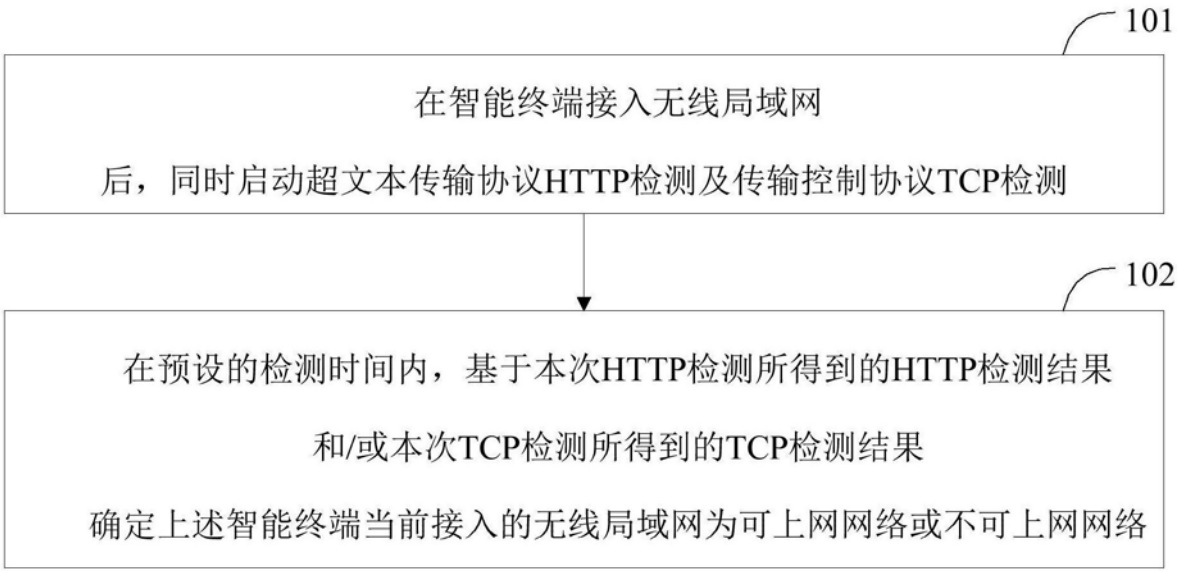

101
在智能终端接入无线局域网
后，同时启动超文本传输协议HTTP检测及传输控制协议TCP检测
102
在预设的检测时间内，基于本次HTTP检测所得到的HTTP检测结果
和/或本次TCP检测所得到的TCP检测结果
确定上述智能终端当前接入的无线局域网为可上网网络或不可上网网络

图1

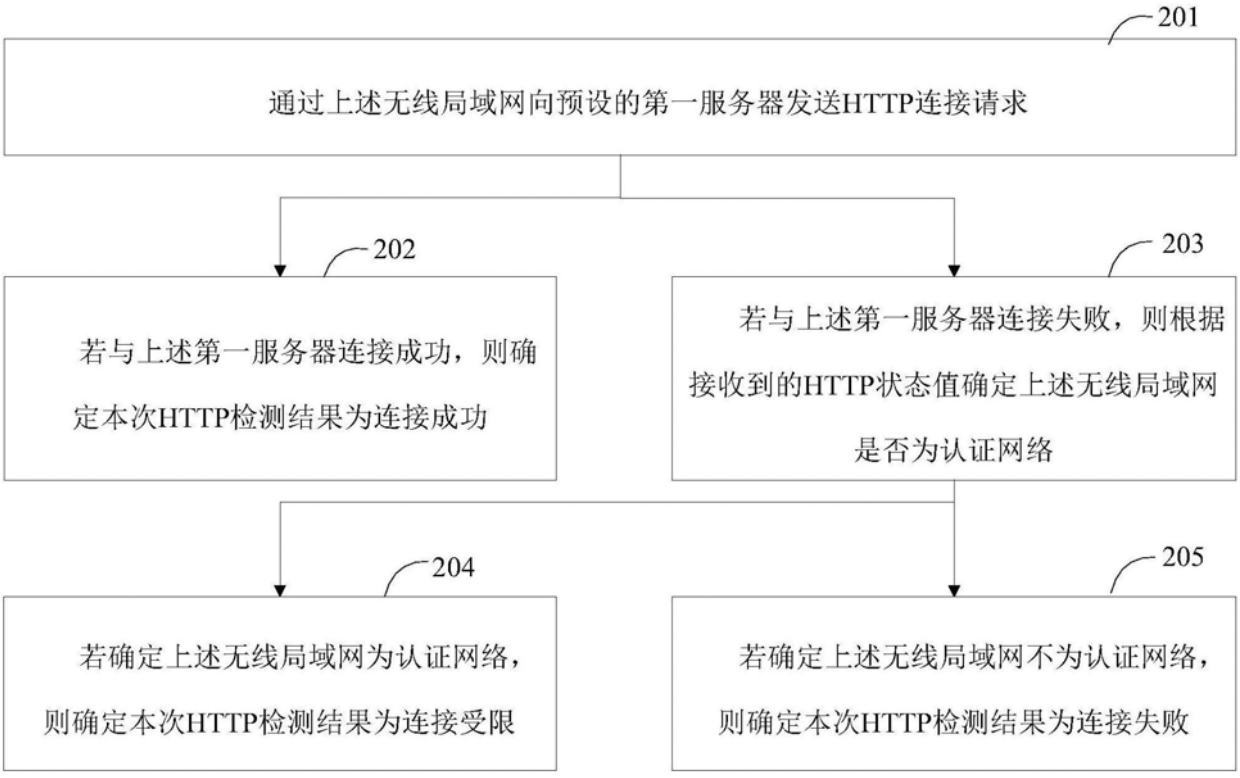

201
通过上述无线局域网向预设的第一服务器发送HTTP连接请求
202
若与上述第一服务器连接成功，则确定本次HTTP检测结果为连接成功
203
若与上述第一服务器连接失败，则根据接收到的HTTP状态值确定上述无线局域网是否为认证网络
204
若确定上述无线局域网为认证网络，则确定本次HTTP检测结果为连接受限
205
若确定上述无线局域网不为认证网络，则确定本次HTTP检测结果为连接失败

图2

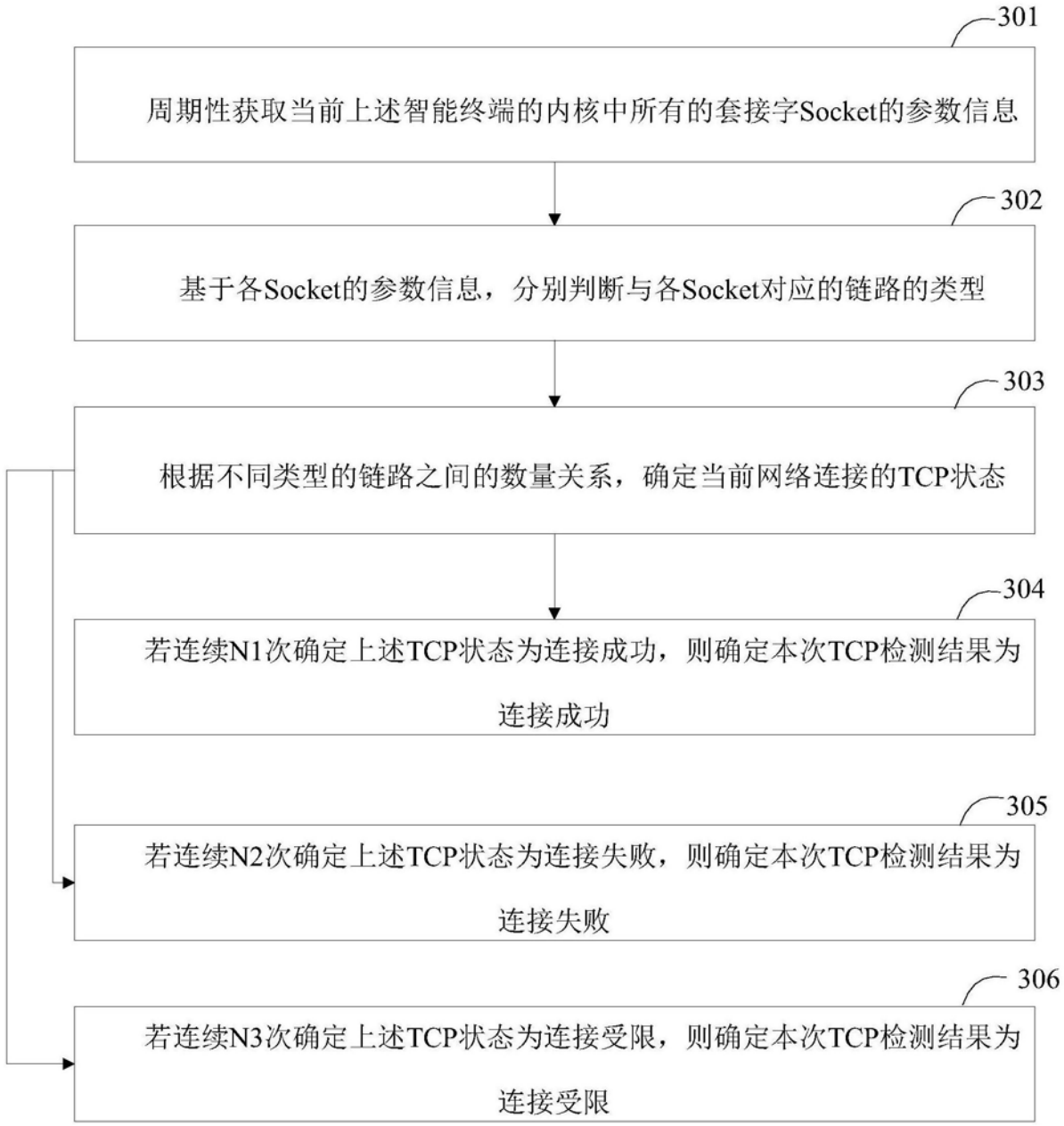

301
周期性获取当前上述智能终端的内核中所有的套接字Socket的参数信息
302
基于各Socket的参数信息，分别判断与各Socket对应的链路的类型
303
根据不同类型的链路之间的数量关系，确定当前网络连接的TCP状态
304
若连续N1次确定上述TCP状态为连接成功，则确定本次TCP检测结果为连接成功
305
若连续N2次确定上述TCP状态为连接失败，则确定本次TCP检测结果为连接失败
306
若连续N3次确定上述TCP状态为连接受限，则确定本次TCP检测结果为连接受限

图3

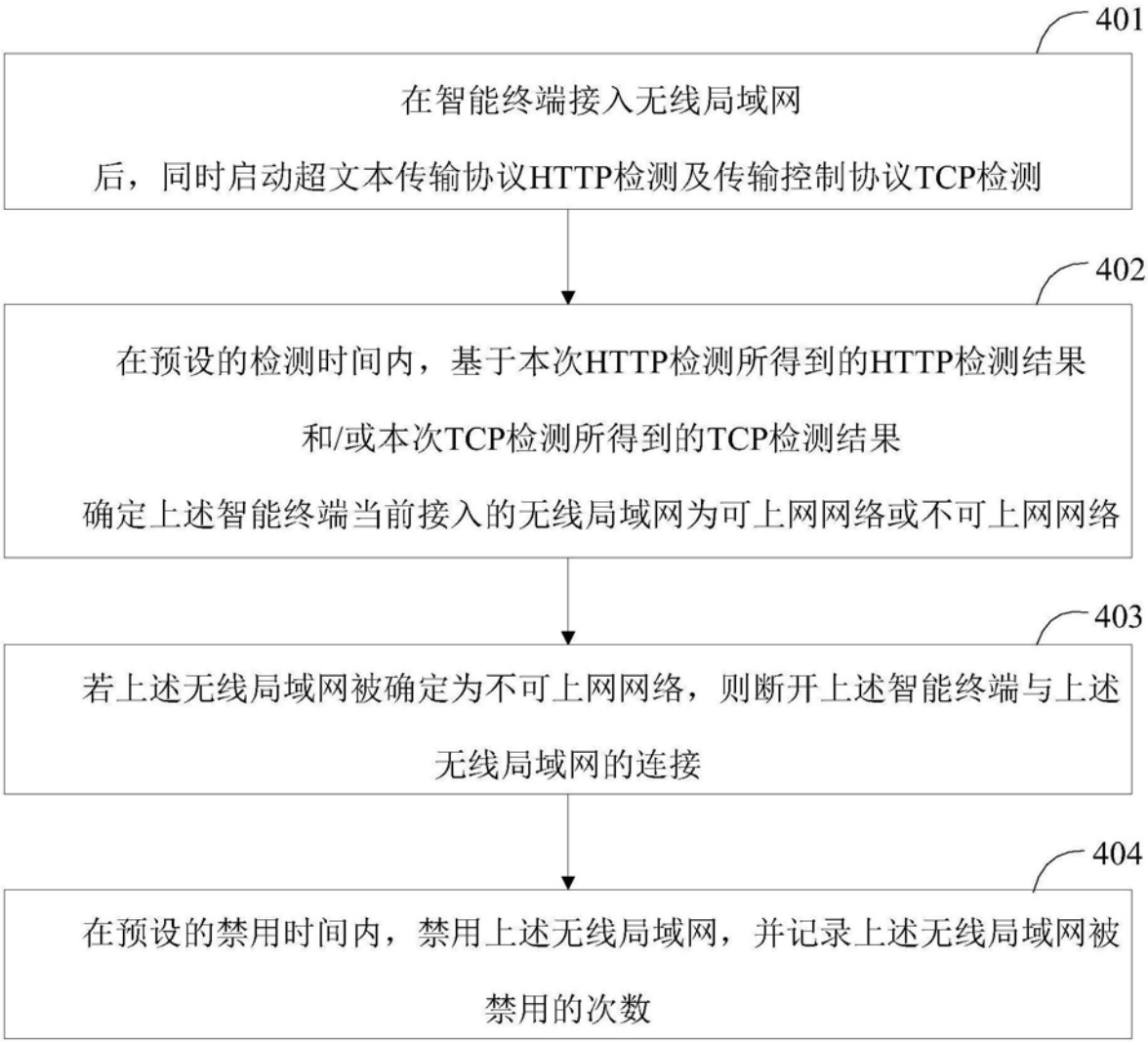

401
在智能终端接入无线局域网
后，同时启动超文本传输协议HTTP检测及传输控制协议TCP检测
402
在预设的检测时间内，基于本次HTTP检测所得到的HTTP检测结果
和/或本次TCP检测所得到的TCP检测结果
确定上述智能终端当前接入的无线局域网为可上网网络或不可上网网络
403
若上述无线局域网被确定为不可上网网络，则断开上述智能终端与上述
无线局域网的连接
404
在预设的禁用时间内，禁用上述无线局域网，并记录上述无线局域网被
禁用的次数

图4

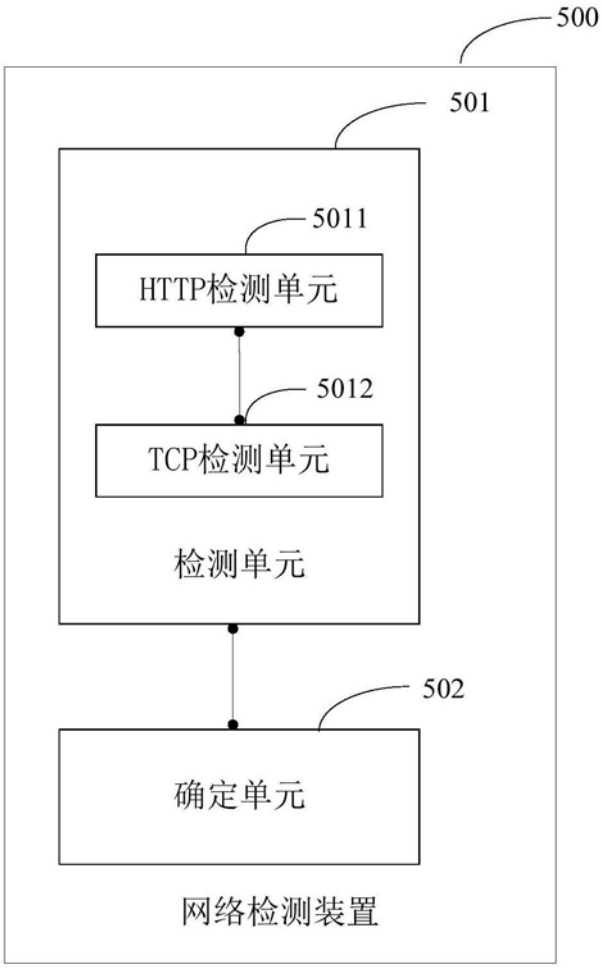

500
501
5011
HTTP检测单元
5012
TCP检测单元
检测单元
502
确定单元
网络检测装置

图5

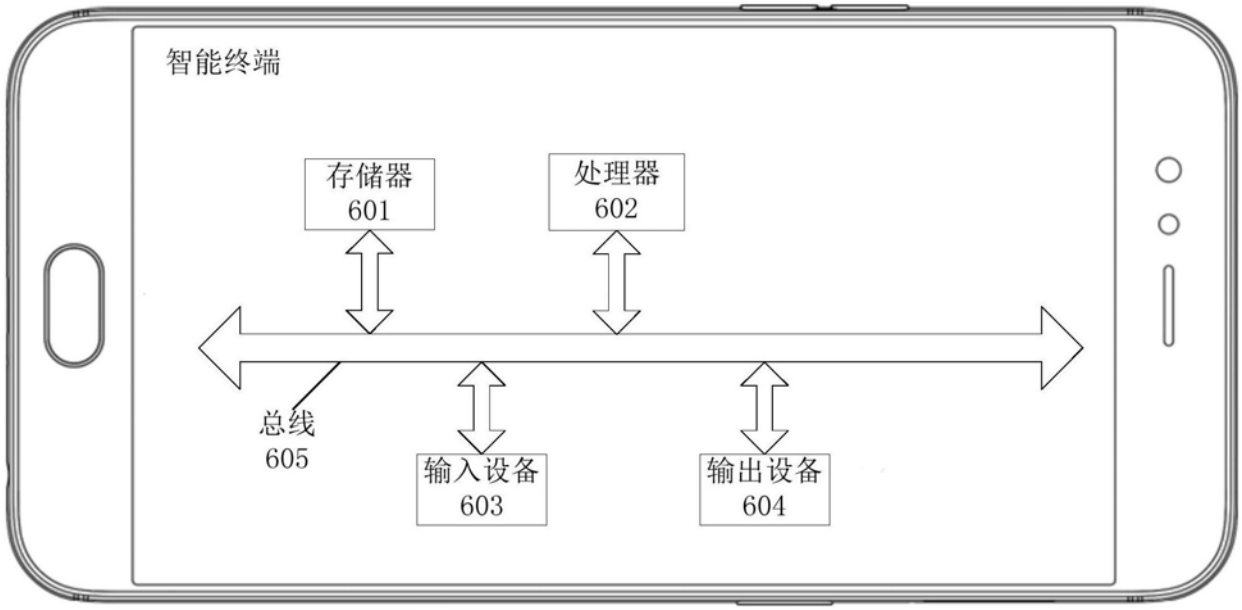

智能终端
存储器
601
处理器
602
总线
605
输入设备
603
输出设备
604

图6