Morgan Trembley

CSE 160

Project 3 Discussion Questions

1. Generally, a random value is better. This limits the chance of a server mistaking a new connection for an old one if the server crashes. This is also susceptible to attacks since the sequence number could be guessed more easily knowing all connections start at sequence 1.
2. This buffer should be large enough to hold data such that an application that reads that data does not have to call the read function an inefficient number of times. The buffer is set to 128 two-byte integers which allows for 16 packets worth of unread data before the server has to tell the client to stop sending packets. With flow control, this buffer can be utilized in a way to keep an efficient flow of data without occupying too many resources of the application reading the data.
3. If my implementation were attacked this way, eventually, no new connections could be created and no data transferring would be allowed to occur. This could be address by removing inactive connections after a certain amount of time in order to make room for new connections but that doesn't solve the problem with an on-going attack. This could be addressed by limiting the number of connections one client can have at a time, limiting the damage that can be done with an attack like this.
4. If a sender never closes the connection, we would eventually run out of sockets for new connections. This could be addressed with a timer that closes inactive sockets on the server side or a server could ask for an acknowledgement from a client that wants to keep the connection open but has no data to send for periods of time. This would have to be limited though because too many open connections not doing anything can be inefficient.