(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104683290 A
(43)申请公布日 2015.06.03

(21)申请号 201310611863.8

(22)申请日 2013.11.26

(71)申请人 腾讯科技(深圳)有限公司
地址 518044 广东省深圳市福田区振兴路赛格科技园2栋东403室

(72)发明人 郭跃华

(74)专利代理机构 深圳中一专利商标事务所 44237
代理人 刘朗星

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 29/12(2006.01)

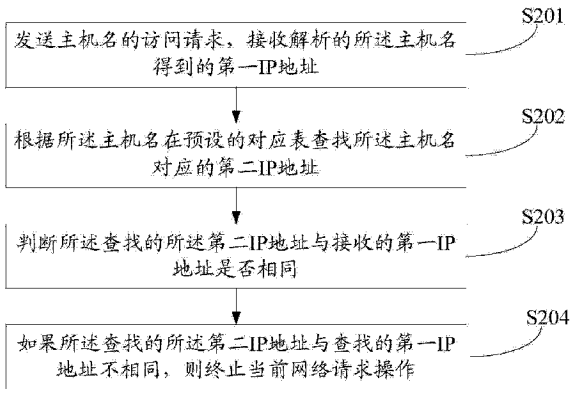
权利要求书2页 说明书8页 附图5页

(54)发明名称

一种监控网络钓鱼的方法、装置和终端

(57)摘要

本发明适用于互联网领域，提供了一种监控网络钓鱼的方法、装置和终端，该方法包括：发送主机名的访问请求，接收由所述主机名解析得到的第一IP地址；根据所述主机名在预设的对应表查找所述主机名对应的第二IP地址，所述对应表存储有主机名与IP地址的对应关系；判断所述查找的所述第二IP地址与接收的第一IP地址是否相同；如果所述查找的所述第二IP地址与查找的第一IP地址不相同，则终止当前网络请求操作。本发明能够有效的防止因网络钓鱼篡改主机名所对应的IP地址，造成用户访问恶意服务器造成的财产损失，更好的保证信息的安全性。



CN 104683290 A

1. 一种监控网络钓鱼的方法，其特征在于，所述方法包括：

发送主机名的访问请求，接收由所述主机名解析得到的第一 IP 地址；

根据所述主机名在预设的对应表查找所述主机名对应的第二 IP 地址，所述对应表存储有主机名与 IP 地址的对应关系；

判断所述查找的所述第二 IP 地址与接收的第一 IP 地址是否相同；

如果所述查找的所述第二 IP 地址与查找的第一 IP 地址不相同，则终止当前网络请求操作。

2. 根据权利要求 1 所述的方法，其特征在于，所述预设的对应表存于校验服务器，所述根据所述主机名在预设的对应表查找所述主机名对应的第二 IP 地址，所述对应表存储有主机名与 IP 地址的对应关系步骤为：

向校验服务器发送校验请求，所述校验请求包括所述主机名、第一 IP 地址；

接收由校验服务器根据所述主机名，在主机名与 IP 地址对应表中，查找得到的所述主机名对应的第二 IP 地址。

3. 根据权利要求 2 所述方法，其特征在于，在所述判断所述查找的所述第二 IP 地址与接收的第一 IP 地址是否相同之前，所述方法还包括：

通过密钥验证所述校验服务器是否为指定的校验服务器。

4. 根据权利要求 2 所述方法，其特征在于，所述向校验服务器发送校验请求步骤和所述接收第二 IP 地址的步骤中，具体为通过虚拟专用网络 VPN 向校验服务器发送请求和通过虚拟专用网络 VPN 接收第二 IP 地址。

5. 根据权利要求 2 所述方法，其特征在于，所述向校验服务器发送校验请求，所述校验请求包括所述主机名、第一 IP 地址步骤中，所述校验请求还包括终端的唯一标识信息；

所述方法还包括：

查询在所述校验服务器是否记录有所述终端的唯一标识对应的网络钓鱼记录；

如果包括所述终端的唯一标识对应的网络钓鱼记录，则接收由所述校验发送的当前终端存在安全隐患的提示指令。

6. 根据权利要求 1 所述方法，其特征在于，所述预设的对应表存于本地的数据库，所述根据所述主机名在预设的对应表查找所述主机名对应的第二 IP 地址，所述对应表存储有主机名与 IP 地址的对应关系步骤为：

根据所述主机名，在所述本地的数据库中查找所述主机名对应的第二 IP 地址。

7. 一种监控网络钓鱼的装置，其特征在于，所述装置包括：

接收单元，用于发送主机名的访问请求，接收由所述主机名解析得到的第一 IP 地址；

查找单元，用于根据所述主机名在预设的对应表查找所述主机名对应的第二 IP 地址，所述对应表存储有主机名与 IP 地址的对应关系；

判断单元，用于判断所述查找的所述第二 IP 地址与接收的第一 IP 地址是否相同；

终止单元，用于如果所述查找的所述第二 IP 地址与查找的第一 IP 地址不相同，则终止当前网络请求操作。

8. 根据权利要求 7 所述装置，其特征在于，所述预设的对应表存于校验服务器，所述查找单元包括：

校验请求发送子单元，用于向校验服务器发送校验请求，所述校验请求包括所述主机

名、第一 IP 地址；

查找子单元，用于接收由校验服务器根据所述主机名，在主机名与 IP 地址对应表中，查找得到的所述主机名对应的第二 IP 地址。

9. 根据权利要求 8 所述装置，其特征在于，所述装置还包括：

验证单元，用于通过密钥验证所述校验服务器是否为指定的校验服务器。

10. 根据权利要求 8 所述装置，其特征在于，所述校验请求发送子单元和查找子单元用于通过虚拟专用网络 VPN 向校验服务器发送请求和通过虚拟专用网络 VPN 接收第二 IP 地址。

11. 根据权利要求 8 所述装置，其特征在于，所述校验请求发送子单元，所述校验请求还包括终端的唯一标识信息；

所述装置还包括：

查询单元，用于查询在所述校验服务器是否记录有所述终端的唯一标识对应的网络钓鱼记录；

指令发送单元，用于如果包括所述终端的唯一标识对应的网络钓鱼记录，则接收由所述校验发送的当前终端存在安全隐患的提示指令。

12. 根据权利要求 7 所述装置，其特征在于，所述预设的对应表存于本地的数据库，所述查找单元用于根据所述主机名，在所述本地的数据库中查找所述主机名对应的第二 IP 地址。

13. 一种终端，其特征在于，所述终端包括权利要求 7-12 任一项所述的监控网络钓鱼的装置。

一种监控网络钓鱼的方法、装置和终端

技术领域

[0001] 本发明属于互联网领域，尤其涉及一种监控网络钓鱼的方法、装置和终端。

背景技术

[0002] 随着网络技术的发展，人们通过使用移动终端如智能手机、PAD 或者使用计算机连接到互联网，可以快捷方便的获取数据，在网上进行信息的交流或者完成网络的购物支付等，大大方便了人们的生活。

[0003] 然后，网络给人们带来方便的同时，也存在一些不安全的因此，比如 WIFI 钓鱼、DNS 劫持等欺诈手段是现在常见的两种网络欺骗手段，如图 1 所示，一个恶意的 WIFI 热点，通过设置简单的密码，或者干脆不设置密码，从而引起其它用户的接入，在用户通过该恶意的 WIFI 热点访问主机名时，虚假的 WIFI 站点通过自己搭建的 DNS 服务器，将本来请求的“主机名服务器 A”转移到“恶意的服务器 B”上，在用户输入相应的账号密码时，恶意服务器接收输入的账号密码，从而对用户的隐私信息进行窃取，也给用户的财产带来威胁。

发明内容

[0004] 本发明实施例的目的在于提供一种监控网络钓鱼的方法，以解决现有技术因错误解析，返回恶意的服务器的 IP 地址，造成对用户的账号密码窃取的问题，从而保证用户的隐私安全。

[0005] 本发明实施例是这样实现的，一种监控网络钓鱼的方法，所述方法包括：

[0006] 发送主机名的访问请求，接收由所述主机名解析得到的第一 IP 地址；

[0007] 根据所述主机名在预设的对应表查找所述主机名对应的第二 IP 地址，所述对应表存储有主机名与 IP 地址的对应关系；

[0008] 判断所述查找的所述第二 IP 地址与接收的第一 IP 地址是否相同；

[0009] 如果所述查找的所述第二 IP 地址与查找的第一 IP 地址不相同，则终止当前网络请求操作。

[0010] 另一方面，本发明提供了一种监控网络钓鱼的装置，所述装置包括：

[0011] 接收单元，用于发送主机名的访问请求，接收由所述主机名解析得到的第一 IP 地址；

[0012] 查找单元，用于根据所述主机名在预设的对应表查找所述主机名对应的第二 IP 地址，所述对应表存储有主机名与 IP 地址的对应关系；

[0013] 判断单元，用于判断所述查找的所述第二 IP 地址与接收的第一 IP 地址是否相同；

[0014] 终止单元，用于如果所述查找的所述第二 IP 地址与查找的第一 IP 地址不相同，则终止当前网络请求操作。

[0015] 本发明还提供了一种终端，包括上述的监控网络钓鱼的装置。

[0016] 在本发明实施例中，通过网络请求解析后得到的第一 IP 地址，在预设的主机名与

IP 地址对应表中查找所述主机名对应的第二 IP 地址，并判断所述第一 IP 地址与第二 IP 地址是否相同，如果不相同，则可能当前所解析的 IP 地址为恶意的服务器所对应的 IP 地址，为保证用户的财产安全和隐私保密，终止当前访问操作。从而能够有效的防止因网络钓鱼篡改主机名所对应的 IP 地址，造成用户访问恶意服务器造成的财产损失，更好的保证信息的安全性。

附图说明

[0017] 图 1 为现有技术中的网络钓鱼欺骗用户的流程示意图；

[0018] 图 2 是本发明第一实施例提供的监控网络钓鱼的方法的实现流程图；

[0019] 图 3 为本发明第一实施例提供的防止网络钓鱼的流程示意图；

[0020] 图 4 是本发明第二实施例提供的监控网络钓鱼的方法的实现流程图；

[0021] 图 5 是本发明第三实施例提供的监控网络钓鱼的方法的实现流程图；

[0022] 图 6 是本发明第四实施例提供的监控网络钓鱼的装置的结构示意图；

[0023] 图 7 为本发明第五实施例提供的终端的结构示意图。

具体实施方式

[0024] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0025] 本发明实施例可用于终端，可以为可通过无线保真(wireless fidelity,WiFi)连接到网络的移动终端，如智能手机、PAD、笔记本电脑等，也可以固定的设备，如台式计算机。

[0026] 针对目前越来越多的 WIFI 钓鱼欺骗，通过恶意的 WIFI 热点接入用户终端，当用户通过所述恶意的 WIFI 热点访问网络时，WIFI 热点通过自己搭建的 DNS 服务器，将本来请求访问的“服务器 A”，转移到“恶意服务器 B”，而恶意服务器可能会记录用户的账户密码信息，特别是网络支付的密码信息，给用户的财产带来威胁，同样也侵犯了用户隐私信息。

[0027] 当然，并不局限于无线网络连接的形式，对于有线连接的网络欺骗，同样可以适用于本发明所述的监控网络钓鱼的方法。

[0028] 本发明所述监控网络钓鱼的方法，包括：

[0029] 发送主机名的访问请求，接收由所述主机名解析得到的第一 IP 地址；

[0030] 根据所述主机名在预设的对应表查找所述主机名对应的第二 IP 地址，所述对应表存储有主机名与 IP 地址的对应关系；

[0031] 判断所述查找的所述第二 IP 地址与接收的第一 IP 地址是否相同；

[0032] 如果所述查找的所述第二 IP 地址与查找的第一 IP 地址不相同，则终止当前网络请求操作。

[0033] 通过网络请求解析后得到的第一 IP 地址，在预设的主机名与 IP 地址对应表中查找所述主机名对应的第二 IP 地址，并判断所述第一 IP 地址与第二 IP 地址是否相同，如果不相同，则可能当前所解析的 IP 地址为恶意的服务器所对应的 IP 地址，为保证用户的财产安全和隐私保密，终止当前访问操作。从而能够有效的防止因网络钓鱼篡改主机名所对应的 IP 地址，造成用户访问恶意服务器造成的财产损失，更好的保证信息的安全性。

[0034] 实施例一：

[0035] 图 2 示出了本发明第一实施例提供的监控网络钓鱼的方法的实现流程，详述如下：

[0036] 在步骤 S201 中，发送主机名的访问请求，接收由所述主机名解析得到的第一 IP 地址。

[0037] 具体的，所述指定的主机名的访问请求，可以为用户在浏览器中输入的访问主机名的 URL（中文全称为：统一资源定位符，英文全称为 Uniform ResourceLocator）的访问请求，也可以为通过其它应用或者点击快捷方式发送对主机名的访问请求，所述主机名包含于所述访问请求当中，如输入 https://mail.qq.com/cgi-bin/loginpage 的 URL 地址时，所包含的主机名为 qq.com，即服务器名称。

[0038] 在接收到用户的访问请求后，根据设定的 DNS（中文全称为：域名系统，英文全称为：Domain Name System）解析服务器解析得到所述域名对应的 IP 地址。

[0039] 此处所述的 DNS 服务器，在默认情况下，为域名服务商提供，其解析结果为主机名的域名所对应的真实的 IP 地址，但是，当解析域名的 DNS 域名服务器被修改，或者使用非法的 DNS 域名服务器进行解析时，所解析得到的 IP 地址就可能不是真实的 IP 地址，或者为虚假的 WIFI 热点相应的虚假的服务器，当用户通过虚假的 IP 地址访问恶意服务器时，当虚假服务器的页面与真实的主机名的页面较为相近的情况下，用户极有可能将账号密码信息发送至虚假的服务器，造成隐私信息公开或者财产不安全。

[0040] 在步骤 S202 中，根据所述主机名在预设的对应表查找所述主机名对应的第二 IP 地址，所述对应表存储有主机名与 IP 地址的对应关系。

[0041] 在步骤 S203 中，判断所述查找的所述第二 IP 地址与接收的第一 IP 地址是否相同。

[0042] 作为本发明与现有技术的主要区别点，在得到解析的 IP 地址后，在预设的一个主机名与 IP 地址对应表中查找所述主机名对应的 IP 地址，得到第二 IP 地址，然后将第二 IP 地址与第一 IP 地址进行比较，判断第一 IP 地址与第二 IP 地址是否相同。

[0043] 在步骤 S204 中，如果所述查找的所述第二 IP 地址与查找的第一 IP 地址不相同，则终止当前网络请求操作。

[0044] 当第一 IP 地址与第二 IP 地址不相符时，表示当前解析得到的第一 IP 地址可能为恶意的 IP 地址，为保护用户隐私和财产，终止当前对第一 IP 地址的网络请求操作，如图 3 所示，也可以根据查询得到的第二 IP 地址，继续访问正常的网页，并提醒用户，当前终端可能受到网络钓鱼的恶意行为。

[0045] 当第一 IP 地址与第二 IP 地址相同时，表示当前解析返回的第一 IP 地址为正常的 IP 地址，可以正常访问。

[0046] 本发明实施例通过网络请求解析后得到的第一 IP 地址，在预设的主机名与 IP 地址对应表中查找所述主机名对应的第二 IP 地址，并判断所述第一 IP 地址与第二 IP 地址是否相同，如果不相同，则可能当前所解析的 IP 地址为恶意的服务器所对应的 IP 地址，为保证用户的财产安全和隐私保密，终止当前访问操作。从而能够有效的防止因网络钓鱼篡改主机名所对应的 IP 地址，造成用户访问恶意服务器造成的财产损失，更好的保证信息的安全性。

[0047] 实施例二：

[0048] 图 4 示出了本发明第二实施例提供的监控网络钓鱼的方法的实现流程，本实施例中预设的主机名与 IP 地址对应表存于校验服务器，详述如下：

[0049] 在步骤 S401 中，发送主机名的访问请求，接收由所述主机名解析得到的第一 IP 地址。

[0050] 在步骤 S402 中，向校验服务器发送校验请求，所述校验请求包括所述主机名、第一 IP 地址。

[0051] 所述校验服务器，为专门针对网络钓鱼的诈骗手段所设置的服务器，其中包括各常用主机名的服务器 IP 地址和主机名的域名的对应关系，并且，对于大型的主机名，其可能会包括多个 IP 地址，因此，还可能包括同一个域名对应多个 IP 地址。

[0052] 在步骤 S403 中，接收由根据所述主机名，在校验服务器的主机名与 IP 地址对应表中，查找所述主机名对应的第二 IP 地址。

[0053] 在步骤 S404 中，判断所述查找的所述第二 IP 地址与接收的第一 IP 地址是否相同。

[0054] 在步骤 S405 中，如果所述查找的所述第二 IP 地址与查找的第一 IP 地址不相同，则终止当前网络请求操作。

[0055] 作为本发明实施例进一步优化的实施方式，为保证校验服务器是否为可靠的、真实的校验服务器，而并非恶意的校验服务器返回的非法 IP，因此，在步骤 S406 中，通过密钥验证所述校验服务器是否为指定的校验服务器。

[0056] 其中，通过密钥验证校验服务器是否为指定的校验服务器，可以将服务器的评书通过公钥加密，终端通过私钥解密后，方可得到证书内容，关判断评书内容的可靠性。由于采用匹配的公钥和私钥加密，可防止对证书的篡改，从而保证其安全性。

[0057] 或者，作为同样可以提高校验服务器安全性的一种方式，所述向校验服务器发送校验请求步骤和所述接收第二 IP 地址的步骤中，具体为通过虚拟专用网络 VPN（Virtual Private Network）向校验服务器发送请求和通过虚拟专用网络 VPN 接收第二 IP 地址。通过虚拟专用网络 VPN 对校验服务器传送的第二 IP 地址进行高可靠度的传送，从而保证校验的正确性。

[0058] 另外，为提高服务器数据的有效性及减少误操作，校验服务器需要定期更新域名服务器与 IP 地址的对应关系。

[0059] 进一步优化的，所述步骤 S402 中，所述校验请求还包括终端的唯一标识信息；所述方法还可包括：

[0060] 在步骤 S407 中，查询在所述校验服务器是否记录有所述终端的唯一标识对应的网络钓鱼记录。

[0061] 其中，对于移动终端，所述唯一标识为 IMEI（英文全称为 International Mobile Equipment Identity，中文全称为国际移动设备身份码），对于计算机终端，其唯一标识可以为 MAC（Media Access Control）地址。

[0062] 在步骤 S408 中，如果包括所述终端的唯一标识对应的网络钓鱼记录，则接收由所述校验发送的当前终端存在安全隐患的提示指令。

[0063] 通过记录可能处于危害中的终端，可以及时的提醒用户当前终端接入的网络不安

全，及时更改密码，方便用户尽早避免损失。

[0064] 本发明实施例与实施例一的不同之处在于，本发明实施例中具体主机名与 IP 地址的对应关系存储于服务器，通过服务器中查找其对应关系，从而完成对主机名的真实 IP 地址，即第二 IP 地址的查找工作。另外通过更新检验服务器中的数据，可以提高判断的准确性，减少误操作；通过记录用户终端的唯一标识，可以提醒用户及时更改密码，减少损失。

[0065] 而通过对校验服务器进行密钥验证的方式，可以保证校验的数据的安全性，而通过虚拟专用网络 VPN 对校验数据进行传输，同样可进一步提高数据的安全性，使其能够可靠的访问目标服务器。

[0066] 实施例三：

[0067] 图 5 示出了本发明第三实施例提供的监控网络钓鱼的方法的实现流程，本实施例中预设的主机名与 IP 地址对应表存于终端，详述如下：

[0068] 在步骤 S501 中，发送主机名的访问请求，接收由所述主机名解析得到的第一 IP 地址。

[0069] 在步骤 S502 中，根据所述主机名，在所述本地的数据库中查找所述主机名对应的第二 IP 地址。

[0070] 在步骤 S503 中，判断所述查找的所述第二 IP 地址与接收的第一 IP 地址是否相同。

[0071] 在步骤 S504 中，如果所述查找的所述第二 IP 地址与查找的第一 IP 地址不相同，则终止当前网络请求操作。

[0072] 作为本发明实施例的进一步优化方式，还包括步骤 S505，接收并更新校验服务器发送的主机名与 IP 地址对应表的更新数据，所述校验服务器包括更新的主机名与 IP 地址的对应数据。

[0073] 另外，作为另一种可选实施的方式，在接收到用户输入的指定主机名的访问请求后，通过查找所述主机名对应的第二 IP 地址，由返回的 IP 地址直接访问服务器读写数据。同样，这种实施方式也适用于实施例二，不同之处在于，返回的第二 IP 地址为从校验服务器处读取。同样通过查询的 IP 地址直接访问网页，可以避免访问到恶意的服务器。

[0074] 本发明实施例与实施例二的不同之处在于，通过将对应关系的数据存储在终端本地，更好的保证终端的访问安全。另外，通过校验服务器更新终端中的对应关系，更好的提高其准确性。

[0075] 实施例四：

[0076] 图 6 为本发明第四实施例提供的监控网络钓鱼的装置的结构示意图，详述如下：

[0077] 本发明实施例所述监控网络钓鱼的装置，包括：

[0078] 接收单元 601，用于发送主机名的访问请求，接收由所述主机名解析得到的第一 IP 地址；

[0079] 查找单元 602，用于根据所述主机名在预设的对应表查找所述主机名对应的第二 IP 地址，所述对应表存储有主机名与 IP 地址的对应关系；

[0080] 判断单元 603，用于判断所述查找的所述第二 IP 地址与接收的第一 IP 地址是否相同；

[0081] 终止单元 604，用于如果所述查找的所述第二 IP 地址与查找的第一 IP 地址不相

同，则终止当前网络请求操作。

[0082] 进一步的，所述预设的主机名与 IP 地址对应表存于校验服务器，所述查找单元 602 包括：

[0083] 校验请求发送子单元 6021，用于向校验服务器发送校验请求，所述校验请求包括所述主机名、第一 IP 地址；

[0084] 查找子单元 6022，用于接收由校验服务器根据所述主机名，在主机名与 IP 地址对应表中，查找所述主机名对应的第二 IP 地址。

[0085] 为提高数据信息的更新的安全性，所述装置还包括：

[0086] 验证单元 605，用于通过密钥验证所述校验服务器是否为指定的校验服务器。

[0087] 可选的，所述校验请求发送子单元和查找子单元用于通过虚拟专用网络 VPN 向校验服务器发送请求和通过虚拟专用网络 VPN 接收第二 IP 地址。

[0088] 更进一步的，所述校验请求发送子单元 6021 中，所述校验请求还包括终端的唯一标识信息；

[0089] 所述装置还包括：

[0090] 查询单元 606，用于查询在所述校验服务器是否记录有所述终端的唯一标识对应的网络钓鱼记录；

[0091] 指令发送单元 607，用于如果包括所述终端的唯一标识对应的网络钓鱼记录，则接收由所述校验发送的当前终端存在安全隐患的提示指令。

[0092] 可选的，所述预设的主机名与 IP 地址对应表存于本地的数据库，所述查找单元 602 用于根据所述主机名，在所述本地的数据库中查找所述主机名对应的第二 IP 地址。

[0093] 本发明实施例所述装置与实施例一到实施例三中所述方法相对应，在此不作重复赘述。

[0094] 实施例五：

[0095] 图 7 为本发明第五实施例提供的终端的结构框图，本实施例所述终端，包括：存储器 720、输入单元 730、显示单元 740、音频电路 760、网络模块 770、处理器 780、以及电源 790 等部件。本领域技术人员可以理解，图 7 中示出的终端结构并不构成对终端的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

[0096] 下面结合图 7 对终端的各个构成部件进行具体的介绍：

[0097] 存储器 720 可用于存储软件程序以及模块，处理器 780 通过运行存储在存储器 720 的软件程序以及模块，从而执行终端的各种功能应用以及数据处理。存储器 720 可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序（比如声音播放功能、图像播放功能等）等；存储数据区可存储根据终端的使用所创建的数据（比如音频数据、电话本等）等。此外，存储器 720 可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。

[0098] 输入单元 730 可用于接收输入的数字或字符信息，以及产生与终端的用户设置以及功能控制有关的键信号输入。具体地，输入单元 730 可包括触控面板 731 以及其他输入设备 732。触控面板 731，也称为触摸屏，可收集用户在其上或附近的触摸操作（比如用户使用手指、触笔等任何适合的物体或附件在触控面板 731 上或在触控面板 731 附近的操作），

并根据预先设定的程式驱动相应的连接装置。可选的，触控面板 731 可包括触摸检测装置和触摸控制器两个部分。其中，触摸检测装置检测用户的触摸方位，并检测触摸操作带来的信号，将信号传送给触摸控制器；触摸控制器从触摸检测装置上接收触摸信息，并将它转换成触点坐标，再送给处理器 780，并能接收处理器 780 发来的命令并加以执行。此外，可以采用电阻式、电容式、红外线以及表面声波等多种类型实现触控面板 731。除了触控面板 731，输入单元 730 还可以包括其他输入设备 732。具体地，其他输入设备 732 可以包括但不限于物理键盘、功能键（比如音量控制按键、开关按键等）、轨迹球、鼠标、操作杆等中的一种或多种。

[0099] 显示单元 740 可用于显示由用户输入的信息或提供给用户的信息以及终端的各种菜单。显示单元 740 可包括显示面板 741，可选的，可以采用液晶显示器（Liquid Crystal Display，LCD）、有机发光二极管（Organic Light-Emitting Diode，OLED）等形式来配置显示面板 741。进一步的，触控面板 731 可覆盖显示面板 741，当触控面板 731 检测到在其上或附近的触摸操作后，传送给处理器 780 以确定触摸事件的类型，随后处理器 780 根据触摸事件的类型在显示面板 741 上提供相应的视觉输出。虽然在图 7 中，触控面板 731 与显示面板 741 是作为两个独立的部件来实现终端的输入和输入功能，但是在某些实施例中，可以将触控面板 731 与显示面板 741 集成而实现终端的输入和输出功能。

[0100] 音频电路 760、扬声器 761，传声器 762 可提供用户与终端之间的音频接口。音频电路 760 可将接收到的音频数据转换后的电信号，传输到扬声器 761，由扬声器 761 转换为声音信号输出；另一方面，传声器 762 将收集的声音信号转换为电信号，由音频电路 760 接收后转换为音频数据，再将音频数据输出处理器 780 处理后，经网络模块 710 以发送给比如另一终端，或者将音频数据输出至存储器 720 以便进一步处理。

[0101] 网络模块 770 可以包括无线保真（wireless fidelity，WiFi）模块，有线网络模块或者射频模块，其中无线保真模块属于短距离无线传输技术，终端通过网络模块 770 可以帮助用户收发电子邮件、浏览网页和访问流式媒体等，它为用户提供了无线的宽带互联网访问。虽然图 7 示出了网络模块 770，但是可以理解的是，其并不属于终端的必须构成，完全可以根据需要在不改变发明的本质的范围内而省略。

[0102] 处理器 780 是终端的控制中心，利用各种接口和线路连接整个终端的各个部分，通过运行或执行存储在存储器 720 内的软件程序和 / 或模块，以及调用存储在存储器 720 内的数据，执行终端的各种功能和处理数据，从而对终端进行整体监控。可选的，处理器 780 可包括一个或多个处理单元；优选的，处理器 780 可集成应用处理器和调制解调处理器，其中，应用处理器主要处理操作系统、用户界面和应用程序等，调制解调处理器主要处理无线通信。可以理解的是，上述调制解调处理器也可以不集成到处理器 780 中。

[0103] 终端还包括给各个部件供电的电源 790（比如电池），优选的，电源可以通过电源管理系统与处理器 780 逻辑相连，从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。

[0104] 尽管未示出，终端还可以包括摄像头、蓝牙模块等，在此不再赘述。

[0105] 在本发明实施例中，该终端所包括的处理器 780 还具有以下功能：执行监控网络钓鱼的方法，包括：

[0106] 发送主机名的访问请求，接收由所述主机名解析得到的第一 IP 地址；

[0107] 根据所述主机名在预设的对应表查找所述主机名对应的第二 IP 地址，所述对应表存储有主机名与 IP 地址的对应关系；

[0108] 判断所述查找的所述第二 IP 地址与接收的第一 IP 地址是否相同；

[0109] 如果所述查找的所述第二 IP 地址与查找的第一 IP 地址不相同，则终止当前网络请求操作。

[0110] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

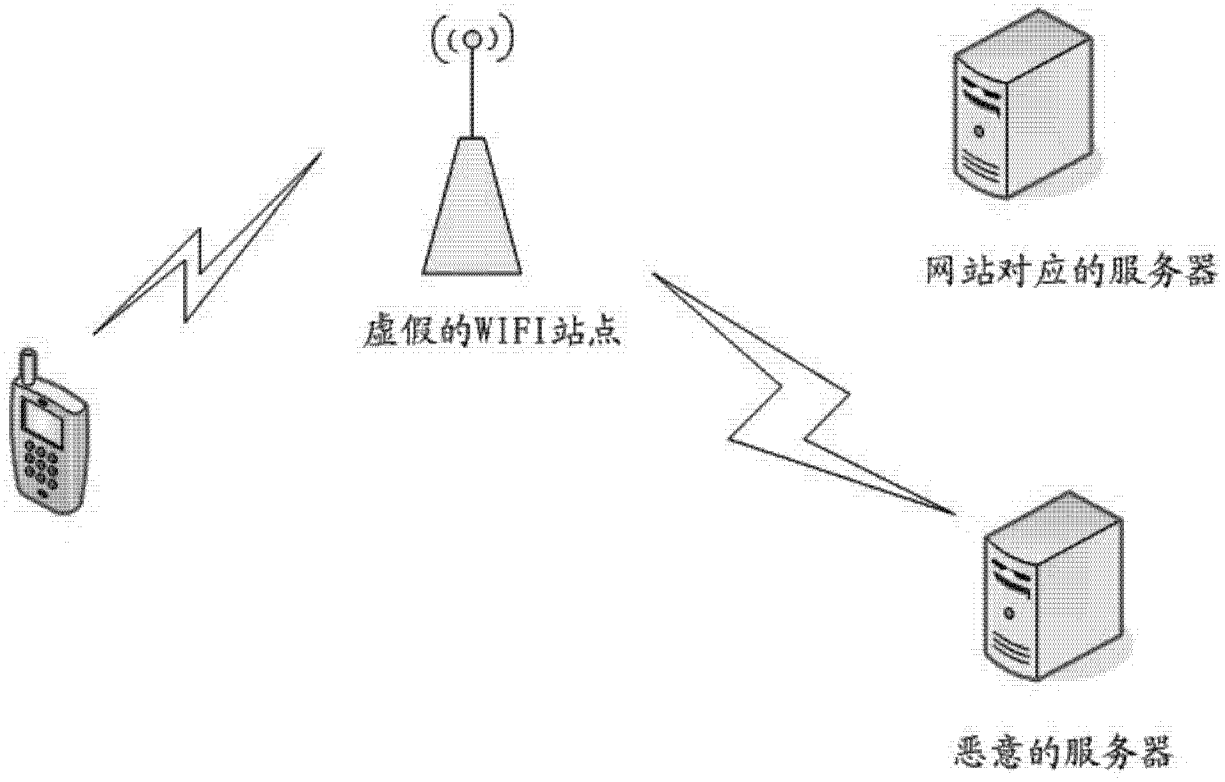

虚假的WIFI站点
网站对应的服务器
恶意的服务器

图 1

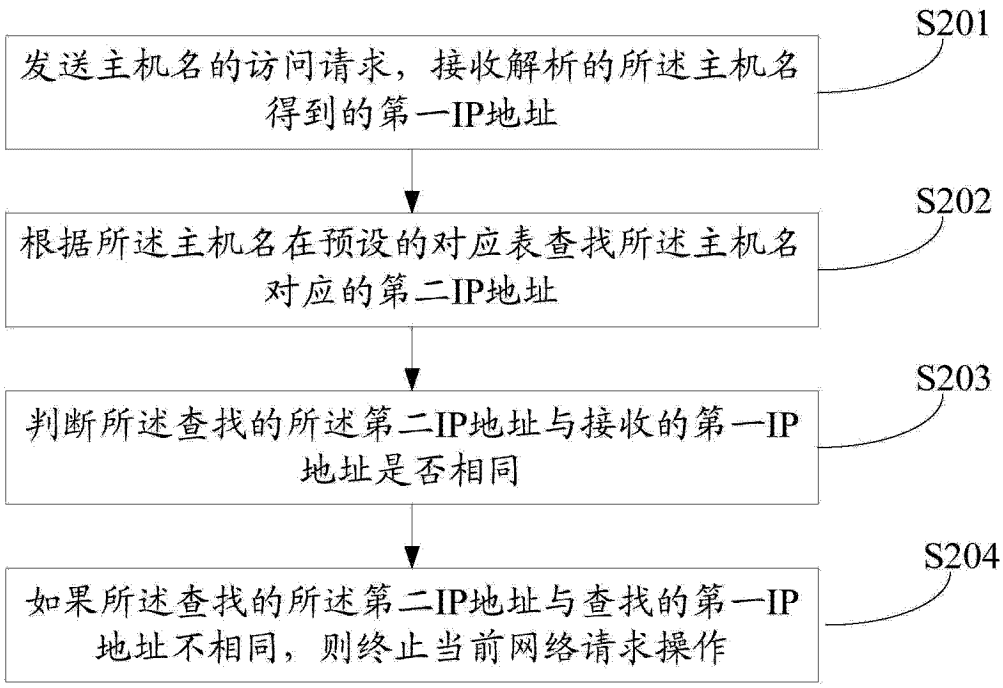

S201
发送主机名的访问请求，接收解析的所述主机名得到的第一IP地址
S202
根据所述主机名在预设的对应表查找所述主机名对应的第二IP地址
S203
判断所述查找的所述第二IP地址与接收的第一IP地址是否相同
S204
如果所述查找的所述第二IP地址与查找的第一IP地址不相同，则终止当前网络请求操作

图 2

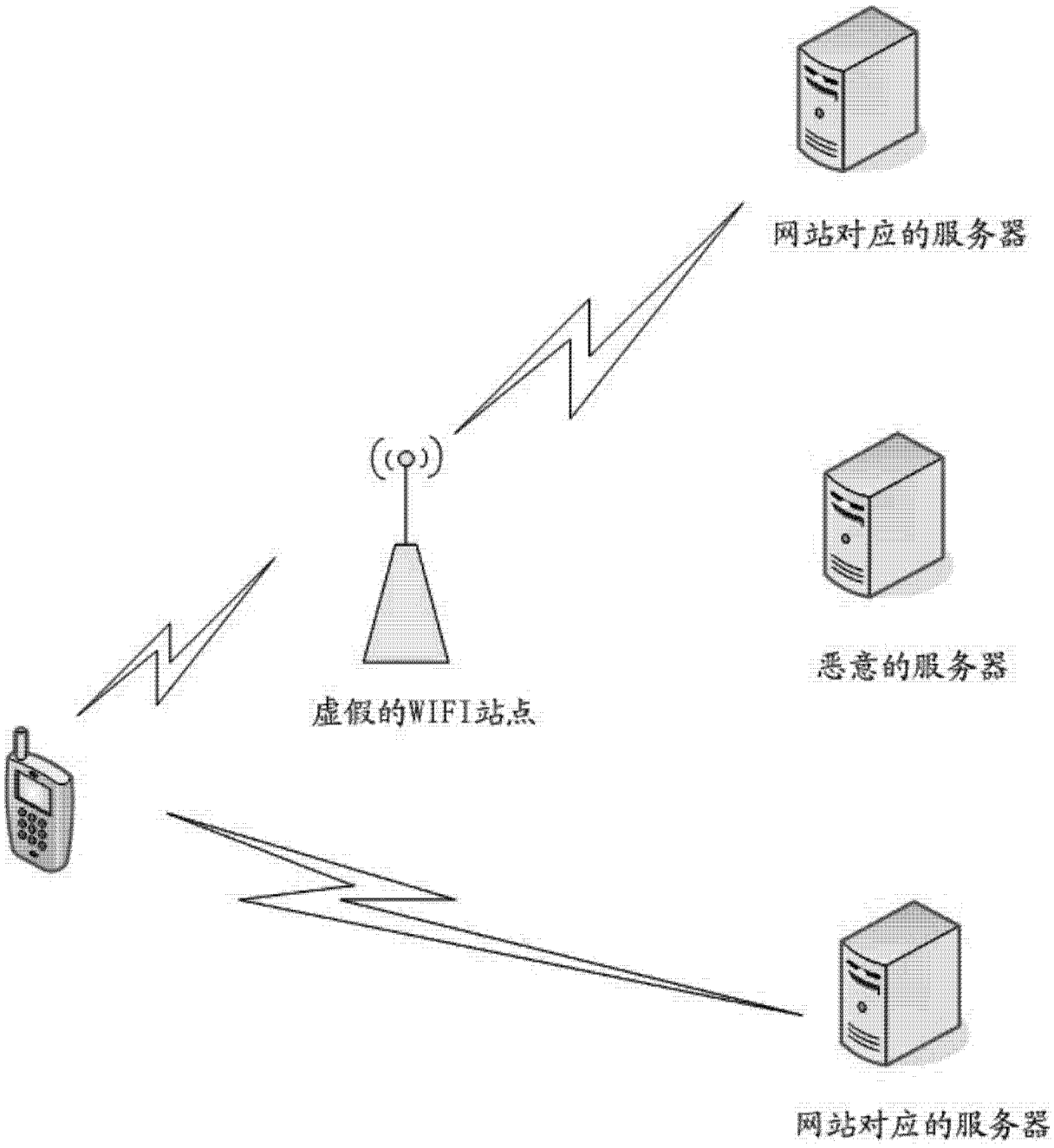


图 3

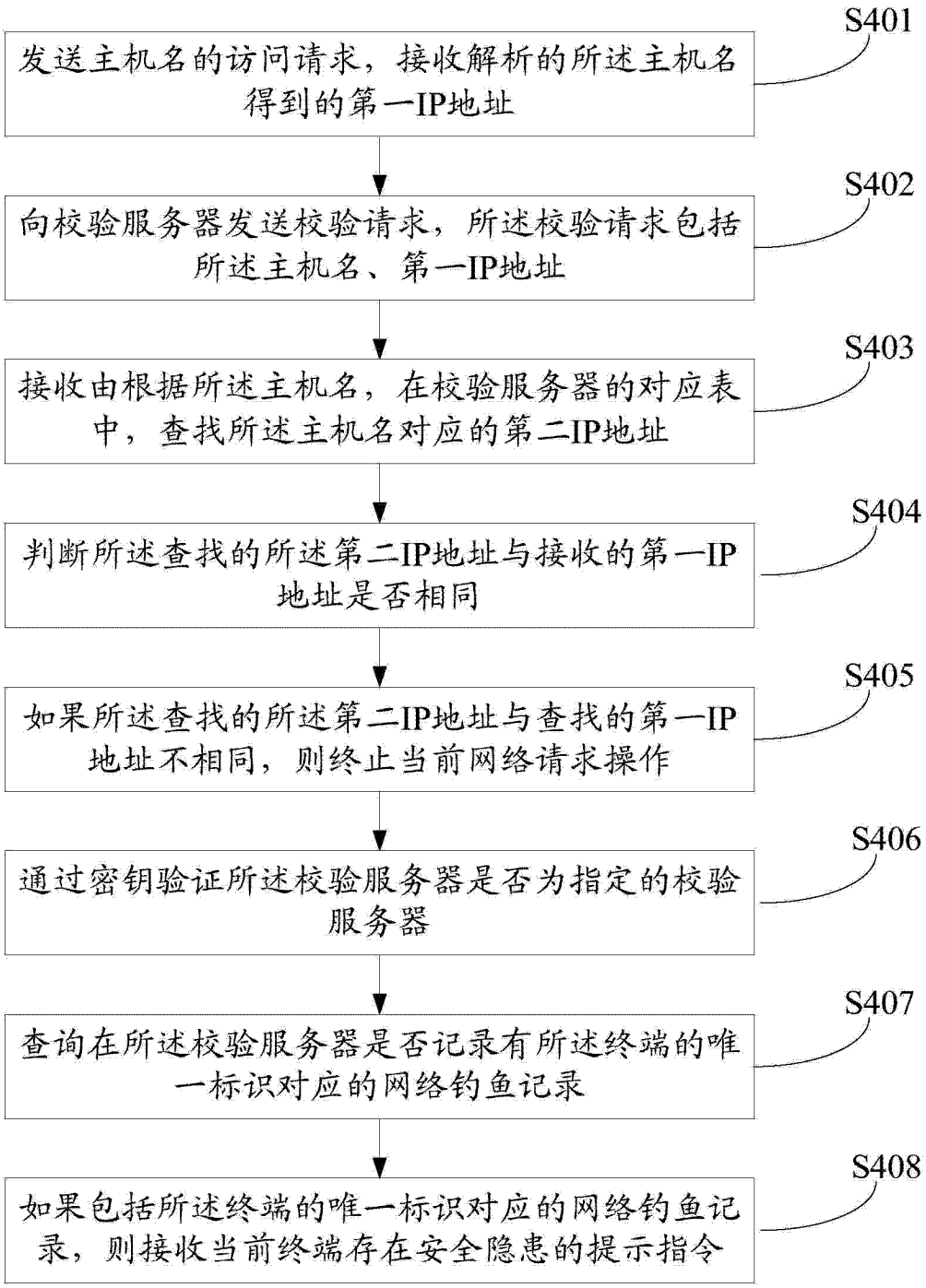

S401
发送主机名的访问请求，接收解析的所述主机名得到的第一IP地址
S402
向校验服务器发送校验请求，所述校验请求包括所述主机名、第一IP地址
S403
接收由根据所述主机名，在校验服务器的对应表中，查找所述主机名对应的第二IP地址
S404
判断所述查找的所述第二IP地址与接收的第一IP地址是否相同
S405
如果所述查找的所述第二IP地址与查找的第一IP地址不相同，则终止当前网络请求操作
S406
通过密钥验证所述校验服务器是否为指定的校验服务器
S407
查询在所述校验服务器是否记录有所述终端的唯一标识对应的网络钓鱼记录
S408
如果包括所述终端的唯一标识对应的网络钓鱼记录，则接收当前终端存在安全隐患的提示指令

图 4

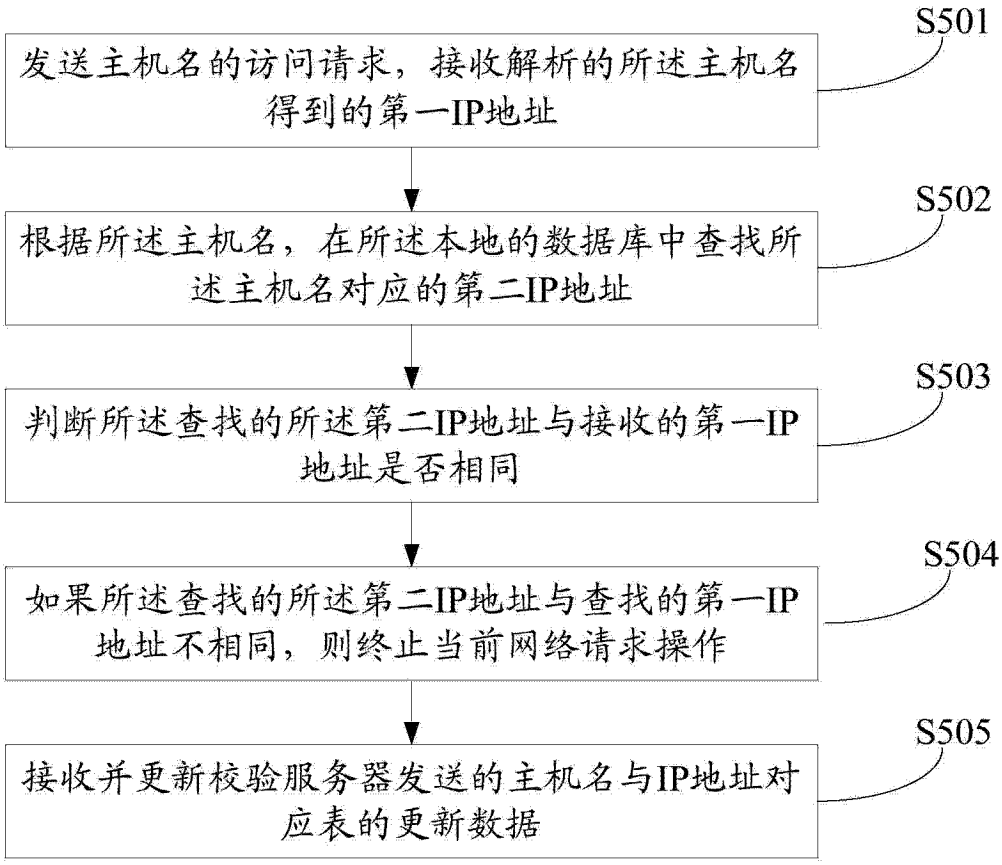

S501
发送主机名的访问请求，接收解析的所述主机名得到的第一IP地址
S502
根据所述主机名，在所述本地的数据库中查找所述主机名对应的第二IP地址
S503
判断所述查找的所述第二IP地址与接收的第一IP地址是否相同
S504
如果所述查找的所述第二IP地址与查找的第一IP地址不相同，则终止当前网络请求操作
S505
接收并更新校验服务器发送的主机名与IP地址对应表的更新数据

图 5

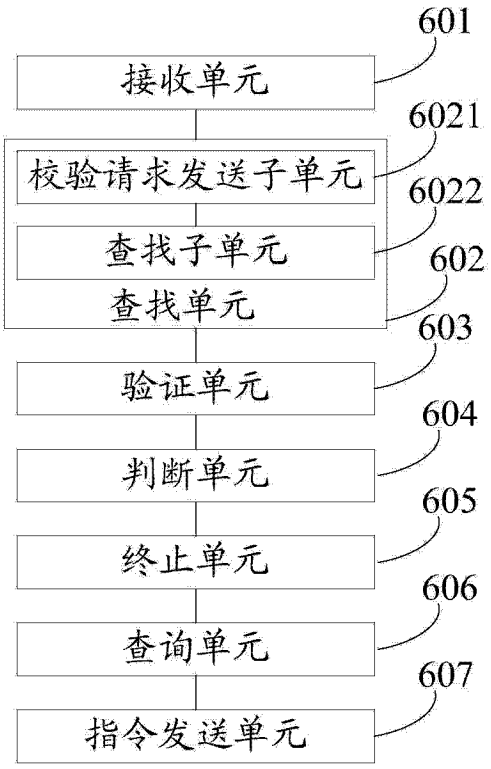

601
接收单元
6021
校验请求发送子单元
6022
查找子单元
602
查找单元
603
验证单元
604
判断单元
605
终止单元
606
查询单元
607
指令发送单元

图 6

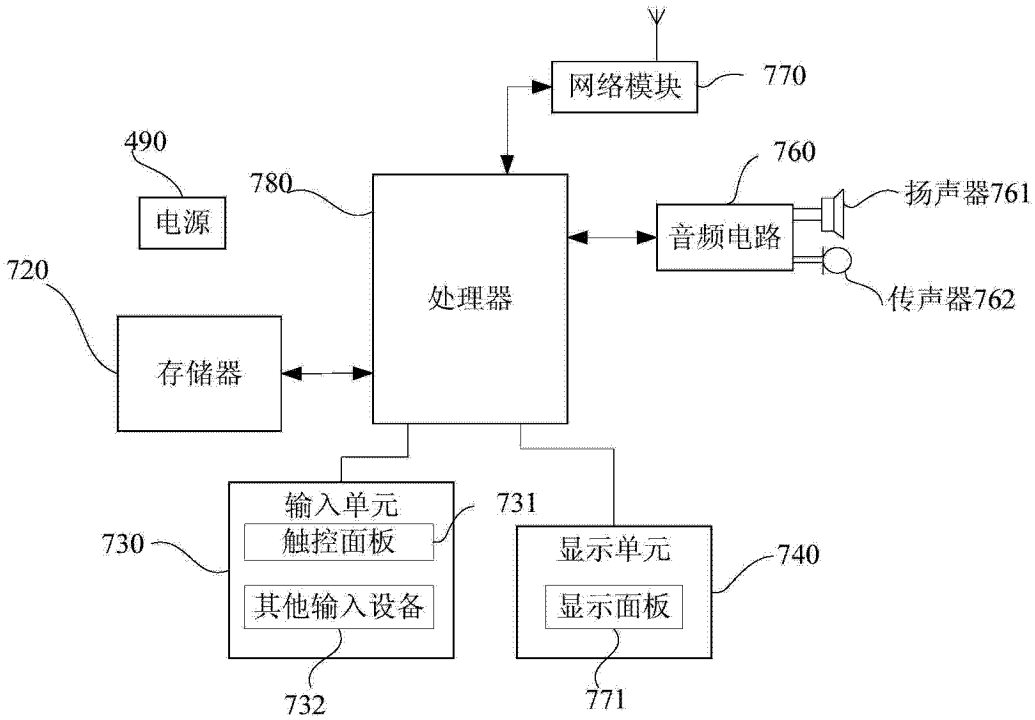

网络模块
770
490
电源
780
处理器
760
音频电路
扬声器761
传声器762
720
存储器
输入单元
731
730
触控面板
其他输入设备
732
显示单元
740
显示面板
771

图 7