David Xiao Dxia063

Question 3

The first security flaw is that all messages are sent out in plain text, and a simple wire shark capture can see the content of all the messages. This breaches the confidentiality of our network system. Any hacker will be able to see all the contents of the packets that are sent across the network. Any vital information will be exposed. To solve this problem, we will need to encrypt our messages. This can be accomplished by using a public key cryptography algorithm like RSA. The use of public and private keys will allow our server to encrypt and decrypt the packets and messages. In addition, this algorithm is extremely hard to break because of the need to calculate factors of large numbers. However, because of this, decrypting and encrypting messages are costly.

Another security flaw is authentication: How do we know that the DV update received is really from the drone we are expecting. Currently, our system does not have any way of properly dealing with this problem, and any anonymous sender can just say they are a drone in the network and send hazardous and unreliable DV updates that may cause the system to crash or other failures. We can use authentication protocol ap5.0 to try and tackle this issue. The ap5.0 protocol uses public key cryptography like in RSA and a random nonce to establish authentication. However, one flaw with this method is that a man in the middle attack can occur. This can happen if a hacker is present when the connection between the drones are initially establishing. When the identification message and nonce are initially sent, they can be intercepted by the hacker and retransmitted accordingly. After the hacker will be able to decrypt, encrypt and send messages as they please.

The final security flaw is we need to ensure the integrity of the messages and make sure they have not been tampered with. A hacker could potentially alter the messages to provide incorrect data. Providing a digitally signature in addition to the message will help prevent this. This can be accomplished by letting the sender use a hash function to create a digital signature, then encrypting using the senders own private key. On the receiving end, the receiver decrypts the hashed signature and compares it with a hash of the message sent. They should be identical. If they are not identical then the message has been tampered with.