Motilal Nehru National Institute of Technology Allahabad

Department of Computer Science & Engineering

B.Tech (CS+IT) VI Semester (End Semester Exam) May 2018

CS 1604: Wireless Network Security

M.Marks: 60 **Time : 180 Minutes**

NOTE:

- All Questions are compulsory
- Attempt the questions **strictly** in sequential order

1. Assume a frame moves from a wireless network using the 802.11 protocol to a wired network using the 802.3 protocol. Show how the field values in the 802.3 frame are filled with the values of the 802.11 frame. Assume that the transformation occurs at the AP that is on the boundary between the two networks. **[6]**

2. In an 802.11 network, three stations (A, B, and C) are contending to access the medium. The contention window for each station has 31 slots. Station A randomly picks up the first slot; station B picks up the fifth slot; and station C picks up the twenty-first slot. Show the procedure each station should follow. **[6]**

3. How authentication and confidentiality are provided in Bluetooth communication? **[6]**

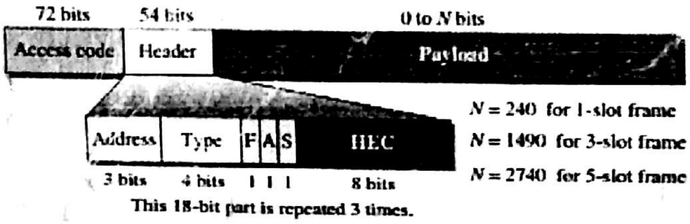

Figure1.Frame format types

Figure 1 shows the frame format of the baseband layer in Bluetooth (802.15). Based on this format, answer the following questions:

a. What is the range of the address domain in a Bluetooth network?

b. How many stations can be active at the same time in a piconet based on the information in the above figure?

4. Draw CCMP encryption and data integrity process flow diagram and explain it. **[6]**

5. What is Frequency-Hopping Spread Spectrum (FHSS)? How it helps in providing security? Explain with an example. **[6]**

6. Answer the following questions in brief **[6]**

   a. Will Bluetooth and Wireless LAN (WLAN) interfere with each other?

   b. What kind of encryption will be used for Bluetooth security?

   c. What are some of the variables that are used during the 4-Way Handshake to produce a pairwise transient key (PTK)?

   d. What operations must occur before the virtual controlled port of the authenticator becomes unblocked?

[1/2] P.T.O

7. In this exercise, you are asked to attack an RSA encrypted message. Imagine being the attacker: You obtain the ciphertext y = 1141 by eavesdropping on a certain connection. The public key is kpub = (n,e) = (2623,2111). [6]

a) Consider the encryption formula. All variables except the plaintext x are known. Why can't you simply solve the equation for x?

b) In order to determine the private key d, you have to calculate $d \equiv e^{-1} \bmod \phi(n)$. There is an efficient expression for calculating ϕ (n). Can we use this formula here?

c) Calculate the plaintext x by computing the private key d through factoring $n = p \cdot q$. Does this approach remain suitable for numbers with a length of 1024 bit or more?

8. We consider AES with 128-bit block length and 128-bit key length. What is the output of the first round of AES if the plaintext consists of 128 ones, and the first subkey (i.e., the first subkey) also consists of 128 ones? You can write your final results in a rectangular array format if you wish. [6]

9. What is the difference between RREQ ID and Destination Sequence number (DestSeqNum) in RREQ packet of AODV protocol? Suppose the DSDV routing protocol is adapted in a mobile ad hoc network. Suppose we have two nodes A and B that are neighbors. Their routing tables are shown in the figures. Please answer the following questions. [12]

Dest.	Next	Metric	Seq.
A	A	0	A-100
B	B	1	B-80
C	E	5	C-90
G	B	7	G-50

(Routing table on A)

Dest.	Next	Metric	Seq.
A	A	1	A-100
B	B	0	B-82
C	F	2	C-88
G	F	3	G-50
M	N	5	M-86

(Routing table on B)

a). Suppose B is going to broadcast its routing information to all neighbors. Please list all entries of the routing information that B is going to send to A.

b). Follow the question in a), please give out the updated routing table of A after receiving the routing information from B.