1.) It's best to start the initial sequence number as a random number. Reason being, we will not be able to tell which is the first packet and which is the next one unless we have prior knowledge where the sequence numbers begin. Therefore, to assure the security of the packets, it is better to use random numbers.

2.) Depending on the size of the file, the buffer size needs to change to be twice the size (if not bigger) of the file in question. Reason being, if the receiving buffer is filled to max before it can send the ACK back, then packets will start to drop, meaning we will lose packets and cause issues.

3.) To make it clear, a SYN flood is a form of attack under the DDoS category. If a SYN flood were to happen to us in our current implementation, we would most likely see that our node will not be able to accept anything else and will start to drop packets from other people, thus basically ruining our transport protocol implementation. To fix this, there are multiple different options. First being to support both inline and out-of-band deployment to ensure there is not one single point of failure on the network, second being able to manage attacks of all sizes by scalability. There are other options too, but those are some options.

4.) A FIN attack is an uncommon way to bypass a firewall to infiltrate a network. That is what it means when a sender transfers data but never closes a connection. In order to fix this, we would need a way to do a TCP ACK scan or a TCP window scan to find the perpetrator.