计算机网络环境中自动报文解析技术的运用

黄祥兴

南昌工学院　江西　南昌　330108

[摘　要]使用信息技术进行数据传输，需要传输的数据总量极大，因此在日常使用过程中，往往选择将海量的信息分解成为数据单元进行传输。各个数据单元传输的内容相对比较同一，使用专门的解析规范能够对数据的单元进行解读。在信息网络系统当中，一般情况下数据单元被称之为报文，对数据的单元进行解析的行为称之为报文的解析。本文主要的目的是以ARP这种使用较为普遍并且应用场景较为广泛的解析协议为代表，对信息网络当中如何通过协议对信息的单元数据进行解读进行更为深入的梳理。

[关键词]网络技术；报文解析；自动化

【DOI】10.12252/j.issn.2096-6288.2021.10.1676

引言

当前社会发展环境下，计算机网络的使用已经深入到所有行业的方方面面，对所有人的生活都造成了一定的影响。从本质而言，计算机的网络同样属于信息传输的网络，使用计算机的信息网络，即利用网络信息数据快速传输的功能实现更为快速且方便的交互。随着需要使用信息传输的数据总量不断扩大，数据传输过程中必须通过对数据的提前处理才能够实现更为有效并快速的传输。而目前使用数据单元的传输方式能够较为有效地提升传输的效率，数据传输的单元一般称之为报文，报文按照一定的协议编写而成，同样需要使用协议进行解读。本文以ARP为代表对协议的使用进行了深入的探讨。

1　使用范围较广的网络协议分析的软件以及其使用的解析技术

网络协议的分析软件主要作用是通过技术手段、依托于计算机本身端口对其他计算机的数据传输情况和内容进行拦截和分析解读的软件类型，这一类型软件使用的主要作为是进行网络安全的维护以及网络信息的管理。作为协议解析的软件，在工作的过程中如同正在进行搜索的声纳，其能够对周遭网络当中传输的信息进行拦截和解读，并且自身依托计算机形成相应的分析解读文件。能够自动进行拦截分析的软件，则如同自动化的声纳系统，能够在无需人力操作的情况下，对影响范围内正在传输的数据进行自动的拦截和解读，能够实现全时段的完全监控。

在能够进行自动化抓取的解析软件当中，WireShark以及Sniffer两种属于使用较为普及的类型，其中WireShark由于操作更为简便，适用的场景更为广阔并且具备较强的实时性，因此使用更为普遍，该软件在10到1000兆的网络环境中均能够使用，也能够同时适用802.11的各类分析。

另外，使用WinPcap能够在本身的主机协议范围外，结合C语言或者C++的技术，对网络的数据传输进行监控，但该种技术无法对数据进行筛选和拦截。

2　地址解析（ARP）的技术在自动解析拦截中的使用方法和作用

2.1 地址解析（ARP）协议的基本原理以及工作方法

计算机主机在进行信息传输的过程当中，需要基于自身的MAC地址完成信息传输的工作，ARP技术即对MAC地址进行记录、解析和使用的一种协议技术。其中MAC地址是基于ARP技术生成的口令地址，该地址的一般格式为FF-FF-FF-FF-FF-FF，ARP协议报文包含硬件以及协议的编号、外传主机硬件及IP地址、接受主机硬件以及IP地址和填充使用的数据六个部分。

本技术使用场景当中，信息的流动为由一台主机传输向另一台主机，因此传输的主体包括信息外传的主机A以及信息接收的主机B。该技术在工作过程当中，基本的流程如下所示：

基于ARP协议，外传以及接受的两台主机均会提供自身的MAC地址，在明确MAC地址的情况下才能够进行信息的传输。

信息外传的主机通过对本级存储的IP与MAC地址进行对比，寻找本级缓存栈地址当中是否包含接收主机的地址。

如果外传主机的缓存中已经包含接收主机的地址，则外传的主机能够使用接收主机的MAC地址作为口令进行信息的传输。

如果外传主机的缓存当中不包含应当接收的主机的地址，则外传的主机将对区域内所有的主机发出询问性口令，口令的内容为接收主机IP地址对应的MAC地址。接收到询问信息的所有主机，非接收主机的，不做任何回应；接收主机收到信息后将向外传主机回复自身MAC地址，便于外传主机进行信息的传输。

本次传输外的主机，接收到以上接收主机的MAC地址后，对照自身缓存，如该地址同样不存在，将直接进行缓存储存。

ARP的技术属于老化技术的一种类型，即针对缓存库当中长期存在且长期未使用的MAC地址，计算机的主机能够在ARP技术的调动下进行定期的清除处理，由此能够有效减少使用频率较低的MAC地址的储存量，因此在建立传输的过程中计算机需要调动查询的缓存库总字节数能够显著降低，借此有效提升调动的效率；并借此技术原理，更新MAC地址及IP地址的对照关系，保证寻址正确。

2.2 软件WireShark自动进行数据抓取解析的基础方法

如上文所述，WireShark这一软件在使用范围方面较为宽泛，能够适用于较多的场景，并且能够通过不同的形式进行不同范围的数据抓取和解读。在明确MAC地址的情况下，该软件能够对单一的对象实现更有针对性的持续监控和解读，在不清楚MAC的情况下，或者不存在针对性主机对象的情况下，使用该种技术同样能够进行范围内的持续性监控。该种软件最大的优势在于其监控和结果生成不需要人为操作，能够通过自动化的技术实现完全的自主运行。

使用WireShark的技术进行区域性的自动抓取和解读时，应当按照以下方法执行：

运行WireShark软件后，需要进行捕获功能的选项设置，该软件当中输入“Capture Options”能够进入到捕获选项设置的环节当中，这一环节需要选择进行混杂的监听模式。混杂模式即不进行针对性对象、对范围内的全部对象进行一致性监听的模式。使用该种模式的情况下，软件能够对范围内所有主机的数据传输情况进行同步的监听和解析，能够同时

进行大量数据包的抓取。

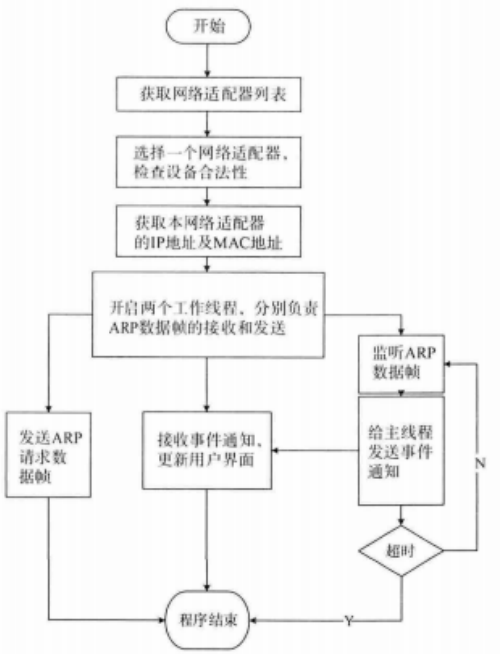
模式设置完成后，即能够返回到软件的主页面窗口，点击“开始”选项开始进行全广播域内的主机传输内容抓取解读。

软件自动进行抓取和解读的过程中，通过在“Windows”平台进行操作，能够获得软件解读内容的可阅读分析结果，获取的过程如下：以管理员的身份登录“Windows”平台上，运行命令行之后，输入删除缓存列表的命令，即arp-d命令符，缓存列表删除完成后进入WireShark软件，能够正确获得ARP的历史运作情况。

最后，通过软件中包含的筛选功能，能够通过使用Filter功能筛选出输入的信息内容，完成拦截和解读的工作。

3 使用WinPcap技术搭建框架进行数据监控的基本技术和方法

3.1 对ARP协议下的数据进行抓取和解读的基础环节展示



对ARP协议下的数据传输进行监控，主要通过IP地址与MAC地址的匹配形式进行。其中，数据外传的主机以数据接收的主机使用的IP地址为主机自动生产的地址，没有任何数据传输的情况下这一地址依然存在并且在使用网络没有发生变化的情况下不会发生任何改变。而MAC的地址则是根据ARP协议，由于协议技术的要求出厂即生成的地址，需要与适配设备进行匹配和设定才能够生产，唯一确定入网设备。

因此，作为匹配设备的适配器设备，能够对其参与进行的数据传输进行完整的整理和记录。监控模式调整到混杂的情况下，能够对所有的ARP技术下的数据传输进行完整的记录，记录的内容通过单元形式的数据帧呈现。在进行解读前，需要对记录的所有数据帧进行对比，分解输入以及输出的数据帧总量，通过对两者的对比筛选出无意义的数据帧后，对具备解析价值的数据帧，需要按照以上图片所示的流程，以数据传输的适配器绑定为基础进行以上的事件，完成解读，获得数据传输的内容。

3.2 WinPcap技术使用模式下核心部分的结构分解

使用WinPcap搭建框架进行数据监控的过程当中，核心部分的数据主要包括以下几个部分，分别是：以太网帧（Ethernet帧）的帧头结构、ARP协议数据的帧头结构以及封装的结构。

其中Ethernet帧的帧头结构主要内容的作用为定位框架内发送以及接受数据的具体地址，并且进行必要的地址核对。

ARP协议作为本框架主要依托的书写和解析数据的协议规范，通过本框架获取的所有数据，均属于使用ARP协议进行打包的数据内容，因此需要通过该协议对数据帧的内容进行拦截和解析。

封装部分的主要作用在于将上述的数据结构打包成为一个单独的完整体，避免在数据交互和使用的过程中与其他的数据单元内容造成彼此的干扰。

3.3 框架运行参数的作用以及确定的方法

框架使用过程当中需要通过设定参数的形式使得框架能够正常运转。对WinPcap的框架而言，需要设置的主要参数包含以下一个类别：自主填充的ARP函数、自主发送的ARP函数、局域网络内部所有监控时间内活跃的ARP主机函数以及解析的相关内容。

ARP的填入和发送函数主要的作用是获取网卡的句柄，帮助WinPcap使用API进行数据帧的发送。该函数主要通过对上一小节当中所述的三个结构进行解读获得，通过键入相应的参数，能够形成相应的结构体，完成数据帧发送的准备工作。

使用ARP响应帧进行数据获取和解读的过程当中，需要开启混杂的模式对所有传输过程中的数据帧进行无差别的监听，由于对所有数据帧进行监视需要进行的解析总量较大，因此在设定过程中一般选择通过加入“Fliter”过滤命令的方法，降低执行环节对处理器的占用。最后，通过最终环节响应帧对命令的相应执行，能够快速获取局部网络内的数据监控结果。

结语

信息的传输涵盖以信息的网络本身为基础的传输类型，在云储存的基础上进行的传输当中主机大多作为接受的终端存在，另外一种较为常见的传输类型为主机之间进行的传输。在主机之间进行的信息交互当中，能够通过对常用的数据协议ARP的有效利用，通过专用的软件或者通过平台搭建框架的形式，对主机间传输的数据内容进行实时的监视乃至过滤和拦截。当前技术条件下，已经能够对具备网络当中所有活跃状态的主机传输的信息进行自动化的、完整地监控并能够根据设置的监控和拦截关键词完成相应的拦截操作。在此类技术的支持下，网络的信息安全能够得到更为有效的保障。针对这一拦截系统进行范围扩展的研发，并进一步降低操作要求，能够促使该项技术获得更为广泛的应用。

参考文献

[1]刘广钟；高军；刘旻；李吉彬.报文分析技术在计算机网络教学中的应用[J].计算机教育，2014，（1）：128-130.

[2]尹友明.报文分析技术在计算机网络教学中的应用探讨[J].新教育时代电子杂志（学生版），2016，（21）：192.

[3]修扬，张月红.网络协议漏洞分析测试平台在实验教学中的应用[J].网络安全技术与应用，2020，（10）：39-40.

[4]窦萌萌.分析安全管理技术在计算机网络数据中的有效应用[J].信息通信，2020，（6）：208，214.

[5]刘祥.网络仿真在计算机网络教学中的应用研究[J].科学大众（科学教育），2019，（10）：180.