**Assumption #1:** **Packets wouldn’t be fragmented when they were sent from a node.**

Whenever a packet was sent for receiving, then we assume that it wouldn’t be broken up into fragments. So, we assume that the payload that would be sent would not be broken into separate messages that we would have to then figure out how to parse. TCP does fragment the messages sent, so this would be an important thing to implement properly in a real world application. Also, if there was a fragmented message, then one part of the data could be sent before something closed.

**Assumption #2:** **Nodes wouldn’t send each other false information to steal that node’s data.**

We designed a protocol so that all nodes would be able to send each other information about costs that could potentially modify all the data that would be flooded from a particular node. In a real world application, this is not the case as nodes could perform a “blackhole attack,” where the neighbor of a node can set the distance to be the lowest on the path so traffic coming through would go through this node and could potentially steal all other node’s information. This would have serious consequences since this node could steal more valuable information to a user, like SSN or credit card information.

**Assumption #3:**

We designed a protocol so that all nodes would be able to send each other information about costs that could potentially modify all the data that would be flooded from a particular node. In a real world application, this is not the case as nodes could perform a “blackhole attack,” where the neighbor of a node can set the distance to be the lowest on the path so traffic coming through would go through this node and could potentially steal all other node’s information. This would have serious consequences since this node could steal more valuable information to a user, like SSN or credit card information.