基于无操作系统的 DHCP 客户端①

蒋星宇, 唐莉萍

(东华大学 信息科学与技术学院, 上海 201620)

摘 要: 以嵌入式设备 ARM Cortex M3/M4 为基础, 研究在无操作系统实现 DHCP 客户端的方法, 对运输层 UDP 校验方案进行优化;采用内存静态分配优化 DHCP 运行效率和系统稳定性; 提出抵御 DHCP 过程中 ARP 欺骗的优化算法; 给出 DHCP 过程中根据 DHCP ACK 进行局域网内 ARP 缓存更新的方法, 以提高 DHCP 客户端网络安全性和服务性能.

关键词: 嵌入式设备; ARM Cortex M3/M4; 无操作系统; DHCP 客户端; ARP

DHCP Client Based on None Operating System

JIANG Xing-Yu, TANG Li-Ping

(College of Information Science and Technology, Donghua University, Shanghai 201620, China)

Abstract: The paper takes embedded devices which consist of ARM Cortex M3/M4 core as the foundation, studies on solution of realizing DHCP client based on none operating system. Checking schemes of transport layer UDP are optimized. Static memory allocation is used for optimizing the running efficiency of DHCP and stability of the system. The optimization algorithm of resisting ARP spoofing in the process of DHCP is proposed. In order to improve the DHCP client network security and service performance, a method of updating the whole LAN's ARP caches according to DHCP ACK is provided.

Key words: embedded device; ARM Cortex M3/M4;none operating system; DHCP client; ARP

1 引言

Dynamic Host Configuration Protocol(DHCP)动态主机配置协议, 能够动态地为网络中的主机配置参数, 减轻 TCP/IP 网络的规划、管理和维护的负担, 解决 IP 地址空间缺乏问题[1]. 通过 DHCP, 大量的 IPTV 客户可以轻松地获得 IP 地址观看网络电视[2]. 需要许多子系统接入互联网的大型集团, 借助于 DHCP 能使得集团的网络应用得到快速的发展[3]. 在 DHCP 的应用方面, 贾小东等人给出了 DHCP 协议中 DHCP 服务器无法获得非 DHCP 客户机 IP 地址, 导致二次或多次 DHCP 过程发生的解决方案[4]. 樊勇兵等人提出了 DHCP+WEB 认证系统的方案[5]. 严学军提出通过配置探测技术保证 DHCP 响应消息的有效性, 避免了虚假 DHCP 服务器回应客户端的请求[6].

如今包括掌上计算机、智能手机、电视机、工控设备等嵌入式设备发展非常迅速, 这些设备大都需要接入网络, 无论是有线网, 还是无线网, 依赖网络拓展自身的应用, 每个嵌入式设备都需要进行网络的基本配置. 若对同一个网段上的每一个嵌入式设备配置静态的 IP, 将会导致网络中 IP 资源的稀缺, 并且无法轻易融入到其他网段的局域网中. DHCP 作为解决该问题中至关重要的一个环节, 为众多的嵌入式设备在一个局域网中或者切换到其它局域网中进行快速的互连提供了保障和支撑, 提高了效率.

本文以嵌入式设备 Cortex-M3/M4 核为基础, 实现并移植无操作系统的 DHCP 客户端, 对 DHCP 涉及的运输层采用对 UDP 校验进行优化; 采用内存静态分配提高程序运行效率; 针对 DHCP 过程中的 Address

① 收稿时间:2014-05-19;收到修改稿时间:2014-06-13

Resolution Protocol(ARP)地址解析协议欺骗, 以文献[7]为基础, 对主动检测和防范算法进行优化, 通过存储IP 冲突检测阶段前后 ARP 的数据状况判断 ARP 响应的真实性, 从而提高 DHCP 网络安全性; 对局域网内的DHCP ACK 报文进行 ARP 缓存更新, 不仅可以降低数据流量, 在一定程度上也可以保证局域网的安全.

2 DHCP客户端的工作原理

DHCP 是基于 BOOTP 的协议, 为应用层协议. 由于BOOTP 使用的是 User Data Protocol(UDP)用户数据报协议, 所以 DHCP 也依赖于 UDP 接收和发送数据.

DHCP 采用服务器-客户端(C/S)模型. DHCP 服务器使用 UDP 端口号 67, DHCP 客户端使用 UDP 端口号68.

DHCP 服务器分配网络地址并且发送网络配置参数给动态配置的主机, 即 DHCP 客户端. DHCP 客户端向 DHCP 服务器请求网络配置参数.

DHCP 客户端向 DHCP 服务器请求网络配置参数的过程为: 启动时先进行状态初始化; 然后通过广播包形式向所有 DHCP 服务器发出 DHCP Discover 包, 申请要求获得 IP 地址, 将自己的状态设定 SELECTING, 进入选择状态; 在选择状态阶段, 若同时收到一台或者多台 DHCP 服务器的确认和发出的DHCP Offer 包, 选择一个服务器的 DHCP Offer, 并发送 DHCP Request 广播包, 将自己的状态切换为REQUESTING, 进入请求状态, 向该 DHCP 服务器请求 IP 地址确认; 接收到对应 DHCP 服务器发送的DHCP ACK 广播包后, 根据服务器提供的 IP 地址向局域网内发送广播 ARP 请求包, 询问是否有主机已经使用了该 IP 地址, 以此进行 IP 冲突检测. 如果网段中没有主机响应该广播包, 表示租约开始, 可以使用服务器提供的 IP, 将状态切换为 BOUND 绑定状态. 当租约时间过半或达到服务器指定的重更新时间时, 客户端通过 DHCP Request 广播包向服务器发送更新租约的信息, 将自己的状态切换为 RENEWING, 进入更新请求. 此时若接收到服务器以 DHCP ACK 广播包形式发送的新的 IP 配置信息, 则续约完成, 将自己的状态切换回到 BOUND, 重新进入绑定状态; 如果租约时间过了 87.5%或达到服务器指定的重绑定时间, 客户端仍然没有收到服务器的更新确认, 则再次发送DHCP Request 广播包, 将自己的状态切换为REBINDING, 申请重新绑定; 在租约时间到达之前收到服务器的 DHCP ACK, 则客户端回复到 BOUND 状态, 否则返回初始状态, 重新开始 IP 租约的申请过程.

3 基于ARM Cortex的DHCP客户端的实现

为了使嵌入式系统能够方便地接入局域网与其它设备通信, 本文提出并实现了基于无操作系统 ARM Cortex 嵌入式设备的 DHCP 客户端的设计思想. 设计的基本依据是上述 DHCP 客户端的工作流程以及客户端侧的状态变迁. 为了减少嵌入式设备对内存、CPU 等资源的较大占用, 客户端采用任务调度的策略, 不需要使用操作系统; 在传输层, 为了简化 UDP 的数据计算, 选择轻量级的用户数据报协议(UDP-Lite)[8]; 通过采用静态内存分配的策略以及构建的相应结构体, 提高嵌入式设备的实时性及稳定性.

3.1 DHCP 报文的处理及优化

DHCP 客户端侧的消息包括 DHCP Discover、DHCP Request、DHCP Decline、DHCP Release, DHCP 客户端向 DHCP 服务器发送的消息内容由消息格式确定, 为了简化数据处理过程, 把 DHCP 的消息定义在一个结构体中. DHCP 的消息中的每个 option 一般由选项类型、长度和内容组成, 在此不赘述详细的 DHCP 的消息格式.

在嵌入式系统中分别定义一段发包和收包的缓冲区, 可以用指针的方法把需要发送的 DHCP 消息的结构体直接存储在发包的缓冲区中.

对于 DNS 域名解析相关信息, 由于所采用的嵌入式设备后续是通过上位机登录浏览器输入相应嵌入式设备的 IP 地址登录该设备的 http 服务器, 可以暂时不做处理, 因此在 DHCP 报文中删除了 DNS 相关信息, 以提高程序运行效率.

DHCP 的交互过程, 无论是建立连接的初期, 还是续约阶段, 超时处理都需要根据规定的状态转移进行. 在没有操作系统的嵌入式设备上, DHCP 的超时处理通过定时器实现. 嵌入式设备的主函数首先对系统初始化, 配置 DHCP 交互过程中对各类事件管理的定时器, 然后进入主循环, 在主循环中通过查询方式了解是否收到数据包, 继而探寻到是否有源自 DHCP 服务器 UDP 67 端口发往客户端 UDP 68 端口数据的状况. 在设计查询数据包收包状况的程序时, 采用基于 Cortex M3 或 M4 核相应的以太网 DMA(直接内存存取)

描述符处理函数, 可以大大减轻 CPU 的负担. DHCP 客户端程序收包处理流程如图 1 所示. DHCP 客户端程序发包处理流程如图 2 所示.

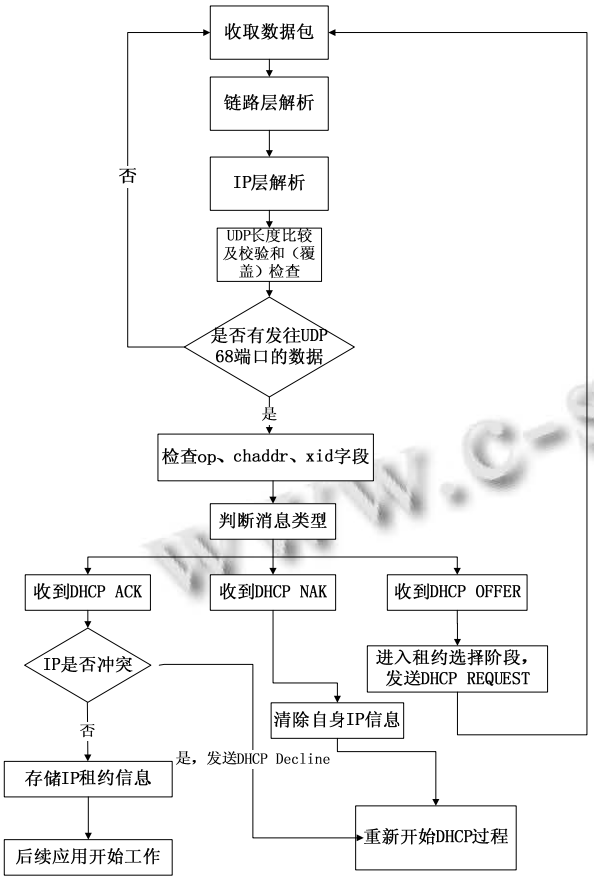


图 1 DHCP 客户端程序收包处理流程图

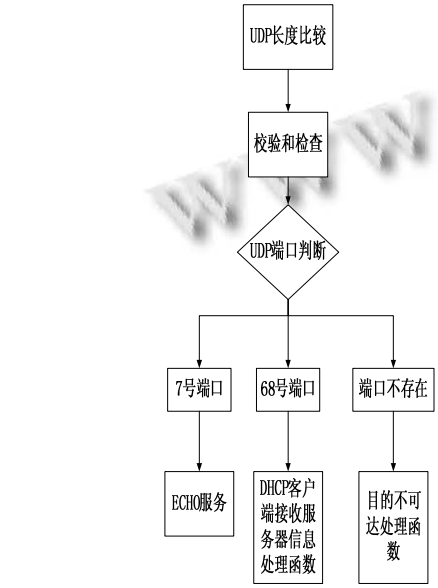


图 2 DHCP 客户端程序发包处理流程图

3.2 运输层优化

应用层的 DHCP 报文数据通过运输层 UDP 收发. 为了使 DHCP 客户端在 CPU 和 RAM 资源有限的嵌入式设备之间更轻便、流畅地运行, 在相应 DHCP 服务器支持的情况下, 采用了轻量级的用户数据报协议 (UDP-Lite).

UDP-Lite 协议更加适用于部分损坏的数据被发送而不是被丢弃的这样一种容易出错的网络环境, 使得数据传输更加稳定.

UDP-Lite 主要是把原来 UDP 首部中的 16 位 UDP 长度改进为 16 位校验和覆盖. 当校验和覆盖为 0 时, 表示对整个 UDP 数据包(UDP 首部加上 UDP 数据)进行校验, 实现和 UDP 相同的报文, 也就和一般的 DHCP 服务器兼容. 当校验和覆盖大于等于 8 时, 则对前面“校验和覆盖”个字节进行校验. , 通常 DHCP 服务器在续约阶段对嵌入式设备 DHCP 客户端提供的参数 (租约时间、更新时间、重绑定时间、分配的 IP 地址、网关路由信息)和第一次所分配的是一样, 因此可以使用 UDP-Lite 中校验和覆盖机制对后续的这些参数不进行覆盖, 以加快处理速度.

在嵌入式系统中, 对运输层的优化还可以借助 Cortex M3 或 M4 核的优势, 配合以太网 DMA 发包检验和插入函数, 预定义宏 CHECKSUM_BY_HARDWARE, 在硬件上包含 UDP 的伪首部, 通过硬件对 UDP 伪首部的内容进行计算, 将计算结果存入数据包的校验和域.

3.3 DHCP 内存分配方案及数据结构体的优化

基于嵌入式系统的 DHCP 客户端需要解决的另一个问题是内存分配策略及数据结构体的优化. 瑞士计算机科学院 Adam Dunkels 等人给出了基于嵌入式系统实现 DHCP 的 Lwip 协议栈[9], 该协议栈整体采用动态内存管理机制, 在满足嵌入式系统高速运行需求方面存在一定的问题. 采用静态内存分配可以提高系统的实时性及安全性.

为了实现 Lwip 栈的静态内存分配, 首先删除了结构体中的 udp_pcb 结构类型指针 pcb、pbuf 类型指针 p; 将 dhcp_msg 结构类型的指针 msg_in 从 dhcp 结构体中移出; 并对 dhcp_msg 的数据类型进行略微的修改, 包括客户的 IP 地址 ciaddr、服务器分配给客户端的 IP 地址 yiaddr 等, 把结构体 ip_addr 修改为 uint32_t. 将 dhcp_msg 结构类型与 DHCP 报文格式对应起来.

4　DHCP客户端性能提高

4.1 DHCP 客户端网络安全性提高

在嵌入式系统上, 当 DHCP 客户端对服务器提供 IP 地址时, 需要向局域网内发送 ARP 广播包, 查询是否有主机已经使用了该 IP 地址, 此时在客户端可能会遭遇 ARP 欺骗. ARP 欺骗是一种黑客常用的攻击手段, 通过 xcap 软件向 DHCP 客户端发送伪造的 ARP 响应数据包, 每隔一定时间告诉客户端“服务器向你提供的 IP 地址已经被我使用”, 使得 DHCP 客户端误认为服务器所提供 IP 地址已经被局域网中的其它主机使用, 向 DHCP 服务器发送 DHCP Decline 广播包, 拒绝服务器所提供 IP 地址, 导致 DHCP 过程失败. 当 DHCP 客户端重新申请 IP 租约时, DHCP 服务器则根据申请者的 MAC 地址继续给客户端分配原来的 IP 地址, ARP 欺骗将导致 DHCP 客户端无法接入网络而无法工作. 通过 wireshark 软件捕获的正常和非正常的网络过程如图 3 和图 4 所示.

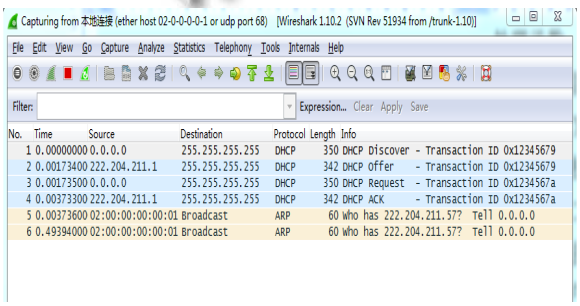


图 3　正常的 DHCP 客户端网络过程

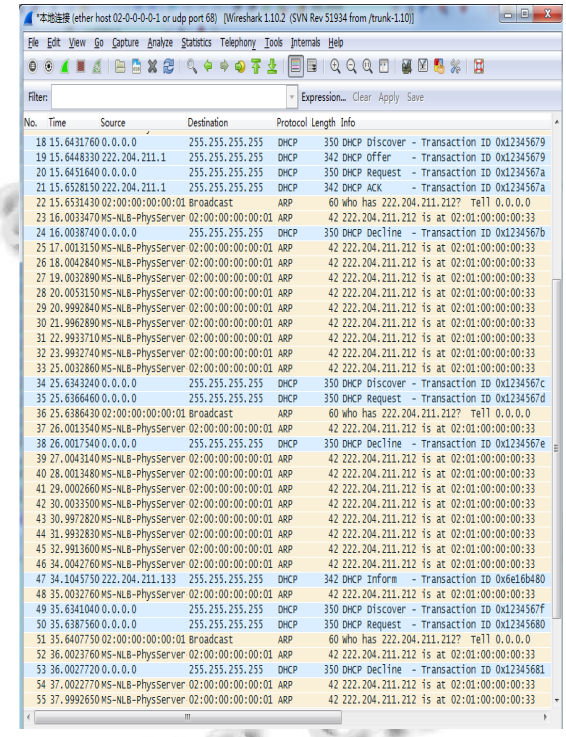


图 4　ARP 欺骗的 DHCP 客户端网络过程

黑客能成功通过 xcap 软件对 DHCP 客户端 ARP 欺骗的原因是 DHCP 客户端没有检查主机的合法性. 为了抵御这类 ARP 欺骗, DHCP 客户端必须建立主机合法性检测机制, 当收到局域网中有其它主机声明 DHCP 服务器提供给 DHCP 客户端的 IP 已经被其所使用时, DHCP 客户端不要马上向 DHCP 服务器发送 DHCP Decline 拒绝服务器提供的租约, 而是先检查该主机的合法性. 若该主机合法, 则向 DHCP 服务器发送 DHCP Decline 拒绝 IP 租约, 否则接受 IP 租约, DHCP 客户端进入 BOUND 状态.

若将最为常见的抵御 ARP 欺骗的策略[10]引入嵌入式系统, 在 DHCP 执行之前, 首先向嵌入式系统上的 DHCP 客户端存入受信任的主机的 MAC 地址, 然后修改 ARP 协议栈的收包处理函数, 检查收到的 ARP 响应包报文是否由受信任的主机发送的. 这种方法效率低, 而且与 DHCP 最初的设计目标——客户端无需手动配置 IP 相违背. 另一种方法是在局域网中建立 ARP 服务器, 由 ARP 服务器检查主机的合法性, 任意两个 DHCP 客户端的 ARP 数据通信都要首先通过 ARP 服务器. 对于类似 xcap 软件发给 DHCP 客户端伪造的 ARP 欺骗数据包, 一旦被 ARP 服务器检测到马上拦截, 从而避免 DHCP 客户端被欺骗.

本文在文献[7]提出的抵御 ARP 欺骗策略的基础上进行策略的优化. 在静态内存区域定义一个结构体数组, 用于储存接收到的 ARP 响应包中的 IP-MAC 对、以及响应是在 DHCP 客户端发出 IP 冲突检测包(ARP 请求)之后还是之前的状况. ARP 欺骗者是在 DHCP 客户端向 DHCP 服务器申请 IP 租约(或者更多的是续约)之前, 通过捕获该 DHCP 客户端和 DHCP 服务器之间第一次交互的报文, 得到 DHCP 服务器分配给该 DHCP 客户端的 IP 地址, 并且揣测在 DHCP 客户端续约或者下次重新申请时, DHCP 服务器一般会分配相同的 IP 给 DHCP 客户端, 因而伪造 ARP 欺骗报文不断地进行欺骗. 通过保存在静态内存区域中的结构体数组中各个元素, 通过对收到的 ARP 响应是在客户端发出用于 IP 冲突检测的 ARP 请求之前还是之后判断, DHCP 客户端可以发现是否存在 ARP 欺骗.

若在 DHCP 客户端发出 IP 地址的 ARP 请求之前, 已经有相同的 ARP 响应包, 那么可以根据“未发出 ARP 请求, 却能收到 ARP 响应”这一不合理的状况, 将该 MAC 地址标记为不可信, 之后在 IP 冲突检测阶段时忽略对不可信 MAC 的 ARP 响应, 继续接受 DHCP 服务器分配的 IP 地址.

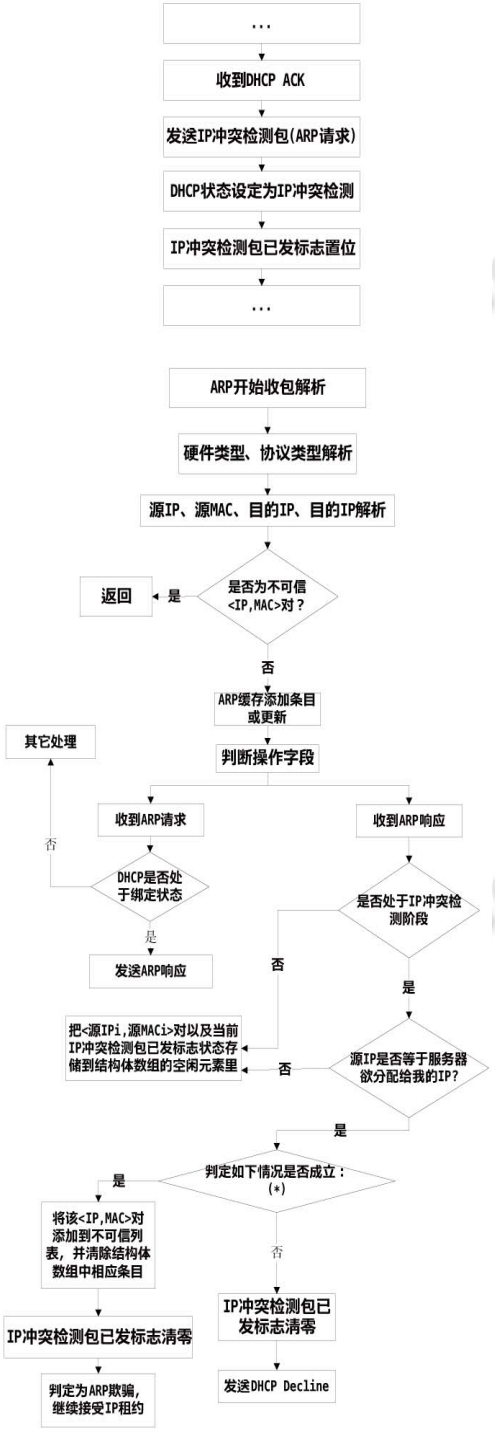


图 5 DHCP 网络安全性提高算法流程图

说明: 上图中判断框(*)处为判断如下条件: 把当前收到的<源 Ipj,源 MACj>和结构体数组中的各个<源 IP ,源 MAC>进行比较, 如果找到有相等的状况, 并且此时结构体数组中该元素的 IP 冲突检测包已发标志为 0.

改进的算法处理流程如图 5 所示. 在系统初始化时, 设置 IP 冲突检测包已发标志, 并清零. 此外在 DHCP REQUEST 发包函数内部要把 IP 冲突检测包已发标志清零.

4.2 DHCP 服务性能提高

Md. Ataullah 等人提出了一种高效、安全的 ES-ARP[11]. 在主机 A 向已知 IP 地址的主机 D 发送 ARP 广播请求主机 D 的 MAC 地址时, 主机 D 和所有其它的主机都会更新主机 A 的 MAC 地址并存储到各自的 ARP 缓存中, 这样所有其它的主机不要向主机 A 发送 ARP 请求获得主机 A 的 MAC 地址就可以直接与主机 A 通信, 这是普通 ARP 没有的高效机制.

本文对 ES-ARP 进行了优化, 对 ES-ARP 应用的时机进行调整, ES-ARP 是在某台主机向另一台主机发送 ARP 请求的瞬间开始对该 ARP 请求包进行整个局域网的 ARP 缓存更新动作, 本文则在 DHCP 服务器向某台等待获得 IP 租约的嵌入式设备发出 DHCP ACK 的瞬间开始对该 DHCP ACK 响应包进行整个局域网的 ARP 缓存更新动作. 优化流程框图如图 6 所示. 其执行过程为: 在申请新加入局域网的嵌入式设备(DHCP 客户端)收到服务器通知客户端 IP 租约开始生效广播包 DHCP ACK 时, 局域网内其它已加入的嵌入式设备(DHCP 客户端)也会同时收到该 DHCP ACK 广播包. 网内其它已有的嵌入式设备将根据收到的 DHCP ACK 广播包中的信息(bootp 报文中的 chaddr 域和 yiaddr 域), 在自己的 ARP 缓存中添加新加入的嵌入式设备的 IP-MAC 地址对. 这样, 当这台新加入的嵌入式设备与其它已有的嵌入式设备进行通信时, 就可以减少一次 ARP 交互过程, 这样可以减少网络流量, 进一步提高 DHCP 端的运行效率.

对 ES-ARP 的优化同时有利于优化 DHCP 客户端的安全性, 其优化流程如图 7 所示. 假设当第 n 台嵌入式设备申请 IP 租约时, 虚假的 DHCP 服务器开始出现, 试图造成局域网中的 IP 冲突. 虚假的 DHCP 服务器在它发出的 DHCP ACK 响应中把真实的 DHCP 服务器已分配给 j 设备的 IP 地址 IP_j 分配给第 n 台嵌入式设备, 其 IP-MAC 地址对为<IP_j,MAC_n>. 由于 j 设备先于 n 设

备接入局域网, 所以设备 j 比设备 n 先获得真实的 IP 租约, 由上述效率优化算法可知: 在第 j 个嵌入式设备收到真实服务器通知客户端 IP 租约开始生效广播包 DHCP ACK 时, 1,…,j-1 嵌入式设备的 ARP 缓存中都存储了第 j 个嵌入式设备真实的 IP-MAC 地址对 $<IP_j,MAC_j>$. 若接收到服务器给出的 IP-MAC 地址对为$<IP_j,MAC_n>$对, 嵌入式设备 1,…,j-1, j 都能判断出这是伪造的 DHCP ACK, 并且通知第 n 个嵌入式设备. 通过这个机制, 能够保证在局域网内检测到这台虚假的 DHCP 服务器, 避免新申请加入局域网的嵌入式设备受到 ARP 欺骗.

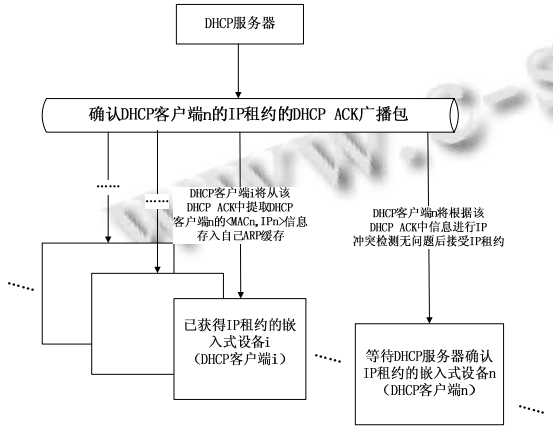


图 6　DHCP 客户端运行效率优化算法流程图

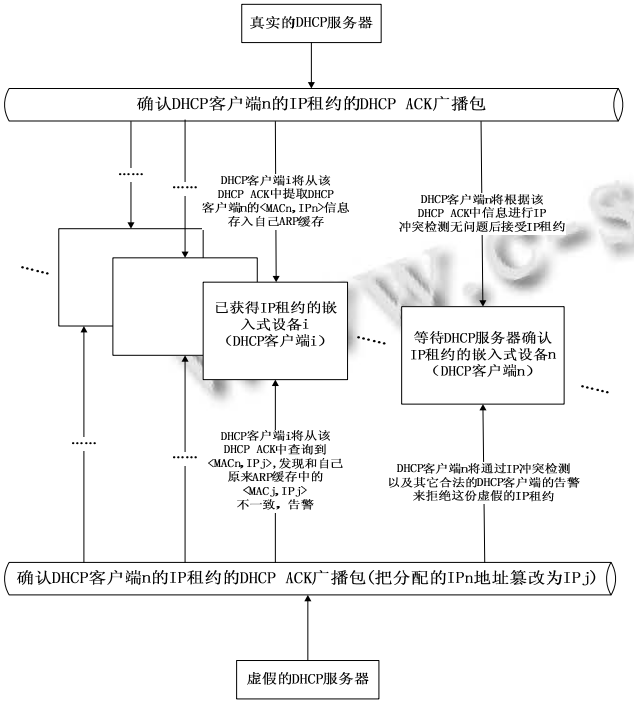


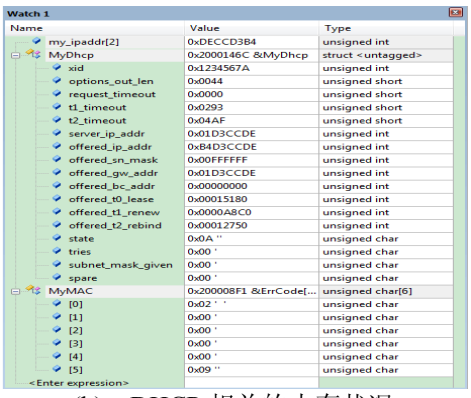
图 7　DHCP 客户端安全性优化算法流程图

5　结论

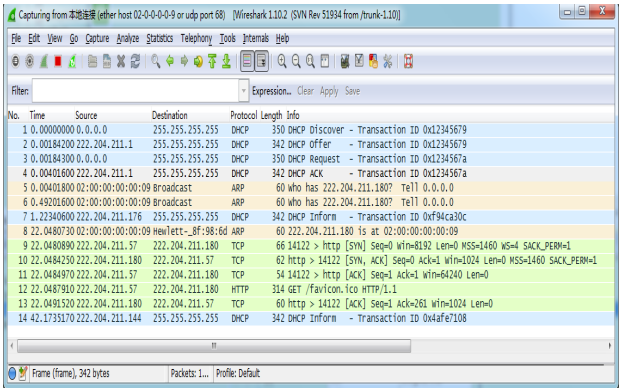
本文提出的无操作系统的嵌入式设备上实现 DHCP 客户端的方法, 在数据结构上采用内存静态分配的机制优化协议栈中运输层 UDP 以及其上层的 DHCP 的程序运行效率和系统安全性. 用 UDP-Lite 协议和 Cortex 核的宏定义 CHECKSUM_BY_HARDWARE 结合的方法加快 UDP 校验和的处理速度. 在网络安全性上, 通过建立主机合法性的检测机制, 判定对于 IP 冲突检测包的响应是否真实, 以提高 DHCP 客户端抵御 ARP 欺骗的能力. 局域网中所有嵌入式设备在 DHCP 过程中根据 DHCP ACK 进行局域网内 ARP 缓存更新, 可以在有效降低整个局域网的流量的同时提高网络的安全性. 本文提出的方案已经成功植入 ARM Cortex M3 和 M4 内核上, 为后续 Cortex M3 和 M4 核上应用的展开奠定了基础.

图 8 是本文算法在 Cortex M4 嵌入式设备上的实现图例. Cortex M4 通过 DHCP 过程获得的 IP 地址, 用户在 PC 端的浏览器址栏内键入(http://222.204.211.180/default.htm)后, PC 与嵌入式设备的 http 服务器进行连接的浏览器状况、嵌入式设备 DHCP 相关的内存状况、wireshark 捕获的总体网络过程以及 wireshark 捕获的 DHCP ACK 报文.

(a)　浏览器状况



(b)　DHCP 相关的内存状况



(c) wireshark 捕获的总体网络过程

(d) wireshark 捕获的 DHCP ACK 报文

图 8 DHCP 客户端在 Cortex M4 的实现

参考文献

1 万春艳.DHCP 安全系统构架的研究[学位论文].杭州:浙江大学,2007.

2 樊滨温,崔志强.DHCP 协议客户端的实现.计算机应用与软件,2007,24(11):114–146.

3 陈丽君.基于 DHCP 的安全方案分析与研究[学位论文].北京:北京邮电大学,2008.

4 贾小东,孙向辉,彭四伟.DHCP 协议缺点及其解决方案.计算机工程,2007,33(23):138–139.

5 樊勇兵,徐建锋,袁志坚,等.关于 DHCP+WEB 认证的若干研究.广东通信技术,2004,24(3):13–16.

6 严学军.使用基于 DHCP 探测的技术防止交换网络的欺骗攻击.计算机光盘软件与应用,2012(21):130–130.

7 林宏刚,陈麟,王标,等.一种主动检测和防范 ARP 攻击的算法研究.四川大学学报(工程科学版),2008,40(3):143–149.

8 Larzon LA, Degermark M, Pink S, et al. RFC 3828: The lightweight user datagram protocol (udp-lite). Request For Comments, IETF, 2004.

9 Dunkels A. Design and implementation of the lwIP TCP/IP Stack. Swedish Institute of Computer Science, 2001, 2: 77.

10 任侠,吕述望.ARP 协议欺骗原理分析与抵御方法.计算机工程,2003,29(9):127–128.

11 Ataullah M, Chauhan N. ES-ARP: An efficient and secure address resolution protocol. 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS). IEEE. 2012. 1–5.