

COMP 3203 Assignment 6

Name: Nirmith Victor D'Almeida

Number: 101160124

1.

- a. Beacon Frame is one of the Management Frames for 802.11. The AP has to broadcast Beacon Frames over one of the 11 channels. It carries the service set identifier and medium access control address of an AP. It contains all information about the network. Therefore, Beacon Frame is used to help a wireless station discover and identify nearby access point to associate with it.
- b. The hidden terminal problem is caused by two factors obstacle and fading. These cause undetectable collision at the receiver's results.
 - i. Obstacle:- physical obstruction in the environment (buildings) may prevent A and C from hearing each other's transmissions (from textbook 539)
 - ii. Fading:- when signals are not strong enough to detect each other's transmissions
 - iii. How to avoid it:-
 - 1. Getting a better layout for the networks to reduce number of obstacles
 - 2. Increase the transmitting power of the AP access point by allowing the cell around each node to increase in size
 - 3. Use enhancement software for the protocols.

2. We are given: length and encryption type

length = 4

encryption type = 4096 bit RSA

We are computationally bounded that is why Brute Force option is not very possible. Thereby, making it hard for us to solve.

According to an online site, they used binary search algorithm to decrypt the message

(link: <https://www.cs.purdue.edu/homes/hmaji/teaching/Spring%202020/lectures/24.pdf>)

However there were certain condition that limited such usage which is not made known to us such as if in that case $x < N^{(1/6)}$

Therefore it will not be possible to efficiently decrypt the message with the given constraints unless we are aware of the private key since if they used a public key with RSA to encrypt data we will need to get the private key to decrypt it.

However, we can get on to them if they use the same key for back and forth communication which is unfortunately not given to us either.