1. We consider a random number to be a better initial sequence number since it is consistent, and we can still increment as needed.

2. The buffer size we chose was 5. The number is large enough for flood control but not too large to cause performance degradation.

3. Our implementation would not be able to handle this sort of attack. To be more robust to this attack we could have designed the initial handshake protocol to detect large numbers of SYN packets and whether packets have data.

4. If the sender transfers data but never closes a connection, our implementation is open to further connections which translates to possible vulnerabilities and attacks. To handle this case, we can differently design the protocol to automatically close a connection or/and prevent further connections after a set amount of time or data transferred.