(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 112887255 A
(43)申请公布日 2021.06.01

(21)申请号 201911200174.1

(22)申请日 2019.11.29

(71)申请人 北京一起教育信息咨询有限责任公司
地址 100102 北京市朝阳区望京东园四区7号楼13层1303室

(72)发明人 万明

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 王娇娇

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

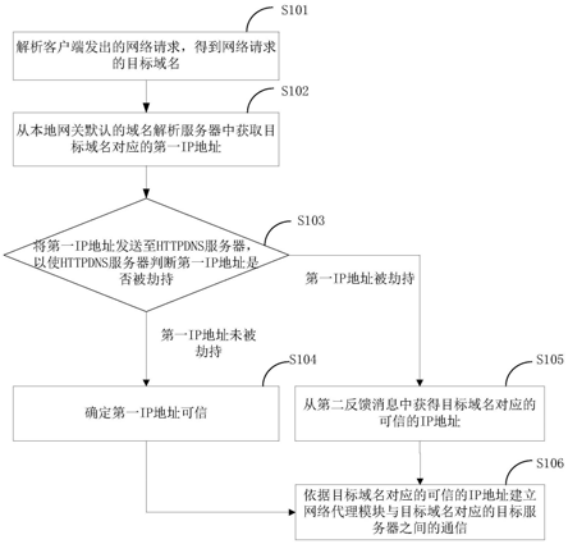
权利要求书2页 说明书10页 附图6页

(54)发明名称

一种网络通信方法及装置

(57)摘要

本发明公开了一种网络通信方法及装置，应用于网络代理模块，网络代理模块集成于客户端中，解析客户端发出的网络请求得到目标域名，从本地网关默认的域名解析服务器中获取目标域名对应的第一IP地址，并发送给HTTPDNS服务器判断第一IP地址是否被劫持，若未被劫持，确定该IP地址可信；若被劫持，由HTTPDNS服务器返回可信的IP地址，依据可信的IP地址建立网络代理模块与目标域名对应的目标服务器之间的安全通信，实现客户端与目标服务器的安全通信，该方案在客户端中的网络代理模块中运行，因此无需将网络请求发送至远端网络侧的代理服务器，从而节省了从客户端至网络侧服务端之间的传输时间，进而加快了网络请求的响应速度。




CN 112887255 A

1.一种网络通信方法,其特征在于,应用于网络代理模块,该网络代理模块集成于客户端中,所述方法包括:

解析所述客户端发出的网络请求,得到所述网络请求的目标域名;

从本地网关默认的域名解析服务器中获取所述目标域名对应的第一IP地址;

将所述第一IP地址发送至HTTPDNS服务器,以使所述HTTPDNS服务器判断所述第一IP地址是否被劫持;

当接收到所述HTTPDNS服务器返回的所述第一IP地址安全的第一反馈消息后,确定所述第一IP地址可信;

当接收到所述HTTPDNS服务器返回的所述第一IP地址被劫持的第二反馈消息后,从所述第二反馈消息中获得所述目标域名对应的可信的IP地址;

依据所述目标域名对应的可信的IP地址建立所述网络代理模块与所述目标域名对应的目标服务器之间的通信。

2.根据权利要求1所述的方法,其特征在于,所述方法还包括:

将所述目标域名及该目标域名对应的可信IP地址存储至所述网络代理模块的本地存储空间中。

3.根据权利要求1所述的方法,其特征在于,在所述从本地网关默认的域名解析服务器中获取所述目标域名对应的第一IP地址之前,所述方法还包括:

从所述网络代理模块的本地存储空间存储的域名及对应的IP地址中查找是否存在所述目标域名对应的IP地址;

若所述本地存储空间中存在所述目标域名对应的IP地址,则确定该IP地址可信;

若所述本地存储空间中不存在所述目标域名对应的IP地址,则执行所述从本地网关默认的域名解析服务器中获取所述目标域名对应的第一IP地址。

4.根据权利要求1所述的方法,其特征在于,依据所述目标域名对应的可信的IP地址建立所述网络代理模块与所述目标域名对应的目标服务器之间的通信,包括:

接收所述客户端发送的所述网络请求,并将所述网络请求以隧道模式发送至所述目标服务器;

以隧道模式接收所述目标服务器返回的响应消息,并将所述响应消息发送至所述客户端。

5.根据权利要求1至4任一项所述的方法,其特征在于,所述依据所述目标域名对应的可信的IP地址建立所述网络代理模块与所述目标域名对应的目标服务器之间的通信,包括:

检测通过所述目标域名对应的可信的IP地址与所述目标服务器是否连接成功;

若通过所述目标域名对应的可信的IP地址与所述目标服务器连接成功,通过该连接实现所述网络代理模块与所述目标域名对应的目标服务器之间的数据交互;

若通过所述目标域名对应的可信的IP地址与所述目标服务器连接失败,继续通过所述目标域名对应的可信的IP地址重新与所述目标服务器连接,当重新连接失败的次数达到预设次数时,生成连接失败消息。

6.根据权利要求1所述的方法,其特征在于,所述方法还包括:

当请求所述HTTPDNS服务器失败后,从可信的域名解析服务器中获取所述目标域名对

应的可信的IP地址。

7.一种网络通信装置,其特征在于,应用于网络代理模块,该网络代理模块集成于客户端中,所述装置包括:

解析单元,用于解析所述客户端发出的网络请求,得到所述网络请求的目标域名;

第一获取单元,用于从本地网关默认的域名解析服务器中获取所述目标域名对应的第一IP地址;

发送单元,用于将所述第一IP地址发送至HTTPDNS服务器,以使所述HTTPDNS服务器判断所述第一IP地址是否被劫持;

第一确定单元,用于当接收到所述HTTPDNS服务器返回的所述第一IP地址安全的第一反馈消息后,确定所述第一IP地址可信;

第二获取单元,用于当接收到所述HTTPDNS服务器返回的所述第一IP地址被劫持的第二反馈消息后,从所述第二反馈消息中获得所述目标域名对应的可信的IP地址;

通信连接建立单元,用于依据所述目标域名对应的可信的IP地址建立所述网络代理模块与所述目标域名对应的目标服务器之间的通信。

8.根据权利要求7所述的装置,其特征在于,还包括:查找单元和第二确定单元;

所述查找单元,用于从所述网络代理模块的本地存储空间存储的域名及对应的IP地址中查找是否存在目标域名对应的IP地址;若本地存储空间中不存在目标域名对应的IP地址,则触发所述第一获取单元执行从本地网关默认的域名解析服务器中获取目标域名对应的第一IP地址;

所述第二确定单元,用于当本地存储空间中存在目标域名对应的IP地址时,确定该IP地址可信。

9.一种存储介质,其特征在于,所述存储介质存储有程序,其中,在所述程序运行时控制所述存储介质所在设备执行如权利要求1-6任一项所述的网络通信方法。

10.一种计算机设备,其特征在于,包括处理器和存储器;

所述存储器内存储有程序;

所述处理器用于调用所述存储器内存储的程序以执行如权利要求1-6任一项所述的网络通信方法。

# 一种网络通信方法及装置

## 技术领域

[0001] 本发明涉及网络通讯技术领域,更具体地说,涉及一种网络通信方法及装置。

## 背景技术

[0002] 域名系统(Domain Name System,DNS),因特网上作为域名和网际互连协议(Internet Protocol,IP)地址相互映射的一个分布式数据库,使用户更方便的访问互联网。

[0003] 目前,中国存在很多通信网络服务运营商,这些通信网络服务运营商的技术实力参差不齐,从而产生了网络安全问题。如果用户接入不安全网络,则在这些用户使用客户端程序发送网络请求时,可能发生DNS被劫持或请求内容被劫持篡改等问题,若发生这些问题,导致影响用户正常使用客户端程序,甚至会把一些不安全的诈骗信息展示给用户,从而造成严重的后果。

## 发明内容

[0004] 有鉴于此,本发明提供了一种网络通信方法及装置,提出了一种跨操作系统的解决DNS劫持问题的方法,实现客户端与目标服务器的安全通信。其公开的技术方案如下:

[0005] 第一方面,本发明公开了一种网络通信方法,应用于网络代理模块,该网络代理模块集成于客户端中,所述方法包括:

[0006] 解析所述客户端发出的网络请求,得到所述网络请求的目标域名;

[0007] 从本地网关默认的域名解析服务器中获取所述目标域名对应的第一IP地址;

[0008] 将所述第一IP地址发送至HTTPDNS服务器,以使所述HTTPDNS服务器判断所述第一IP地址是否被劫持;

[0009] 当接收到所述HTTPDNS服务器返回的所述第一IP地址安全的第一反馈消息后,确定所述第一IP地址可信;

[0010] 当接收到所述HTTPDNS服务器返回的所述第一IP地址被劫持的第二反馈消息后,从所述第二反馈消息中获得所述目标域名对应的可信的IP地址;

[0011] 依据所述目标域名对应的可信的IP地址建立所述网络代理模块与所述目标域名对应的目标服务器之间的通信。

[0012] 可选地,所述方法还包括:

[0013] 将所述目标域名及该目标域名对应的可信IP地址存储至所述网络代理模块的本地存储空间中。

[0014] 可选地,在所述从本地网关默认的域名解析服务器中获取所述目标域名对应的第一IP地址之前,所述方法还包括:

[0015] 从所述网络代理模块的本地存储空间存储的域名及对应的IP地址中查找是否存在所述目标域名对应的IP地址;

[0016] 若所述本地存储空间中存在所述目标域名对应的IP地址,则确定该IP地址可信;

[0017] 若所述本地存储空间中不存在所述目标域名对应的IP地址，则执行所述从本地网关默认的域名解析服务器中获取所述目标域名对应的第一IP地址。

[0018] 可选地，依据所述目标域名对应的可信的IP地址建立所述网络代理模块与所述目标域名对应的目标服务器之间的通信，包括：

[0019] 接收所述客户端发送的所述网络请求，并将所述网络请求以隧道模式发送至所述目标服务器；

[0020] 以隧道模式接收所述目标服务器返回的响应消息，并将所述响应消息发送至所述客户端。

[0021] 可选地，所述依据所述目标域名对应的可信的IP地址建立所述网络代理模块与所述目标域名对应的目标服务器之间的通信，包括：

[0022] 检测通过所述目标域名对应的可信的IP地址与所述目标服务器是否连接成功；

[0023] 若通过所述目标域名对应的可信的IP地址与所述目标服务器连接成功，通过该连接实现所述网络代理模块与所述目标域名对应的目标服务器之间的数据交互；

[0024] 若通过所述目标域名对应的可信的IP地址与所述目标服务器连接失败，继续通过所述目标域名对应的可信的IP地址重新与所述目标服务器连接，当重新连接失败的次数达到预设次数时，生成连接失败消息。

[0025] 可选地，所述方法还包括：

[0026] 当请求所述HTTPDNS服务器失败后，从可信的域名解析服务器中获取所述目标域名对应的可信的IP地址。

[0027] 第二方面，本发明公开了一种网络通信装置，应用于网络代理模块，该网络代理模块集成于客户端中，所述装置包括：

[0028] 解析单元，用于解析所述客户端发出的网络请求，得到所述网络请求的目标域名；

[0029] 第一获取单元，用于从本地网关默认的域名解析服务器中获取所述目标域名对应的第一IP地址；

[0030] 发送单元，用于将所述第一IP地址发送至HTTPDNS服务器，以使所述HTTPDNS服务器判断所述第一IP地址是否被劫持；

[0031] 第一确定单元，用于当接收到所述HTTPDNS服务器返回的所述第一IP地址安全的第一反馈消息后，确定所述第一IP地址可信；

[0032] 第二获取单元，用于当接收到所述HTTPDNS服务器返回的所述第一IP地址被劫持的第二反馈消息后，从所述第二反馈消息中获得所述目标域名对应的可信的IP地址；

[0033] 通信连接建立单元，用于依据所述目标域名对应的可信的IP地址建立所述网络代理模块与所述目标域名对应的目标服务器之间的通信。

[0034] 可选地，还包括：查找单元和第二确定单元；

[0035] 所述查找单元，用于从所述网络代理模块的本地存储空间存储的域名及对应的IP地址中查找是否存在目标域名对应的IP地址；若本地存储空间中不存在目标域名对应的IP地址，则触发所述第一获取单元执行从本地网关默认的域名解析服务器中获取目标域名对应的第一IP地址；

[0036] 所述第二确定单元，用于当本地存储空间中存在目标域名对应的IP地址时，确定该IP地址可信。

[0037] 第三方面，本发明公开了一种存储介质，所述存储介质存储有程序，其中，在所述程序运行时控制所述存储介质所在设备执行如第一方面任一种可能的实现方式公开的所述的网络通信方法。

[0038] 第四方面，本发明公开了一种计算机设备，包括处理器和存储器；

[0039] 所述存储器内存储有程序；

[0040] 所述处理器用于调用所述存储器内存储的程序以执行如第一方面任一种可能的实现方式公开的网络通信方法。

[0041] 经由上述技术方案可知，本发明公开了一种网络通信方法及装置，应用于网络代理模块，网络代理模块集成于客户端中，解析客户端发出的网络请求得到目标域名，从本地网关默认的域名解析服务器中获取目标域名对应的第一IP地址，并发送给HTTPDNS服务器判断第一IP地址是否被劫持，若未被劫持，确定该IP地址可信；若被劫持，由HTTPDNS服务器返回可信的IP地址，依据可信的IP地址建立网络代理模块与目标域名对应的目标服务器之间的安全通信，实现客户端与目标服务器的安全通信，该方案在客户端中的网络代理模块中运行，因此无需将网络请求发送至远端网络侧的代理服务器，从而节省了从客户端至网络侧服务端之间的传输时间，进而加快了网络请求的响应速度。

## 附图说明

[0042] 为了更清楚地说明本发明实施例或现有技术中的技术方案，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的前提下，还可以根据提供的附图获得其他的附图。

[0043] 图1为本发明实施例公开的一种网络通信方法的流程示意图；

[0044] 图2为本发明实施例公开的另一种网络通信方法的流程示意图；

[0045] 图3为本发明实施例公开的一种网络通信装置的结构示意图；

[0046] 图4为本发明实施例公开的另一种网络通信装置的结构示意图；

[0047] 图5为本发明实施例公开的另一种网络通信装置的结构示意图；

[0048] 图6为本发明实施例公开的另一种网络通信装置的结构示意图。

## 具体实施方式

[0049] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0050] 中国存在很多通信网络服务运营商，这些通信网络服务运营商的技术实力参差不齐，从而产生了网络安全问题。如果用户接入不安全网络，则在这些用户使用客户端程序发送网络请求时，可能发生DNS被劫持或请求内容被劫持篡改等问题，若发生这些问题，导致影响用户正常使用客户端程序，甚至会把一些不安全的诈骗信息展示给用户，从而造成严重的后果。

[0051] 为了解决该问题，本发明公开了一种网络通信方法及装置，提供目标域名对应的

可信的IP地址，并建立网络代理模块与可信的IP地址对应的目标服务器之间的通信，该方案作为网络代理模块运行在客户端内，因此不需要将网络请求发送至远端网络侧的代理服务器，从而节省了从客户端至远端网络侧服务端之间的传输时间；并且提供目标域名对应的可信的IP地址，建立网络代理模块与目标域名对应的目标服务器之间的安全通信，实现客户端与目标服务器进行安全通信。

[0052] 如图1所示，为本发明实施例公开的一种网络通信方法的流程示意图，该方法作为网络代理模块运行在客户端中，在客户端程序的一个常驻线程中，网络代理模块作为一个轻量级的线程运行。客户端启动网络代理模块，客户端把自身所有的网络请求转发到该网络代理模块，网络代理模块利用以下流程就可以防止DNS劫持和内容劫持的发生。

[0053] 如图1所示，该方法可以包括如下步骤：

[0054] S101：解析客户端发出的网络请求，得到网络请求的目标域名。

[0055] 在本发明的一个实施例中，网络代理模块监听客户端发出的网络请求，根据代理协议的格式要求，客户端向网络代理模块发送数据包，网络代理模块收到数据包后按照代理协议对该网络请求进行解析，得到目标域名。

[0056] 客户端通过网络代理模块与目标服务器进行间接的通信，网络代理模块与服务器连接时选用的协议在客户端启动网络代理模块时作为配置参数传给网络代理模块。

[0057] 需要说明的是，超文本传输协议(Hyper Text Transfer Protocol，HTTP)代理协议是一个基于HTTP协议的通用的代理协议。根据代理实现方式的不同，还有其他种类的代理协议，本发明优选采用HTTP代理协议。

[0058] 与网络侧的网络代理服务器相比，网络代理模块运行在客户端侧，客户端与网络代理模块之间的数据交互不需要经过外部的公共网络来传输，大大缩短网络代理模块与客户端之间的数据交互消耗的时间，从而提高了网络请求的响应速度。

[0059] S102：从本地网关默认的域名解析服务器中获取目标域名对应的第一IP地址。

[0060] 首先获取本地网关默认的域名解析服务器的列表，然后利用域名解析服务器的列表中的域名解析服务器，通过请求域名解析服务器对目标域名进行地址解析，得到目标域名对应的IP地址，称为第一IP地址。

[0061] 需要说明的是，本地网关是指本地网络运营商提供的网关设备。网络代理模块与默认的域名解析服务器之间基于用户数据报协议(User Datagram Protocol，UDP)进行通信。

[0062] S103：将第一IP地址发送至HTTPDNS服务器，以使HTTPDNS服务器判断第一IP地址是否被劫持。

[0063] 当接收到HTTPDNS服务器返回的第一IP地址安全的第一反馈消息后，执行S104，当接收到HTTPDNS服务器返回的第一IP地址被劫持的第二反馈消息后，执行S105。

[0064] 需要说明的是，与HTTPDNS服务器的通信是基于HTTP协议的，HTTPDNS服务器接收到域名解析请求，绕过了运营商的LocalDNS服务器，从而能够避免Local DNS服务器造成的域名劫持问题和调度不精准问题。

[0065] 将第一IP地址发送至HTTPDNS服务器，以使HTTPDNS服务器判断第一IP地址是否被劫持的过程如下：

[0066] 首先，网络代理模块将第一IP地址封装为HTTPDNS的请求参数发送给HTTPDNS服务

器，然后HTTPDNS服务器基于该HTTPDNS的请求参数对该第一IP地址进行校验。例如，HTTPDNS服务器校验第一IP地址是否在域名解析池IP列表中，若HTTPDNS服务器确定第一IP地址不在域名解析池IP列表中，则确定第一IP地址被劫持，并向客户端发送第一IP地址被劫持的第二反馈消息；若HTTPDNS服务器确定第一IP地址在域名解析池IP列表中，则确定第一IP地址未被劫持，并向客户端发送第一IP地址安全的第一反馈消息。

[0067] 优选地，无论第一IP地址是否被劫持，HTTPDNS服务器都可以根据域名地区解析规则获取最优的可信的IP地址。

[0068] 例如，最优的可信的IP地址可以是离客户端所在的地理位置最近服务器对应的可信的IP地址。

[0069] 为了方便理解根据域名地区解析规则获取最优的可信的IP地址的过程，这里举例进行说明：

[0070] 从本地网关默认的域名解析服务器中获取目标域名对应的可信的IP地址59.49.201.39和183.197.59.179；其中，IP地址59.49.201.39为中国海南省的IP地址，IP地址183.197.59.179为中国河北省的IP地址，而客户端所在的地理位置为广东省，根据域名地区解析规则，离客户端所在的地理位置最近服务器对应的可信的IP地址为59.49.201.39。

[0071] 在本发明的一个优选实施例中，HTTPDNS服务器不仅存储了目标域名及第一IP地址，还存储了用户网络的出口IP地址，以便给优化请求的调度提供数据支持。

[0072] S104：确定第一IP地址可信。

[0073] 然后，网络代理模块通过该第一IP地址建立与目标服务器之间的通信连接，从而实现客户端通过该网络代理模块与目标服务器间接通信。

[0074] 这种情况下，网络代理模块可以直接利用从本地网关默认的域名解析服务器中获得的IP地址与目标服务器建立连接，不需要从其它域名解析服务器中获取可信的IP地址，因此加快了网络请求的响应速度。

[0075] S105：从第二反馈消息中获得目标域名对应的可信的IP地址。

[0076] 如果HTTPDNS服务器判定第一IP地址被劫持，HTTPDNS服务器会返回目标域名对应的可信的IP地址，如果HTTPDNS服务器返回了可信的IP地址，则解析流程就结束了。

[0077] 此外，需要说明的是，如果网络代理模块对HTTPDNS服务器的请求失败，例如，HTTPDNS服务器出错，或者请求HTTPDNS服务器的过程失败，还可以从第三方可信的域名解析服务器对该目标域名进行解析，获得可信的IP地址。

[0078] S106：依据目标域名对应的可信的IP地址建立网络代理模块与目标域名对应的目标服务器之间的通信。

[0079] 通过目标域名对应的可信的IP地址，建立网络代理模块与目标域名对应的目标服务器连接成功后，根据HTTP代理协议通知客户端程序开始进行网络通信，即客户端把数据发送至网络代理模块，网络代理模块再把数据发送至目标服务器，相对的，目标服务器把响应数据发送至网络代理模块，网络代理模块再把响应数据发送至客户端。

[0080] 为了提高客户端与目标服务器通信的安全性，在本发明的一个优选实施例中，网络代理模块与客户端及目标服务器之间的通信可以采用隧道方式实现，具体的，在隧道模式下网络代理模块将网络请求发送至目标服务器，在隧道模式下网络代理模块接收目标服

务器返回的响应消息,再将响应消息发送至客户端。

[0081] 需要说明的是,隧道模式是按照要求建立起一条与其他服务器的通信线路,使用安全套接层(Secure Sockets Layer,SSL)等加密手段进行通信的一种模式,隧道模式可以支持超文本传输安全协议(Hyper Text Transfer Protocolover Secure Socket Layer,HTTPS),隧道模式会在通信双方断开连接时结束。在隧道模式下,客户端与目标服务器通过网络代理模块进行数据交换。当数据交互完成后,客户端或目标服务器会主动断开与网络代理模块的连接。

[0082] 由于隧道模式能够支持HTTPS协议的通信,因此隧道模式能够防止数据内容被监听和劫持,使得客户端能与目标服务器进行安全的通信。

[0083] 在本发明的另一个实施例中,网络代理模块检测通过目标域名对应的可信的IP地址与目标服务器连接是否成功;若通过该可信的IP地址与目标服务器连接成功,通过该连接实现客户端与目标服务器之间的数据交互;若通过目标域名对应的可信的IP地址与目标服务器连接失败,网络代理模块通过目标域名对应的可信的IP地址继续与目标服务器连接,当连续连接失败的次数达到预设次数时,生成连接失败消息。

[0084] 需要说明的是,当网络代理模块与目标服务器连接的连续连接失败次数达到预设的次数时,根据HTTP代理协议生成连接失败消息,其中,连接失败消息用于提示客户端,网络代理模块与目标服务器连接失败。

[0085] 预设次数的确定根据实际情况进行设置,本发明不做具体限定,本发明中的预设次数优选3。

[0086] 在本发明实施例中,网络代理模块检测通过目标域名对应的可信的IP地址与目标服务器是否连接成功,从而实现客户端与目标服务器通过网络代理模块进行数据交换的目的。

[0087] 本发明公开了一种网络通信方法,该方法先从本地网关默认的域名解析服务器中获取所要访问的目标域名对应的第一IP地址,并发送至HTTPDNS服务器,由HTTPDNS服务器判断第一IP地址是否被劫持;当接收到HTTPDNS服务器返回的第一IP地址安全的第一反馈消息后,确定第一IP地址可信;当接收到HTTPDNS服务器返回的第一IP地址被劫持的第二反馈消息后,从第二反馈消息中获得目标域名对应的可信的IP地址,依据目标域名对应的可信的IP地址建立网络代理模块与目标域名对应的目标服务器之间的通信。通过上述方案,不需要将网络请求发送至网络侧的代理服务器,从而节省了从客户端至网络侧服务端之间的传输时间;若第一IP地址未被劫持,则直接利用该第一IP地址建立网络代理模块与目标服务器之间的通信,从而加快了网络请求的响应速度;若第一IP地址被劫持,则从HTTPDNS服务器返回的第二反馈消息中获取目标域名对应的可信的IP地址,并建立网络代理模块与目标域名对应的目标服务器之间的安全通信,实现客户端与服务器的安全通信。

[0088] 为了能够快速地获得目标域名对应的可信的IP地址,本发明还提供了另一种网络通信方法,如图2所示,该方法在图1所示实施例的基础上增加了将目标域名对应的IP地址存储至本地存储空间中的过程,如图2所示,为本发明实施例公开的另一种网络通信方法的流程示意图,该方法在图1的基础上还包括S202-S203,该方法可以包括如下步骤:

[0089] S201:解析客户端发出的网络请求,得到网络请求的目标域名。

[0090] 上述S201的执行过程与图1示出的S101的执行过程相同,且执行原理也相同,这里

不再赘述。

[0091] S202:从网络代理模块的本地存储空间中存储的域名及对应的IP地址中查找是否存在目标域名对应的IP地址。如果存在,则执行S203;如果不存在,则执行S204。

[0092] 需要说明的是,本发明中的本地存储空间优选为缓存空间,即分配给网络代理模块的内存。

[0093] 在获得目标域名对应的可信的IP地址之后,将该目标域名及该可信的IP的映射关系存储至本地存储空间中,即缓存空间,当再次接收到包含该目标域名的网络请求后,首先从本地存储空间中查找与该目标域名对应的IP地址,如果在本地存储空间中查找到与该目标域名对应的IP地址,该IP地址可信,如果在本地存储空间中未查找到与该目标域名对应的IP地址,则从本地网关默认的域名解析服务器中获取该目标域名的第一IP地址。

[0094] 由于缓存空间中访问数据的速度较快,使得能够快速获取目标域名对应的可信的IP地址,提高网络请求的响应速度。

[0095] S203:确定该IP地址可信。

[0096] 在确定该IP地址可信后,执行S208。

[0097] S204:执行从本地网关默认的域名解析服务器中获取目标域名对应的第一IP地址。

[0098] S205:将第一IP地址发送至HTTPDNS服务器,以使HTTPDNS服务器判断第一IP地址是否被劫持,当接收到HTTPDNS服务器返回的第一IP地址安全的第一反馈消息后,执行S206,当接收到HTTPDNS服务器返回的第一IP地址被劫持的第二反馈消息后,执行S207。

[0099] S206:确定第一IP地址可信。

[0100] S207:从第二反馈消息中获得目标域名对应的可信的IP地址。

[0101] S208:依据目标域名对应的可信的IP地址建立网络代理模块与目标域名对应的目标服务器之间的通信。

[0102] 上述S205-S208的执行过程与图1示出的S103-S106的执行过程相同,且执行原理也相同,可参见,这里不再进行赘述。

[0103] 本发明公开了另一种网络通信方法,在解析获得客户端发出的网络请求对应的目标域名后,先查找网络代理模块本地存储空间中是否包含与该目标域名对应的可信的IP地址,如果存在则直接利用该IP地址实现网络代理模块与目标服务器之间的通信,不需要从网络侧(如,本地网关默认的域名解析服务器或第三方可信的域名解析服务器)获取可信的IP地址。而且,从本地存储空间查找IP地址所需的时间远小于从网络侧的域名解析服务器获取可信的IP地址的时间,因此,该方案能够进一步提高网络请求的响应速度。

[0104] 基于上述本发明实施例公开的一种网络通信方法,本发明实施例还对应公开了一种网络通信装置,如图3所示,主要包括:

[0105] 解析单元301,用于解析客户端发出的网络请求,得到网络请求的目标域名。

[0106] 第一获取单元302,用于从本地网关默认的域名解析服务器中获取目标域名对应的第一IP地址。

[0107] 发送单元303,用于将第一IP地址发送至HTTPDNS服务器,以使HTTPDNS服务器判断第一IP地址是否被劫持。

[0108] 第一确定单元304,用于当接收到HTTPDNS服务器返回的第一IP地址安全的第一反

馈消息后,确定第一IP地址可信。

[0109] 第二获取单元305,用于当接收到HTTPDNS服务器返回的第一IP地址被劫持的第二反馈消息后,从第二反馈消息中获得目标域名对应的可信的IP地址-。

[0110] 通信连接建立单元306,用于依据目标域名对应的可信的IP地址建立网络代理模块与目标域名对应的目标服务器之间的通信。

[0111] 进一步的,通信连接建立单元306,包括:

[0112] 第一发送模块,用于接收客户端发送的网络请求,并将网络请求以隧道模式发送至目标服务器。

[0113] 第二发送模块,用于以隧道模式接收目标服务器返回的响应消息,并将响应消息发送至客户端。

[0114] 进一步的,通信连接建立单元306,包括:

[0115] 检测模块,用于检测通过目标域名对应的可信的IP地址与目标服务器是否连接成功。

[0116] 数据交互模块,用于通过目标域名对应的可信的IP地址与目标服务器连接成功,通过该连接实现客户端与所述目标域名对应的目标服务器之间的数据交互。

[0117] 生成模块,用于若通过目标域名对应的可信的IP地址与目标服务器连接失败,通过目标域名对应的可信的IP地址继续与目标服务器连接,当连续连接失败的次数达到预设次数时,生成连接失败消息。

[0118] 如图4所示,为本发明实施例公开的另一种网络通信装置,该装置在图3的基础上还包括:存储单元401。

[0119] 存储单元401,用于将所述目标域名及该目标域名对应的可信IP地址存储至网络代理模块的本地存储空间中。

[0120] 本发明实施例公开了另一种网络通信装置,将目标域名及第一IP地址发送至HTTPDNS服务器进行存储,还存储了用户网络的出口IP地址,以便给优化请求的调度提供数据支持。

[0121] 如图5所示,为本发明实施例公开的另一种网络通信装置,该装置在图4的基础上还包括:查找单元501和第二确定单元502。

[0122] 需要说明的是,图5是本发明实施例的一个示意图,还可以在图3实施例的基础上增加查找单元501和第二确定单元502,此处不再进行详述。

[0123] 查找单元501,用于从本地存储空间中存储的域名及对应的IP地址中查找是否存在目标域名对应的IP地址;若本地存储空间中不存在目标域名对应的IP地址,则触发第一获取单元302执行从本地网关默认的域名解析服务器中获取目标域名对应的第一IP地址。

[0124] 第二确定单元502,用于若本地存储空间中存在目标域名对应的IP地址,则确定该IP地址可信。

[0125] 本发明实施例公开了另一种网络通信装置,在解析获得客户端发出的网络请求对应的目标域名后,先查找本地存储空间中是否包含与该目标域名对应的可信的IP地址,如果存在则直接利用该IP地址实现客户端与目标服务器之间的通信,不需要从网络侧(如,本地网关默认的域名解析服务器或第三方可信的域名解析服务器)获取可信的IP地址。而从本地存储空间查找IP地址所需的时间远小于从网络侧的域名解析服务器获取可信的IP地

址的时间,因此,该方案能够进一步提高网络请求的响应速度。

[0126] 如图6所示,为本发明实施例公开的另一种网络通信装置,该装置在图3的基础上还包括:第三获取单元601。

[0127] 第三获取单元601,用于当请求HTTPDNS服务器失败后,从可信的域名解析服务器中获取目标域名对应的可信IP地址。

[0128] 本发明实施例公开了另一种网络通信装置,当请求HTTPDNS服务器失败后,从可信的域名解析服务器中获取目标域名对应的可信的IP地址,实现请求HTTPDNS服务器失败后,依旧可以获得目标域名对应的可信的IP地址。

[0129] 本发明还提供了一种网络代理模块,应用于客户端中,包括轻量级网络库,轻量级网络库能够与基于不同操作系统平台开发的客户端融合。当检测到启动指令后,启动轻量级网络库启动事件处理线程,以执行上述任意一种网络通信方法。

[0130] 需要说明的是,轻量级网络库能够跨平台,与不同操作系统平台开发的客户端融合。

[0131] 通过使用开源的跨平台自动化构建系统(Cross PlatformMake,CMake)进行管理构建,并根据第三方跨平台的网络库libevent进行跨平台开发。

[0132] 不同操作系统可以是Android操作系统、Windows操作系统、IOS操作系统等,具体的操作系统本发明不做具体限定。

[0133] 基于Android平台和Windows平台构建动态库,并将动态库打包到Android平台和Windows平台各自平台对应的客户端程序中,基于IOS平台构建静态库,并将静态库打包到IOS平台对应的客户端程序中。

[0134] 本发明还提供了一种存储介质,该存储介质内存储有程序指令,该程序指令被处理器加载并执行时实现上述任意一种网络通信方法实施例。

[0135] 本发明还提供了一种计算机设备。该设备包括处理器和存储器;存储器内存储有程序指令;处理器调用该存储器内的程序指令以执行上述任意一种网络通信方法实施例。

[0136] 本文中的处理器可以是终端的CPU,或者,是终端内集成的MCU,或者,还可以是CPU和MCU的结合。而且,处理器中包含内核,由内核从存储器中调取相应的程序,内核可以设置一个或以上。

[0137] 存储器可能包括计算机可读介质中的非永久性存储器,随机存取存储器(RAM)和/或非易失性内存等形式,如只读存储器(ROM)或闪存(flashRAM),存储器包括至少一个存储芯片。

[0138] 对于前述的各方法实施例,为了简单描述,故将其都表述为一系列的动作组合,但是本领域技术人员应该知悉,本发明并不受所描述的动作顺序的限制,因为依据本发明,某些步骤可以采用其他顺序或者同时进行。其次,本领域技术人员也应该知悉,说明书中所描述的实施例均属于优选实施例,所涉及的动作和模块并不一定是本发明所必须的。

[0139] 需要说明的是,本说明书中的各个实施例均采用递进的方式描述,每个实施例重点说明的都是与其他实施例的不同之处,各个实施例之间相同相似的部分互相参见即可。对于装置类实施例而言,由于其与方法实施例基本相似,所以描述的比较简单,相关之处参见方法实施例的部分说明即可。

[0140] 本发明各实施例方法中的步骤可以根据实际需要进行顺序调整、合并和删减。

[0141] 本发明各实施例中的装置及终端中的模块和子模块可以根据实际需要进行合并、划分和删减。

[0142] 本发明所提供的几个实施例中，应该理解到，所揭露的终端，装置和方法，可以通过其它的方式实现。例如，以上所描述的终端实施例仅仅是示意性的，例如，模块或子模块的划分，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，例如多个子模块或模块可以结合或者可以集成到另一个模块，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信连接可以是通过一些接口，装置或模块的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0143] 作为分离部件说明的模块或子模块可以是或者也可以不是物理上分开的，作为模块或子模块的部件可以是或者也可以不是物理模块或子模块，即可以位于一个地方，或者也可以分布到多个网络模块或子模块上。可以根据实际的需要选择其中的部分或者全部模块或子模块来实现本实施例方案的目的。

[0144] 另外，在本发明各个实施例中的各功能模块或子模块可以集成在一个处理模块中，也可以是各个模块或子模块单独物理存在，也可以两个或两个以上模块或子模块集成在一个模块中。上述集成的模块或子模块既可以采用硬件的形式实现，也可以采用软件功能模块或子模块的形式实现。

[0145] 最后，还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0146] 对所公开的实施例的上述说明，使本领域技术人员能够实现或使用本发明。对这些实施例的多种修改对本领域技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本发明的精神或范围的情况下，在其它实施例中实现。因此，本发明将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

[0147] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

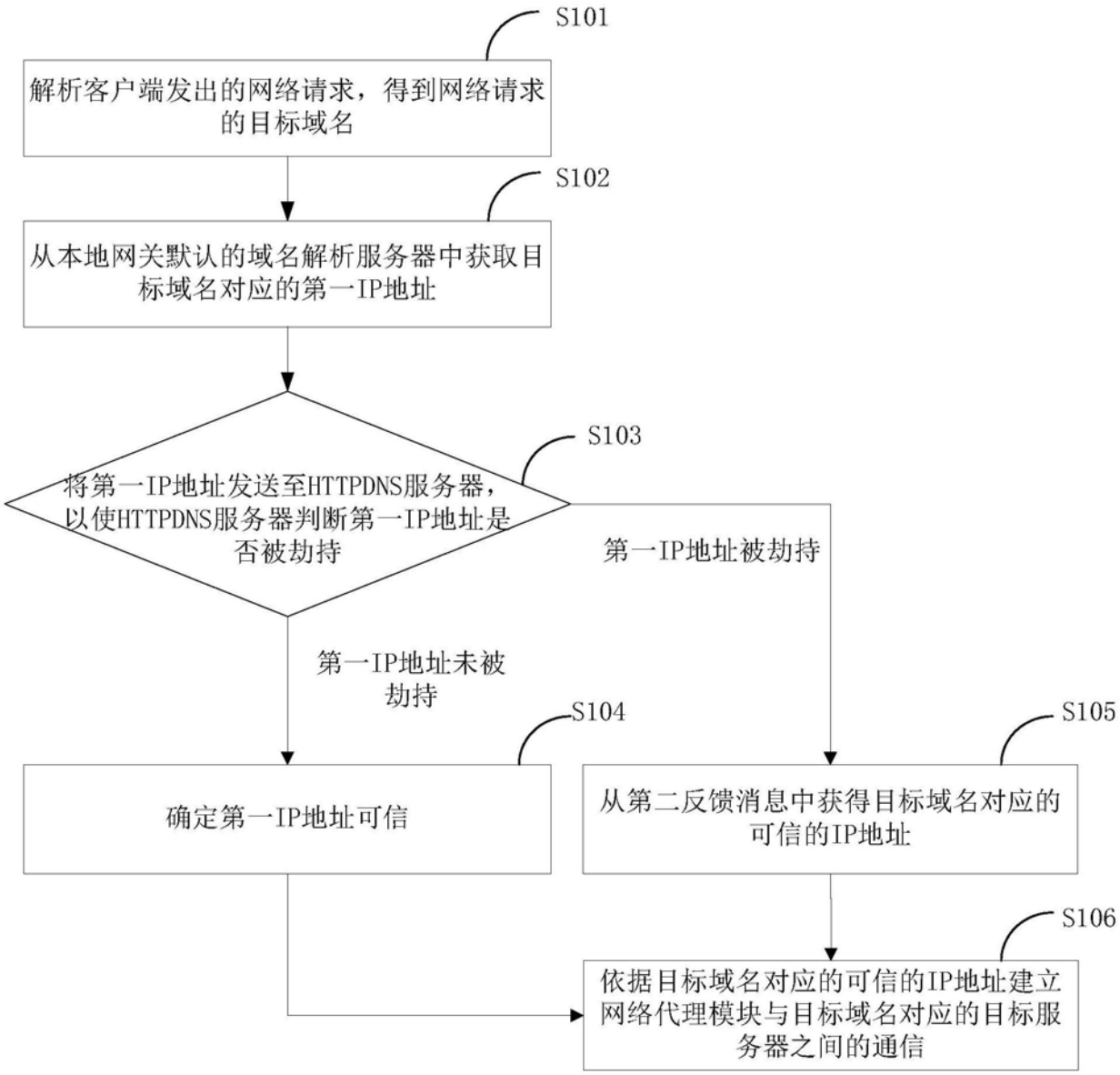

S101
解析客户端发出的网络请求，得到网络请求的目标域名
S102
从本地网关默认的域名解析服务器中获取目标域名对应的第一IP地址
S103
将第一IP地址发送至HTTPDNS服务器，以使HTTPDNS服务器判断第一IP地址是否被劫持
第一IP地址被劫持
第一IP地址未被劫持
S104
确定第一IP地址可信
S105
从第二反馈消息中获得目标域名对应的可信的IP地址
S106
依据目标域名对应的可信的IP地址建立网络代理模块与目标域名对应的目标服务器之间的通信

图1

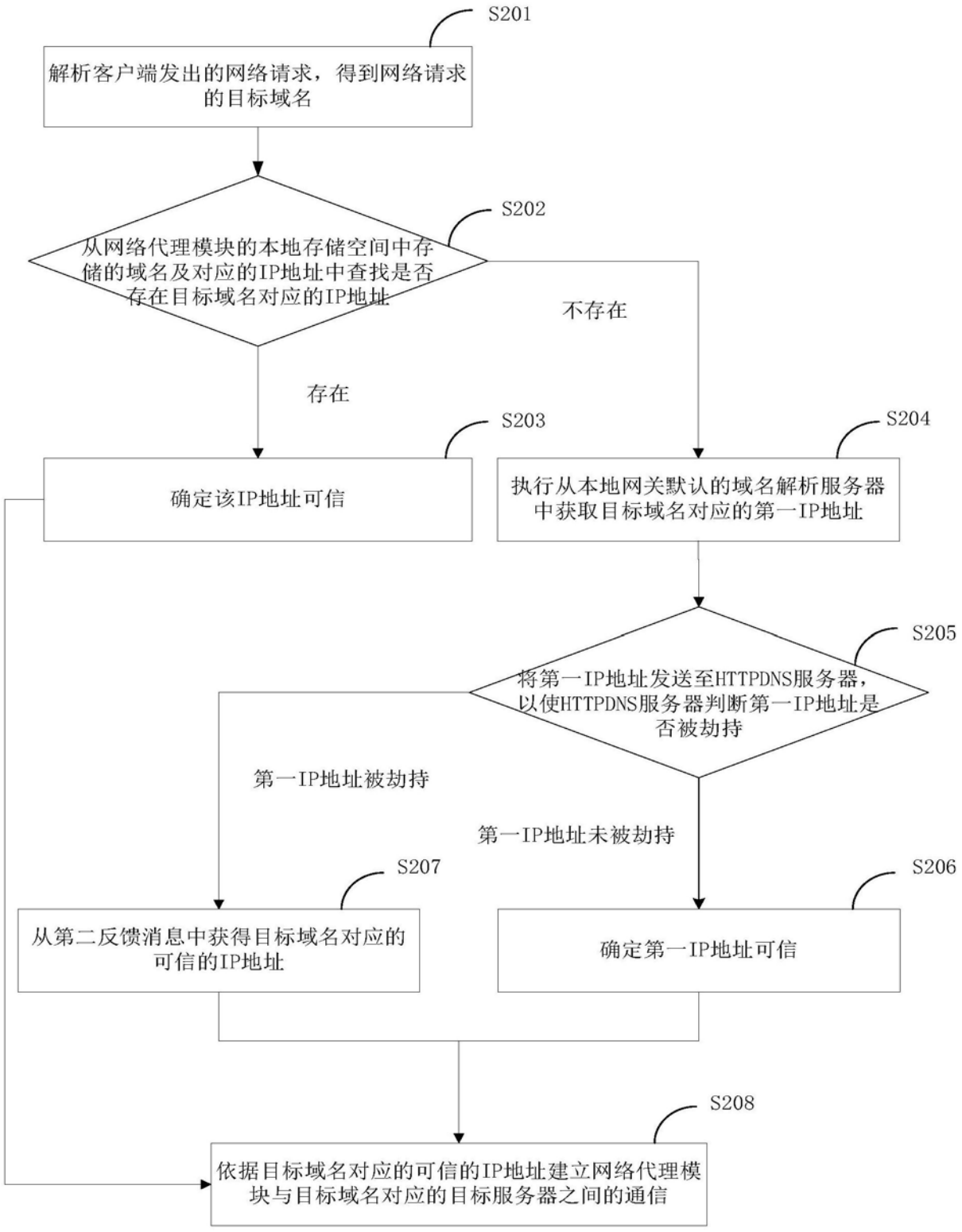

S201
解析客户端发出的网络请求，得到网络请求的目标域名
S202
从网络代理模块的本地存储空间中存储的域名及对应的IP地址中查找是否存在目标域名对应的IP地址
不存在
存在
S203
确定该IP地址可信
S204
执行从本地网关默认的域名解析服务器中获取目标域名对应的第一IP地址
S205
将第一IP地址发送至HTTPDNS服务器，以使HTTPDNS服务器判断第一IP地址是否被劫持
第一IP地址被劫持
第一IP地址未被劫持
S207
从第二反馈消息中获得目标域名对应的可信的IP地址
S206
确定第一IP地址可信
S208
依据目标域名对应的可信的IP地址建立网络代理模块与目标域名对应的目标服务器之间的通信

图2

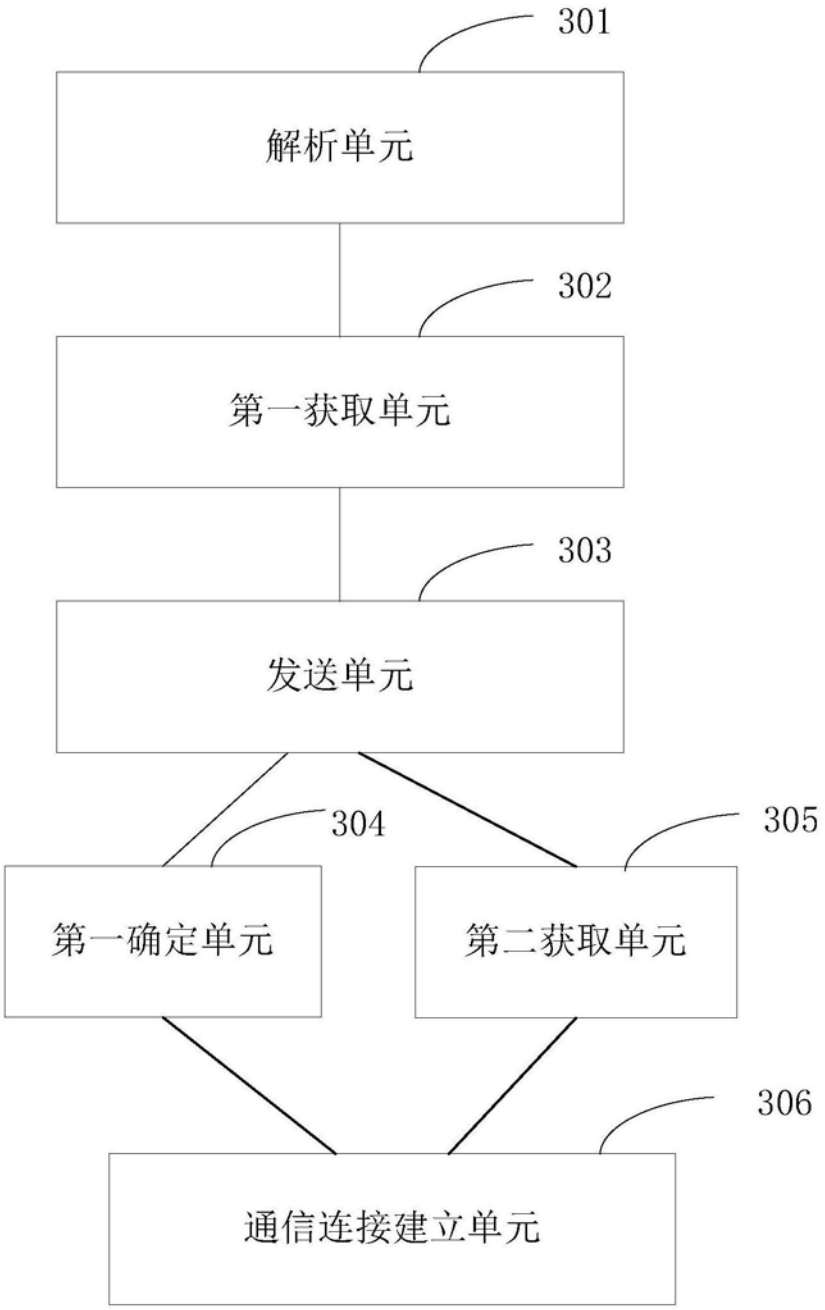

301
解析单元
302
第一获取单元
303
发送单元
304
第一确定单元
305
第二获取单元
306
通信连接建立单元

图3

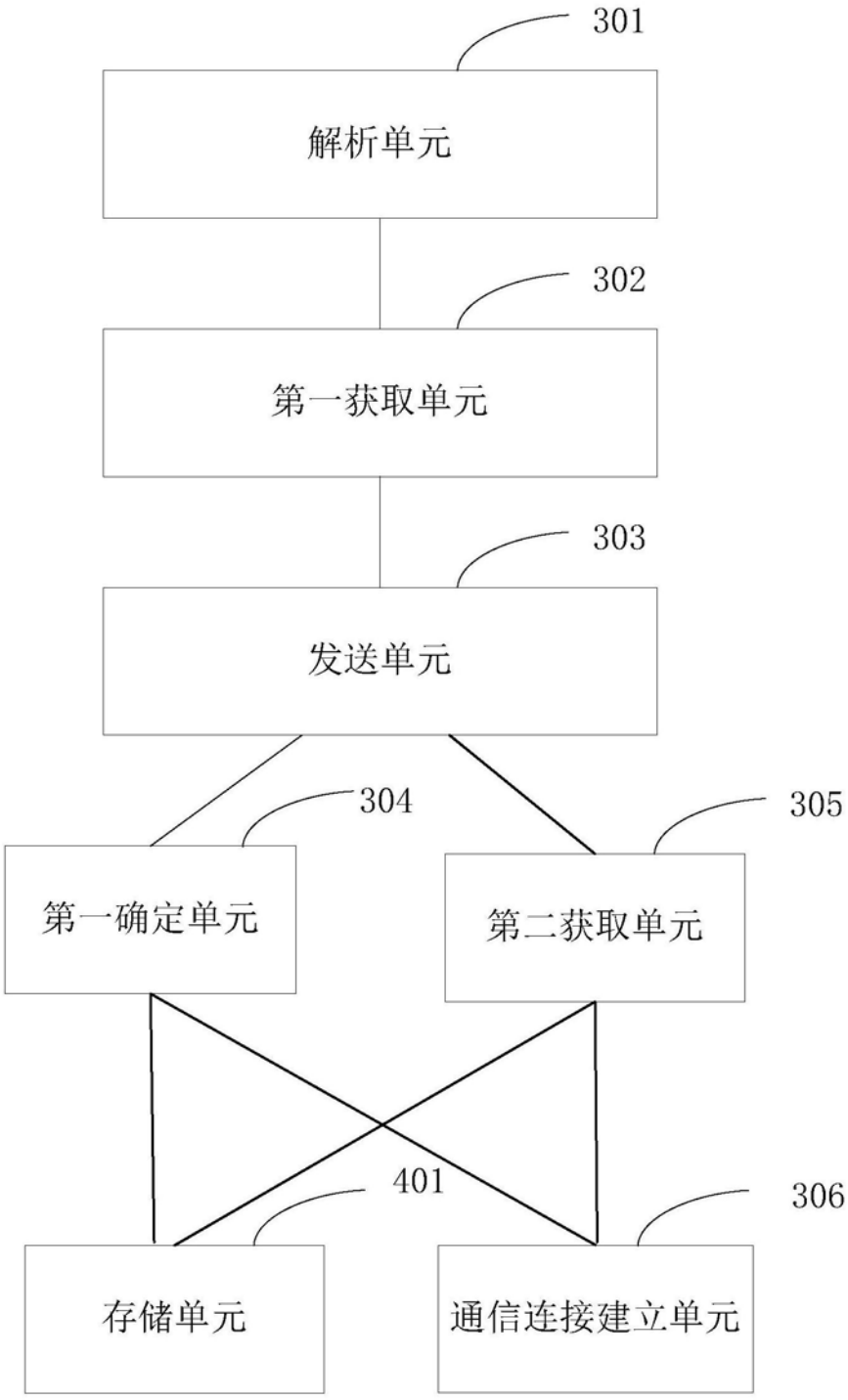

301
解析单元
302
第一获取单元
303
发送单元
304
第一确定单元
305
第二获取单元
401
306
存储单元
通信连接建立单元

图4

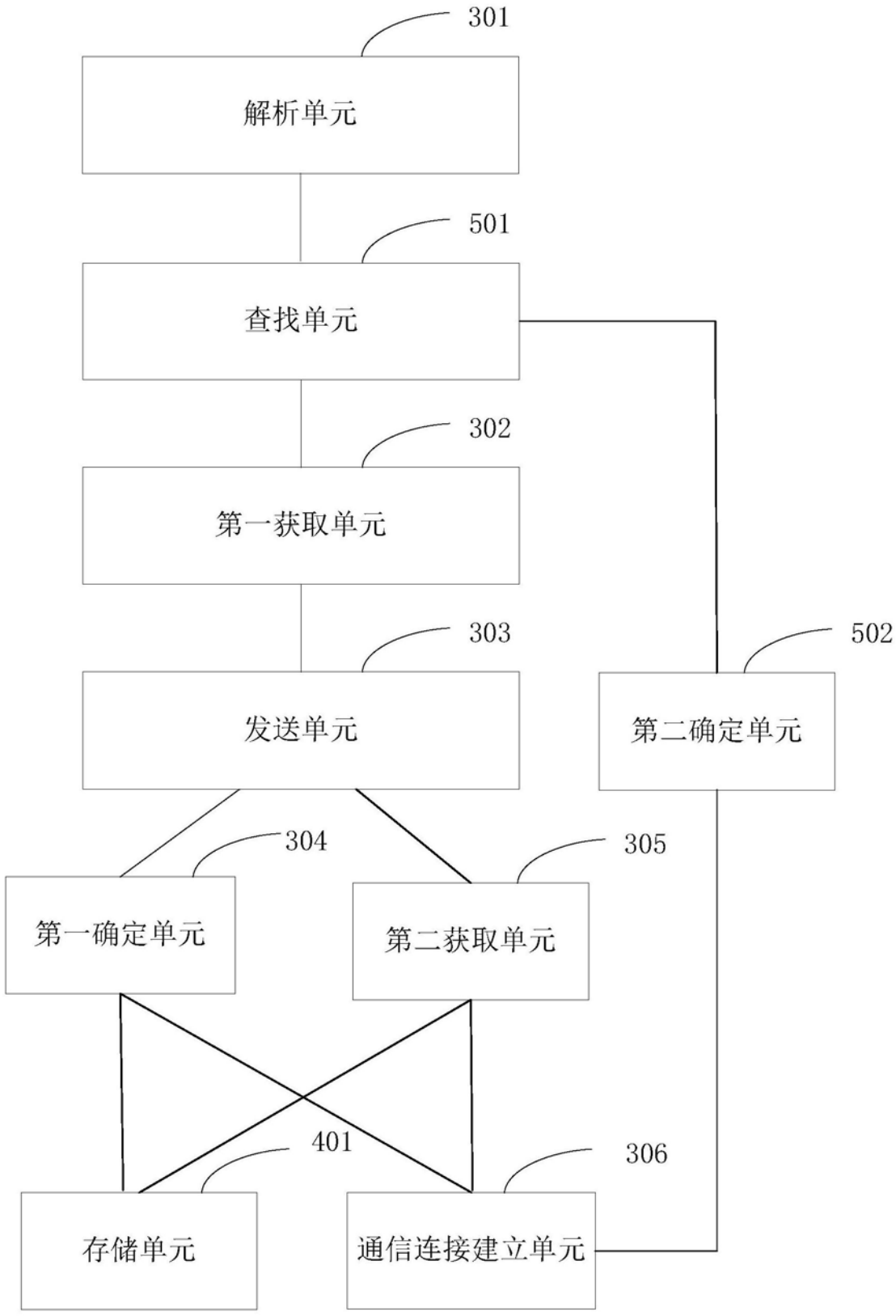

301
解析单元
501
查找单元
302
第一获取单元
303
发送单元
502
第二确定单元
304
第一确定单元
305
第二获取单元
401
存储单元
306
通信连接建立单元

图5

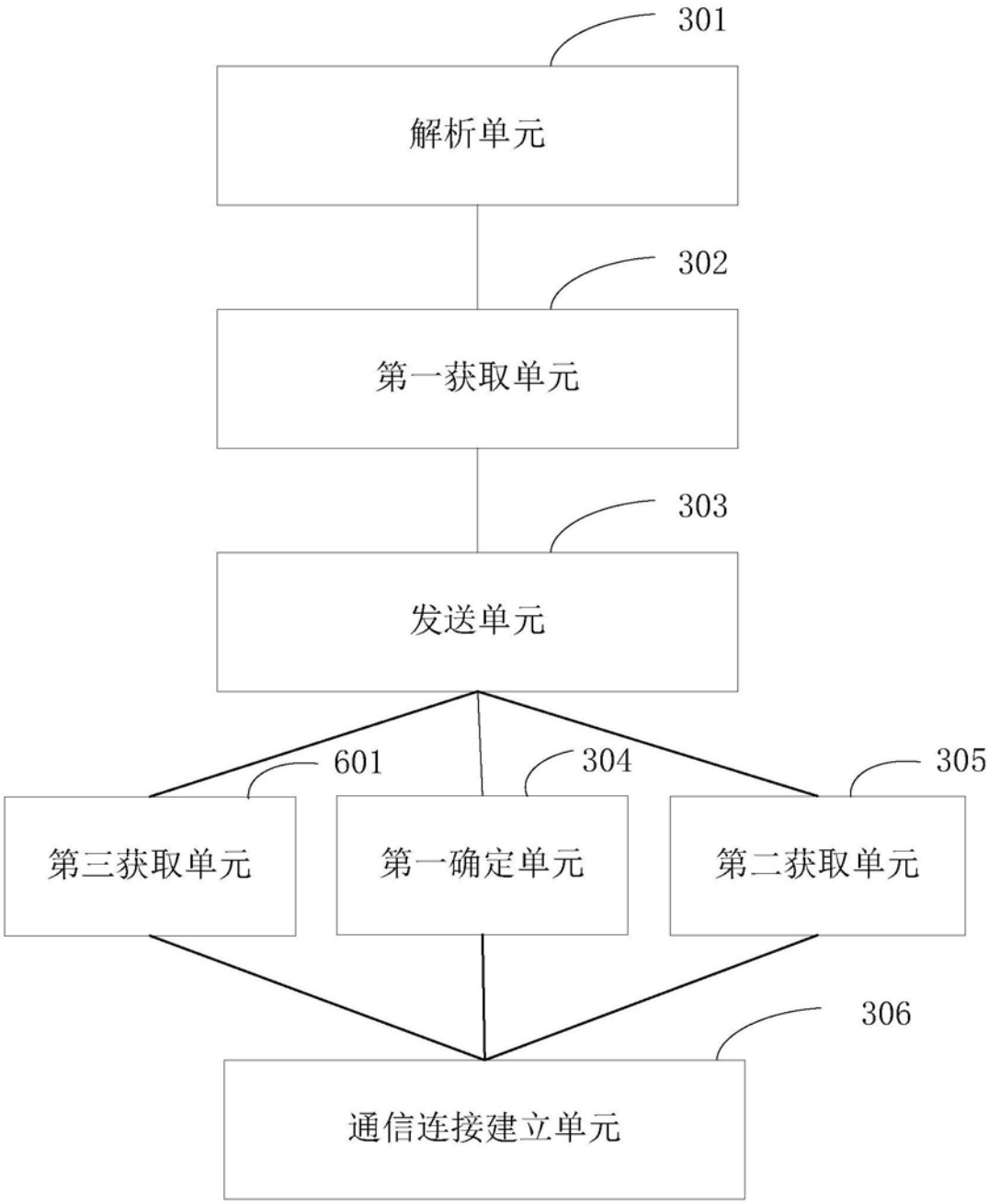

301
解析单元
302
第一获取单元
303
发送单元
601
304
305
第三获取单元
第一确定单元
第二获取单元
306
通信连接建立单元

图6