当服务器以TCP的方式提供服务时，客户端通过tcp连接上服务器。这时，恶意的程序，也可以通过tcp连接我们的服务器，如果恶意的程序采用循环与我们的服务器建立成千上万的连接，并在每个连接上都发送恶意的数据包给服务器，慢慢的就会导致服务器资源耗尽而崩溃。
为了增强tcp服务器在遭受“拒绝服务攻击”时的稳定性，我采用的方案时这样的：

1.通信协议的消息头增加token字段，并且它是消息头的第一个字段。当服务器收到一段数据，如果这段数据不是以token打头，则关闭对应的tcp连接。这样，只要恶意程序连上服务器一发送数据，服务器就可以识别它。
如果恶意程序只是与服务器建立成千上万个连接，而不发送任何数据，以此来耗尽的可用tcp连接数了，这就需要第二步。

2.服务器可以设定，在客户端脸上服务器后指定的时间内(比如50ms)内不发送任何数据，则标志该连接为非法连接，马上关闭它。

3.使用建立连接的“带外部数据”存储标志，如果一个客户连接上来时，没有带任何外部数据，或带外部数据不正确时，则关闭该连接。

4.如果，如果，黑客破解了客户端和服务端的通信协议，并写了一个恶意客户端，那你的服务器就分辨不了哪个连接时合法，哪个不合法了，这种情况下为一的出路就是修改协议，并采用各种加密方式使之更难破解。