



(12)发明专利

(10)授权公告号 CN 104468866 B

(45)授权公告日 2017.11.21

(21)申请号 201410828558.9

H04W 8/02(2009.01)

(22)申请日 2014.12.26

(56)对比文件

(65)同一申请的已公布的文献号  
申请公布号 CN 104468866 A

CN 101827013 A,2010.09.08,  
CN 101621449 A,2010.01.06,  
CN 101420762 A,2009.04.29,  
CN 103024720 A,2013.04.03,  
CN 101534238 A,2009.09.16,  
CN 102395167 A,2012.03.28,  
CN 102638873 A,2012.08.15,  
US 8483192 B2,2013.07.09,

(43)申请公布日 2015.03.25

(73)专利权人 陈晨  
地址 710054 陕西省西安市经九路新南花园  
专利权人 刘乃安

张鹏.无线Mesh网络环境中多网关路由和切换机制的研究.《中国优秀硕士学位论文全文数据库(电子期刊)》.2010,第I136-334页.

(72)发明人 陈晨 刘乃安 郭峰 王在刚

(74)专利代理机构 西安长和专利代理有限公司  
61227

审查员 胡燕

代理人 黄伟洪

(51)Int.Cl.

H04L 29/12(2006.01)

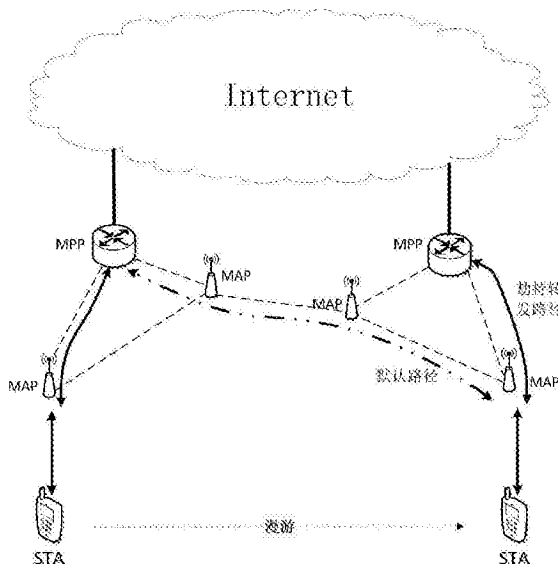
权利要求书4页 说明书10页 附图7页

(54)发明名称

一种无线局域网中多网关终端快速漫游方法

(57)摘要

本发明公开了一种无线局域网中多网关终端快速漫游方法,将STA(station移动终端)发往外网的数据包截获,然后将截获的数据包发给一个通信条件最佳的MPP(Mesh Portal Point Mesh网关节点)节点,由该MPP节点将数据包转发到外网,从而降低了STA发往外网的数据包时延。本发明适用于使用多个MPP节点的无线Mesh网络场景。本发明可以应用到其他使用多个MPP节点的无线Mesh网络中,用以减小STA上网时延;本发明减轻了Mesh网络中的负载,缩短了STA发往外网的数据包时延,提高了用户上网速度。



1. 一种无线局域网中多网关终端快速漫游方法,其特征在于,该无线局域网中多网关终端快速漫游方法在STA接入的Mesh节点处,将STA发往外网的数据包截获,然后将截获的数据包发给一个通信条件最佳的MPP节点,由该MPP节点将数据包转发到外网;

该无线局域网中多网关终端快速漫游方法包括一个新的对应表和三个数据包劫持机制;

对应表,即终端mac地址和DNS服务器地址的对应表;mac地址是STA的mac地址,DNS服务器地址是STA的DNS服务器地址,即STA所选MPP节点的IP地址;

三个数据包劫持机制包括:普通数据包的劫持转发机制、ARP请求包的劫持与应答机制和DNS查询应答包的劫持转发机制;

普通数据包的劫持转发机制,Mesh节点收到STA的普通数据包后,截获该数据包,提取数据包源mac地址,根据源mac地址判断是否是接入本Mesh节点的STA,只对接入本Mesh节点的STA的数据包进行劫持处理,然后判断数据包是发往外网还是内网,只对发往外网的数据包进行劫持处理;数据包是接入本Mesh节点的STA的且发往外网,则将数据包目的mac地址修改为Mesh网络中一个通信条件最佳的MPP节点的mac地址;

ARP请求包的劫持与应答机制,L2P协议是分布式ARP表DAT机制,该机制的核心是存储网络中传播的所有ARP相应内容在一些特定的节点组中,给定一个IP地址,客户端发起一个ARP请求,Mesh节点收到ARP请求包后,截获并直接将它转发到存储有相应条目的节点组中的节点,请求被作为单播分组发送,对于使用DAT机制仍无法获得相应条目的ARP请求,协议将按普通ARP请求包广播出去;

DNS查询应答包的劫持转发机制,STA会先发送一个DNS查询包给DNS服务器,查找域名对应的IP地址,得到应答之后才能访问网址,STA的DNS服务器地址和IP地址是自动获取的,通常STA的DNS服务器地址即是默认网关的IP地址,对于DNS应答包,将数据包中源IP地址由公网服务器地址修改回STA的默认网关的IP地址。

2. 如权利要求1所述的无线局域网中多网关终端快速漫游方法,其特征在于,该无线局域网中多网关终端快速漫游方法MAP节点普通数据包劫持转发机制的具体步骤如下:

步骤一,MAP节点收到单播数据包后,提取出数据包的源mac地址,然后查询本地转换表判断源mac地址是否在表中,在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤二;否则,节点只是转发该数据包,不进行处理;

步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理;

步骤三,提取出数据包的IP层头部,然后获取目的IP地址,目的IP是10或192网段的,则说明数据包是发往网内的,不进行处理;否则进入步骤四;

步骤四,获取当前MAP节点所选MPP的mac地址,与数据包目的mac地址进行比较,相同,则说明数据包是发往当前MAP所选MPP节点的,不进行任何处理;不同,则将数据包的目的mac地址修改成当前MAP节点所选MPP节点的mac地址,进入步骤五;

步骤五,将数据包目的mac地址修改后,根据新的目的mac地址查找最佳下一跳节点,然后添加L2P协议定义的单播数据包头并调用l2p\_transmit\_skb\_to\_initi函数发送到MAP节点所选MPP节点去,并由该MPP节点转发出去。

3. 如权利要求1所述的无线局域网中多网关终端快速漫游方法,其特征在于,该无线局域网中多网关终端快速漫游方法的ARP请求包劫持与应答机制的具体步骤如下:

步骤一,MAP节点收到ARP请求包后,提取出源mac地址,然后查询本地转换表判断源mac地址是否在表中,在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤二;否则,不进行处理;

步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理;

步骤三,提取ARP请求包目的IP地址,判断是否为MPP节点IP地址,是MPP节点IP,则进入步骤四;否则,不进行处理;

步骤四,查找本地DAT表中是否有相应条目,有,则直接生成一个ARP应答包进行应答;否则进入步骤五;

步骤五,获取MAP节点所选MPP节点的mac地址,并使用该mac地址作为应答构造ARP应答包发给ARP请求者。

4. 如权利要求1所述的无线局域网中多网关终端快速漫游方法,其特征在于,该无线局域网中多网关终端快速漫游方法DNS查询包劫持转发机制的具体步骤如下:

步骤一,MAP节点收到数据包后,提取出源mac地址,然后查询本地转换表判断源mac地址是否在表中,在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤二;否则,不进行处理;

步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理;

步骤三,提取出数据包IP头部,判断是否是UDP包,是,则进入步骤四;否则不进行处理;

步骤四,提取出数据包的UDP头部,根据UDP头部的目的端口号判断是否是DNS请求包,是,则进入步骤五;否则不进行处理;

步骤五,将数据包的源mac地址和目的IP地址保存到mac地址和DNS地址对应表中,然后将DNS请求包的目的IP地址修改为一个公网DNS服务器地址,再调用函数ip\_fast\_csum((unsigned char\*)iphdr,iphdr->ihl)重新计算IP头部校验和并设置UDP头部校验和为0,最后将修改过的DNS请求包按普通外网数据包交由普通数据包的劫持转发机制处理。

5. 如权利要求4所述的无线局域网中多网关终端快速漫游方法,其特征在于,DNS应答包的劫持是在函数l2p\_interface\_rx中进行,处理发往本节点或本节点所连接客户端的数据包,收到数据包后,函数先将L2P协议给这些数据包添加的mac层头部剥离,然后再进行处理,DNS应答包的劫持是在剥离了L2P协议添加的mac头后进行,具体的步骤如下:

步骤一,MAP节点提取出数据包源mac地址,然后查询本地转换表判断源mac地址是否在表中,在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤二;否则,不进行处理;

步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理;

步骤三,提取出数据包IP头部,判断是否是UDP包,是,则进入步骤四;否则不进行处理;

步骤四,提取出数据包的UDP头部,根据UDP头部的源端口号判断是否是DNS应答包,是,则进入步骤五;否则不进行处理;

步骤五,查找mac地址和DNS地址对应表查找到该STA对应的原先DNS服务器IP地址,并将DNS应答包的源IP地址改成该地址,在重新计算IP头部校验和并设置UDP头部校验和为0,然后将修改后的DNS应答包发给STA。

6.如权利要求1所述的无线局域网中多网关终端快速漫游方法,其特征在于,该无线局域网中多网关终端快速漫游方法MPP普通数据包劫持转发机制的具体步骤如下:

步骤一,MPP节点收到单播数据包后,提取出数据包的源mac地址,然后查询本地转换表判断源mac地址是否在表中,在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤二;否则,节点只是转发该数据包,不进行处理;

步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理;

步骤三,提取出数据包的IP层头部,然后获取目的IP地址,目的IP是10或192网段的,则说明数据包是发往网内的,不进行处理;否则进入步骤四;

步骤四,获取本MPP节点的mac地址,与数据包目的mac地址进行比较,相同,则说明数据包是发往此MPP节点的,不进行任何处理;不同,则进入步骤五;

步骤五,将数据包目的mac地址修改为本MPP节点mac地址,并设置skb->pkt\_type为PACKET\_HOST,调用函数eth\_type\_trans(),返回值赋给skb->protocol,最后调用系统函数netif\_rx()将数据包发给Linux网络协议栈由上层协议接收处理并发送出去。

7.如权利要求1所述的无线局域网中多网关终端快速漫游方法,其特征在于,该无线局域网中多网关终端快速漫游方法ARP请求包劫持与应答机制的具体步骤如下:

步骤一,MPP节点收到ARP请求包后,提取出源mac地址,然后查询本地转换表判断源mac地址是否在表中,在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤二;否则,不进行处理;

步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理;

步骤三,提取ARP请求包目的IP地址,判断是否为MPP节点IP地址,是MPP节点IP,则进入步骤四;否则,不进行处理;

步骤四,查找本地DAT表中是否有相应条目,有,则直接生成一个ARP应答包进行应答;否则进入步骤五;

步骤五,获取本MPP节点的mac地址,并使用该mac地址作为应答构造ARP应答包发给ARP请求者。

8.如权利要求1所述的无线局域网中多网关终端快速漫游方法,其特征在于,该无线局域网中多网关终端快速漫游方法DNS查询包劫持转发机制的具体步骤如下:

步骤一,MPP节点收到数据包后,提取出源mac地址,然后查询本地转换表判断源mac地址是否在表中,在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤

二;否则,不进行处理;

步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理;

步骤三,提取出数据包IP头部,判断是否是UDP包,是,则进入步骤四;否则不进行处理;

步骤四,提取出数据包的UDP头部,根据UDP头部的目的端口号判断是否是DNS请求包,是,则进入步骤五;否则不进行处理;

步骤五,将数据包的源mac地址和目的IP地址保存到mac地址和DNS地址对应表中,然后将DNS请求包的目的IP地址修改为一个公网DNS服务器地址,再调用函数ip\_fast\_csum((unsigned char\*)iphdr,iphdr->ihl)重新计算IP头部校验和并设置UDP头部校验和为0,最后将修改过的DNS请求包按普通外网数据包交由普通数据包的劫持转发机制处理。

9.如权利要求8所述的无线局域网中多网关终端快速漫游方法,其特征在于,DNS应答包的劫持是在函数l2p\_interface\_rx中进行,是处理发往本节点或本节点所连接客户端的数据包,收到了数据包后,函数先将L2P协议给这些数据包添加的mac层头部剥离,然后再进行处理,DNS应答包的劫持是在剥离了L2P协议添加的mac头后进行,具体包括以下步骤:

步骤一,MPP节点提取出数据包源mac地址,然后查询本地转换表判断源mac地址是否在表中,在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤二;否则,不进行处理;

步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理;

步骤三,提取出数据包IP头部,判断是否是UDP包,是,则进入步骤四;否则不进行处理;

步骤四,提取出数据包的UDP头部,根据UDP头部的源端口号判断是否是DNS应答包,是,则进入步骤五;否则不进行处理;

步骤五,查找mac地址和DNS地址对应表查找到该STA对应的原先DNS服务器IP地址,并将DNS应答包的源IP地址改成该地址,在重新计算IP头部校验和并设置UDP头部校验和为0,然后将修改后的DNS应答包发给STA。

## 一种无线局域网中多网关终端快速漫游方法

### 技术领域

[0001] 本发明属于局域网技术领域,尤其涉及一种无线局域网中多网关终端快速漫游方法。

### 背景技术

[0002] 在存在多个MPP的无线Mesh网络中,MPP通常作为DHCP服务器给STA分配IP地址,STA从MPP获得IP地址后会将其设为自身默认网关,所有发往外网的数据包都会交由该默认网关进行转发。如果STA漫游到距离其默认网关较远距离后,STA仍会将外网数据包通过网络中的其它MP节点发往其默认网关再由默认网关转发出去,而不管距离STA较近处是否有其它MPP节点可以提供连接外网服务,这将造成STA发往外网的数据包时延很大。

### 发明内容

[0003] 本发明的目的在于提供一种无线局域网中多网关终端快速漫游方法,旨在解决现有的STA发往外网的数据包时延较长,影响用户上网速度的问题。

[0004] 本发明是这样实现的,一种无线局域网中多网关终端快速漫游方法,该无线局域网中多网关终端快速漫游方法在STA接入的Mesh节点处,将STA发往外网的数据包截获,然后将截获的数据包发给一个通信条件最佳的MPP节点,由该MPP节点将数据包转发到外网。

[0005] 进一步,该无线局域网中多网关终端快速漫游方法包括一个新的对应表和三个数据包劫持机制;

[0006] 对应表,即终端mac地址和DNS服务器地址的对应表;mac地址是STA的mac地址,DNS服务器地址是STA的DNS服务器地址,即STA所选MPP节点的IP地址;

[0007] 三个数据包劫持机制包括:普通数据包的劫持转发机制、ARP请求包的劫持与应答机制和DNS查询应答包的劫持转发机制;

[0008] 普通数据包的劫持转发机制,Mesh节点收到STA的普通数据包后,截获该数据包,提取数据包源mac地址,根据源mac地址判断是否是接入本Mesh节点的STA,只对接入本Mesh节点的STA的数据包进行劫持处理,然后判断数据包是发往外网还是内网,只对发往外网的数据包进行劫持处理;数据包是接入本Mesh节点的STA的且发往外网,则将数据包目的mac地址修改为Mesh网络中一个通信条件最佳的MPP节点的mac地址;

[0009] ARP请求包的劫持与应答机制,L2P协议本身实现了一个分布式ARP表(DAT)机制,该机制的核心是存储网络中传播的所有ARP相应内容在一些特定的节点组中,给定一个IP地址,客户端发起一个ARP请求,Mesh节点收到ARP请求包后,截获并直接将它转发到存储有相应条目的节点组中的节点,请求被作为单播分组发送,对于使用DAT机制仍无法获得相应条目的ARP请求,协议将按普通ARP请求包广播出去;

[0010] 当STA的默认网关MPP1无法正常工作时,由于STA发往外网的数据包是使用默认网关mac地址作为数据包目的mac地址,会发起ARP请求去获取默认网关的mac地址,在STA接入的Mesh节点处截获STA对其默认网关的ARP请求包,查找本地DAT表中是否有相应条目,有,

则直接生成一个ARP应答包进行应答；否则使用一个通信条件最佳MPP节点的mac地址进行相应，STA收到ARP应答后，就将发往外网的数据包发出；

[0011] DNS查询应答包的劫持转发机制，STA会先发送一个DNS查询包给DNS服务器，查找该域名对应的IP地址，得到应答之后才能访问该网址，STA的DNS服务器地址和IP地址是自动获取的，通常STA的DNS服务器地址即是默认网关的IP地址，STA的默认网关无法正常工作，相当于STA的DNS服务器故障了，无法给STA提供域名解析服务，从而无法通过访问域名的方式上网，在STA接入的Mesh节点将STA的DNS查询包进行劫持并将DNS查询包中的目的IP地址由STA的默认网关IP地址修改为一个公网DNS服务器地址，然后将DNS查询包转发到通信条件最佳MPP节点，由该MPP节点发送出去，对于DNS应答包，将数据包中源IP地址由公网服务器地址修改回STA的默认网关的IP地址。

[0012] 进一步，该无线局域网中多网关终端快速漫游方法MAP节点普通数据包劫持转发机制的具体步骤如下：

[0013] 步骤一，MAP节点收到单播数据包后，提取出数据包的源mac地址，然后查询本地转换表判断源mac地址是否在表中，在本地转换表中，则说明是本节点连接的客户端发送的数据包，进入步骤二；否则，节点只是转发该数据包，不进行处理；

[0014] 步骤二，根据源mac地址查找到对应的本地转换表条目后，提取出本地转换表中的标志域flags，与L2P\_NCL\_CLIENT\_WIFI进行按位&运算，结果为1，则说明数据包由wifi客户端发出，进入步骤三；否则，不进行处理；

[0015] 步骤三，提取出数据包的IP层头部，然后获取目的IP地址，目的IP是10或192网段的，则说明数据包是发往网内的，不进行处理；否则进入步骤四；

[0016] 步骤四，获取当前MAP节点所选MPP的mac地址，将其与数据包目的mac地址进行比较，相同，则说明数据包是发往当前MAP所选MPP节点的，不进行任何处理；不同，则将数据包的目的mac地址修改成当前MAP节点所选MPP节点的mac地址，进入步骤五；

[0017] 步骤五，将数据包目的mac地址修改后，根据新的目的mac地址查找最佳下一跳节点，然后添加L2P协议定义的单播数据包头并调用l2p\_transmit\_skb\_to\_initi函数将其发送到MAP节点所选MPP节点去，并由该MPP节点转发出去。

[0018] 进一步，该无线局域网中多网关终端快速漫游方法的ARP请求包劫持与应答机制的具体步骤如下：

[0019] 步骤一，MAP节点收到ARP请求包后，提取出源mac地址，然后查询本地转换表判断源mac地址是否在表中，在本地转换表中，则说明是本节点连接的客户端发送的数据包，进入步骤二；否则，不进行处理；

[0020] 步骤二，根据源mac地址查找到对应的本地转换表条目后，提取出本地转换表中的标志域flags，与L2P\_NCL\_CLIENT\_WIFI进行按位&运算，结果为1，则说明数据包由wifi客户端发出，进入步骤三；否则，不进行处理；

[0021] 步骤三，提取ARP请求包目的IP地址，判断是否为MPP节点IP地址，是MPP节点IP，则进入步骤四；否则，不进行处理；

[0022] 步骤四，查找本地DAT表中是否有相应条目，有，则直接生成一个ARP应答包进行应答；否则进入步骤五；

[0023] 步骤五，获取MAP节点所选MPP节点的mac地址，并使用该mac地址作为应答构造ARP

应答包发给ARP请求者。

[0024] 进一步,该无线局域网中多网关终端快速漫游方法DNS查询包劫持转发机制的具体步骤如下:

[0025] 步骤一,MAP节点收到数据包后,提取出源mac地址,然后查询本地转换表判断源mac地址是否在表中,在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤二;否则,不进行处理;

[0026] 步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理;

[0027] 步骤三,提取出数据包IP头部,判断是否是UDP包,是,则进入步骤四;否则不进行处理;

[0028] 步骤四,提取出数据包的UDP头部,根据UDP头部的目的端口号判断是否是DNS请求包,是,则进入步骤五;否则不进行处理;

[0029] 步骤五,将数据包的源mac地址和目的IP地址保存到mac地址和DNS地址对应表中,然后将DNS请求包的目的IP地址修改为一个公网DNS服务器地址,再调用函数ip\_fast\_csum((unsigned char\*)iphdr,iphdr->ihl)重新计算IP头部校验和并设置UDP头部校验和为0,最后将修改过的DNS请求包按普通外网数据包交由普通数据包的劫持转发机制处理。

[0030] 进一步,DNS应答包的劫持是在函数l2p\_interface\_rx中进行,处理发往本节点或本节点所连接客户端的数据包,收到了这些数据包后,函数先将L2P协议给这些数据包添加的mac层头部剥离,然后再进行其它处理,DNS应答包的劫持是在剥离了L2P协议添加的mac头后进行,具体的步骤如下:

[0031] 步骤一,MAP节点提取出数据包源mac地址,然后查询本地转换表判断源mac地址是否在表中,在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤二;否则,不进行处理;

[0032] 步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理;

[0033] 步骤三,提取出数据包IP头部,判断是否是UDP包,是,则进入步骤四;否则不进行处理;

[0034] 步骤四,提取出数据包的UDP头部,根据UDP头部的源端口号判断是否是DNS应答包,是,则进入步骤五;否则不进行处理;

[0035] 步骤五,查找mac地址和DNS地址对应表查找到该STA对应的原先DNS服务器IP地址,并将DNS应答包的源IP地址改成该地址,在重新计算IP头部校验和并设置UDP头部校验和为0,然后将修改后的DNS应答包发给STA。

[0036] 进一步,该无线局域网中多网关终端快速漫游方法MPP普通数据包劫持转发机制的具体步骤如下:

[0037] 步骤一,MPP节点收到单播数据包后,提取出数据包的源mac地址,然后查询本地转换表判断源mac地址是否在表中,在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤二;否则,节点只是转发该数据包,不对其进行处理;



[0038] 步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理;

[0039] 步骤三,提取出数据包的IP层头部,然后获取目的IP地址,目的IP是10或192网段的,则说明数据包是发往网内的,不进行处理;否则进入步骤四;

[0040] 步骤四,获取本MPP节点的mac地址,与数据包目的mac地址进行比较,相同,则说明数据包是发往此MPP节点的,不进行任何处理;不同,则进入步骤五;

[0041] 步骤五,将数据包目的mac地址修改为本MPP节点mac地址,并设置skb->pkt\_type为PACKET\_HOST,调用函数eth\_type\_trans(),返回值赋给skb->protocol,最后调用系统函数netif\_rx()将数据包发给Linux网络协议栈由上层协议接收处理并发送出去。

[0042] 进一步,该无线局域网中多网关终端快速漫游方法ARP请求包劫持与应答机制的具体步骤如下:

[0043] 步骤一,MPP节点收到ARP请求包后,提取出源mac地址,然后查询本地转换表判断源mac地址是否在表中,在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤二;否则,不进行处理;

[0044] 步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理;

[0045] 步骤三,提取ARP请求包目的IP地址,判断是否为MPP节点IP地址,是MPP节点IP,则进入步骤四;否则,不进行处理;

[0046] 步骤四,查找本地DAT表中是否有相应条目,有,则直接生成一个ARP应答包进行应答;否则进入步骤五;

[0047] 步骤五,获取本MPP节点的mac地址,并使用该mac地址作为应答构造ARP应答包发给ARP请求者。

[0048] 进一步,该无线局域网中多网关终端快速漫游方法DNS查询包劫持转发机制的具体步骤如下:

[0049] 步骤一,MPP节点收到数据包后,提取出源mac地址,然后查询本地转换表判断源mac地址是否在表中,在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤二;否则,不进行处理;

[0050] 步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理;

[0051] 步骤三,提取出数据包IP头部,判断是否是UDP包,是,则进入步骤四;否则不进行处理;

[0052] 步骤四,提取出数据包的UDP头部,根据UDP头部的目的端口号判断是否是DNS请求包,是,则进入步骤五;否则不进行处理;

[0053] 步骤五,将数据包的源mac地址和目的IP地址保存到mac地址和DNS地址对应表中,然后将DNS请求包的目的IP地址修改为一个公网DNS服务器地址,再调用函数ip\_fast\_csum((unsigned char\*)iphdr,iphdr->ihl)重新计算IP头部校验和并设置UDP头部校验和为0,

最后将修改过的DNS请求包按普通外网数据包交由普通数据包的劫持转发机制处理。

[0054] 进一步,DNS应答包的劫持是在函数l2p\_interface\_rx中进行,是处理发往本节点或本节点所连接客户端的数据包,收到了数据包后,函数先将L2P协议给这些数据包添加的mac层头部剥离,然后再进行其它处理,DNS应答包的劫持是在剥离了L2P协议添加的mac头后进行,具体包括以下步骤:

[0055] 步骤一,MPP节点提取出数据包源mac地址,然后查询本地转换表判断源mac地址是否在表中,在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤二;否则,不进行处理;

[0056] 步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理;

[0057] 步骤三,提取出数据包IP头部,判断是否是UDP包,是,则进入步骤四;否则不进行处理;

[0058] 步骤四,提取出数据包的UDP头部,根据UDP头部的源端口号判断是否是DNS应答包,是,则进入步骤五;否则不进行处理;

[0059] 步骤五,查找mac地址和DNS地址对应表查找到该STA对应的原先DNS服务器IP地址,并将DNS应答包的源IP地址改成该地址,在重新计算IP头部校验和并设置UDP头部校验和为0,然后将修改后的DNS应答包发给STA。

[0060] 本发明提供的无线局域网中多网关终端快速漫游方法,在STA接入的Mesh节点处,将STA的外网数据包截获并转交给一个通信条件最佳MPP节点,由该节点转发出去;当STA漫游至距离其默认MPP节点较远位置时,本发明将STA的外网数据包转发至距离较近的MPP节点而非较远的默认MPP节点,从而减轻了Mesh网络中的负载,缩短了STA发往外网的数据包时延,提高了用户上网速度;本发明将发往默认MPP节点的外网数据包转发到几个通信条件更好的MPP节点,从而均衡了网络流量,降低了能量损耗;当STA的默认MPP节点无法正常工作时,本发明将STA的数据包转发至其他MPP节点,从而使得用户在部分MPP节点无法正常工作时继续上网,提高了网络稳定性。

## 附图说明

[0061] 图1是本发明实施例提供的无线局域网中多网关终端快速漫游方法流程图;

[0062] 图2是本发明实施例提供的MAP节点普通数据包劫持转发流程图;

[0063] 图3是本发明实施例提供的MAP节点ARP请求包劫持与应答流程图;

[0064] 图4是本发明实施例提供的MAP节点DNS查询应答包劫持转发流程图;

[0065] 图5是本发明实施例提供的MPP节点普通数据包劫持转发流程图;

[0066] 图6是本发明实施例提供的MPP节点ARP请求包劫持与应答流程图;

[0067] 图7是本发明实施例提供的MPP节点DNS查询应答包劫持转发流程图。

## 具体实施方式

[0068] 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。

[0069] 下面结合附图及具体实施例对本发明的应用原理作进一步描述。

[0070] 如图1所示,本发明实施例的无线局域网中多网关终端快速漫游方法包括以下步骤:

[0071] 本发明是在STA接入的Mesh节点处,将STA发往外网的数据包截获,然后将截获的数据包发给一个通信条件最佳的MPP节点,由该MPP节点将数据包转发到外网。从而降低STA发往外网的数据包时延,提高用户上网体验。该方法适用于使用多个MPP节点的无线Mesh网络场景。本发明可以应用到其他使用多个MPP节点的无线Mesh网络中,用以减小STA上网时延。

[0072] 本发明包括一个新的对应表和三个数据包劫持机制:

[0073] (1) 一个新的对应表

[0074] 表1终端mac地址及其DNS服务器地址对应表

[0075]

mac地址	DNS服务器地址
00:11:22:33:44:55	192.168.1.1

[0076] 表中,mac地址是STA的mac地址,DNS服务器地址是STA的DNS服务器地址,即STA所选MPP节点的IP地址。

[0077] (2) 普通数据包的劫持转发机制:

[0078] Mesh节点收到STA的普通数据包后,截获该数据包,提取数据包源mac地址,根据源mac地址判断是否是接入本Mesh节点的STA,只对接入本Mesh节点的STA的数据包进行劫持处理。然后判断数据包是发往外网还是内网,只对发往外网的数据包进行劫持处理;若数据包是接入本Mesh节点的STA的且发往外网,则将数据包目的mac地址修改为Mesh网络中一个通信条件最佳的MPP节点的mac地址。

[0079] (3) ARP请求包的劫持与应答机制:

[0080] L2P协议本身实现了一个分布式ARP表(DAT)机制,该机制的核心是存储网络中传播的所有ARP相应内容在一些特定的节点组中。给定一个IP地址,由于分布式哈希函数,每个其它Mesh节点知道包含它相关的ARP条目的节点组。按这种方式,不论何时客户端发起一个ARP请求,Mesh节点可以进行拦截并直接将它转发到存储有相应条目的节点组中的节点。请求被作为单播分组发送,因而分组丢失的概率要远小于广播分组丢失的概率。对于使用DAT机制仍无法获得相应条目的ARP请求,协议将其按普通ARP请求包广播出去。

[0081] 当STA的默认网关MPP1无法正常工作时,由于STA发往外网的数据包是使用其默认网关mac地址作为数据包目的mac地址的,因而当STA不知道默认网关mac地址时,会发起ARP请求去获取其默认网关的mac地址。传统情况下,由于STA默认网关无法正常工作,使得没法对STA的ARP请求进行相应,导致STA由于不能获取默认网关mac地址而使其无法发出发往外网的数据包。因此,需要在STA接入的Mesh节点处截获STA对其默认网关的ARP请求包,查找本地DAT表中是否有相应条目,如果有,则直接生成一个ARP应答包进行应答;否则使用一个通信条件最佳MPP节点的mac地址进行相应。STA收到ARP应答后,就能够将发往外网的数据包发出。

[0082] (4) DNS查询应答包的劫持转发机制

[0083] 该机制和机制二是相互配合实现STA在其默认网关无法正常工作时可上网的功能。STA访问外网都是基于域名进行访问的,STA会先发送一个DNS查询包给其DNS服务器,查找该域名对应的IP地址,得到应答之后才能访问该网址。STA的DNS服务器地址和IP地址一样一般是自动获取的,通常STA的DNS服务器地址即是其默认网关的IP地址,如果STA的默认网关无法正常工作,相当于STA的DNS服务器故障了,无法给STA提供域名解析服务,从而无法通过访问域名的方式上网。

[0084] 因此,需要在STA接入的Mesh节点将STA的DNS查询包进行劫持并将DNS查询包中的目的IP地址由STA的默认网关IP地址修改为一个公网DNS服务器地址(如8.8.8.8),然后将DNS查询包转发到通信条件最佳MPP节点,由该MPP节点发送出去。对于DNS应答包,需要将数据包中源IP地址由公网服务器地址修改回STA的默认网关的IP地址。

[0085] 本发明的具体实施例:

[0086] 实施例一:

[0087] 本发明是在STA接入的MAP节点处,将STA发往外网的数据包截获,然后将截获的数据包发给MAP节点通过网关选择算法选择的通信条件最佳MPP节点,由该MPP节点将数据包转发到外网。从而降低STA发往外网的数据包时延,提高用户上网体验。

[0088] (1) 一个新的对应表,如表1

[0089] (2) 本发明中使用的普通数据包的劫持转发机制:

[0090] MAP节点普通数据包劫持转发流程如图2所示,详细步骤如下:

[0091] 步骤一,MAP节点收到单播数据包后,提取出数据包的源mac地址,然后查询本地转换表判断源mac地址是否在表中,如果在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤二;否则,节点只是转发该数据包,不对其进行处理。

[0092] 步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,将其与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,如果结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理。

[0093] 步骤三,提取出数据包的IP层头部,然后获取目的IP地址,若目的IP是10或192网段的,则说明数据包是发往网内的,不进行处理;否则进入步骤四。

[0094] 步骤四,获取当前MAP节点所选MPP的mac地址,将其与数据包目的mac地址进行比较,若相同,则说明数据包是发往当前MAP所选MPP节点的,不进行任何处理;若不同,则将数据包的目的mac地址修改成当前MAP节点所选MPP节点的mac地址,进入步骤五。

[0095] 步骤五,将数据包目的mac地址修改后,根据新的目的mac地址查找最佳下一跳节点,然后添加L2P协议定义的单播数据包头并调用l2p\_transmit\_skb\_to\_initi函数将其发送到MAP节点所选MPP节点去,并由该MPP节点转发出去。

[0096] (3) 本发明中使用的ARP请求包的劫持与应答机制,如图3所示,具体步骤如下:

[0097] 步骤一,MAP节点收到ARP请求包后,提取出源mac地址,然后查询本地转换表判断源mac地址是否在表中,如果在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤二;否则,不进行处理。

[0098] 步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,将其与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,如果结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理。

[0099] 步骤三,提取ARP请求包目的IP地址,判断其是否为MPP节点IP地址(此处通过给所有网关节点划分一个固定的IP地址段来区分网关和非网关),如果是MPP节点IP,则进入步骤四。否则,不进行处理;

[0100] 步骤四,查找本地DAT表中是否有相应条目,如果有,则直接生成一个ARP应答包进行应答;否则进入步骤五。

[0101] 步骤五,获取MAP节点所选MPP节点的mac地址,并使用该mac地址作为应答构造ARP应答包发给ARP请求者。

[0102] (4) 本发明中使用的DNS查询应答包的劫持转发机制:

[0103] 如图4所示,DNS请求包的劫持转发处理和普通数据包的劫持转发处理基本相同,只是在进行普通数据包的处理流程之前先进行DNS请求数据包的处理流程,详细的步骤如下:

[0104] 步骤一,MAP节点收到数据包后,提取出源mac地址,然后查询本地转换表判断源mac地址是否在表中,如果在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤二;否则,不进行处理。

[0105] 步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,将其与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,如果结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理。

[0106] 步骤三,提取出数据包IP头部,判断是否是UDP包,如果是,则进入步骤四;否则不进行处理。

[0107] 步骤四,提取出数据包的UDP头部,根据UDP头部的目的端口号判断是否是DNS请求包,如果是,则进入步骤五;否则不进行处理。

[0108] 步骤五,将数据包的源mac地址和目的IP地址保存到mac地址和DNS地址对应表中,然后将DNS请求包的目的IP地址修改为一个公网DNS服务器地址,再调用函数ip\_fast\_csum((unsigned char\*)iphdr,iphdr->ihl)重新计算IP头部校验和并设置UDP头部校验和为0,最后将修改过的DNS请求包按普通外网数据包交由普通数据包的劫持转发机制处理。

[0109] DNS应答包的劫持主要是在函数l2p\_interface\_rx中进行。该函数主要功能是处理那些发往本节点或本节点所连接客户端的数据包,收到了这些数据包后,该函数先将L2P协议给这些数据包添加的mac层头部剥离,然后再进行其它处理。DNS应答包的劫持主要是在剥离了L2P协议添加的mac头后进行,具体的步骤如下:

[0110] 步骤一,MAP节点提取出数据包源mac地址,然后查询本地转换表判断源mac地址是否在表中,如果在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤二;否则,不进行处理。

[0111] 步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,将其与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,如果结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理。

[0112] 步骤三,提取出数据包IP头部,判断是否是UDP包,如果是,则进入步骤四;否则不进行处理。

[0113] 步骤四,提取出数据包的UDP头部,根据UDP头部的源端口号判断是否是DNS应答包,如果是,则进入步骤五;否则不进行处理。

[0114] 步骤五,查找mac地址和DNS地址对应表查找到该STA对应的原先DNS服务器IP地址,并将DNS应答包的源IP地址改成该地址,在重新计算IP头部校验和并设置UDP头部校验和为0,然后将修改后的DNS应答包发给STA。

[0115] 实施例二:

[0116] 本发明是在STA接入的MPP节点处,将STA发往外网的数据包截获,然后将截获的数据包由本MPP节点转发到外网。从而降低STA发往外网的数据包时延,提高用户上网体验。

[0117] (1) 一个新的对应表,如表1:

[0118] (2) 本发明中使用的普通数据包的劫持转发机制,如图5所示,具体流程如下:

[0119] 步骤一,MPP节点收到单播数据包后,提取出数据包的源mac地址,然后查询本地转换表判断源mac地址是否在表中,如果在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤二;否则,节点只是转发该数据包,不对其进行处理。

[0120] 步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,将其与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,如果结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理。

[0121] 步骤三,提取出数据包的IP层头部,然后获取目的IP地址,若目的IP是10或192网段的,则说明数据包是发往网内的,不进行处理;否则进入步骤四。

[0122] 步骤四,获取本MPP节点的mac地址,将其与数据包目的mac地址进行比较,若相同,则说明数据包是发往此MPP节点的,不进行任何处理;若不同,则进入步骤五。

[0123] 步骤五,将数据包目的mac地址修改为本MPP节点mac地址,并设置skb->pkt\_type为PACKET\_HOST,调用函数eth\_type\_trans(),将其返回值赋给skb->protocol,最后调用系统函数netif\_rx()将数据包发给Linux网络协议栈由上层协议接收处理并发送出去。

[0124] (3) 本发明中使用的ARP请求包的劫持与应答机制,如图6所示,具体的步骤如下:

[0125] 步骤一,MPP节点收到ARP请求包后,提取出源mac地址,然后查询本地转换表判断源mac地址是否在表中,如果在本地转换表中,则说明是本节点连接的客户端发送的数据包,进入步骤二;否则,不进行处理。

[0126] 步骤二,根据源mac地址查找到对应的本地转换表条目后,提取出本地转换表中的标志域flags,将其与L2P\_NCL\_CLIENT\_WIFI进行按位&运算,如果结果为1,则说明数据包由wifi客户端发出,进入步骤三;否则,不进行处理。

[0127] 步骤三,提取ARP请求包目的IP地址,判断其是否为MPP节点IP地址(此处通过给所有网关节点划分一个固定的IP地址段来区分网关和非网关),如果是MPP节点IP,则进入步骤四。否则,不进行处理;

[0128] 步骤四,查找本地DAT表中是否有相应条目,如果有,则直接生成一个ARP应答包进行应答;否则进入步骤五。

[0129] 步骤五,获取本MPP节点的mac地址,并使用该mac地址作为应答构造ARP应答包发给ARP请求者。

[0130] (4) 本发明中使用的DNS查询应答包的劫持转发机制,如图7所示,具体的步骤如下:

[0131] DNS查询包的劫持转发处理和普通数据包的劫持转发处理基本相同,只是在进行普通数据包的处理流程之前先进行DNS请求数据包的处理流程。

[0132] 步骤一, MPP节点收到数据包后, 提取出源mac地址, 然后查询本地转换表判断源mac地址是否在表中, 如果在本地转换表中, 则说明是本节点连接的客户端发送的数据包, 进入步骤二; 否则, 不进行处理。

[0133] 步骤二, 根据源mac地址查找到对应的本地转换表条目后, 提取出本地转换表中的标志域flags, 将其与L2P\_NCL\_CLIENT\_WIFI进行按位&运算, 如果结果为1, 则说明数据包由wifi客户端发出, 进入步骤三; 否则, 不进行处理。

[0134] 步骤三, 提取出数据包IP头部, 判断是否是UDP包, 如果是, 则进入步骤四; 否则不进行处理。

[0135] 步骤四, 提取出数据包的UDP头部, 根据UDP头部的目的端口号判断是否是DNS请求包, 如果是, 则进入步骤五; 否则不进行处理。

[0136] 步骤五, 将数据包的源mac地址和目的IP地址保存到mac地址和DNS地址对应表中, 然后将DNS请求包的目的IP地址修改为一个公网DNS服务器地址, 再调用函数ip\_fast\_csum((unsigned char\*)iphdr, iphdr->ihl)重新计算IP头部校验和并设置UDP头部校验和为0, 最后将修改过的DNS请求包按普通外网数据包交由普通数据包的劫持转发机制处理。

[0137] DNS应答包的劫持主要是在函数l2p\_interface\_rx中进行。该函数主要功能是处理那些发往本节点或本节点所连接客户端的数据包, 收到了这些数据包后, 该函数先将L2P协议给这些数据包添加的mac层头部剥离, 然后再进行其它处理。DNS应答包的劫持主要是在剥离了L2P协议添加的mac头后进行, 具体包括以下步骤:

[0138] 步骤一, MPP节点提取出数据包源mac地址, 然后查询本地转换表判断源mac地址是否在表中, 如果在本地转换表中, 则说明是本节点连接的客户端发送的数据包, 进入步骤二; 否则, 不进行处理。

[0139] 步骤二, 根据源mac地址查找到对应的本地转换表条目后, 提取出本地转换表中的标志域flags, 将其与L2P\_NCL\_CLIENT\_WIFI进行按位&运算, 如果结果为1, 则说明数据包由wifi客户端发出, 进入步骤三; 否则, 不进行处理。

[0140] 步骤三, 提取出数据包IP头部, 判断是否是UDP包, 如果是, 则进入步骤四; 否则不进行处理。

[0141] 步骤四, 提取出数据包的UDP头部, 根据UDP头部的源端口号判断是否是DNS应答包, 如果是, 则进入步骤五; 否则不进行处理。

[0142] 步骤五, 查找mac地址和DNS地址对应表查找到该STA对应的原先DNS服务器IP地址, 并将DNS应答包的源IP地址改成该地址, 在重新计算IP头部校验和并设置UDP头部校验和为0, 然后将修改后的DNS应答包发给STA。

[0143] 本发明可以降低STA发往外网的数据包时延, 提高用户上网体验, 传统的多网关无线Mesh网络中, STA发往外网的数据包必须交由给其分配IP地址的MPP节点转发出去, 本发明将截获的STA的外网数据包转交给一个通信条件最佳MPP节点, 由该节点转发出去, 当作为STA默认网关的MPP节点距离STA较远时, 本发明可以降低STA的外网数据包的时延, 并可减轻Mesh网络中的负载。

[0144] 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。

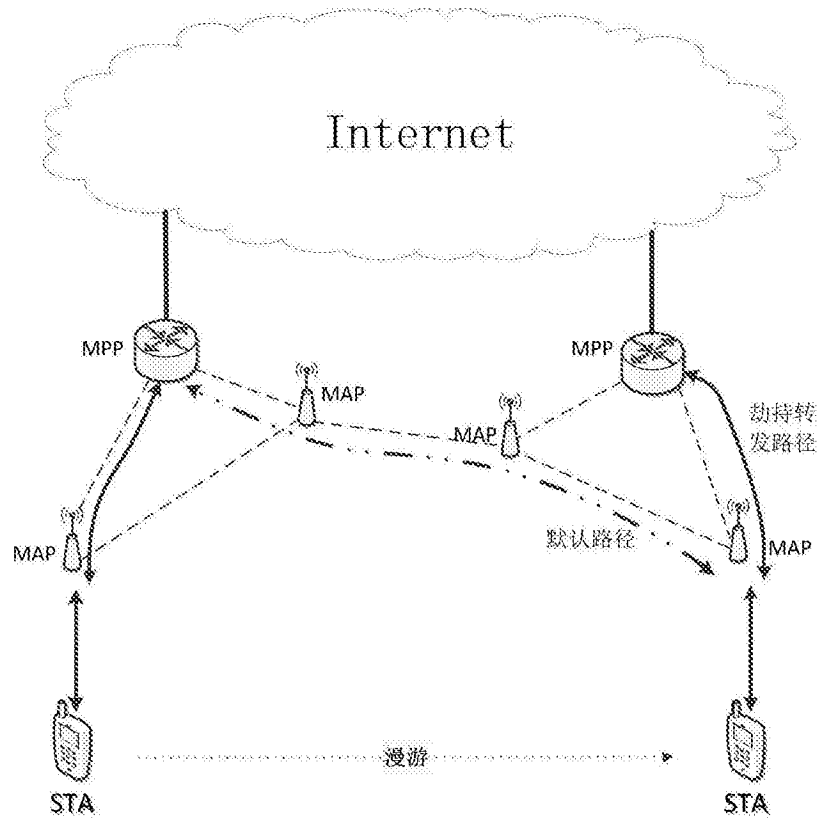


图1



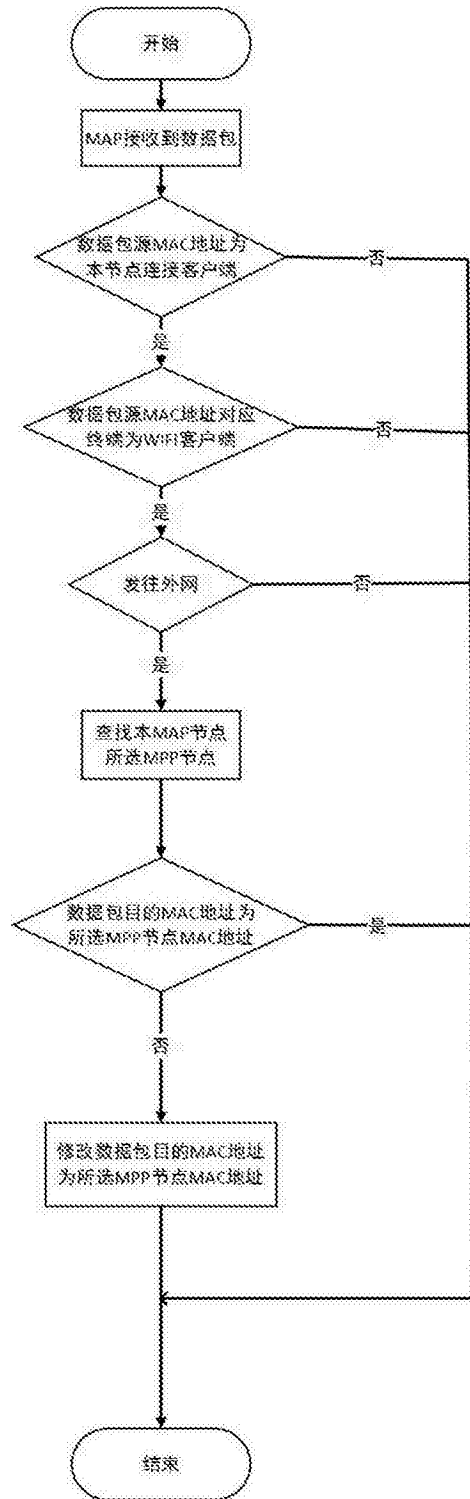


图2

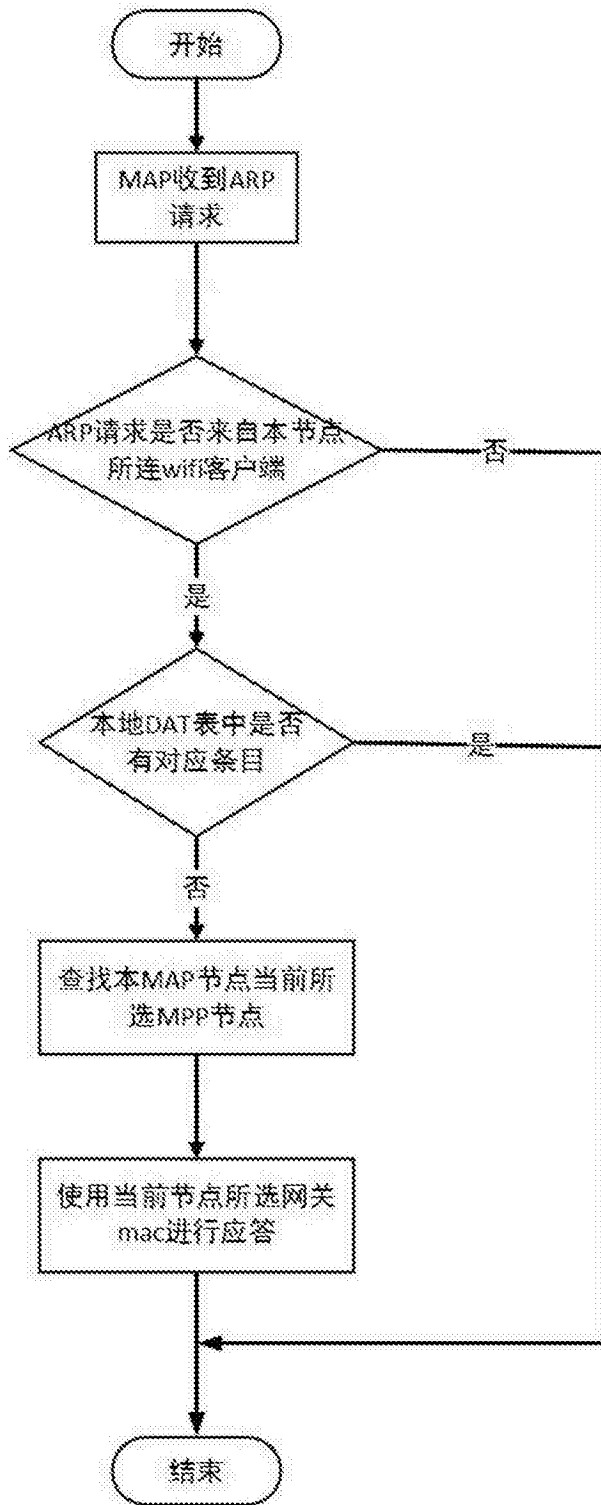


图3

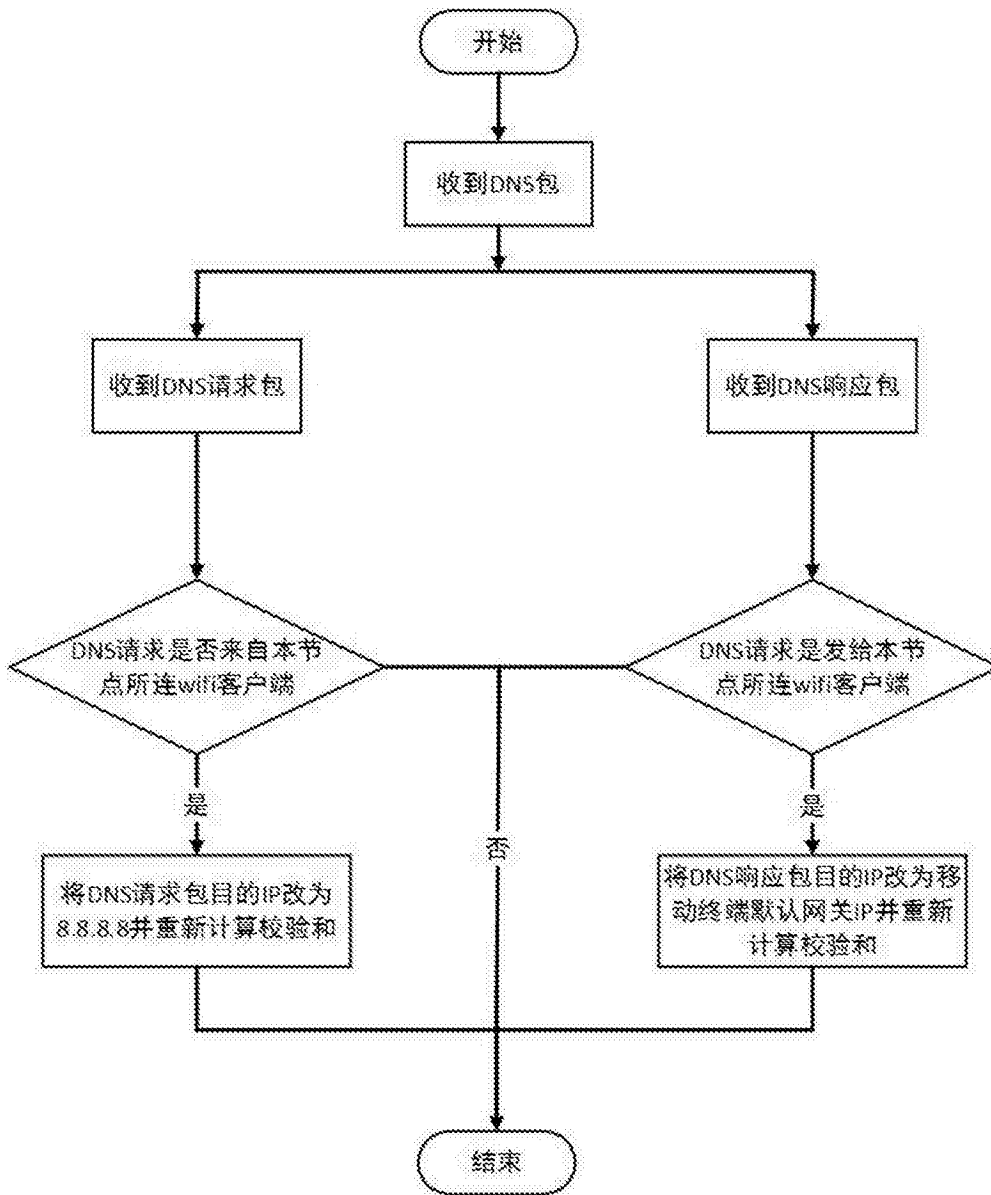


图4

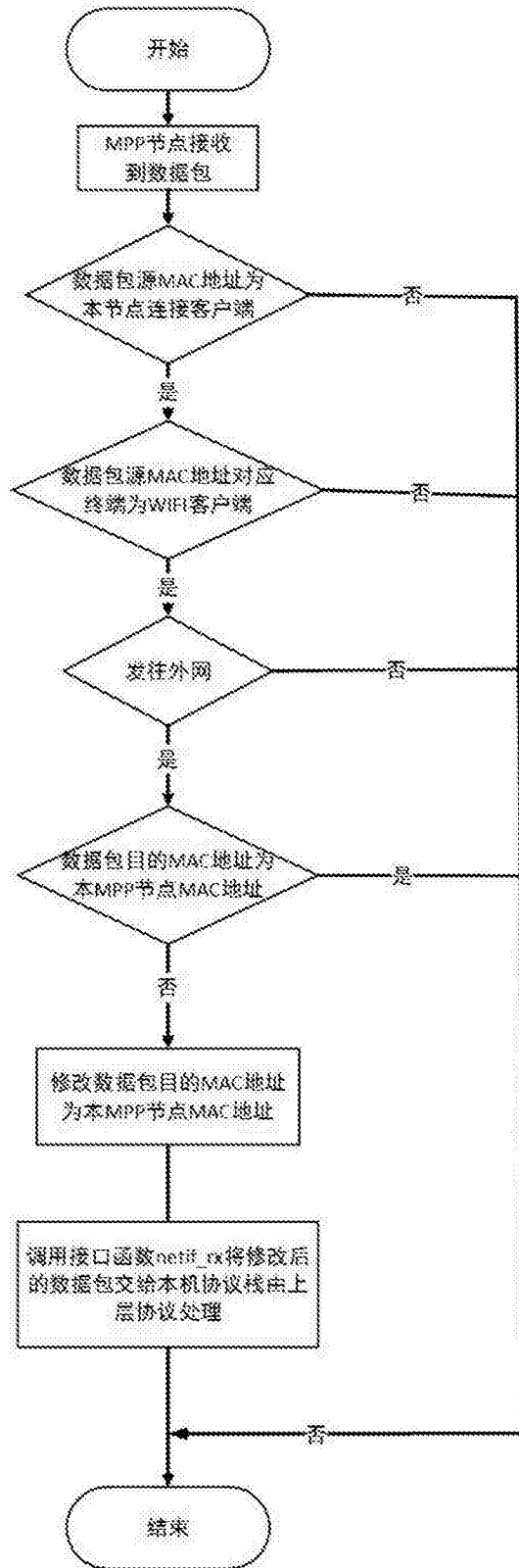


图5

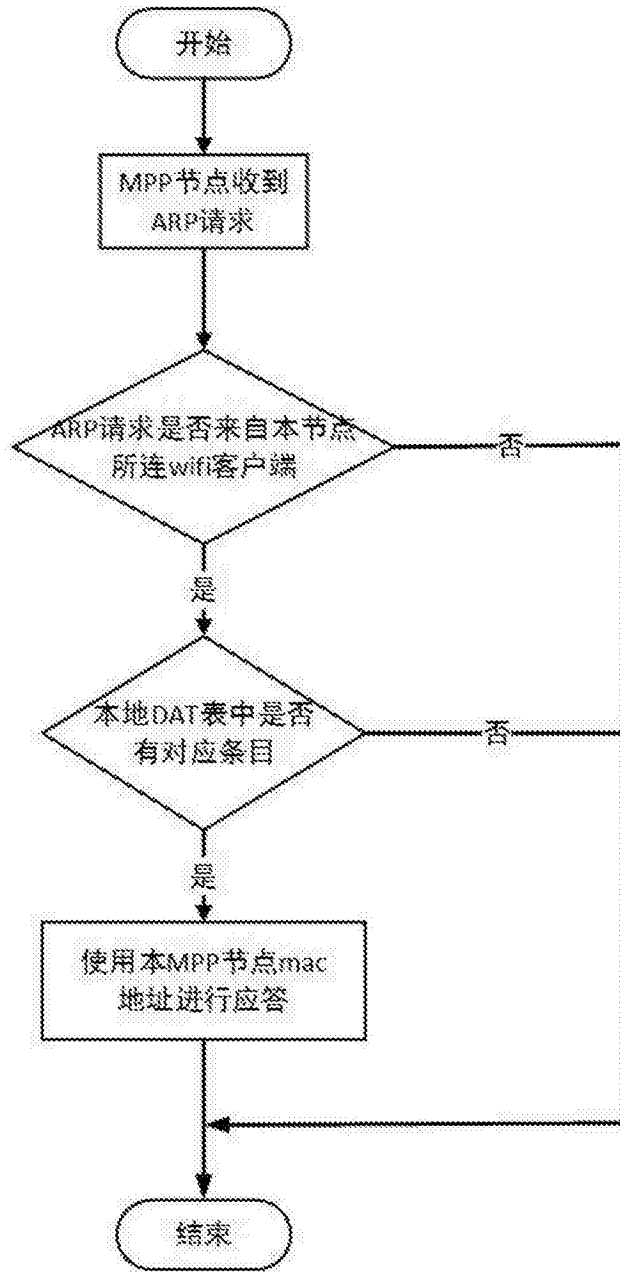


图6

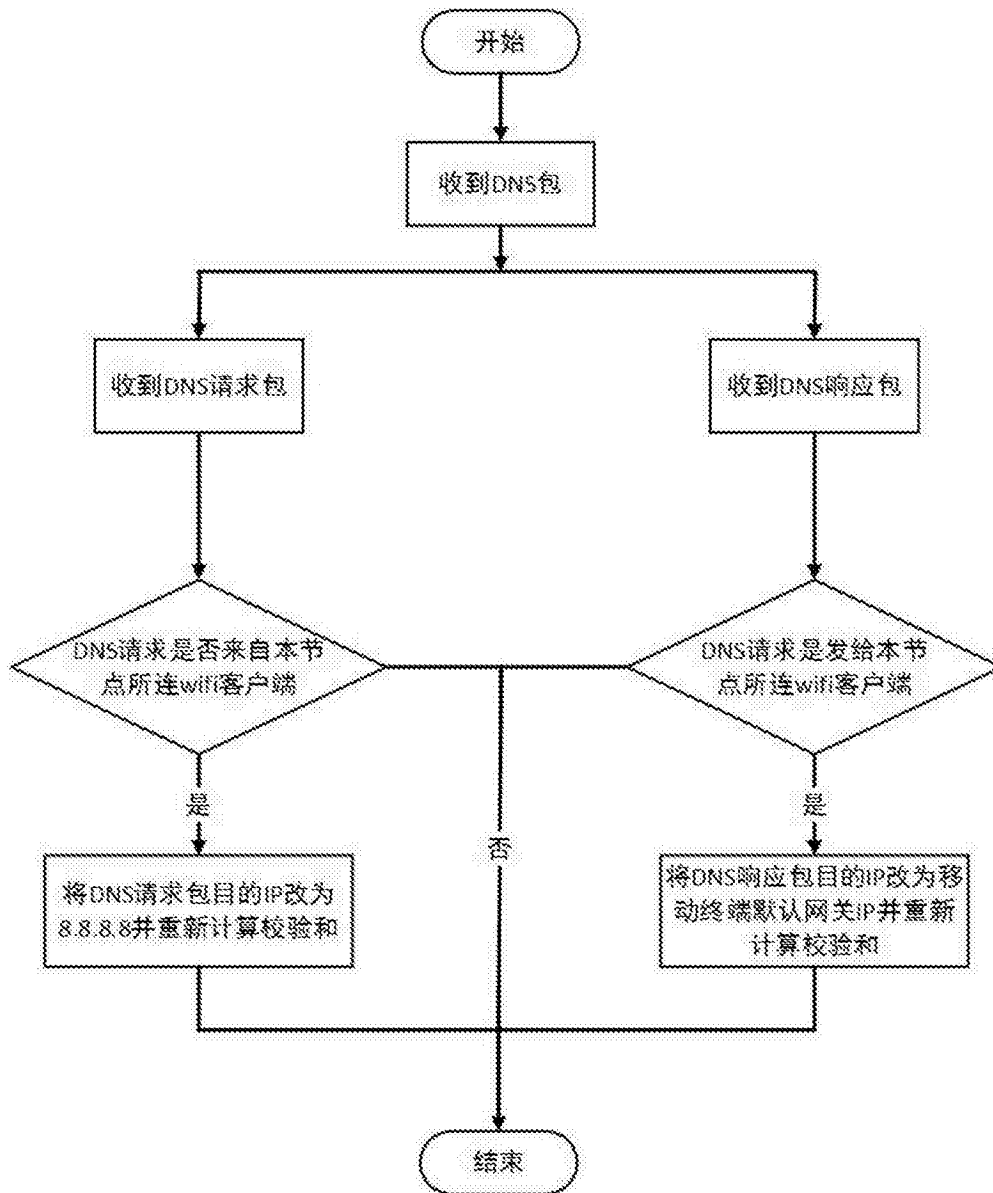


图7