TCP 会话重组研究

张家勇
辽宁工程技术大学 电子与信息工程系 葫芦岛 125105
E-mail：zjy8829@sina.com

摘 要：本问通过对 TCP/IP 协议的分析，提出了一种利用序列号确定 TCP 报文顺序的方法。解决了数据包非按顺序到达及重传问题，并且利用二维链表对 TCP 会话进行还原。

关键字：TCP/IP 协议　TCP 连接　会话重组
中图分类号：TP309

1. 引言

TCP/IP 协议现在已经广泛的被应用。数据在网络上应用 TCP/IP 协议进行传输的时候，需要将数据分成多个数据包。目前在网络安全领域都将用到 TCP 会话的重组问题。只有将数据包重组以后，才能还原一次完整的 TCP 会话。由于网络问题，数据包可能会经过不同的路由传输到目的地，并且到达目的地的数据包可能顺序会发生改变。在传输过程中，协议对数据的传输进行控制，对在传输过程中丢失的数据包协议将控制系统将丢失的数据包重新传送。这些都是 TCP 会话在重组的时候将遇到的问题。本文经过对 TCP/IP 协议的分析，解决了 TCP 会话还原过程的常见问题，并且给出了一个 TCP 会话重组的方法。

2. TCP 会话

TCP 是一种面向连接的协议，客户与服务器之间的任何一次会话都必须建立连接[1]，退出会话时必须断开连接。连接的时候需要 3 个报文，断开的时候需要 4 个报文。

2.1 TCP 建立连接

一次 TCP 会话建立的时候需要 3 个报文交换，即需要 3 次握手（如图 1）。其 SEQ 和 ACK 的关系如下：

（1）客户发送一个 SYN 段，SYN=1 表示发起一个连接，生成随机 SEQ。

（2）对方收到后将 SEQ+1 置于 ACK 发回给本机。表示对前者的确认，生成随机 SEQ 发回本机。

（3）本机收到后将 SEQ+1 置于 ACK 发回给对方，将对方 ACK 置于 SEQ。

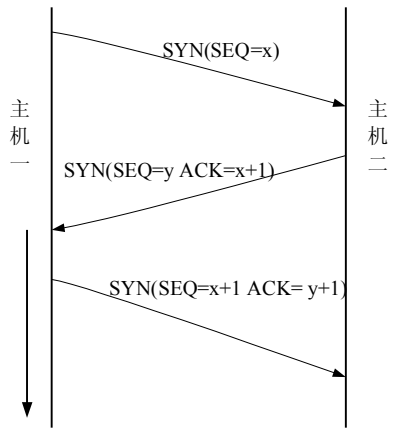

图 1　TCP 会话的建立

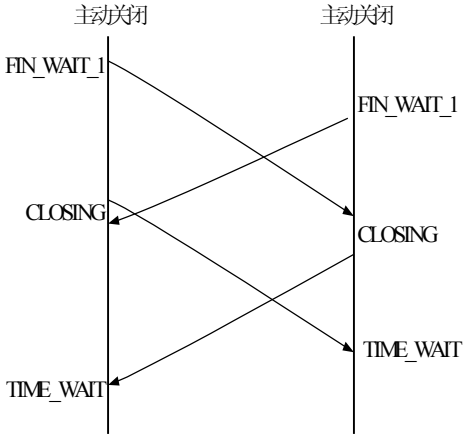

图 2　TCP 会话的关闭

2.2 TCP 数据传输

当双方建立 TCP 连接以后，就可以传输数据了，传输过程中发送方每发送一个数据包，接收方都要给予一个应答。数据包的先后关系可以由 TCP 首部的序号和确认序号确定。双方序号的及确认序号之间的关系为：设发送方发送的数据包长度为 N，序号为 SEQ，确认序号 ACK, 则下一个将要发送的数据包的序号为 SEQ+N；接收方应答的数据包序号为 ACK，确认序号为 SEQ+N，表示对序号 SEQ 长度为 N 的数据包的确认。

2.3 TCP 断开连接

建立一个连接需要 3 次握手，而终止一个连接要经过 4 次握手（如图 2）。这是因为一个 TCP 连接是全双工（即数据在两个方向上能同时传递），每个方向必须单独地进行关闭。4 次握手实际上就是双方单独关闭的过程。

3. TCP 会话的还原

3.1 SYN 的计算

在 TCP 建立连接的以后，会为后续 TCP 数据的传输设定一个初始的序列号。以后每传送一个包含有效数据的 TCP 包，后续紧接着传送的一个 TCP 数据包的序列号都要做出相应的修改。序列号是为了保证 TCP 数据包的按顺序传输来设计的，可以有效的实现 TCP 数据的完整传输，特别是在数据传送过程中出现错误的时候可以有效的进行错误修正。在 TCP 会话的重新组合过程中我们需要按照数据包的序列号对接收到的数据包进行排序。

一台主机即将发出的报文中的 SEQ 值应等于它所刚收到的报文中的 ACK 值，而它所要发送报文中的 ACK 值应为它所收到报文中的 SEQ 值加上该报文中所发送的 TCP 数据的长度，即两者存在：

（1）本次发送的 SEQ=上次收到的 ACK；

（2）本次发送的 ACK=上次收到的 SEQ+本次发送的 TCP 数据长度；

表 1 中初始的序列号 Init_seq 可以从携带 SYN 标记的 TCP 包中获得。

表 1　TCP 数据包和与初始序列号的关系

	数据包长度	序列号
初始值	1	Init_seq
报文段 1	len1	Init_seq+1
报文段 2	len2	Init_seq+1+len1
报文段 3	Len3	Init_seq+1+len1+len2

3.2 报文的还原

以上我们讨论的内容都是针对一次 TCP 会话的情况，但是实际应用网络同时传输的数据同时来自很多机器，对应很多个不同的 TCP 会话。

每个 TCP 传输的报文过程都有一个源、目的 MAC 地址、IP 地址和端口（如图 3），根据这个六元组的可以确定唯一的一次 TCP 会话，因此我们建立了一个链表 TCPSESSIONList，每一个节点指向一次 TCP 会话组装链表 TCPList，链表的表头即为六元

组。用于区分不同的 TCP 会话。其中 mac_src 表示源 MAC 地址，mac_dst 表示目的 MAC 地址，ip_src 表示源 IP 地址，ip_dst 表示目的 IP 地址，th_sport 表示源端口，th_dport 表示目的端口，next 表示一个指向下个 TCP 会话接点的指针，tcplisthead 表示一个指向 TCPList 头节点的指针。

一个报文节点是一个 7 元组（如图 4），包括：IP 首部标志位 syn 和 fin 分别用来表示会话的开始和结束；seq 表示数据包序列号；len 表示数据包的长度；prev 指向上一个 TCPList 节点的指针，首节点时为空，next 指向下一个 TCPList 节点的指针，尾节点时为空，data 为传输的 TCP 数据。显然对于一个完整的报文，重装链表的第一个包的 syn 为 1，最后一个包的 fin 为 1，且所有节点的 seq 应该是连续的，计算方法可以按照 3.1 节中所给的方法进行计算。

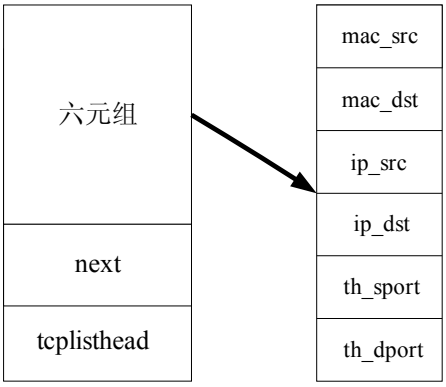

图 3　TCPSESSION 节点

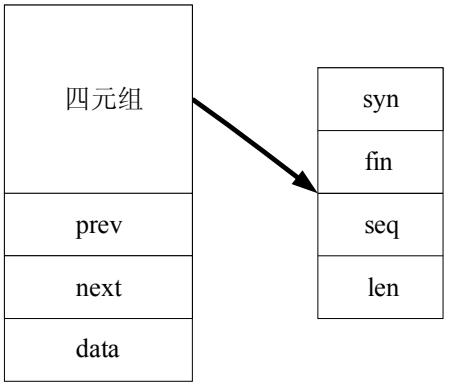

图 4　TCPNODE 节点

数据结构如下：

```
typedef struct TCPSESSION{
    unsigned char mac_src[6];
    unsigned char mac_dst[6];
    long ip_src;
    long ip_dst;
    unsigned short th_sport;
    unsigned short th_dport;
    struct TCPSESSION* next;
    TCPNODE tcplisthead;
}
```

```
typedef struct TCPNODE{
    int syn;
    int fin;
    unsigned long seq;
    int len;
    struct TCPNODE *prev;
    struct TCPNODE *next;
    unsigned char data[MAXETHERLEN];
}
```

数据在传输的过程中，可能由于路由，数据校验错误等网络原因，会导致数据包的乱序或重传。因此我们建立一个二维链表用来对众多的 TCP 进行管理（如图 5）。

TCP 会话的重组过程实际上就是对链表的插入和删除的过程。针对每一次 TCP 会话建立一个 TCPSESSION，以后每当捕获一个数据包以后首先检查此数据包所属的 TCP 会话是否已经在链表中存在，如果存在找到相应的 TCP 会话过程，根据序列号将其插入到适当的位置。如果所属的 TCP 会话不在链表中，则新建立一个 TCPSESSION 节点插入到链表的尾部。在此过程中，如果一个数据包与链表中某一个数据包的序列号和数据长度相同的话，则说明是重发包，做丢弃处理。最后链表的每一个数据包序列号连续，且第一个数据包为 SYN

包，最后一个数据包为 FIN 包（或是连接复位包 RST），此时认为报文是完整的。程序流程图如图 6。

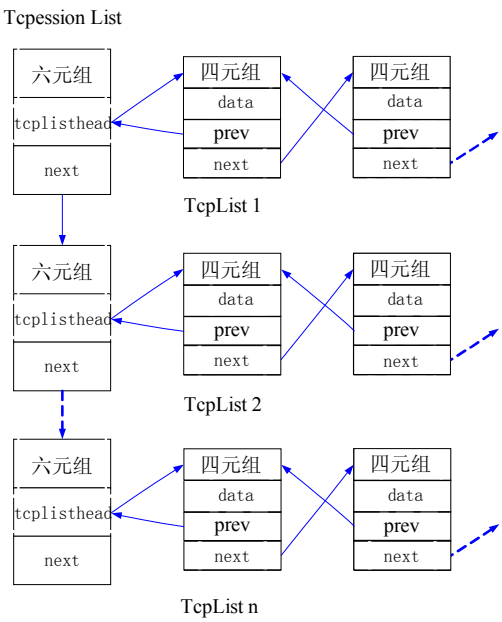

图 5　二维链表

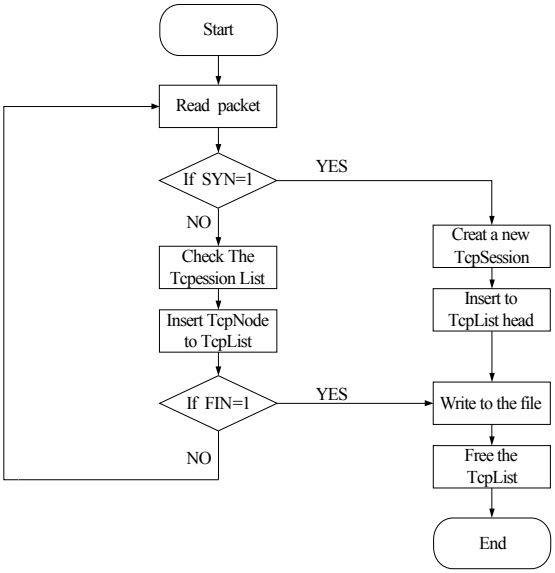

图 6　程序流程图

4. 结束语

网络传输数据时，传输到目的主机的数据包是通过 TCP/IP 协议实现报文的还原，我们利用这一原理实现了网络数据传输中的 TCP 会话的还原问题。经过测试我们发现，利用二维链表可以快速有效的处理还原多个 TCP 会话，利用序列号能够准确的确定 TCP 数据包的位置，并且可以有效的解决 IP 数据包乱序和 TCP 数据包的重传问题。

参考文献

[1] 范建华，胥光辉，等。TCP/IP 详解卷 1：协议。北京：机械工业出版社，2000—4

Research of TCP session reassignment

ZHANG Jia-yong
Dept.of Electronics and Information Engineering, Liaoning Technical University Huludao 125105

Abstract

This paper analyses the TCP/IP protocol, and proposes a way to confirm sequence of TCP packet.This method will settle the problem of order confusion in data transmission .We reassignment the TCP session by the twodimensional list.

Key words: TCP/IP protocol, TCP connect, session reassignment

作者简介：张家勇（1978-），男，硕士研究生，主要研究方向为网络通信与应用。